Indexed and technically co-sponsored by:
Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

**CALL FOR PAPERS**

**International Journal of Computer Science and Information Security (IJCSIS)**

**January-December 2016 Issues**

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.

See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

**Deadline:** see web site  
**Notification:** see web site  
**Revision:** see web site  
**Publication:** see web site

- Context-aware systems
- Networking technologies
- Security in network, systems, and applications
- Evolutionary computation
- Industrial systems
- Evolutionary computation
- Autonomic and autonomous systems
- Bio-technologies
- Knowledge data systems
- Mobile and distance education
- Intelligent techniques, logics and systems
- Knowledge processing
- Information technologies
- Internet and web technologies
- Digital information processing
- Cognitive science and knowledge
- Agent-based systems
- Mobility and multimedia systems
- Systems performance
- Networking and telecommunications
- Software development and deployment
- Knowledge virtualization
- Systems and networks on the chip
- Knowledge for global defense
- Information Systems [IS]
- IPv6 Today - Technology and deployment
- Modeling
- Software Engineering
- Optimization
- Complexity
- Natural Language Processing
- Speech Synthesis
- Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)
Editorial
Message from Editorial Board

It is our great pleasure to present the June 2016 issue (Volume 14 Number 6 Part 1, 2 & 3) of the International Journal of Computer Science and Information Security (IJCSIS). High quality research, survey & review articles are proposed from experts in the field, promoting insight and understanding of the state of the art, and trends in computer science and technology. It especially provides a platform for high-caliber academics, practitioners and PhD/Doctoral graduates to publish completed work and latest research outcomes. According to Google Scholar, up to now papers published in IJCSIS have been cited over 6390 times and the number is quickly increasing. This statistics shows that IJCSIS has established the first step to be an international and prestigious journal in the field of Computer Science and Information Security. There have been many improvements to the processing of papers; we have also witnessed a significant growth in interest through a higher number of submissions as well as through the breadth and quality of those submissions. IJCSIS is indexed in major academic/scientific databases and important repositories, such as: Google Scholar, Thomson Reuters, ArXiv, CiteSeerX, Cornell's University Library, Ei Compendex, ISI Scopus, DBLP, DOAJ, ProQuest, ResearchGate, Academia.edu and EBSCO among others.

On behalf of IJCSIS community and the sponsors, we congratulate the authors and thank the reviewers for their outstanding efforts to review and recommend high quality papers for publication. In particular, we would like to thank the international academia and researchers for continued support by citing papers published in IJCSIS. Without their sustained and unselfish commitments, IJCSIS would not have achieved its current premier status.

“We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication.” For further questions or other suggestions please do not hesitate to contact us at ijcsiseditor@gmail.com.

A complete list of journals can be found at: http://sites.google.com/site/ijcsis/

IJCSIS Vol. 14, No. 6, June 2016 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

Open Access This Journal is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source.
Bibliographic Information
ISSN: 1947-5500
Monthly publication (Regular Special Issues)
Commenced Publication since May 2009

Editorial / Paper Submissions:
IJCSIS Managing Editor
(ijcsiseditor@gmail.com)
Pennsylvania, USA
Tel: +1 412 390 5159
## IJCSIS Editorial Board

<table>
<thead>
<tr>
<th>IJCSIS Editorial Board</th>
<th>IJCSIS Guest Editors / Associate Editors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dr. Shimon K. Modi</strong></td>
<td><strong>Dr. Riktesh Srivastava</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Director of Research BSPA Labs, Purdue University, USA</td>
<td>Associate Professor, Information Systems, Skyline University College, Sharjah, PO 1797, UAE</td>
</tr>
<tr>
<td><strong>Professor Ying Yang, PhD.</strong></td>
<td><strong>Dr. Jianguo Ding</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Computer Science Department, Yale University, USA</td>
<td>Norwegian University of Science and Technology (NTNU), Norway</td>
</tr>
<tr>
<td><strong>Professor Hamid Reza Naji, PhD.</strong></td>
<td><strong>Dr. Naseer Alquraishi</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran</td>
<td>University of Wasit, Iraq</td>
</tr>
<tr>
<td><strong>Professor Yong Li, PhD.</strong></td>
<td><strong>Dr. Kai Cong</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China</td>
<td>Intel Corporation, &amp; Computer Science Department, Portland State University, USA</td>
</tr>
<tr>
<td><strong>Professor Mokhtar Beldjhem, PhD.</strong></td>
<td><strong>Dr. Omar A. Alzubi</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Sainte-Anne University, Halifax, NS, Canada</td>
<td>Al-Balqa Applied University (BAU), Jordan</td>
</tr>
<tr>
<td><strong>Professor Yousef Farhauoi, PhD.</strong></td>
<td><strong>Dr. Jorge A. Ruiz-Vanoye</strong></td>
</tr>
<tr>
<td>Department of Computer Science, Moulay Ismail University, Morocco</td>
<td>[Profile] Universidad Autónoma del Estado de Morelos, Mexico</td>
</tr>
<tr>
<td><strong>Dr. Alex Pappachen James</strong></td>
<td><strong>Prof. Ning Xu</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Queensland Micro-nanotechnology center, Griffith University, Australia</td>
<td>Wuhan University of Technology, China</td>
</tr>
<tr>
<td><strong>Professor Sanjay Jasola</strong></td>
<td><strong>Dr. Bilal Alatas</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Gautam Buddha University</td>
<td>Department of Software Engineering, Fırat University, Turkey</td>
</tr>
<tr>
<td><strong>Dr. Siddhivinayak Kulkarni</strong></td>
<td><strong>Dr. Ioannis V. Koskosas</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>University of Ballarat, Ballarat, Victoria, Australia</td>
<td>University of Western Macedonia, Greece</td>
</tr>
<tr>
<td><strong>Dr. Reza Ebrahimi Atani</strong></td>
<td><strong>Dr. Venu Kuthadi</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>University of Guilan, Iran</td>
<td>University of Johannesburg, Johannesburg, RSA</td>
</tr>
<tr>
<td><strong>Dr. Dong Zhang</strong></td>
<td><strong>Dr. Zhihan Iv</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>University of Central Florida, USA</td>
<td>Chinese Academy of Science, China</td>
</tr>
<tr>
<td><strong>Dr. Vahid Esmaeielzadeh</strong></td>
<td><strong>Prof. Ghulam Qasim</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Iran University of Science and Technology</td>
<td>University of Engineering and Technology, Peshawar, Pakistan</td>
</tr>
<tr>
<td><strong>Dr. Jiliang Zhang</strong></td>
<td><strong>Dr. Musa Peker</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Northeastern University, China</td>
<td>Faculty of Technology, Mugla Sitki Kocman University, Turkey</td>
</tr>
<tr>
<td><strong>Dr. Jacek M. Czerniak</strong></td>
<td><strong>Dr. Yilun Shang</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Casimir the Great University in Bydgoszcz, Poland</td>
<td>Tongji University, Shanghai, China</td>
</tr>
<tr>
<td><strong>Dr. Binh P. Nguyen</strong></td>
<td><strong>Dr. Sachin Kumar</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>National University of Singapore</td>
<td>Indian Institute of Technology (IIT) Roorkee</td>
</tr>
<tr>
<td><strong>Professor Seifeidne Kadry</strong></td>
<td><strong>Dr. Ijaz Ali Shoukat</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>American University of the Middle East, Kuwait</td>
<td>King Saud University, Saudi Arabia</td>
</tr>
<tr>
<td><strong>Dr. Riccardo Colella</strong></td>
<td><strong>Dr. Yilun Shang</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>University of Salento, Italy</td>
<td>Tongji University, Shanghai, China</td>
</tr>
<tr>
<td><strong>Dr. Sedat Akleyelek</strong></td>
<td><strong>Dr. Sachin Kumar</strong></td>
</tr>
<tr>
<td>[Profile]</td>
<td>[Profile]</td>
</tr>
<tr>
<td>Ondokuz Mayis University, Turkey</td>
<td>Indian Institute of Technology (IIT) Roorkee</td>
</tr>
<tr>
<td><strong>Dr Basit Shahzad [Profile]</strong></td>
<td>King Saud University, Riyadh - Saudi Arabia</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td><strong>Dr. Sherzod Turaev [Profile]</strong></td>
<td>International Islamic University Malaysia</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1. PaperID 31051608: ESSPI: Exponential Smoothing Seasonal Planting Index, a New Algorithm for Prediction Rainfall (pp. 1-9)

Kristoko D. Hartomo, Faculty of Information Technology, Satya Wacana Christian University, Salatiga, Indonesia
Subanar, Faculty of Mathematics and Natural Sciences, GadjahMada University, Yogyakarta, Indonesia
Edi Winarko, Faculty of Mathematics and Natural Sciences, GadjahMada University, Yogyakarta, Indonesia

Abstract — Exponential smoothing algorithm is a prediction algorithm recommended by the Food and Agriculture Organization. The weakness of exponential smoothing prediction algorithm is low accuracy for the prediction of long-term and ineffective in determining the value of smoothing to minimize error. The proposed research is to build a model rainfall prediction using a new algorithm Seasonal Planting Index (ESSPI). By using the algorithm planting seasonal index, rainfall prediction model will generate higher accuracy. The results showed seasonal planting method is the dominant index (5 of 6 test size) have an average accuracy is better than the method of exponential smoothing. Index planting seasonal prediction accuracy of 95.73% better than the exponential smoothing $\alpha = 0.1$ by 56.55%, and exponential smoothing of $\alpha = 55.53$. Novelty of this research is new algorithms for classifying data based on seasonal planting index, a new algorithm for determining the smoothing (value), the new fitting algorithm using seasonal planting index, and new algorithms using seasonal rainfall prediction planting index for the determination of the growing season.

Keywords—exponential; smoothing; algorithm; seasonal planting index; predictions; accuracy; rainfall; novelty

2. PaperID 31051609: A New MultiPathTCP Flooding Attacks Mitigation Technique (pp. 10-15)

Adwan Yasin, Department of Computer Science, Arab American University, Jenin, Palestine
Hamzah Hijawi, Department of Computer Science, Arab American University, Jenin, Palestine

Abstract — MPTCP is a new protocol proposed by IETF working group as an extension for standard TCP, it adds the capability to split the TCP connection across multiple paths. It provides higher availability and improves the throughput between two multi-address endpoints. Many Linux distributions have been developed to support MPTCP, most of them are open source which can be modified and compiled to support different experimental scenarios. Splitting the single path TCP connection across multiple paths adds new challenges in paths management and raises new security threats. Some of these threats include flooding and hijacking attacks performed by on-path and offpath attackers. In this article, we propose a new algorithm to mitigate the flooding and hijacking attacks in MPTCP, the proposed method allows a stateful processing of the initial SYN message and it’s following SYN_JOIN messages.

Keywords — TCP, MPTCP, flooding, hijack, on-path, off-path, flooding, DoS

3. PaperID 31051613: Temporal Performances Evaluation of Multi-Robot Demining System Inspired by Ant Behavior (pp. 16-24)

Riadh SAAIDIA, Mohamed Sahbi BELLAMINE, Abdessattar BEN AMOR
Computer Laboratory for Industrial Systems (LISI), National Institute of Applied Sciences and Technology (University of Carthage), INSAT, TUNISIA

Abstract — In this paper we adopt a cooperative strategy based on ACO (Ant Colony Optimization) algorithms to coordinate a Multi Robots System (MRS). Our principal objective is to evaluate temporal performances for this system by choosing demining operations as a benchmark problem. In this work, we try to adapt the ACO algorithm parameters for different mine distribution in order to reduce time demining operations. In particular, we report effects of evaporation pheromone rate model and minefield configuration on temporal performances.
Index Terms— ACO algorithms, multi-robot system (MRS), evaporation pheromone rate, demining system.

4. PaperID 31051614: Towards Developing a Cost Effective Solution for Environmental Monitoring (pp. 25-28)

Muhammad Soban Khan, Ans Ali Raza, Zeeshan Musawar, Shoaib Hassan, Taimoor Hassan
Department of Computer Science, COMSATS Institute of Information Technology, Sahiwal, COMSATS Road off GT road, Sahiwal 57000, Pakistan

Abstract - Environment refers to everything that surrounds a person. Environment contains many types of pollution. Most dangerous pollution is air pollution. Most important factor that causes human health is air pollution. Many countries are suffering from air pollution. There are many factors that cause air pollution. Some major factors are smoke, carbon monoxide and high temperature. Many developing countries are creating solutions for detecting and analyzing the air pollution. The main idea of our research is based on proposing a cost effective solution for environmental detection. Our system is a connection between sensors, Raspberry Pi, Microsoft Azure and Android Mobiles. Raspberry Pi gets environmental values with help of Raspberry Pi and sends the data to Microsoft Azure through API, from where Android Mobile gets those values with the help of HTTP request. Our proposed system successfully detected temperature, humidity, hydrogen, methane, propane, carbon monoxide and air level. The results show that our system is most cost effective, secure and easy to use. It will helpful in saving lives.

Keywords: Environment Pollution, Environmental monitoring system, Raspberry Pi, Air pollution

5. PaperID 31051615: AV Encryption Algorithm to Protect Audio visual Content for IPTV (pp. 29-39)

Muhammad Akram, C. A. Rahim, Amjad Hussain Zahid
The Institute of Management Sciences (PAK-AIMS), 54660 Lahore, Pakistan

Abstract — Crypt analytical techniques for multimedia technologies particularly audio visual applications have shown some existing flaws while maintaining the security and computational time. This case study is a representative algorithm especially for protection of IPTV contents. The network's reliability and security of contents is the major issue in IPTV media business. The proposed algorithm is the Audio Video MPEG file encryption technique in which the synchronization between audio and video and the frame sequence is shuffled before the transmitting end or vertical device. The shuffling process is guided by input key frames to point out frame positions. The MPEG video frames are first extracted via spatial pyramid kernel. It divides the stream into regions over different scales and to find out the frame similarity while on merging of AV frames. Then ciphers are implemented to locate the shuffled frames and further genetic algorithm such as AES is used to encrypt. By this way, AV contents of IPTV can be secure from malicious users.

Keywords— MPEG, IPTV, CAS, DRM, DES, AES

6. PaperID 31051616: Secure Speaker Biometric System using GFCC with Additive White Gaussian Noise and Wavelet Filter (pp. 40-47)

Gaganpreet Kaur, Dept. of CSE, I.K. Punjab Technical University, Punjab, India
Dr. Dheerendra Singh, Dept. of CSE, Chandigarh College of Engineering and Technology, Sector-26, Chandigarh, India

Abstract — Speaker Identification (SI) aims to identify the speaker’s identity from the given list of speakers. Speaker identification is efficient under the clean training and testing environment conditions. In real environment application, there occurs mismatch between training and testing environments due to background noise, which degrades the system’s performance and security. So, robust speaker identification is the important issue in research. This paper
describes the recently used front end algorithm based on Gammatone Frequency Cepstral Coefficients (GFCC) along with speech detection algorithm and Cepstral mean normalization (CMN). System makes model using Gaussian Mixture Model (GMM) Classifier, which uses iterative Expectation Maximization (EM) Algorithm to estimate the Gaussian model parameters. Training data is taken in clean environment and all test utterances are corrupted by adding White Gaussian Noise (AWGN). This paper aims to improve the robustness of speaker identification even when additive noise is added during testing phase. For improvement Wavelet Filter is implemented to de-noise the speech signal. Experiment is carried out in real database oriented and stored database oriented relative to the Attendance System application. Experiment is carried on 100 speakers saying phrases like ‘Yes mam’ ‘present mam’, ‘Yes sir’, ‘present sir’ with 4 types of utterances for each phrase (so database includes 400 utterances). Experiment results obtained shows better performance in noisy environment. The results for stored database oriented experiment show that the algorithm gives 85% of Correct Recognition Rate (CORR) while using wavelet filter and 73% without using the filter. The results for real database oriented experiment shows 74% of identification rate while using wavelet filter and 45% without using the filter.

Keywords — Gammatone Frequency Cepstral Coefficients (GFCC); Gaussian Mixture Model (GMM); Cepstral mean normalization (CMN); Robust Speaker Identification, Additive White Gaussian Noise (AWGN); Wavelet Filter.

7. PaperID 31051620: A Novel Algorithm for Load Balancing using HBA and ACO in Cloud Computing Environment (pp. 48-52)

Seyed Majid Mousavi, University of Debrecen, Faculty of Informatics, Debrecen, Hungary
Fazekas Gábor, University of Debrecen, Faculty of Informatics, Debrecen, Hungary

Abstract — Cloud computing is an emerging technology and new trend for computing based on virtualization of resources. Scheduling of tasks to reach load balancing is a challenge in cloud environment. Load balancing is the process of distribution of the load among VMs in order to efficiently utilize of resources and avoiding the situation where some VMs are overloaded or idle. Load balancing of non-preemptive tasks is one of the critical issues in task scheduling in clouds environment. To improve throughput at cloud resources, an intelligent and dynamic load balancing can significantly increase cloud’s performance and minimize the costs. Although, many algorithms, strategies and methods have been proposed, but load balancing is still one of the challenging issues in resource allocation in cloud computing environment. In this paper we propose a novel load balancing strategy using Honey Bees and Ant Colony behavior algorithms in cloud environment. The proposed algorithm strives to balance the load of the virtual machines, trying to minimize the completion time of given tasks and reduce response time in cloud infrastructure.

Keywords: load balancing, ant colony, honey bee, cloud computing.

8. PaperID 31051621: Route Optimization in MANET Using Hopfield Neural Networks: MANET-HOP (pp. 53-59)

Sanjeev Gangwar, Department of Computer Application, V. B. S. Purvanchal University, Jaunpur, India
Dr. Krishan Kumar, Department of Computer Science, Gurukul Kangri University, Haridwar, India

Abstract — As we know that Mobile Ad Hoc Network is the combination of nodes having unstable setup which usually formed instantly in independent manner. It does not have any centralized administration. Moreover they don’t have any permanent setup and routers. In such situations routing becomes the responsibility of individual nodes and also routing is equally important to realize the practical benefits of MANET. Traditional protocols of MANET: DSR, AODY, DSDV, OLTP work well but still need improvements time-to-time as per the new issues like QoS provisioning and routing. Above protocols mainly depends on hop count measurement. In this paper we have implemented a specific problem of six nodes situated at different locations with primary goal to find the shortest route visiting each node at least once which is based on the concept of Travelling Salesman Problem using Feedback/Hopfield Neural Network. And we found that Hopfield networks are suitable to find the shortest route.
9. PaperID 31051629: A Modified Black hole-Based Task Scheduling Technique for Cloud Computing Environment (pp. 60-67)

Fatemeh Ebadifard, Department of computer, Iran University of science and technology, Tehran, Iran
Zeinab Borhanifard, Department of computer, Qom University, Qom, Iran
Ahmad Akbari, Department of computer, Iran University of science and technology, Tehran, Iran

Abstract — The issue of scheduling is one of the most important ones to be considered by providers of the cloud computing in the data center. Using a suitable solution lets the providers of cloud computing use the available resources more. Additionally, the satisfaction of clients is met through provision of service quality parameters. Most of the solutions for this problem aim at one of the service quality factors and in order to achieve this goal, variety of methods are used. Using the algorithm of modified black hole in this paper, a proper solution is presented to tackle the problem of scheduling the affairs in cloud environment. The proposed method reduces makespan, increases degree of load balancing, and improves the resource’s utilization by considering the capability of each virtual machine. We have compared the proposed algorithm with existing task scheduling algorithms. Simulation results indicate that the proposed algorithm makes a good improvement regarding the makespan and amount of resource utilization compared to schedulers based on Random assignment and particle swarm optimization Algorithms.

Keywords- cloud computing; task scheduling; Black hole; makespan; resource utilization.

10. PaperID 31051631: A Multicast Routing Protocol Based on ODMRP with Stable link in Mobile Ad Hoc Networks (pp. 68-75)

Ebrahim Asadi, Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran
Ali Ghaffari, Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran

Abstract — Mobile ad hoc networks are more flexible than tradition networks since they do not require fixed infrastructure and allow all nodes move in a random trajectory, which leads frequent rerouting and degrades network performance. So, an important issue in mobile computer network research is routing in mobile ad hoc networks. Multicast sending is one of the methods used for routing in mobile ad hoc networks because of its group activities. However, some problems exist in multicast sending. For example, when receiver nodes attempt to send acknowledgments or path repetition packets simultaneously, crashes may occur, which leads to packet loss. On the other hand, link expiration is another reason for packet loss. In this study, a multicast routing protocol is offered, which uses a combination of two parameters of the received signal's power and the remaining energy to estimate the stability of the link. SINR is used at each node in conjunction with various transmitters to determine a reliable path that reduces link failure and end-to-end delay. The aim is to find the best link with probability of the highest life cycle for each path. Simulation results of the proposed method using NS-2 simulator indicate the good performance of IMP-ODMRP measures in packet delivery rate, end-to-end delay, packet loss rate, and packet collision rate.

Keywords-Mobile ad hoc networks; multicast; routing; IMP-ODMRP protocol; Standard ODMRP; Stable Link.


Thanh Tung Khuat, My Hanh Le
DATIC Laboratory, IT Faculty, University of Science and Technology – The University of Danang, Vietnam

Abstract — The problem of seeking the optimal solution in the field of science and engineering has been becoming complex and challenging due to the explosion of dimensions and the interdependence of variables. Over the past few decades, a variety of new concepts, techniques and computational applications inspired from nature have been proposed and used to deal with a wide range of optimization problems in diverse fields. Many of nature-inspired algorithms generate high-quality solutions for real-world optimization tasks. Nevertheless, the majority of these
methods are inspired by either biological phenomena or social behaviors of mainly animals and insects. There are few works relied on social phenomena of human being used to form optimization algorithms. This paper aims at presenting an adequate review of most predominant and successful groups of optimization approaches based on human social phenomena.


12. PaperID 31051641: Mammogram Classification Using Selected GLCM Features and Random Forest Classifier (pp. 82-87)

Vibhav Prakash Singh, Ayush Srivastava, Devang Kulshreshtha, Arpit Chaudhary, Rajeev Srivastava
Department of Computer Science & Engineering, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh-221005, India

Abstract - Early diagnosis of breast cancer can improve the survival rate by detecting the cancer at initial stage. Mammogram is a low dose X-ray image of the breast region, used to diagnose the breast cancer at early stage. In this paper, an efficient computer added diagnosis (CAD) system is proposed, automatically detects the normal and abnormal images of mammogram. The proposed pre-processing steps include, cropping of mammograms (for avoiding the pectoral muscle, unwanted tags) and suppression of Gaussian noise. Further, gray level co-occurrence matrix (GLCM) based statistical texture feature from different distances of neighboring and angles are extracted. Furthermore, most relevant features are also examined using AdaBoost feature selection method. Finally, normal and abnormal mammograms are classified using Random forest (RF) classifier. Experiments on benchmark mammography image analysis society (MIAS) database confirm the effectiveness of this work.

Keywords-CAD; Mammography; GLCM features; Feature selection; Random forest classifier.

13. PaperID 31051643: Enhancement of Intrusion-Detection System in MANETs with the Digital Signature via Elliptic Curve Cryptosystem (pp. 88-94)

K. Spurthi, T. N. Shankar, S. Sabari Giri Murugan
Computer Science & Engineering, KL University, AP, India

Abstract- The watchdog scheme is popular in MANET to defend the malicious attacks, but the major pitfall of this method is unable to detect some destructive actions. The technique Enhanced adaptive acknowledgment EAACK is designed to handle some weaknesses as false misbehavior, limited transmission power, and receiver collision of the watchdog scheme that is not fully efficient to resolve all the problems. This paper focuses intrusion detection system on MANETs with the collaboration of three IDS approach and with the techniques ACK, 2-ACK, and misbehavior report identification MRI. This paper proposes digital signature with Elliptic Curve Cryptosystem to avoid forging acknowledgment packets from attackers.

Keywords: DSR, MANET, AOMDV, watchdog, ACK, 2-ACK, MRI.


Shahram Zandiyan, Department of Computer Engineering, Ardabil branch, Islamic Azad University, Ardabil, Iran
Reza Fotohi, Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
Marzieh Koravand, Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
Abstract — Mobile ad hoc networks are regarded as a group of networks consisted of wireless systems which developing together a network with self-arrangement capability. No constant communication infrastructure and use central nodes to communicate with other nodes. Despite lots of advantages, these networks face severe security challenges, since their channels are wireless and each node is connected to central node. One of these concerns is the incidence of network layer attacks (Black and worm hole attack) is one kind of routing disturbing attacks and can bring great damage to the network. In this attack, an attacker cheats nodes, absorbs their packets and then deletes them. Hence, black hole and wormhole disrupts communication, or even makes it impossible in some cases. In this paper, we proposed P-Method for against network layer attacks in mobile Ad-Hoc networks based on hop count and RTT test. The proposed algorithm is implemented in ns2.35 environments and is compared with AODV And DSR under attacks, and improved AODV in different scenarios. Simulation results revealed that the (P-method), is better than AODV And DSR under attack in terms of packet dropped, packet loss, throughput, and jitter.

Keywords- Mobile ad hoc networks, AODV and DSR routing protocol, Black hole attack, Worm hole, P-Method.

15. PaperID 31051653: Check the Use of Raise in Wireless Sensor Networks Based on Heuristic Algorithms Along with Soft Computing Approach (pp. 104-119)

Abolfazl Akbari, Department of Computer Engineering, Ayatollah Amoli Branch, Islamic Azad University, Amol, Iran
Pourya Khodabandeh, Marlik Higher Education Institute, Nowshahr, Iran
Ali Khosrozadeh, Department of Computer Engineering, Ayatollah Amoli Branch, Islamic Azad University, Amol, Iran

Abstract - The use of Wireless Sensor Networks (WSNs) has grown dramatically in recent decades, and the use of these networks in the areas of military, health, environment, business, etc. increases every day. A wireless sensor network consists of many tiny sensor nodes with wireless communications and work independently. In applications of such sensor nodes, hundreds or even thousands of low-cost sensor nodes are dispersed over the monitoring area, in which each sensor node periodically reports its sensed data to the base station (sink). Due to limitations in the communication range, sensor nodes transmit their sensed data through multiple hops. Each sensor node acts as a routing element for other nodes for transmitting data. One of the most important challenges in designing such networks is the management of energy consumption of nodes; because replacing or charging the batteries of these nodes are usually impossible. One of the main characteristics of these networks is that the network lifetime is highly related to the route selection. Unbalanced energy consumption is an inherent problem in WSNs characterized by the multi-hop routing and many-to-one traffic pattern. This uneven energy dissipation in many routing algorithms can cause network partition because some nodes that are part of the efficient path are drained from their battery energy quicker. To efficiently route data through transmission path from node to node and to prolong the overall lifetime of the network, In this thesis we proposed three new routing algorithms using a combination of both Fuzzy approach and A-star algorithm seeks to investigate the problems of balancing energy consumption and maximization of network lifetime for WSNs: A-Star with 3 parameters fuzzy system (A*3F), A-Star with 3 fuzzy system with 2 parameters using majority vote (A*3FMV) and A-Star with 3 fuzzy system with 2 parameters using simple additive weighting (A*3FSAW). The new methods is capable of selecting optimal routing path from the source node to the sink by favoring the highest remaining energy, minimum number of hops, lowest traffic load and energy consumption rate. We evaluate and compare the efficiency of the proposed algorithms with each other methods under the same criteria in four different topographical areas. Simulation results show that A*3FSAW and A*3FMV balances the energy consumption well among all sensor nodes and achieves an obvious improvement on the network lifetime that randomly scattered nodes and flat routing.

Keywords: Wireless Sensor Networks, A-Star algorithm, Fuzzy logic, Network lifetime, Multi-hop routing.

16. PaperID 31051654: Allocation Algorithm based on CAC Scheme for LTE Network (pp. 120-127)

Radhia Khdhir, LETI Laboratory, ENIS, University of Sfax, Tunisia
Kais Mnif, LETI Laboratory, ENETCOM, University of Sfax, Tunisia
Khitem Ben Ali, LETI Laboratory, ENIS, University of Sfax, Tunisia
Lotfi Kammoun, LETI Laboratory, ENIS, University of Sfax, Tunisia

Abstract — To reduce network congestion and to guarantee a certain level of Quality of Service (QoS) for service requests, Call Admission Control (CAC) as a part of Radio Resource Management (RRM) aims to accept or reject a call based on available resources. In this paper, we proposed new CAC and resources allocation schemes for Long Term Evolution (LTE). The proposed CAC scheme gives the priority of Handoff Calls (HC), without totally neglecting the requirements of a New Calls (NC). The main objective of this approach is to provide QoS and to prevent network congestion. Simulation results show that the call admission control scheme leads to increased session establishment success and resource utilization compared with existing admission control and resources allocation schemes. Moreover, the resources allocation scheme achieves a considerable gain in the system throughput and fairness.

Keywords — Call admission control; QoS; Scheduling; LTE; Uplink; Throughput.

17. PaperID 31051657: A Facebook Identical Data Detection and Deletion Algorithm (pp. 128-134)

Harshita Shukla, Dept. of Computer Engineering and Applications, National Institute of Technical Teachers’ Training and Research (NITTTR), Bhopal (M.P), India.
Shailendra Singh, Senior Member IEEE, Dept. of Computer Engineering and Application, National Institute of Technical Teachers’ Training and Research (NITTTR), Bhopal (M.P), India.

Abstract — Facebook is becoming very popular as millions of users are sharing their thoughts by using various data formats. The motive behind its launch was to find old friends and relatives and make new friends. All Social Networks need to meet the increasing user demands of data storage and retrieval. The Social Networks are based on cloud to deal with dynamic speed of data generation. The success of Facebook has resulted in increased user traffic and large amount of data is continuously generated by its users’. It requires novel ways of storing data and removal and removal of duplicates as much as possible while maintaining the speed of responding to a query. In this paper, an attempt is made for the identification of data duplication and its removal. Social networking sites need dynamic data management by identifying duplicate data and its deletion technique. The removal of duplicate data is necessary, not only to reduce runtime, but also to improve search accuracy and efficiency. The implementation of this method reduces the indexing time to a great extent by decreasing the collection length, resulting in the reduction of the amount of hardware required to support the system.

Keywords- Hashing; indexing; similarity checking; unique documents; detecting replicate; data duplicity; web mining; Facebook.

18. PaperID 31051660: Rule Generation for Proton Pump Inhibitor Regimen Using Learning Vector Quantization and C4.5 (pp. 135-140)

Anifuddin Azis, Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia
Sri Hartati, Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia
Edi Winarko, Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia
Zullies Ikawati, Department of Pharmacy, Gadjah Mada University, Yogyakarta, Indonesia

Abstract — The excessive or irrational use of drugs categorized as Proton Pump Inhibitor (PPI) was indicated in Baptis Hospital of Kediri, Indonesia. In the PPI-based drug regimen among patients with digestive disorders from December 2009 to February 2010, many cases that the PPI-based drug regimen was not in accordance with the prevailing procedures were found, i.e. the drug regimen among patients who should not be given it. In this study, a method was developed to generate the PPI-based drug regimen rule. Data on the PPI-based drug regimen were trained using Learning Vector Quantization (LVQ) algorithm. The results of LVQ were stored as new data, which were extracted into IF-THEN rule with C4.5 algorithm. Based on the test, eighteen rules were generated for the PPI-based drug regimen with an accuracy rate of 82.5% on test data.
PaperID 31051661: APMS: Construction and Assessment of Hospital Process for Outpatients Process Analysis (pp. 141-147)

Mohammad Taha Khan, Suresh Gyan Vihar University Jaipur Rajasthan India, email: ertaha82@gmail.com
Dr. Shamimul Qamar, College of Computer Science, King Khalid University Abha KSA, email: Dr. Ripu Ranjan Sinha, Suresh Gyan Vihar University Jaipur India

Abstract - Management Information Systems is the process of transforming the accumulated data into useful and helpful information systems. This paper work is on design and construction of Advanced Pathology Management System (APMS). The objectives of the APMS is to i) Well-secured login system ii) Simple and easy patient registration form iii) Better test processing system i.e scheduling for the test and tracking the reports iv) Efficient Report Management system i.e, creation, searching and verification of the required reports v) Well-defined privacy management systems. The developed APMS is tested over Urgent care hospital, New Delhi. The event logs of outpatients are accumulated from the hospital and preprocessed using process mining approaches. Performance indices such as wait time for consultation wait time for test and the aggregate time spent on the outpatient care are analyzed. Experimental results prove the efficiency of the developed Advanced Pathology Management System (APMS).

Keywords: Management Information Systems, Clinical Pathology, Report Management, Outpatients and Process mining approaches.

PaperID 31051666: Anonymity of Base Station in Wireless Sensor Network via Backup Base Station (pp. 148-154)

Faisal Taj (1), Shahzad Anwar (2), Muhammad Imran (1), Irshad Ullah (1)
(1) Department of Computer Science, Iqra National University, Peshawar Pakistan
(2) Institute of Mechatronics, University of Engineering and Technology Peshawar, Pakistan

Abstract - Sensor nodes covers surrounding area and report any events to a base station over multi-hop communication. The base station plays a key role in the network. The adversary, wants to disrupt network operation, would excitedly look for the base station and target it with attacks in order to inflict maximum damage. To avoid maximum damage a novel approach is proposed for boosting the anonymity of the base station. In the proposed research the numbers of base stations are increased from one to many (such as 2 to 5) in the network operation. The purpose is to divert the adversary attention about the base station and adversary considers the base station as a sensor node. Experimentation results suggest that the approach provide a backup facility in case if one of the base stations is failed due to adversary or due to energy failure. Therefore enhances network security.

Keywords – Anonymity, Base Station, Backup Base Station, Wireless Sensor Network

PaperID 31051668: Neural Feed Forward Fault Tolerant Backbone Tree Construction to Increase the Lifetime of Wireless Sensor Network (pp. 155-159)

K. Vimal Kumar Stephen, Mathivinan V.
Computer Science and Engineering Department, AMET University, Chennai, India.

Abstract - In the recent times, the demands of Wireless Sensor Networks (WSN) increase the challenges in terms of scalability and energy efficiency. One of the key challenges in the wireless sensor network is how to prolong the lifetime of the network. To improve the lifetime of the sensor, static and movable mobile sinks are deployed. Movable sinks are used to receive sensed data from the sensor where it is located. The static mobile sinks act as a trusted third party for computing and distributing keys between sensor nodes and the clusters. It is not necessary to chose new
cluster head often because of trusted third party sink, performs all the computations of cluster head. The energy is retained when computation is reduced in cluster head thereby increases the life time of the particular cluster. Feed forward Back propagation algorithm is proposed using adaptive learning in neural networks followed by link aware routing. This algorithm deals with fault tolerant backbone tree construction for data transmission whereas it produces optimal path for the sink to transmit data. Since the optimal path is established, the life of the sink also to be prolonged thereby increase the overall network lifetime. Result shows that the lifetime of the network is improved and energy depletion is reduced.

Keywords – Sensor Networks, mobile sink, clusters

22. PaperID 31051669: An Efficient Neural Network Model for Software Effort Estimation (pp. 160-167)

Nesa Khandoozi GholiAbad, Islamic Azad University, Gorgan branch, Iran
Sanaz Khandoozi GholiAbad, Islamic Azad University, Sari branch, Iran

Abstract — Software development effort estimation is the process of predicting the effort required to develop a software system. Estimating development effort accurately in the early stage of software life cycle plays a crucial role in effective project management. Effort estimation is a key factor for software project success, defined as delivering software of agreed quality and functionality within schedule and budget. Traditionally effort estimation has been used for planning and tracking project resources. It has become an important task. This paper proposed a neural network model for software effort estimation. This model has 3 layers. The train, validation and test data used are from COCOMO data set. Inputs and targets data randomly divided in train (60 %), validation (20%) and test (20%) group. When the number of neurons in hidden layer was 20, Number of training samples was 37, number of validation samples was 13 and number of testing samples was 13, the network has best performance. In this case, the value of training, validation and testing MSE was 0.01044, 0.0475 and 0.0375 respectively and value of training, validation and testing R was 0.9167, 0.7741 and 0.7410 respectively.

Keywords- Software Engineering, Effort Estimation, Artificial Neural Network


Gurleen Kaur, Baljit Singh Khehra,
Department of Computer Science and Engineering, Baba Banda Singh Bahadur Engg. College Fatehgarh Sahib, India

Abstract — Forgery detection is the most important task in our national judicial system and criminal investigation procedure. Today digital images have become powerful source of communication. With the advancement of technology, it becomes very easy to change the content of digital images. Due to which these images are no more taken as a proof of authenticity or legitimacy. In this paper, we deal with the widely used form of image tampering known as image composition(or image splicing).We demonstrate an effective algorithm to detect the spliced images based on illumination inconsistencies present in images. An adaptive support vector machine (a-SVM) is used to classify the given images as either genuine or forged.

Keywords—Digital image forensic, forgery detection, image splicing, Adaptive SVM.

24. PaperID 31051675: Comparison and Analysis of Image Splicing Detection Using Artificial Neural Networks (pp. 174-178)

Lovepreet Kaur, Dr. Baljit Singh Khehra
Department of CSE & IT, BBSBEC, Fatehgarh Sahib, India
Due to advancement in technology it is easy to modify the digital images and the discovery of modified images can be the difficult task as the images are the very powerful source of communication in every field. So, one of the major issue in today’s world regarding digital images is the authenticity of given images. Therefore, digital image forgery detection is a growing research field with important implication for ensuring the credibility of digital images. In this research, we proposed a credible method to detect image splicing based on illuminant color. Artificial neural network techniques are implemented as a classifier to detect the tampered images. The results describe that artificial neural network is effective to detect tampered images.

Keywords— Forgery Detection, Image splicing, Illuminant color, Artificial Neural network.

25. PaperID 31051676: Efficient Random Sampling Statistical Method to Improve Big Data Compression Ratio and Pattern Matching Techniques for Compressed Data (pp. 179-184)

Dr. Nishad P M, Department of Computer Applications, Mar Athanasios College for Advanced Studies Tiruvalla Kerala, India.
Syam Sankar, Department of Computer Science & Engineering, NSS College of Engineering Palakkad, Kerala, India.

Abstract - This paper surveys various possibilities for pattern matching in compressed big data volume. Although various compression standards are available for compressing data, entire volume decompression is compelled before pattern matching, this in turn leads to increase in computational complexity as well as the space complexity. Some compressions algorithms give better compression ratio, at the same time, they are inefficient in decompression required for pattern matching. This paper evaluates the possibilities of pattern matching after compression without decoding. Also this paper experiments and proposes how the random sampling and its statistics will help to make better compression ratio in big data. The another objective of this work is to investigate the possibilities of pattern matching in big data without decoding and some of the standards are suggested based on this study and survey.

Keywords - Compression, Encoding, Decoding, Big data, compression ratio, computational complexity, space complexity, random sampling.

26. PaperID 31051686: A New Dynamic Data Replication Algorithm to Improve Execution Time in Data Grid (pp. 185-190)

Sohela Malmoli Abbasi, * Mohammadreza Noorimehr
Department of Computer Engineering, Khouzesan Science and Research Branch, Islamic Azad University, Ahvaz, Iran

Department of Computer, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran

Abstract — Data grids provide large-scale geographically distributed data resources for data intensive applications. These applications handle large data sets that need to be transferred and replicated among different grid sites so availability and efficient access are the most important factors affecting the performance. It is obvious that, managing the volume of data is very important. Data replication is an important technique to reduces data access time which improves the performance of the system by creating identical replicas of data files and distributing them on grid sites. In this paper, we propose a novel dynamic data replication strategy called DRPF (Dynamic Replication of Popular File), which is based on access history and file’s popularity. As grid sites within a virtual organization(VO) have similar interest of files, the basic idea of DRPF is to improve locality in accesses through increasing the the number of replicas in the VO. DRPF first selects the popular files that are needed to be copied to other nodes, then tries to find the best places for placement of new replicas by taking into account parameters such as the number of demands per site for files and bandwidth between replication sites. The algorithm is simulated using a data grid simulator, OptorSim. The simulation results show that our proposed algorithm has better performance in comparison with other algorithms in terms of job execution time and effective network usage.

Keywords-Data grid; replication; popular file; placement
27. PaperID 31051687: Image Steganography Method for Concealing Secret Data into Coefficients Based on High Scalable Sub-Bands of Integer Wavelet Transform (pp. 191-197)

Yahya E. A. Al-Salhi, Songfeng Lu
School of Computer Science, Huazhong University of Science and Technology, Wuhan 430074, PR china

Abstract — In information security, an image steganography technique uses one of the most popular transforms; either a spatial domain or the frequency domain to conceal the secret information. In this paper, an image steganography system using the spatial domain technique to conceal secret information in the frequency domain is proposed to conceal secret image information in another cover image. The Integer Wavelet Transform (IWT) used to obtain high scalable sub bands for each LL, LH, HL and HH of the cover image file. Then, the steganography approach is used to conceal the secret information in the wavelet coefficients for all sub bands. The results show high quality of stego image, and the stego image is analyzed for different attacks. It is found that the technique is robust, and it can withstand the attacks. The quality of the stego image is measured by Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), and Universal Image Quality Index (UIQI). The quality of extracted secret image is measured by Signal to Noise Ratio (SNR) and Squared Pearson Correlation Coefficient (SPCC).

28. PaperID 31051693: Managing and Tracking Alumni in Saudi Universities (pp. 198-204)

Dr. Amr Jadi, Department of Computer Science and Engineering, College of Computer Science and Engineering, University of Hail, Hail, Saudi Arabia

Abstract — Managing Alumni System is one of the greatest challenges in the present market of Saudi Arabia. An alumni system is a channel between different universities and labor market to deliver various services to students as per the merit and priorities. There is no constructive method in present system of Labor office to monitor job requests from the students and communicate them with potential changes of market policies. This research aims to provide an architecture building a Functional Alumni System in Saudi Universities. The loop holes of current alumni system are highlighted and a consolidated methodology is implemented to develop a unique approach for increasing challenges. To overcome these deficiencies between Alumni Systems and Labor Market, the preset research provides a runtime monitoring system based on Labor policies to attain quality and manageability. The requests placed by students, applications executed by labor office and job requests in pending can be monitored and processed with a flexible approach by using this method. In turn lot of financial wastage can be avoided by reducing the complexity between job seekers and providers by the proposed approach.

Keywords - Runtime Monitoring, Policy, Alumni System, Saudi Universities, Labor Office, Integration


S. Suresh, Department of Information Technology, SRM University, Kattankulathur Campus, Kancheepuram District, TamilNadu, India
Giridhar R., Department of Information Technology, SRM University, Kattankulathur Campus, Kancheepuram District, TamilNadu, India

Abstract — Security is one crucial requirement in Wireless Sensor network. To overcome this issue, security protocol called Didrip was developed for flat based network which allows for distributed data discovery and dissemination. But in terms of clustering approach which is most efficient one in terms of energy conservation, there are lot of security vulnerability i.e. checking the cluster head for vulnerability to the network. In addition sensor nodes joining the cluster head during user joining phase is also not secure as the nodes can be vulnerable too. These two are most vulnerable security issues which are not addressed in existing security protocol of WSN including the one mentioned which is Didrip. The above said problems for clustering approach in WSN are overcome with a Cluster-based Certificate Authority (CA) scheme which is combination of voting and Nonvoting schemes towards detecting malicious node.
We also use digital signature to sign all the nodes present in the network. These are simulated using standard network simulator ns-2 and results analysed in terms of packet delivery, network life time and energy efficiency.

Keywords - Didrip, WSN, CA, ns-2

30. PaperID 31051696: A Multi-step Method to Calculate the Equilibrium Point of the Continuous Hopfield Networks: Application to the Max-stable Problem (pp. 216-221)

Mohammed El ALAOUI (1), Karim EL MOUTAOUAKIL (2) and Mohamed ETTAOUIL (1)
(1) Modelling and Scientific Computing Laboratory, University Sidi Mohammed ben Abdellah, Fez, MOROCCO
(2) National school of applied sciences Al-Hoceima (ENSAH) BP 03, Ajdir Al-Hoceima

Abstract — The Continuous Hopfield Networks (CHN) is a neural network tools which can be used to solve many problems like auto-memory and optimization problems. The dynamics of the CHN is described by differential equations system which is hard to solve analytically. That is why, the researchers use the Euler Cauchy method to calculate the CHN equilibrium point. Unfortunately, this method suffers from several problems, especially quality of the decision for a large step, sensibility to the slope function parameters and to the initial conditions. In this work, we use the well-known multi-step numerical method called Adams–Bashforth method, which is strong in terms of stability and performance, to calculate the equilibrium point of the CHN associated with the max stable problem. This method introduces an intermediary step to improve the Euler Cauchy method precision. The experimental results show that the (CHN+Adams-Bashforth) method produce a large max stable sets in comparison with the (CHN+Euler-Cauchy) method.

Keywords: - Continuous Hopfield Networks, Euler Cauchy method, Adams–Bashforth method, max-stable problem.

31. PaperID 31051699: An Event Grouping Based Algorithm for University Course Timetabling Problem (pp. 222-229)

Velin Kralev, Radoslava Kraleva, Borislav Yurukov,
Department of Informatics, South West University "Neofit Rilski", Blagoevgrad, Bulgaria

Abstract — This paper presents the study of an event grouping based algorithm for a university course timetabling problem. Several publications which discuss the problem and some approaches for its solution are analyzed. The grouping of events in groups with an equal number of events in each group is not applicable to all input data sets. For this reason, a universal approach to all possible groupings of events in commensurate in size groups is proposed here. Also, an implementation of an algorithm based on this approach is presented. The methodology, conditions and the objectives of the experiment are described. The experimental results are analyzed and the ensuing conclusions are stated. The future guidelines for further research are formulated.

Keywords – university course timetabling problem; heuristic; event grouping algorithm

32. PaperID 300416114: Digital Image Watermarking Using DCT and DWT to Improve Robustness (pp. 230-234)

Priyanka Rani, Anupam Singh, Avinash Kumar Singh
Computer Science and Engineering, Shri Ramswaroop Memorial University, Lucknow, India

Abstract — Watermarking is the concept that provides protection in digital multimedia. This paper uses Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Discrete Cosine Transform (DCT) concept for watermarking and extraction purpose. In result analysis we analyze extracted image from watermarked image after applying different attacks (like rotation, Gaussian noise, average filter attack, low pass filter, high pass filter, salt and...
pepper, Histogram Equalization etc). We find that this concept is robust against these types of attacks and provide high security.

Keywords- Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Cover Image, Watermark Message.

33. PaperID 310316102: A New Efficient two tire secure protocol (pp. 235-240)

Rehan Ullah, IT Department Hazara University, Mansehra, Pakistan
Noor ul Amin, IT Department Hazara University, Mansehra, Pakistan
Faisal Bahadur, IT Department Hazara University, Mansehra, Pakistan
Abdul Hakeem, IT Department Hazara University, Mansehra, Pakistan
Insaf Ullah, IT Department Hazara University, Mansehra, Pakistan

Abstract — Signcrypion is a cryptographic method in which signature and encryption apply on message in a single step. On other hand image steganography is a strongest technique for hiding data or information. Therefore Communication through insecure channel is challengeable task for an organization. Recently two tier security gain popularity because most of the business organizations wants maximum security of data/information. In this paper we design a new scheme using cryptographic and stenographic techniques at once on the basis of image steganography and elliptic curve cryptography. In proposed design scheme we use both of the steganography as well as cryptography. The cryptographic technique encrypts the data by using Elliptic curve cryptography in such a manner that third party not understands the original message contents. Stenographic technique is used to hide the text in image and then we take hash as well as signature. It also assures the security properties like message confidentiality, message integrity, message non repudiation and also message authentication.

Keywords-component Cryptography, Steganography, Signcrypion, Elliptic curve cryptography.

34. PaperID 310516111: Formal Model of Smart Traffic Monitoring and Guidance System (pp. 241-252)

Umber Noureen Abbas, Farhan Ullah, Nazir Ahmad Zafar
Department of Computer Science, COMSATS Institute of Information Technology Sahiwal COMSATS Road off GT road, Sahiwal 57000, Pakistan

Abstract — Emergency Services Rescue 1122 and Smart Sticker components of our proposed Smart traffic monitoring and guidance system model are presented in this paper to provide smart emergency services and to identify vehicles to develop advanced transportation system. It involves the Wireless Sensors and actors to communicate with the system. The proposed components require fewer resources in terms of sensors and actors. Further, Sensors component identifies vehicles through Smart Stickers and it is readable through sensors from its barcode and barcode consists of vehicles details in terms of vehicles registration, model, engine and color. Secondly, Emergency Services Rescue 1122 component provides emergency services as it locates the vehicles through sensors and informs the local authority for providing emergency services. Third, violation of rules detects intruders on roads to provide smooth flow of traffic. Fourth, to avoid congestion, traffic signals are configured and communicated with sensors to update the system if congestion occurs. The proposed components of our model are implemented by developing formal specification using VDM-SL. VDM-SL is a formal specification language used for analysis of complex systems. The developed specification is validated, verified and analyzed using VDM-SL Toolbox.

35. PaperID 310516113: Anonymous and Secure Routing Protocol for Multi-hop Cellular Networks (pp. 253-258)

Salwa Othmen (1), Faouzi Zarai (1), Aymen Belghith (2), Lotfi Kamoun (1)
(1) LETI laboratory, University of Sfax, Tunisia
(2) Saudi Electronic University (SEU), Computer Science Departement, Saudi Arabia
Abstract — In single cellular networks, the mobile stations cannot communicate directly with each other. All communications are relayed through the base stations. Such topology suffers from many limitations such as congestion problem when a large number of users are communicating in the same time to a base station. In this context, the device-to-device communications have been proposed to overcome the limitations of the conventional cellular architecture. Indeed, a mobile station can allow two nearby stations to communicate with each other without involving a base station. However, security becomes an important challenge that must be taken into consideration as the mobile stations participate in routing data between each other. In this paper, we propose a secure routing protocol for Multi-hop Cellular Networks (MCNs). Our goal is to discover a secure and short route between the source and the destination. To evaluate this proposed protocol, we perform some simulations using Network Simulator (NS-2). The simulation results show that it provides acceptable performance in terms of throughput and routing overhead as comparing with Secure Ad hoc on demand Distance Vector (SAODV).

Keywords-component; single cellular networks, base stations, Device-to-device, secure routing protocol, MCNs, NS-2;

36. PaperID 310516118: Performance Analysis of Heterogeneous Data Normalization with a New Privacy Metric (pp. 259-264)

J. Hyma (†), PVGD Prasad Reddy (††), and A. Damodaram (†††)
(†) Department of CSE, GIT, GITAM University, Visakhapatnam, INDIA
(††) (†) Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, INDIA
(†††) Department of CSE, Sri Venkateswara University, Tirupathy, INDIA

Abstract - Investigation on privacy preserving data mining is in extensive need to the present day technological situation. Storage of the data and its usage through various computational processes is becoming very easy and efficient. At the other end the primary concern or sometimes can be termed as limitation to this extensive data analysis is privacy. There are existing privacy preserving techniques that solve this problem and also guarantee privacy as well as data utility. But these techniques have to be updated in parallel to the expansion of digital technology. In view of this, the part of research in this paper analyses various normalization techniques with heterogeneous data distortion. The experimental consideration is done with the comparison of various statistical measures on the distorted data and their preservation with respect to the original data. We evaluated the performance of heterogeneous data distortion with three types of transformations namely Min-Max Normalization, Z-Score Normalization and Decimal Scaling. The performance is evaluated with various data distortion measures and privacy measures.

Keywords: Privacy Preserving Data Mining (PPDM), Data Normalization, Privacy, Data utility.

37. PaperID 310516121: Image Compression using Clustering Algorithms (pp. 265-268)

Lale Fathi Ajirlou, Department of Computer, Germi Branch, Islamic Azad University, Germi, Iran
Seyed Naser Razavi, Department of Computer, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Abstract — There is a correlation between pixels in each image so that each pixel value of adjacent pixels can be guessed. By removing these dependencies can be compressed images. Our goal is to reduce the amount of compressed image data needed to display the digital images and therefore reduce the cost of transmission and storage. Compression has a key role in many important applications. These applications include image database, transmission of images, remote sensing, medical imaging, military and space equipment remote control and so on. In addition to the compression, image coding, there's talk. That after quantization matrix should be coded range of conversions. In reconstruction after decoding to achieve our desired image obtained with the difference that the picture is far less than the original image. What we've done in this thesis using a fractal method utilizes a Kohonen neural networks and clustering to increase the compression ratio and reduction coding and decoding the image. We have implemented three methods based on fractal coding. The first method is simple fractal coding. In the second method to create the codebook of multiple tree fractal coding is used. In the second method of vector quantization LBG algorithm for
Kohonen neural network-based clustering algorithm and code book for coding image is used. Results in the second method show faster encoding. The method is simple fractal compression rate is higher than other methods.

**Keyword:** image compression; clustering; vector quantization

38. **PaperID 310516122:** A Joint Duty Cycle and Optimal Energy Adaptation Algorithm for the Body Area Sensor Networks (pp. 269-274)

Ali Raza, Dept. of computer science, City University of Science & Information Technology, Peshawar, Pakistan
Arshad Farhad, Dept. of computer science, COMSATS, Sahiwal, Pakistan
Wajid Ullah Khan, Dept. of computing, Abasyn University, Peshawar, Pakistan
Muhammad Arif, Dept. of computer science, City University of Science & Information Technology, Peshawar, Pakistan

**Abstract** — IEEE 802.15.4 standard is widely adapted for Body Area Sensor Networks (BANs) due to its low duty cycle and low power operation. However, IEEE 802.15.4 recommends the use of fixed duty cycle operation which results in high energy consumption and end-to-end delay. Therefore, an efficient algorithm is needed to adapt duty cycle operation to overcome the end-to-end delay and energy consumption. In this paper, we propose a Joint Duty Cycle algorithm (JDCA) for the BAN to enhance the network lifetime, throughput and decrease the end-to-end delay. Dynamic duty cycle can be adapted by the two MAC parameters: Beacon Order (BO) and Super frame Order (SO). However, these parameters are set by the network administrator before the network deployment. During simulation, JDCA algorithm is capable of adapting dynamic duty cycle at run time based on traffic load. Furthermore, simulation results show enhanced network lifetime, network throughput and less end-to-end delay when compared with IEEE 802.15.4.

**Index Terms** — Dynamic duty cycle, IEEE 802.15.4, Body area sensor networks, Wireless personal area network.

39. **PaperID 310516124:** Performance Evaluation of High Performance Data Transfer in Grid Environment over Broadband Hybrid Satellite Constellation Communication System (pp. 275-279)

Anupon Boriboon, Vincent Mary School of Science and Technology, Assumption University of Thailand, Bangkok, Thailand
Siriwhaddhanah Pongpadpinit, Department of Business Information System, Martin de Tours School of Management and Economics, Assumption University of Thailand, Bangkok, Thailand

**Abstract** — This paper presents the evaluation performance of broadband hybrid satellite constellation communication system (BHSCCS) networks which provides high performance data transfer in grid network environment based on TCP protocols. The evaluated hybrid satellite network uses the COMMS5ellationTM constellation topology on lower orbital. We adopt the GridFTP to improve network performance. GridFTP is a high-performance, reliable data transfer protocol optimized for high-speed Internet to suitable WAN networks. The simulation results show the network performance of GridFTP which different AQMs, TCPS, PERs, over BHSCCS networks.

**Keywords:** COMMS5ellationTM; GridFTP; Hybrid Satellite; Queue; TCP

40. **PaperID 310516127:** A Lasso-LTS Method for DNA Sequence Classification Based on Beta Wavelet Networks (pp. 280-292)

Abdesselem DAKHLI, Department of Computer Science, REGIM, University of Gabes, Tunisia
Wajdi BELLIL, Department of Computer Science, REGIM University of Gafsa 2110 Gafsa, Tunisia
Chokri BEN AMAR, Department of Computer Science, REGIM University of Sfax 3018, Sfax, Tunisia

**Abstract** — This paper presents a method for DNA sequence classification based on beta wavelet networks using the Lasso-LTS regression. The proposed method is evaluated on several DNA datasets and compared with other existing methods. The experimental results show that the proposed method outperforms the existing methods in terms of classification accuracy.

**Keywords:** DNA sequence classification; beta wavelet; Lasso-LTS regression; classification accuracy.
Abstract — Wavelet Neural Network (WNN) is attracting interest in field of classification system, because they are universal approximations, particularly due to rapid and accurate representation of nonlinear dynamic systems. The satisfying performance of the WNN depends on an appropriate determination of the Wavelet Neural Network structure. In this paper we provide a new method to solve this problem based on the Least Absolute Shrinkage and Selection Operator (LASSO). At first, the scale of WNN is managed by using the time-frequency locality of wavelet. Furthermore, the unconstrained optimization problem (LASSO) is used to solve the structure and learning of the WNN. This optimization problem can be solved efficiently using the iteratively reweighted least squares (IRLS) and the Least Trimmed Square (LTS) methods to enhance the ineffectiveness; they are applied to train the wavelet neural network. The advantage of the method lies in the oracle properly of the LASSO can guarantee the optimal structure of the WNN. The proposed method has been able to optimize the wavelet neural network and this method is able to classify the DNA sequences. Our goal is to construct predictive models that are highly accurate. In fact, the proposed method permits to avoid the complex problem of form and structure in different clusters of organisms. The empirical results and their classification performances are compared with other methods. We compared the WNN-Lasso model with the other five alignment-free models, i.e., k-tuple, DMK, TSM, AMI, and CV, on several large-scale DNA datasets on the DNA classifying application by means of the K-means method. The experimental results have shown that the WNN-Lasso model outperformed the other models in terms of both the classifying results and the running time. Evenly, in this study, we present our approach consists of three phases. The first one, which is called transformation, is composed of two sub steps; binary codification of the DNA sequences and the Signal Processing of the DNA sequences. The second phase step is the approximation; it is empowered by the use of the Multi Library Wavelet Neural Networks (MLWNN). Finally, the third section, which is the classification of the DNA sequences, is realized by applying the algorithm of k-means classification.

Index Terms— LASSO, LTS, Wavelet Neural Networks, DNA sequences, MLWNN, IRLS.

41. PaperID 310516129: Sindhi Morphological Analysis: An Algorithm for Sindhi Word Segmentation into Morphemes (pp. 293-302)

Department of Computer Science, Shah Abdul Latif University, Khairpur Mir’s, Sindh, Pakistan

Abstract- Morphological analysis is the process of constructing and deconstructing the words of a language, the process is based on the basic grammatical units which are stem, prefixes, suffixes and infixes. Sindhi is rich in morphological features with a great variety of affixes. The problem for Sindhi to come into computerization is the large number of variants in its morphology. This complexity is created due to different positions of prefixes, suffixes and stems in the words. The automatic word segmentation system normally faces such embedded hurdles in Sindhi language. An algorithm is required with a capability of dealing with such issues for the segmentation of Sindhi words. In this paper, an algorithm is designed and implemented to resolve the problem of segmenting Sindhi complex and compound words into possible morphemes. The developed words segmentation system has been tested on a list of 109 compound words, 179 prefix words, 1343 suffix words and 50 prefix-suffix words. The cumulative segmentation error rate of 5.02% is calculated. This system can also be used as pre-requisite in various Sindhi language and speech processing applications.

Keywords — Sindhi Morphology; Morphological Analysis; Word Segmentation; Morphemes

42. PaperID 310516130: A New Secret Sharing Scheme Using Rational Interpolation (pp. 303-307)

Ali Nakhaei Amroudi, Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran
Ali Zaghian, Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran, Mahdi Sajadieh, Department of Electrical Engineering, Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran
Abstract — Most of the existing secret sharing schemes are based on polynomial interpolation. In other word, they use polynomial functions in their schemes. In this paper, we solve the problem of creating a secret sharing scheme based on rational interpolations. We show that if support points have the same width then the rational interpolation of the support points, which is called \( (\cdot,\cdot)\), has pole points. Finally, we give an example for the accuracy of the proposed scheme.

Keywords-component; Secret Sharing Scheme; Shamir’s Scheme; Polynomial Interpolation; Rational Interpolation, Pole Points.

43. PaperID 310516133: A Novel Face Recognition System based on Skin Detection, HMM and LBP (pp. 308-316)

Mejda Chihaoui, Akram Elkefi, Wajdi Bellil, Chokri Ben Amar
REGIM: Research Groups on Intelligent Machines, University of Sfax
National School of Engineers (ENIS), Sfax, 3038, Tunisia.

Abstract — Although there are various biometric techniques, like fingerprints, iris scan as well as hand geometry, the most efficient and widely-used one is face recognition because it is inexpensive, non-intrusive and natural. In our paper, we present an approach aiming at implementing a full architecture which represents an efficient system of face recognition. For this, an attempt is proposed for each system stage. At the beginning, we develop a novel approach to detect faces existing in 2D color image. This approach focuses mainly on how to implement a selection of skin color before using neural networks and Gabor filters. This approach represents an improvement of existing approach especially because it aims to minimize the computation time. Indeed, the skin detection step avoids wrong detection and to help the system detect the face in the right areas and minimize the research time and subsequently the Gabor filter will be applied only on the localized skin space. Later, the face features obtained by the Gabor filter represent the input of the neural network classifier to decide whether an input image pixel is a face pixel or not. For 2D face recognition, we propose likewise a novel approach that we call HMMLBP (a combination of the two tools Hidden Markov Models HMM and Local Binary Pattern LBP). It allows classifying a given 2D face image through utilizing an LBP tool to extract features. In order to validate our whole system performance, we show experimental results obtained when applying our proposed algorithm on benchmark face databases, respectively AT&T, Yale and Feret.

44. PaperID 310516134: Energy Efficiency Techniques in Cloud Computing (pp. 317-323)

Altaf Ur Rahman, Fiaz Gul Khan, Waqas Jadoon
Department Computer Science, COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad

Abstract — Cloud computing gaining popularity at enormous rate since from its emergence. CC changed the way that computing services are provided. On demand platform (PaaS), infrastructure as a service (IaaS) and software (SaaS) as a service through internet. Consumer use third party services instead of building his own infrastructure which need up-front investment and expertise. Cloud computing becoming popular for unlimited computing power, availability, nice pricing, on demand services and quality of service. For availability and computing power the service provider expands their resource capacity to handle user requirements. This expansion in resources capacity lead to high energy demand. Two big issues for cloud computing is energy demand and security/privacy requirements. In this survey we will give a review on the latest techniques for energy efficiency in cloud computing. The main focus is on software base energy efficiency techniques in which we will explain the workload consolidation and resource management in detail.

Index Terms — cloud computing, data center, energy efficiency techniques.

45. PaperID 310516135: Service Level Agreement in Cloud Computing: A Survey (pp. 324-330)
Usman Wazir, Dr. Fiaz Gul Khan, Dr. Sajid Shah
Department of Computer Science, COMSATS Institute of Information Technology, University Road ToBe Camp, Abbottabad, Pakistan

Abstract — Cloud computing provides distributed resources to the users globally. Cloud computing contains a scalable architecture which provides on-demand services to the organizations in different domains. However, there are multiple challenges exists in the cloud services. Different techniques has been proposed for different kind of challenges exists in the cloud services. This paper reviews the different models proposed for SLA in cloud computing, to overcome on the challenges exists in SLA. Challenges related to Performance, Customer Level Satisfaction, Security, Profit and SLA Violation. We discuss SLA architecture in cloud computing. Then we discuss existing models proposed for SLA in different cloud service models like SaaS, PaaS and IaaS. In next section, we discuss the advantages and limitations of current models with the help of tables. In the last section, we summarize and provide conclusion.

Index Terms— Service Level Agreement (SLA), Cloud Computing.

46. PaperID 310516136: Blind Watermarking Algorithm for 3D Multiresolution Meshes based on Spiral Scanning Method (pp. 331-342)

Ikbel Sayahi, Akram Elkefi, Chokri Ben Amar
REGIM-Lab.: REsearch Groups in Intelligent Machines, University of Sfax, ENIS, Sfax,3038 Tunisia

Abstract — 3D mesh is a new data type appeared in the last decades. Since its emergence, it has been used in several areas which raise major security problems. As a solution, we propose a blind watermarking algorithm for 3D meshes. For doing spiral scanning method decomposes the mesh into GOTs (a Group of Triangles). At each time, only one GOT will be uploaded into memory. It undergoes a wavelet transform to generate vector of wavelet coefficients. This latter undergoes modulation then embedding steps using data coded with BCH code. Once watermarked, the next GOT will be uploaded. This process stopped when the entire mesh is watermarked. Experimental tests show that the quality of meshes is kept despite the high insertion rate and that memory consumption is reduced. As for robustness, our algorithm overcomes the following attacks: translation, rotation, smoothing, uniform scaling, coordinate quantization, noise addition, simplification and compression.

Index Terms — Digital watermarking, 3D meshes, Multiresolution, Wavelet transform, Spiral scanning, Attacks, Compression.

47. PaperID 310516141: Towards the Development of an Efficient and Cost Effective Intelligent Home System based on the Internet of Things (pp. 343-350)

A. Imtar Chaudary, Dept. of Computer Science, CIIT, Sahiwal, Pakistan
Muhammad Usman, Dept. of Computer Science, CIIT, Sahiwal, Pakistan
Arshad Farhad, Dept. of Computer Science, CIIT, Sahiwal, Pakistan
Wajid Ullah Khan, Dept. of Computing and Technology, Abasyn University, Peshawar, Pakistan

Abstract — Internet of Things (IoT) is an emerging technology which is covering everyday things from industrial machinery to consumer goods in order to exchange information and complete tasks while involved in other work. IoT based smart home automation system is a system that uses PCs, mobile phones or remote devices to control basic operations for home automatically from anyplace around the world using internet. The proposed intelligent home automation system differs from existing systems as it allows the user to operate the system from anywhere around the world by using internet connection along with intelligent nodes that can take decisions according to the environmental conditions. We implemented a home automation system using sensor nodes that are directly connected to Arduino microcontrollers. Microcontroller is programmed so that it can perform some basic operations on the basis of sensors data. e.g. fan is controlled on basis of temperature value and light is controlled on the basis of occurrence of motion in the room etc. Furthermore Arduino board is connected to the internet using Wi-Fi module. An extra feature this system provides is to monitor power consumption of different home appliances. The designed system provides the
user remote control of numerous appliances locally as well as outside the home. This designed system is expandable, allowing multiple devices to be controlled. The objective of the proposed system is to provide a low cost and efficient solution for home automation system by using IoT. Results show that the proposed system is able to handle all controlling and monitoring of home.


48. PaperID 310516142: A Threshold-Based Predictive Scheme for Mobile Subscribers in Publish/Subscribe Systems (pp. 351-357)

*Fatma Abdennadher, Maher Ben Jemaa*

National School of Engineers of Sfax, University of Sfax, ReDCAD Laboratory, B.P.1173, 3038 Sfax, Tunisia

*Abstract —* In this paper, we present our strategy adopted to deal with the mobility into publish/subscribe. Specifically, we focus on the management of the mobile users from one broker to another. In fact, the topic of mobility into publish/subscribe systems may cause many problems such as the increasing of the traffic into the network and the messages loss. To overcome these problems, we have created a selective scheme on the basis of an accurate selection. In fact, a threshold value is devoted to be the criterion for the selection of caching points. On the basis of this principle, we apply various network settings to explore the effectiveness of our approach. Hence, we extract the improvement of our approach on the messages loss, the caching cost and the propagation cost in function of buffer size, publication rate, period of disconnection and connect time.

*Keywords-Distributed Networks; Mobile Computing; Publish/Subscribe; Prediction Management; Performance Efficiency.*

49. PaperID 310516147: A Novel Protocol Stack for Improving QoS in Vehicular Networks (pp. 358-367)

*Mohammadreza Pourkiani, Department of Information Technology Science and Research Branch, Islamic Azad University, Tehran, Iran*

*Sam Jabbehdari, Department of Computer Engineering, Tehran North Branch, Islamic Azad University, Tehran, Iran*

*Ahmad Khademzadeh, Department of National and International Cooperation, Iran Telecommunication Research Center, Tehran, Iran*

*Abstract —* Intelligent Transportation Systems are defined as those systems utilizing synergistic technologies and systems engineering concepts to develop and improve transportation systems of all kinds. Vehicular Ad-hoc Network (VANETs) which is an application of Mobile Ad-hoc Networks (MANETs) play an important role in ITS and emerged to provide Vehicle to Vehicle, Vehicle to Roadside and Vehicle to Infrastructure communications, aiming to improve safety on roads, exchange data between vehicles and provide different services to the users. According to special characteristics of VANETs like bandwidth limitation, high mobility, signal fading and real-time data communications, QoS provisioning in these networks is a challenging task. In this paper, we introduce an architecture for vehicular networks and a protocol stack which aims to reduce the processing overhead, make routing easier and provide Quality of Service in vehicular networks. Finally, after designing protocols and headers of the mentioned protocol stack, we will simulate our proposed idea in a vehicular environment and after simulation process, we will compare the achieved results with another scenario in which regular TCP/IP protocols are used.

*Keywords-component; VANETs; ITS; QoS; Protocol Stack*

50. PaperID 310516149: Performance Analysis of VoIP over IPv4, IPv6 and 6-to-4 Tunneling Networks (pp. 368-372)

*Abstract —* In this paper, we analyze the performance of voice over IP (VoIP) over IPv4, IPv6 and 6-to-4 tunneling networks. We use a simulation tool to evaluate the quality of service provided by these networks, and we compare the results to determine which network is more suitable for VoIP applications.

*Keywords—VoIP, IPv4, IPv6, 6-to-4 tunneling, performance analysis.*
Abstract — Transition from IPv4 to IPv6 is a cumbersome process because of their irreconcilability with each other and coexists during the transition period. This work examines the behavior of transition mechanisms that involve communication among IPv4 and IPv6 in various scenarios and traffic conditions. A network analyst faces variable traffic and data rates at different nodes in such a heterogeneous network, that requires more attention to make it able to work with stable network flow and data rate. We analyse an end-to-end delay of VOIP data packets in IPv4 and IPv6 homogeneous and heterogeneous networks using 6 to 4 tunneling techniques. This work shows that IPv6 has better performance than IPv4 and IPv6-to-IPv4 tunneling. The tunneling technique improves the network throughput and queuing delay over the intermediate nodes of the heterogeneous network.

Keywords: IPv4, IPv6, VoIP, 6-to-4 tunneling, DSTM

51. PaperID 310516151: Investigation of Collusion Attack Detection in Android Smartphones (pp. 373-379)

M. Kireet, Dept of CSE, JNTUH, Hyderabad, India
Dr. Meda Sreenivasa Rao, JNTUSIT, Hyderabad

Abstract — Today as Android is used by majority of the smartphone users it has become one of the effortless platform for the malware-writers to introduce their malicious activities into smartphone world through this android mobile applications. The main loophole in Android applications is permission based security control. The User unawareness of accepting every permission as a mandatory requirement by an app is making more and more convenient for the hackers to extract the users’ private data. In this paper we have analysed all the leakages which are done by using permissions required by an app. We carefully made an investigation to detect collusion attacks. We analyzed the present detection methods of inter-permission leaks especially on Collusion attacks and mentioned the areas where the enhancements are needed with limitations that existed in present detection methods.

Keywords - Collusion attacks, inter-permission leaks

52. PaperID 310516152: A Hybrid Machine Learning Model for Selecting Suitable Requirements Elicitation Techniques (pp. 380-391)

Nagy Ramadan Darwish, Department of Computer and Information Science, Institute of Statistical Studies and Research, Cairo University, Egypt
Ahmed Abdelaziz Mohamed, Department of Information Systems, Higher Technological Institute, Cairo, Egypt
Abdelghany Salah Abdelghany, Department of Information Systems, Higher Technological Institute, Cairo, Egypt

Abstract — Requirements elicitation is the first and the most critical phase of Requirements Engineering (RE). Many techniques have been proposed to support the elicitation process. Each technique has its strengths and weaknesses. This variety makes the selection of technique or combination of techniques for a specific project a difficult task. Mostly techniques are selected based on personal preferences rather than on attributes of project, technique, and stakeholders. In this paper, the researchers propose a three-component approach for elicitation techniques selection. First, a literature review is conducted to identify the attributes affecting techniques selection and common elicitation techniques. Second, a multiple regression model is built to analyze these attributes in order to find the critical attributes influencing techniques selection. Finally, an Artificial Neural Network (ANN) based model for selecting adequate elicitation techniques for a given project is proposed. The ANN model helps reduce the human involvements in this process. It was implemented using Neural Network Fitting Tool in MATLAB. The network has accuracy of 81%. The ANN model was empirically validated by conducting a case study in a software company.
Keywords: Requirements Engineering, Requirements Elicitation, Multiple Regression Analysis, Neural Network.


Anum Khurshid, Fiaz Gul Khan, Abdul Nasir Khan
Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, Pakistan

Abstract — Proxy Re-Encryption has been used since the need for forwarding an encrypted message to a party for whom it was not encrypted was highlighted in the form of delegation rights by Blaise, Bleumer and Strauss. Various Proxy Re-Encryption schemes have been introduced till today mainly focusing on demonstrating features like transitivity and collusion-resistance to ensure minimal trust on the proxy and maximum key-privacy. This survey highlights some major schemes introduced, classifies them based on their directionality, brings to light their major advantages and disadvantages, and provides a detailed comparative study based on the key features a Proxy Re-Encryption Scheme must possess in order for its widespread.

Index words— bilinear maps, CCA secure, collusion resistance, CPA secure, delegation rights, Diffie-Hellman key exchange, DBDH assumptions, Proxy Re-Encryption; transitivity.


Owais Khan, Fiaz Gul Khan, Babar Nazir, Usman Wazir
Department of Computer Science, COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad, Pakistan

Abstract — WSN is an evolving technology since last ten years. As wireless nodes work have less power supply in the form of a battery, it is necessary for the nodes to work for maximum time. Different techniques are adopted to achieve better energy optimization. This paper presents a survey on energy efficient routing techniques, which will help in understanding the factors which affect energy efficiency and other performance parameters and will help to analyse the techniques for further optimizations.


55. PaperID 310516166: Improved Face Recognition Rate Using Face Partitioning in Eigen and Fisher Feature Based Algorithms (pp. 407-417)

Harihara Santosh Dadi, Gopala Krishna Mohan Pillutla

Abstract — Face partitioning technique is presented in this paper. Instead of directly giving the face to the face recognition system, first the face is partitioned in to different face parts using face partitioning technique. The face parts are namely mouth, left eye, right eye, head, eye pair and nose. Eigen and Fisher features based algorithms are considered for experimental purpose. These face part features are given to the SVD classifiers individually. The outputs of the classifiers are again given to the decision making algorithm. Based on the maximum likely hood principle, this decision making algorithm outputs a face. ORL data base is used for evaluating the performance of this new technique. The first two faces of all the 40 people in the data base are considered for testing and the remaining eight faces are used for training purpose. Results are separately calculated with and without face partitioning technique. Results show that face recognition rate is increased by using the combination of face partitioning technique and basic face recognition algorithm. The new algorithm is also verified on 8 different data sets. Experimental results show that this face partitioning is improving the face recognition rate both Eigen and Fisher feature based algorithms.
Index Terms—Face Partitioning, Facial features, Recognition engine, Support Vector Machine, Decision making algorithm.

56. PaperID 310516168: Elastic Extension Tables for Multi-tenant Cloud Applications (pp. 418-431)

Haitham Yaish (1, 2, 3), Madhu Goyal (1, 2), George Feuerlicht (2, 4)
(1) Centre for Quantum Computation & Intelligent Systems
(2) Faculty of Engineering and Information Technology, University of Technology, Sydney
P.O. Box 123, Broadway NSW 2007, Australia
(3) Faculty of Engineering, American University of the Middle East, Kuwait
(4) Faculty of Information Technology, University of Economics, Prague, Czech Republic

Abstract — Software as a service (SaaS) is a Cloud Computing service model that exploits economies of scale for SaaS service providers by offering a single configurable software and computing environment for multiple tenants. This contemporary multi-tenant service requires a multi-tenant database that accommodates data for multiple tenants using a single database schema. In general, traditional Relational Database Management Systems (RDBMS) do not support multi-tenancy and require schema extensions to provide multi-tenant capabilities. This paper proposes a multi-tenant database schema called Elastic Extension Tables (EET), which is highly flexible in enabling the creation of database schemas for multiple tenants by extending a preexisting business domain database, or by creating tenant business domain database from the scratch at runtime. The empirical results presented in this paper indicate that the EET schema has potential to be used for implementing multi-tenant databases for multi-tenant SaaS applications.

Index Terms—Cloud Computing, Software as a Service, Multi-tenancy, Elastic Extension Tables, Multi-tenant Database.

57. PaperID 310516174: Triangle Area Based MCA Technique and Anomaly Based Detection Technique for Detecting DOS Attacks (pp. 432-440)

Varsharani Dudhande, Sharmila Wagh
Modern Education Society’s College of Engg., Computer Department, Savitribai Phule Pune University, India

Abstract — The availability of network services are being menaced by the increasing number of Denial-of-Service (DoS) attacks. The availability of such interconnected systems is severally degraded by increasing number of DOS attacks. Denial-of-Service (DoS) attacks cause serious impact on these computing systems such as router, host or entire network. DoS attack detected using Multivariate Correlation Analysis (MCA) technique. Multivariate correlation analysis employs for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. The proposed system uses the Multivariate Correlation Analysis (MCA) technique for accurate characterization also uses the anomaly based detection technique in attack recognition. Anomaly based detection makes system capable of detecting seen and unseen attacks. Moreover, a triangle area based technique is planned to reinforce and increases performance of MCA. The impact of each non-normalized information and normalized information on the performance of the proposed detection system is tested.

Keywords — Denial- of- Service attack, network traffic characterization, multivariate correlations, triangle area.

58. PaperID 310516176: Proposed Hybrid Model to Detect and Prevent SQL Injection (pp. 441-448)

Mrs. Teresa K. George, Dr. Rekha James, Dr. Poulose Jacob
Dept. of Computer Science, CUSAT, Cochin

Abstract - SQL Injection vulnerability takes advantages of the poorly coded web application and exploits the sensitive and critical information stored in an application’s database by compromising the authentication logic of the database server. In Most of the web applications user inputs in the dynamic web pages are the vulnerable points for SQL
injection attack. A single detection tool cannot handle the sophisticated injection attacks by the intelligent hackers. The proposed hybrid model with SQLI-Rejuvenator on an Application Program Interface is tested and proved as an efficient technique to detect and prevent SQL injection. In this architecture, the malicious queries are blocked and an alert message is generated if the injection is detected. Only the benign query is allowed to access the data from the backend database server. The Unique identity created by the template creator application, the Rejuvenator module and evaluation engine are significant features of the proposed model to prevent the injection attack and can facilitate better availability of the application.

Keywords – Authentication; Injection; Vulnerability; Hackers; Detection; Rejuvenation;

59. PaperID 310516179: Hand Gesture Recognition System (pp. 449-453)

ABBES Zeineb, CHIBANI Chaala
Dept of industrial computing, Higher Institute of Computer and Multimedia, Gabes, Tunisia
Tarek Frihka, Abir Hadriche
CES Lab, REGIM Lab, Sfax, Tunisia

Abstract - In this article, we will propose a real-time human hand gesture recognition system which will perform translations from the sign language to the common French language. The processes is composed by three basic steps: The detection and extraction of the hand pattern characteristics during the image stream acquisition, which is obtained from an integrated camera. The analysis process, in which the obtained characteristics are classified as either a recognized sign language gesture or an unclassified hand movement. Preset characteristics of each effective hand gesture are stored locally. The message-assembling phase: at the end of cycle of each iteration of the two previous steps, the obtained result is either neglected or concatenated with the assembled message so far. The message is then displayed.

Keywords: human-machine communication, gestural interaction, French sign language, linked gesture recognition.

60. PaperID 310516180: An Optimization Technique for Brain Tumor Recognition (pp. 454-464)

Dr. D. Rajya Lakshmi, CSE Dept in JNTUK Vizianagaram
Shaik Salma Begum, CSE Dept in Gudlavalleru Engineering College

Abstract - In this paper, we have proposed a robust technique to detect and classify the tumour part from medical brain images. In recent times, a number of image segmentation and detections techniques have been proposed in the literature. But, the detection of brain tumour through the help of classification technique has received significant interest among the research community. By considering the above issue, here, we combine three different techniques such as, cuckoo search, neural network and fuzzy classifier to detect the tumour part effectively. Our proposed approach consists of four phases, such as, pre-processing, region segmentation, feature extraction and classification. In the pre-processing phase, the anisotropic filter is used for reducing the noise and in the segmentation process; K-means clustering technique is applied. For the feature extraction, the parameters such as contrast, energy and gain are extracted. In classification, a modified technique called Cuckoo-Neuro Fuzzy (CNF) algorithm is developed and applied to detection of tumour region. In the modified algorithm, cuckoo search algorithm is employed for training the neural network and the fuzzy rules are generated according to the weights of the training sets. Then, classification is done based on the fuzzy rules generated. Experimental results shows that the proposed technique achieved the accuracy of 79.49% but existing technique achieved only 76.92%.

Keywords: CNF, contrast, energy, entropy, K-Means, anisotropic filter, sensitivity, specificity, accuracy

61. PaperID 310516183: Permission Based Android Malware Detection System using Machine Learning Approach (pp. 465-470)
Mayuri Magdum, Computer Engineering, Modern Education Society’s College of Engineering, Pune, India
Prof. Sharmila K. Wagh, Computer Engineering, Modern Education Society’s College of Engineering, Pune, India

Abstract — Mobile computing has grown and developed in recent years with huge popularity. Gadgets like Smart phones, Tablets, etc have become trendy by the ease of use. Android is more famous platform and turned out to be the most important target of Malware developers in precedent years. The malware hazard for cellular telephones is evaluated to increment security and usefulness of smartphones. Hackers and malware program developers are benefitted by the limited capabilities and lack of standard security mechanism of Android. Nowadays smart phones are omnipresent, i.e. they fill numerous needs such as data storage, personal mobile communication, multimedia and entertainment etc. therefore, implementing secure mobile connections is challenging. As a result, it becomes essential to have some valuable and probabilistic detection along with preventive mechanisms. Many preventive tools are available in market but current trend for malware security is before installing the app user should be able to identify possible threats. Hence we propose permission based mobile malware detection system. It has 3 components in it 1) Client 2) Server 3) Signature Database. In the whole analysis process, Server plays important role and user is warned at the end of analysis process whether the requested app contains malware or not.

Keywords- Mobile, Android, Malware, Security, Machine Learning, Static Analysis.

Dileep Kumar Singh, Praveen Kaushik
Dept of CSE, MANIT Bhopal, India

Abstract — Increasing amount of dependability on computer networks and internet services are also increasing intrusions. Intrusion Detection System (IDS) tools detect the intrusions and produce alerts. An automated Intrusion Response System (AIRS) is required to analyze the alert and trigger appropriate response to mitigate the intrusion without delay. In this paper, cost evaluation methods and response decision making capabilities of various AIRS models are analyzed. Various decision making factors that are involved in the response selection process are also identified and then categorized in response, attack and system level factors.

Index Terms—Intrusion Response System, AIRS, Response selection, Response factors, Response cost.

63. PaperID 310516192: SQL Injection Prevention using Query Dictionary Based Mechanism (pp. 479-485)
Adwan F. Yasin, Nael Zidan
Department of Computer Science, Arab American University, Jenin, Palestine.

Abstract — SQL Injection Attack (SQLIA) is a technique of code injection, used to attack data driven applications especially front end web applications, in which heinous SQL statements are inserted (injected) into an entry field, web URL, or web request for execution. “Query Dictionary Based Mechanism” which help detection of malicious SQL statements by storing a small pattern of each application query in an application on a unique document, file, or table with a small size, secure manner, and high performance. This mechanism plays an effective manner for detecting and preventing of SQL Injection Attack (SQLIA), without impact of application functions and performance on executing and retrieving data. In this paper we proposed a solution for detecting and preventing SQLIAs by using Query Dictionary Based Mechanism.

Index Terms—SQL Injection Attack, SQL Injection Attack Detection, SQL Injection Attack Prevention, Query Dictionary.
**PaperID 310516195: An Optimized Approach toward Intrusion Detection Using Cluster-Like Behavior of Attacks (pp. 486-490)**

Aliakbar Tajari Siahmarzkooh, Jaber Karimpour, Shahriar Lotfi  
*Faculty of Mathematical Sciences, Department of Computer Science, Iran, Tabriz, University of Tabriz*

**Abstract** — Most of intrusion detection researches suffer from the following drawbacks: Dependencies between network nodes and cluster-like behavior of anomalies. Hence, this paper proposes a cluster-based approach in which the anomalies are detected using a new criterion related to the behavior of attacks. In addition, we provide a cluster-based data set which uses the flow-based data and graph properties to model the network traffic over time. The data set is built over the DARPA. Moreover, the anomalies are revealed by means of a criterion which is computed from internal and external weight of clusters. Finally, the proposed approach is evaluated and compared to other approaches. The evaluation results show the preference of our approach relative to other ones.

**Keywords** — Anomaly; DARPA data set; flow; graph clustering; intrusion detection

---

**PaperID 310516197: A Comparative Study of Smoothing a Vehicle’s Trajectory which is calculated by an Evolutionary Algorithm (pp. 491-496)**

B.A. Buran is with the Department of Basic Sciences, Turkish Air Force Academy, Istanbul, Turkey.  
S.H. Caglar is with the Department of Mathematics and Computer Science, Istanbul Kultur University, Istanbul, Turkey.  
O.K. Sahingo is with the Department of Computer Engineering, Turkish Air Force Academy, Istanbul, Turkey

**Abstract** — Determining a vehicle’s trajectory is a complex and hard to solve type problem in the literature and it is identified as a NP-Hard optimization problem which is studied in different engineering disciplines such as computer, electrical and industrial engineering. It has been observed that such complex problems can be solved by using various approaches and lots of them are focused on the usage of Evolutionary Algorithms especially in case of a large number of controls points which are needed to be visited. Although these algorithms provide near optimal solutions, in the real world, vehicles are not able to follow this determined path (trajectory) without any deviation. Because vehicles are moving objects and each one moves with a certain speed. Therefore it is impossible for a vehicle to make a sharp turn after visiting control points. These vehicles need to make smoothed turns over these points. Therefore there will be a certain difference between the calculated path and the real path. It is needed to determine the real path by using necessary mathematical solutions for smoothing these paths. To ensure the motion continuity of vehicles, they need to follow paths determined according to a certain criterion. In this study, the most common smoothing methods which are used to ensure these continuities (Bezier, B-Spline and Dubins) have been compared and it is aimed to show the different approaches in an application area of path planning problems as a comparative study.

**Keywords** — Unmanned Aerial Vehicle, Path Planning Evolutionary Algorithm, Bezier Curves; B-Spline Curves, Dubins Path.

---

**PaperID 310516200: Location-Based Routing Protocols GAF and its enhanced versions in Wireless Sensor Network a Survey (pp. 497-504)**

Hanane AZNAOUI, Said RAGHAY & Layla AZIZ  
*Laboratory (LAMAI), Faculty of sciences and technology, University Cadi Ayyad Marrakech, Morocco*

**Abstract** — Since the last two centuries, humanity has made scale steps in this attraction to innovation and technological progress. The emergence of global networks of computers corresponding to Wireless Sensor network WSN is one of those great steps that man could do. WSN is an advanced technology that occur in response to overcome user needs. It resolves many problem such as, controlling phenomena, monitoring places, and diagnostic. Nevertheless, this
advanced technology still incomplete in order to different constraints such as energy consumption, routing, aggregated data and security, also routing information represents a critical issue in it. For that, great researches designed. In this paper, we present a survey of GAF and their enhanced versions as Location-Based routing protocols in WSN, which allows reducing the consumed energy in the network and prolonging the network lifetime.

Keywords: WSN, routing protocols, location-based, GAF.

67. PaperID 310516201: Comparison of RC2 and AES Using Windows Azure for Data Security in Cloud (pp. 505-509)

Muhammad Inaam ul haq, Department of Computer Science COMSATS, Institute of Information Technology, Sahiwal, Pakistan
Muhammad Umar, Department of Computer Science COMSATS, Institute of Information Technology, Sahiwal, Pakistan
Syed Muhammad Owais, Department of Computer Science COMSATS, Institute of Information Technology, Sahiwal, Pakistan

Abstract - Cryptography is a very useful tool to protect the properties of data like integrity, privacy, confidentiality in any environment. This paper explores some useful aspects of cryptography in cloud computing environment. There are different types of encryption algorithms used in order to ensure the data security. These algorithms are of different types like symmetric, a symmetric and hashing algorithms. The objective of this paper is performance analysis of selected set of algorithms on the basis of different parameters, so that the best out of all these options is chosen or combinations of some of them can be utilized to secure data in cloud computing environment. The algorithms included in this study are RC2 and AES. The parameters which are used for performance analysis are running time of the algorithm, data encryption capacity. These are the performance parameters which are calculated for every algorithm in cloud based environment i.e. windows azure simulator by utilizing visual studio IDE and profiler services by integrating windows azure SDK. The interpretation of these results are done by using various graphs which shows trend of a particular algorithms on basis of time of encryption and decryption.

Keywords: Cryptography, Cloud Security, RC2, AES, Windows Azure

68. PaperID 31011659: Optimized and Secure Authentication Proxy Mobile IPv6 (OS-PMIPv6) Scheme for Reducing Packet Loss (pp. 510-515)

Arun Kumar Tripathi, Department of Computer Science and Engineering, KIET Group of Institutions, Ghaziabad, India
R. Radhakrishnan, Department of Computer Science and Engineering, ABES Engineering College, Ghaziabad, India
J.S. Lather, Department of Electrical Engineering, National Institute of Technology, Kurukshetra, India

Abstract — Due to continuous evolution in hand handled mobile devices such as Smartphones, Laptops, tablets and Personal Digital Assistants (PDAs) have increases the volume of traffic on Internet radically. To provide seamless Internet services and perpetual mobility to these devices, Internet Engineering Task Force (IETF) has proposed various mobility management protocols such as MIPv6, HMIPv6, and PMIPv6. MIPv6 is a host-based mobility management protocol and suffers from handover latency, packet loss etc. Recently the IETF proposed network-based mobility management protocol, known as Proxy Mobile IPv6 (PMIPv6). PMIPv6 sufficiently reduces signaling overhead but still have long authentication latency during handover and packet loss issues. To resolve these issues, an optimized and secure authentication mechanism for handover management scheme for PMIPv6 networks is proposed in this paper. Due to less authentication delay, the proposed scheme reduces the setup time and as a result has low handover latency. Subsequently, decreases the amount of packet loss during handover. The proposed scheme provides higher security infrastructure than the basic PMIPv6 protocol and additionally reduces the handover latency to contemporary protocols. The performance and results are mathematically analyzed. Numerical results show that the proposed scheme
gives better performance than the existing MIPv6 in terms of signaling delay and provide higher security than PMIPv6 protocol.

69. PaperID 31051605: Design for ALL: Catering for Culturally Diverse Users (pp. 516-524)

Mahdi H. Miraz (1,2), Maaruf Ali (2), Peter S. Excell (1)
(1) Department of Computing, Glyndŵr University, Wrexham, UK
(2) Department of Computer Science & Software Engineering, University of Hail, KSA

Abstract — Due to mass global migration and increased usage of the Internet, it is now very important to address the cultural aspects of the usability problems of any Information and Communication Technology (ICT) products such as software, websites or applications (apps) whether to be used on PCs, Laptops, Smartphones, Tablets, Smart TVs or any other devices. To augment the “Design for All” concept, this research demonstrates the need to cater for culturally diverse users while designing user interfaces. This has been achieved, by investigating ICT products and conducting an extensive literature survey. The study concludes that it is very important to work on cross-cultural usability problems and bring these issues under focus.

Index Terms — Human Computer Interaction (HCI), Universal Usability, Cross-cultural Usability, User Interface (UI) Design, Design for All, Users’ Behaviour.

70. PaperID 31051611: Urban Traffic Control with Pedestrian Handling (pp. 525-534)

Ayesha Shahid, Wilayat Ali Khan, Nazish Naheed, Salman Hafeez, Syeda Nazhat Subi Naqvi, Aihab Khan
Department of Software Engineering, Foundation University Rawalpindi Campus

Abstract - Over the years road traffic flow has seen pedestrian crossing as a major issue in the society, particularly in urban areas where there is no control for pedestrian road crossing. In mixed traffic conditions pedestrian road crossing behavior is a serious hazard for pedestrians crossing uncontrolled bi-intersection localities. Due to increase in motor vehicle growth there is an increase in the regulation of motor vehicles only and the regulation of pedestrian is completely neglected in urban area. An increase the uncontrolled road crossing behavior of pedestrian is raises different safety and economic concerns. This paper employs computational modeling to regulate the traffic flow across a two way intersection. It is caters how pedestrians can cross a bi-intersection traffic signal without disrupting the traffic flow. Existing computational models that have been presented by other authors are discussed which gives more understanding how to control traffic flow for vehicles and pedestrians handling. This study deals three scenarios of real environment for control of traffic flow for pedestrians; with no turns, with turns and with turns. All scenarios provides proper notation for ‘on states’ and ‘off states’ of signal. Experimental result demonstrates that the proposed method achieved waiting time for vehicles 143.35 seconds and 200.23 seconds for pedestrians respectively. Furthermore, result shows the decrement of time and economical resources that are used in the daily commute.

Index Terms— Pedestrian, Bi-intersection, uncontrolled traffic, Computational Modeling, Traffic Control System

71. PaperID 31051625: New Image Encryption Technique Based on Wavelet / DCT Transforms Using Lorenz Chaotic Map (NIETWDL) (pp. 535-547)

(1) Abdullah M. Awad, (2) Rehab F. Hassan, (1) Ali M. Sagheer
(1) University of Anbar, Ramadi, Iraq
(2) University of Technology, Baghdad, Iraq

Abstract - In communication networks, the data encryption has been used to safe the security of information. There are different encryption techniques that can be used to protect the data from unauthorized third person to access. This paper deals with chaos image encryption environment to hide the secret information and make communication undetectable. In this paper integer wavelet transform (IWT) and discrete cosine transform are used for increasing
hiding pixel distribution. The work uses IWT and DCT as a decorrelation stage for adjacent pixels. The performance evaluation for the proposed algorithm has been done by measuring the application using a series of tests. The tests include histogram analysis and visual test, correlation analysis encryption quality, information entropy, randomness test, sensitivity analysis and differential analysis. The proposed cipher algorithm experimental results show satisfactory security and efficiency levels for image encryption.

Keywords: Chaotic Encryption; AES; RC4; Statistical Analysis

72. PaperID 31051626: Stability Analysis of Reliable Ensemble Classifiers (pp. 548-557)
Zeinab Khatoun Pourtaheri, Seyed Hamid Zahiri, Seyed Mohammad Razavi
Department of Electrical and Computer Engineering, University of Birjand, Birjand, Iran

Abstract - In this paper, Multi-Objective Inclined Planes Optimization (MOIPO) algorithm, as a novel multi-objective technique, is used to design ensemble classifiers with high reliability and high diversity. It is noteworthy that sometimes, the reliability in decision of a classifier is more important than its recognition rate. Security and military applications are obvious instances to show the importance of this measure. In addition to reliability, diversity, as a main issue in ensemble classifiers, is considered as objective function. So, designing heuristic ensemble classifiers with high reliability and also, high diversity has a special importance but the basic point is that the applied heuristic algorithm has a stochastic nature and hence, stability analysis of this system is necessary. In this research, statistical method is used to do stability analysis of designed ensemble classifier.

73. PaperID 31051628: Design an Adaptive Kalman Filter for INS/GPS based Navigation for a Vehicular System (pp. 558-567)
Mohammad Nasiri, Department of Electrical Engineering, Faculty of Engineering, University of Birjand, Iran
Seyed-Hamid Zahiri, Department of Electrical Engineering, Faculty of Engineering, University of Birjand, Iran
Ramezan Havangi, Department of Electrical Engineering, Faculty of Engineering, University of Birjand, Iran

Abstract — Kalman filter is a very effective approach for data fusion. But, the definition of process, measurement noises, and the matrices Q, R have a great impact on the filter performance. Research works show that adjustment of matrices Q, R during the prediction process is very useful to reduce the estimation errors. So, in this paper, we attempt to increase the accuracy of Kalman filter used in INS/GPS integration algorithm by estimating measurement covariance matrix, R, based on measurement data from GPS. Our objective is to show a performance enhancement of a conventional extended Kalman filter used in an INS/GPS integrated navigation system by adjusting adaptively measurement noise covariance matrix R. This adaptive adjustment is necessary. Because, environment conditions in many systems usually are not constant and change continually.

Index Terms— Integrated navigation, Extended Kalman filter, Adaptive Kalman filter

74. PaperID 31051642: Efficient Image Enhancement Using Image Mining and Hadoop MapReduce (pp. 568-575)
M. Anand, V. Mathivanan
AMET University, Kanathur - 603 112 Chennai, India

Abstract - Multimedia has become part of our day today life especially when it comes as images. Many studies have proved that images are the most efficient way of expressing our feelings rather than a page of paragraphs. An example we can state here is the smileys we use in our messages for expressing our thoughts. The ultimate rise of social websites like Google+, Twitter and Facebook, playing major role in the Internet World has proved it wright since these websites are rich in content and huge number of images shared. The revolutionary technology development in the mobile industry is also playing the major role in using such multimedia content. Since the images are being shared in different
ways, people start compressing the images to reduce the huge amount of memory space. This compression leads to data loss (pixel) in images which affects the quality of the images. Many solutions have been identified to solve the issues. One such system uses one dimensional approach in all four directions (Row, Column, Diagonal and Inverse Diagonal); the recovery process is performed by considering the edge pattern of the existing image adjacent to the damaged data (pixel). The system also uses the method of determining the weighted sum \[1\] of selected point functions. Many more techniques followed like enhancement performed using: Spatial and Time domain \[1\], Frequency Domain Techniques \[1\], Brightness Preserving Bi-Histogram Equalization (BBHE) \[2\].

*Keywords: Image Enhancement, Data Loss, Recovery process*

75. PaperID 31051646: An Efficient Image Encryption Technique by Using Cascaded Combined Permutation (pp. 576-588)

*Muslim Mohsin Khudhair*

*Department of Computer Information Systems, College of Computer Science & Information Technology, University of Basrah, Basrah, IRAQ*

*Abstract* - In this paper, a new simple encryption technique is proposed for gray scale image encryption. The current technique, Cascaded Combined Permutation (CCP), is a simple technique based on the primary well known 2-D permutation algorithms. The application at the permutations is performed on three steps: (1) one permutation algorithm is applied on the image; (2) the image that resulting from the first step is decomposed into four quarters. Pixels in each quarter image are then permuted with one of the permutation algorithms. The resulting encrypted quarters are combined as one image; (3) the encrypted image resulting from the second step is further encrypted by performing another permutation algorithm. Experimental results show efficient encryption that is simple in implementation and has high degree of security. It has several key points of strength such as the sequence in which the primary permutation algorithms are applied.

*Keywords: Permutation, Image Encryption, Image Decryption, correlation.*

76. PaperID 31051658: Component Based Face Recognition using Feature Matching through Hu Moment Invariants (pp. 589-604)

*Sushil Kumar Paul, Mohammad Shorif Uddin*

*Department of Computer Science and Engineering, Jahangirnagar University, Dhaka-1342, Bangladesh*

*Saida Bouakaz, LIRIS Lab, University Claude Bernard Lyon1, 69622 Villeurbanne Cedex, France*

*Abstract* — In this paper, a Face Recognition Algorithm using Hu moment invariants (HMs) is described for identifying human faces based on the facial component-features (FCFs). Algorithm is adopted by Viola Jones detector which is applied the concept on the AdaBoost algorithm for detecting the face from a face database having diverse illuminations and expressions with complex background. Then only the face region is cropped and illumination correction is done using histogram equalization technique. Finally, face is converted into binary image by applying cumulative distribution function (CDF) with adaptive thresholding. Three types of statistical pattern matching tools such as Standard deviation of Hu moment invariants (StdDevHMI), absolute difference of probability of white pixels (AbsDiffPWP) and pixel brightness values (PBVs) through L2 norms are determined using five facial components such as two eyes, nose, mouth and whole face for both binary and gray level images, respectively. Lastly, face recognition is carried out by taking these statistical pattern matching tools with logical and conditional operators along with appropriate threshold values. Experimental studies are performed on the BioID database and algorithm shows a better result as compare to the existing popular methods.

*Keywords -- Cumulative distribution function, adaptive thresholding, probability of white pixels, facial component-features, shape matching, Hu moment invariants, pixel brightness values.*
77. PaperID 31051664: A Robust and Efficient Optical Flow Analysis Based Vehicle Detection and Tracking System for Intelligent Transport System (pp. 605-613)

*S Sri Harsha, Department of IT, VR Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India
K. R. Anne, Director Academics, Veltech University, Chennai, Tamilnadu, India

Abstract - In this paper, an enhanced optical flow analysis based moving vehicle detection and tracking system has been developed. A novel multidirectional brightness-intensity constraints (MBIGC) estimation and fusion based optical flow analysis (MDFOA) technique has been proposed that performs simultaneous pixel’s intensity and velocity estimation in a moving frame for detecting and tracking the moving vehicle. The conventional Lucas Kanade and Horn Schunck optical flow analysis algorithms have been enhanced by incorporating a multidirectional BIGC estimation, which has been further enriched with a non-linear adaptive median filter based denoising. Such novelties have significantly enhanced the video segmentation and detection. A vector magnitude threshold based MDOFA algorithm has been developed for motion vector retrieval that eventually enables swift and precise moving vehicle segmentation from the background frame. A heuristic filtering based blog analysis has been applied for vehicle tracking. The MATLAB based simulation reveals that MDFOA-HS outperforms LK in terms of execution time and detection accuracy. In addition, the accurate traffic density estimation affirms robustness of the proposed system to be used in intelligent transport system.

Keywords: Multidirectional brightness-intensity constraint Optical flow analysis, intelligent transport system, Lucas Kanade, Horn Schunck.

78. PaperID 31051681: Area Efficient Digital Logic Circuits based on 5-input Majority Gate Using QCA (pp. 614-623)

D. Ajitha, JNTUA, Ananthapuramu, India
A. Harika, SITAMS, Chittoor, India

Abstract - Quantum-dot Cellular Automata (QCA) is one of the most significant technology among the Nano devices for computing at the Nanoscale. The key logic elements in QCA are majority gate and inverter. The majority gates are 3-input majority gate and 5-input majority gate. In earlier designs all the digital logic circuits are implemented using 3-input majority gate based on 2:1 multiplexer. The limitations of the 3-input majority gate are it requires the number of cells for constructing large architectures involves high complexity, connectivity is difficult, laborious and low reliability. Hence, the design of digital circuits in this paper is implemented with 5-input majority gate based 2:1 multiplexer. The 5-input majority gate reduces cell counts, the number of clocks required and area compared to existing designs. The proposed designs such as XOR gate, XNOR gate, D-latch, D flip-flop, T-latch, and T flip-flop have significant improvements regarding the number of gates, cell count, and delay. The proposed circuits are simulated with QCADesigner and results were included to verify the functionality.

Keywords: Quantum-dot Cellular Automata (QCA), Five-input Majority gate, Multiplexer, Logic gates, Sequential logic.

79. PaperID 31051689: Human Emotion Recognition and Prediction Using Socialism Media (pp. 624-633)

Dr. Tanvir Ahmed, Tanoor Khan
Lahore Leads University, Pakistan, Department of Computer Science

Abstract - Humans are unpredictable; there is no exact way or definition of emotion prediction. Detection of human emotion is difficult because when we want to observe people’s behavior then they behave in normal way or better than abnormal behavior. May be another way where people want to collaborate with others to share their emotions, their daily basis problems, where they feel easy to share their expression without any fear. Maximum people are not agreeing to share their emotion due to shame and fear. We need a platform where people can share their actual problem (which they are internally facing) and release their frustration. Many people want solution without sharing of their
problems to anyone. In order to solve this problem, social media is a best way where people can share their emotional behavior without any fear and we can detect their emotion as silent observer through social media. In this paper we will analyze their posted data on social media and we have provided the suggestion to solve their problems; also we detected the emotion of people through social media. We collected data from social website (Twitter .etc.) where people have shared their thoughts or feelings. Meanwhile, we designed an algorithm which takes data from that social website and on the basis of that data; application provides the result as previous emotional state of a person. A systematic approach was used to detect the emotion of people through social media data. This is a better way where a person wants to collaborate with other to share his emotions, his daily basis problems and he feels easy to share his expression without getting panic. This Emotional based approach described things in a new way, where all predictions can be measured according to the subject environment and application can provide better results in decision making. This approach has used the data from social portals like Twitter etc. where peoples are posting their data in form of emotions. Prediction and recognition of emotions is a better way to analyze the emotion of people as silent observers.

**Keywords — Emotion, Silent Observer, Parts of Speech (POS), Social Media(SM), Adjective**

80. PaperID 31051690: Using Adaptive Filters for Object Tracking and Improving the Method Using Metaheuristic (pp. 634-640)

_Farzad Khadem Mohtaram, Majid Mohammadi_

_Deptartment of Computer, Buin-Zahra Branch, Islamic Azad University, Buin-Zahra, Iran_

**Abstract** - The video detection based on the image sequence of the area of interest has attracted considerable attention. Particles filtration is one of the most development algorithms particularly in restoration of probability density function of goal state. Accordingly, the main objective of present study is utilization of adaptive algorithm for detection of inflexible objects. The simulation method was applied and data analysis is done by MATLAB software. The results represent that, filtration of the suggested particle achieved better performance than filtration of the standard particle in terms of prediction error of status, detection of video error, and the number of significant particles. It revealed that, the particle filtering enhanced the number of significant particles by IGA and, forced the collection of particles to better expression of actual status. This could enhance the accuracy of status prediction and reduced the error.

**Keywords: adaptive algorithm, inflexible, objects detection, particle filtration**

81. PaperID 31051695: Agile Practicing and Outsourcing (pp. 641-648)

_Muhammad Sarfraz (1), Maria Ramzan (2), Akhter Rasheed (3), Fateh Ali (1) _

(1) Department of Mathematics and Statistics, Riphah International University Islamabad, Pakistan  
(2) Govt. Post Graduate College for Women Satellite Town Rawalpindi, Pakistan  
(3) Department of Mathematics, COMSATS Institute of Information Technology Abbottabad, Pakistan

**Abstract** - The software industry can be widely seen as a key driver for business improvement. Outsourcing of software development tasks has become a major issue for large software enterprises. Software outsourcing has been progressively increasing. However significant outsourcing failure rates have also been reported. Therefore, outsourcing occurred by the wrong decision can cause major technological and economic setbacks. The objective of this research is to develop a model for outsourcing in order to improve outsourcing process and to help out the organizations to overcome barriers (communication, coordination & quality) that may have a negative impact on software outsourcing as well as to improve their success rate. Literature is consulted to highlight various issues of outsourcing. A case study is conducted to validate the effectiveness of our proposed model. The purposed model contains different practices of agile which provide an effective way to improve coordination, quality assurance and reduces communication gaps in outsourcing.

**Index Terms- Agile, Outsourcing.**
82. PaperID 310516101: Model Driven Architecture for Secure Software Development Life Cycle (pp. 649-661)

Muhammad Asad, Shafique Ahmed
National University of Sciences and Technology, Islamabad

Abstract — Secure Software Development is an important issue for the software industry for couple of years as security issues in the software development life cycle are not easy to handle. Success of a software deeply depends on the fact that it is not easily vulnerable to security threats and breaches. Many organizations have made security guidelines to cope with these challenges to bring them in an organized and secure way. Besides so much advancements in the field, securing the software from vulnerabilities is not achieved in all modules of software development life cycle. The guidelines and methods designed for the secure software development have put a lot contributions but they are so verbose that these measures are nearly not implementable. In this paper a model is proposed for secure software development life cycle in model driven architecture level (MDA-SDLC). In the proposed model, modeling methods and approaches are used to ensure the advances in secure model driven architecture with simplified integrity of security modules in security critical software’s development lifecycles.

Keywords — Model Driven Architecture, Security, SDLC, UML,

83. PaperID 310516108: Social Relation Based Recommendation System For Information Overloaded Social Networks (pp. 662-671)

S. Uma Shankari, Bharathiyar University, Coimbatore
Dr. M. Chidambaram, Rajah Serfojii College, Thanjavur

Abstract - Social persuade plays vital part in the product marketing. Though, it’s seldom been regarded in traditional Recommender systems (RS). This paper provides new paradigm RS which can exploit data in the social networks, with general approval of items, user preferences, and persuade from the social friends. The probabilistic representation is improved to build personalized recommendations like data. In world e-marketing, new commerce representations are normally introduced, new tendency started to materialize. Latest trend is the social networking websites, several of which concerned not only huge number of visitors and users, however online advertise company to put their ads on sites. This paper discovers online social networking like new e-marketing trend. We first inspect online social network like new web-based services, also evaluate social networks by other delegate web-based service. We extort information from real online social network, also our investigation of this huge dataset expose that friends contain tendency to choose similar items and provide similar ratings. The experimental outcome on the dataset illustrates that proposed scheme not only progress prediction accuracy RS but gives solution cold-start and data sparsity problems intrinsic in the collaborative filtering. Moreover, we recommend improving system performance by concern social networks semantic filtering, and authenticate its improvement through class project research. In this research we reveal how related friends may be choose for deduction based on the semantics friend relations and finer-grained customer ratings. Such technologies may be organized by mainly content providers.

Keywords: Recommender systems, collaborative filtering, social network

84. PaperID 310516109: Software Reengineering - A Frame of Reference (pp. 672-678)

A. Cathreen Graciamary, Bharathiyar University, Coimbatore
Dr. Chidambaram, Rajah Serfojii College, Thanjavur

Abstract — Now day development of software is describe by immediate process. Old systems have to take on the recent technologies; It can be achieved by changing or finding the features, i.e, Reengineering. Our proposed paper clarifies about the reengineering process of software. It also explains the efficient and better process in reengineering. There are two type common reengineering objectives. Improved feature: the existing software system will be of minimum quality, because of more changing during the time course. The main objective of reengineering is to increase
software quality and to provide present working documentation. A higher quality degree is needed to enhance reliability, to minimize the maintenance cost, to develop maintainability, and to make for functional improvement.

**Keyword**: Software Reengineering, Reverse Engineering, Enhanced Reengineering, SVM classification, Software component.

85. PaperID 310516137: Analyzing Virtualization based Energy Efficiency Techniques in Cloud Data Centers (pp. 679-686)

**Beenish Gul, Fiaz Gul Khan, Iftikhar Ahmed**
Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, Pakistan

**Abstract** - Cloud computing provides IT services to users worldwide. Data centers in Clouds consume large amount of Energy leading to highly effective costs. Therefore green energy computing is solution for decreasing operational costs. This survey presents efficient resource allocation and Scheduling algorithm/Techniques analyzed on different network parameters without compromising network performance and SLA constraints. Results are analyzed on different measures, providing a significant cost saving and improvement in Energy Efficiency.

**Keywords**: Data Centers, Virtualization, Consolidation, Virtual Machines, SLA

86. PaperID 310516145: Image Share Pane Tool: Image Sending Approach to Mobile via Bluetooth Device (pp. 687-690)

**Farhan Ali Surahio, Awais Khan Jumani, Javed Ahmed Mahar, Hidayatullah Shaikh**
Department of Computer Science, Shah Abdul Latif University, Khairpur Mirs, Sindh, Pakistan

**Abstract** — Nowadays, Microsoft Word is commonly used in various areas including industries and academia. Microsoft word has introduced great user friendly features, for instance, Screenshot and Screen Clipping, Smart lookup, Tell Me and others. Among them, Layout option button has given us to set objects with line in text. Furthermore, Different types of panes have provided for various tasks. Microsoft Word has given us a facility to greet with thumbnail image of every window you have opened at the moment. Many users while working on document need to insert or capturing images with Screenshot and Screen Clipping, they want to share inserted images to mobile via Bluetooth. But, Users are disappointed because there is no any tool provided to accomplish that task and user takes a long procedure to apply for sharing images to mobile through the Bluetooth. This paper provides an application which helps users to send an inserted image via Bluetooth while working on Microsoft word and they do not to switch any window. By adding it into existing Microsoft Word it will helpful for people living across the world.

**Keywords**- Screen Clipping; Layout Option; Share Option Button; Share Image Pane; Image capture format type

87. PaperID 310516154: An Optimal Approach for Securing the Data in Cloud Storage using Block Division and Predicate Encryption (pp. 691-696)

**P. Vijaya Bharati**, Department of Computer Science & Engineering, Vignan’s Institute of Engineering for Women Kapujaggarajupet, Visakhapatnam

**Prof. (Dr.) T. Sita Mahalakshmi**, Department of Computer Science & Engineering, Gitam college of Technology Gitam University, Visakhapatnam

**Abstract** — The “pay-as-you-go” cloud computing model is an efficient alternative to store the data at a cheaper cost. Ensuring data security in cloud computing platforms is critical and has become one of the most significant concerns in the emerging field of cloud computing. The location of the servers where the data is stored and being accessed are not known to the end user. There are many numbers of different security models and algorithms which are applied to secure the data stored in the cloud. While these techniques are very nice, we cannot really always tell that they are
“unhackable”. Given enough time, brains and tools any technique might be breakable because the techniques are not fine grained. The existing algorithms have their own flaws and so in this paper we proposed a method that is been improved in such a way that the data stored on the cloud is secured. The proposed method initially uses a lossless block division which divides the data into blocks and then division is applied storing the remainder and the group to which it belongs to separately and later we apply predicate encryption scheme on the data to be stored (remainder data) in which the keys correspond to predicates and cipher texts are associated with attributes. The public key PK with an attribute ‘x’ is used to encrypt the text and the secret key SKf corresponding to predicate f can be used to decrypt a cipher text with attribute ‘x’ if and only if f(x)=1.

Keywords: Block Division, Predicate Encryption, Predicates, Attributes, Secret Key

88. PaperID 310516164: A Collaboration between Two Readers for Clustering and Identification in RFID systems (pp. 697-706)

OUAKASSE Fathia, Applied Mathematics and Computer Science Laboratory (LAMAI) Cadi Ayyad University Marrekesh, Morocco.
RAKRAK Said, Applied Mathematics and Computer Science Laboratory (LAMAI) Cadi Ayyad University Marrekesh, Morocco.

Abstract - Radio Frequency Identification RFID is one of the most important technologies used in the internet of things. It is increasingly used in various applications because of their high quality as well as their low costs; however the avoidance of collision of tags during the identification process represents a great challenge, especially when the number of tags is too large. In this paper we propose a new mechanism, based on Progressive Scanning Algorithm, to group tags in the interrogation zone of a reader. The proposed mechanism consists in the deployment of two readers having the same interrogation zone. Simulated results show that the proposed mechanism can appropriately achieve higher performance compared to other existing algorithms in terms of the number of time slots allowing identifying tags and effectively in terms of total time required to do this.

89. PaperID 310516177: Web Page Classification based on Context’s Semantic Correlation (pp. 707-713)

Mehrdad Ranjbar-Khadivi (1), Mohammad-Reza Feizi-Derakhshi (2)
(1) Department of Computer, East Azerbaijan Science and Research Branch, Islamic Azad University, Tabriz, Iran
(2) Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran.

Abstract - Automatic web pages' classification is one way to deal with the increasing range of the World Wide Web. Considering that most of the content of web pages is text, so classification based on text is seems to be an efficient solution. The methods used for text classification are usually based on the key words. But if illusive keywords appear within the web page, then the class of the webpage will not be properly diagnosed. Therefore, rather than paying attention to the words, it is needed to be given to content and words meaning. In this paper, a method based on content semantic correlation has been proposed. A text consists of paragraphs, sentences and words. In this study at first text is divided into its components and stop words is removed. Then, in order to forms the basis of the words, it will be needed to find the root of the words. The Hypernyms Tree of words can be extracted by using FARSNET. By using this method not only is the meaning of the terms considered but also there is no need to clarify the words. After extracting the Hypernyms Tree for all keywords, text feature vector is created. Then the similarity of the text to each of the available categories measured. Finally, KNN classification algorithm is used to recognize the right class of the webpage. The results show that by using this method, classification accuracy is increased by 0.17 in compared with other methods.

90. PaperID 310516178: Relevance Feedback in XML Retrieval Based on Classification of Elements (pp. 714-734)
Abstract - Unlike classical information retrieval systems, the systems that treat structured documents include the structural dimension through the document and query comparison. Thus, the relevant results are all elements that match the user needs rather than the entire document. In such a case, the document and query structure should be taken into account in the retrieval process as well as during the reformulation. Query reformulation should also include the structural dimension. In this paper, we propose an approach of query reformulation based on structural relevance feedback. We start from the original query and the fragments judged as relevant by the user. The analysis of the structure of document fragments and textual content of elements enables identify elements that match the user query and rebuild it during the relevance feedback step. The main goal of this paper is to show the impact query reformulation based on an analysis of the structure and content of each relevant element retrieved by an initial search process. Some experiments have been undertaken into a dataset provided by INEX to show the effectiveness of our proposals.

Keywords: Information retrieval; XML document; relevance feedback; Line of descent matrix; Classification.
previous approaches carried out to improve the quantity and quality of ideas, significance of creative thinking, target to increase productivity, requirement of group brainstorming and effectiveness of E-Brainstorming.

*Keywords: Brainstorming, Decision Support System, Creativity, Management Information System.*

93. PaperID 310516191: A Neural Network Model for Predicting Insulin Dosage for Diabetic Patients (pp. 770-777)

*Bilal M. Zahran, Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqaa Applied University, Jordan*

*Abstract -* Diabetes Mellitus is a chronic metabolic disorder. Normally, with a proper adjusting of blood glucose levels (BGLs), diabetic patients could live a normal life without the risk of having serious complications that normally developed in the long run. However, blood glucose levels of most diabetic patients are not well controlled for many reasons. Although the traditional prevention techniques such as eating healthy food and conducting physical exercise are important for the diabetic patients to control their BGLs, however taking the proper amount of insulin dosage has the crucial rule in the treatment process. In this paper we have proposed a model based on artificial neural network (ANN) to predict the proper amount of insulin needed for the diabetic patient. The proposed model was trained and tested using several patients' data containing many factors such as weight, fast blood sugar and gender. The proposed model showed good results in predicting the appropriate amount of insulin dosage.

*Keywords: Diabetes, Artificial Neural Network (ANN), Blood Glucose Levels (BGLs)*


*Mohammad Salman Hafeez & Farhan Rasheed
Department of Software Engineering, Foundation University Islamabad, Pakistan*

*Abstract -* Process Management is one of the primary tasks achieved by the Operating Systems. The system’s performance sententiousely depends upon CPU scheduling algorithms. Round Robin, contemplated as the most extensively endorsed CPU scheduling algorithm, is an optimal solution for the timeshared systems. In timeshared systems, selection of the time quantum plays a pivotal role in performance of CPU. In Round Robin, the static nature of the time quantum emerges some problems directly related to the quantum size which decreases the performance of CPU. In this paper, selection of time quantum is reviewed and a new algorithm for CPU scheduling, Optimum Dynamic Time Slicing Using Round Robin (ODTSRR) is proposed for timeshared systems. The proposed algorithm is based upon dynamic time quantum. Round Robin algorithm is redressed in this paper, ODTSSRR also contains the advantages of RR (Round Robin) CPU scheduling algorithm have less chances of starvation. Performance of proposed algorithm is compared with RR and other shades of RR and the results revealed that the proposed algorithm is better in response time & waiting time, context switch rates, turnaround time and throughput hence resulting in optimized CPU performance.

*Keywords: Operating System, Scheduling, Round Robin CPU scheduling algorithm, Time Quantum, Context switching, Response time, Turnaround time, Waiting time, fairness.*

95. PaperID 310516194: Profile Screening and Recommending using Natural Language Processing (NLP) and Leverage Hadoop Framework for Bigdata (pp. 799-811)

*Mrs. D.N.V.S.L.S. Indira, Dr. R. Kiran Kumar
Dept. of Computer Science, Krishna University, Machilipatnam,*
Abstract - Recommendation has been a major area that any recruiter would look for on a given job description. Increase in digital communication has made things easy to upload resumes and make it available for recruiters; on the other hand increase in technologies would make any recruiter difficult to scan it manually. Here we introduce an application which processes text data, understands sentence behavior unlike conventional keyword search applications and gives out required resume as per job description provided to application. This application makes use of Natural Language Processing (NLP) which helps in data training and feature extraction of the text data. Using NLP methods, semi structured text data is converted to structured format with required extracted features. To make this application scalable to any size of data we propose this implementation on Hadoop framework, which can handle any number of resumes or even more than petabytes of data, termed as bigdata.

Keywords: BigData, Attribute Tagger, NLP Methods, Named Entity Recognition (NER), Map-Reduce, Hadoop, HBase, Hive

96. PaperID 310516199: Real Time Variable Voltage Scaling to Design Energy Efficient Systems (pp. 812-820)

Ankita Soni & Praveen Kaushik
Department of Computer science and Engineering, Maulana Azad National Institute of Technology, Bhopal, India

Abstract - With the immense increase in the processing power over the past few decades, battery life has proved to be a crucial resource. Since energy varies quadratically with voltage in the CMOS based processors, Dynamic Voltage Scaling (DVS) offers a solution to conserve the battery power by lowering the supply voltage. However, reducing the voltage increases the execution time and therefore, real time scheduling has to be combined with DVS so as to provide the deadline guarantee. This paper presents an algorithm, Recurring Variable Voltage Scheduling(RVVS) to extend the battery life using a combination of variable voltage and a real time scheduling algorithm (Earliest Deadline First). The paper also mathematically proves that if two voltage levels are used such that one is twice the other, up to 50% energy can be saved. Mathematical proof of delay increment due to voltage reduction has also been presented. RVVS has been optimized in order to reduce the overall energy dissipated by switching by introducing a factor ‘n’ that denotes the number of time units after which the voltage switch can occur. RVVS has been applied to task sets having different number of tasks providing an average energy saving of 27%. This significant amount of energy saving helps extending the battery life to a remarkable extent and proves the worth of RVVS in the field of real time DVS.

Keywords: Dynamic Voltage Scaling; Earliest Deadline First; Real time scheduling; Voltage switching; Energy efficiency; Variable voltage

97. PaperID 310516202: Design and Detection of Network Covert Channel - An Overview (pp. 821-828)

R. Rajamenakshi, Department of Computer Science, Avinashilingam Deemed University, Coimbatore, India
Dr. G. Padmavathi, Department of Computer Science, Avinashilingam Deemed University, Coimbatore, India

Abstract - Sensitive information leakage is increasing due to widespread use of internet and technology. The attackers find new ways to exfiltrate data that pose threat to data security and privacy. Here our focus is on the covert information leakage over the network that exploits the various network protocols and their behavior. Information leak over covert channels exploit a variety of protocols of network protocols including Wireless, mobile and virtualized cloud platforms etc. Current network security solutions like IDS, IPS, firewalls etc. are not designed to handle these type of attacks. These type of attacks are dynamic in nature and mimics the legitimate traffic behavior, there by posing a challenge to detect and prevent. This article presents comprehensive review of the network covert channel, design, detection and mitigation. We have reviewed the classification of covert channels based on the attacks.

98. PaperID 31051678: Generalized Intuitionistic Fuzzy Interior Ideals of Semigroups (pp. 829-836)

Muhammad Sajjad Ali Khan, Muhammad Shakeel, Khaista Rahmat
Department of Mathematics, Hazara University, Mansehra, Pakistan
Saleem Abdullah, Department of Mathematics, Abdul Wali Khan University, Mardan, KPK, Pakistan

Abstract — In this paper we introduce and study a new sort of intuitionistic fuzzy interior -hyperideals of a semi-hypergroup, called (, )-intuitionistic fuzzy interior -hyperideals by using the combined notions of belongingness and quasicoincidence of intuitionistic fuzzy points and intuitionistic fuzzy sets and some interesting properties are investigated. We show that an IFS $A = \langle A, A \rangle$ is an ($\in, \in \vee q$)-intuitionistic fuzzy interior -hyperideal of $H$ if and only if $U(t, s) = \{x \in H: x(t, s) \in A\}$ for all $t \in (0, 0.5]$ and $s \in [0.5, 1)$ is interior $\Gamma$-hyperideal of $H$. Moreover, we show that an IFS $A = \langle A, A \rangle$ is an ($\in, \in \vee q$)-intuitionistic fuzzy interior -hyperideal of $H$ if and only if $[A](t, s) = \{x \in H: x(t, s) \in \vee qA\}$ for all $t \in (0, 1]$ and $s \in [0, 1)$ is an interior $\Gamma$-hyperideal of $H$. These showed that ($\in, \in \vee q$)-intuitionistic fuzzy interior -hyperideals of $H$ are generalization of existence of intuitionistic fuzzy interior $\Gamma$-hyperideal of $H$.

Keywords: Semigroup, Intuitionistic fuzzy point; Intuitionistic fuzzy sets; (, )-Intuitionistic fuzzy interior ideal.

99. PaperID 310516138: Pythagorean Fuzzy Hybrid Geometric Aggregation Operator and Their Applications to Multiple Attribute Decision Making (pp. 837-854)

Khaista Rahman, Muhammad Sajjad Ali Khan, Muhammad Shakeel
Department of Mathematics, Hazara University, Mansehra, KPK, Pakistan
Saleem Abdullah, Department of Mathematics, Abdul Wali Khan University, Mardan, KPK, Pakistan

Abstract: There are many aggregation operators and its applications have been developed up to date, but in this paper, we develop the Pythagorean fuzzy hybrid geometric (PFHG) operator, and also study some properties, such as monotonicity, idempotency, and boundedness of the proposed operator. Pythagorean fuzzy hybrid geometric operator is the generalization of the Pythagorean fuzzy weighted geometric (PFWG) operator and the Pythagorean fuzzy ordered weighted geometric (PFOWG) operator. Finally, we apply the Pythagorean fuzzy hybrid geometric (PFHG) operator to deal with multiple attribute decision making (MADM) problems under Pythagorean fuzzy information. Using Pythagorean fuzzy hybrid geometric aggregation operator, we also develop an algorithm for multiple attribute decision making (MADM) problems. Lastly we construct an example for multiple attribute decision making MADM problems.

Key words: Pythagorean fuzzy sets, Pythagorean fuzzy hybrid geometric PFHG operator. Decision making problems.

100. PaperID 310516143: Cultural Factors Affecting ICT Acceptance Case Study: Industries Located in Science and Technology Park, Tehran (pp. 855-865)

Mina Babazadeh Farokhran (*1), Behrouz Eskandarpour (2), Hossein Eskandarpour (3), Rogaye Rezaee Giglo (1), (1) Young Researchers and Elite Club, Germi Branch, Islamic Azad University, Germi, Iran (2) Department Of Management Payamenoor University (Pnu) Iran, (3) Zanjan Islamic Azad University, Zanjan, Iran

Abstract - Application of new technologies is considered as a key factor for the development of companies in recent years. This puts emphasis on the importance of reviewing factors influencing the acceptance of information technology culture. This study has been done aiming to identify factors influencing the information technology acceptance in companies located in the Tehran science and technology park. 80 companies from industries located in science and technology parks in Tehran were selected of these, 72 questionnaires have been evaluated and Cronbach's alpha was used to measure the reliability and validity of measurement tools. The reliability coefficient of the questionnaire is 0.86, which indicates high reliability of the applied questionnaire and content validity was confirmed by instructors. The research data is analyzed by SPSS which uses the correlation analysis along with significance levels and in the following, t and f tests have been used to study the research additional hypotheses. The results of this study showed that the usefulness and ease of use and subjective norms affect the information technology acceptance through
behavior intent and using independent t test, it was found that looking at research indicators is alike among men and women. Based on the f statistics, attitude to these indices among different education levels is different and the respondents' education has an impact on attitudes to these indicators.

Keywords: cultural factors, Information Technology, technology acceptance, TAM, UTA
A New Efficient Two-Tier Secure Protocol

Rehan Ullah  
IT Department Hazara University  
Mansehra, Pakistan

Noor ul Amin  
IT Department Hazara University  
Mansehra, Pakistan

Faisal Bahadur  
IT Department Hazara University

Mansehra, Pakistan

Abdul Hakeem  
IT Department Hazara University  
Mansehra, Pakistan

Insaf Ullah  
IT Department Hazara University  
Mansehra, Pakistan

Abstract—Signcryption is a cryptographic method in which signature and encryption apply on message in a single step. On other hand image steganography is a strongest technique for hiding data or information. Therefore Communication through insecure channel is challengeable task for an organization. Recently two tier security gain popularity because most of the business organizations wants maximum security of data/information. In this paper we design a new scheme using cryptographic and stenographic techniques at once on the basis of image steganography and elliptic curve cryptography. In proposed design scheme we use both of the steganography as well as cryptography. The cryptographic technique encrypts the data by using Elliptic curve cryptography in such a manner that third party not understands the original message contents. Stenographic technique is used to hide the text in image and then we take hash as well as signature. It also assures the security properties like message confidentiality, message integrity, message non repudiation and also message authentication.

Keywords-component Cryptography, Steganography, Signcryption, Elliptic curve cryptography. (Key words)

I. INTRODUCTION

Communicating data through noisy channel needs Secrecy. Most of the organization needs maximum security to protect their data from third party. Thus we collectively used steganographic as well as cryptographic techniques for better security. Cryptography is a technique in which plain text (message) is converting into cipher text using key and encryption algorithm. While steganography used for hiding of data. Steganography is derived from two Greek word “Stegano” mean hide and “graphics” means writing [1]. So it is the art of science in which we study how to hide secure data. The major aims of steganography is that the text of secret message is hidden or conceal while in that of cryptography the text of secret message is readable but not understandable to third party. Sometime needs the extra security properties like authentication and integrity. Thus integrity ensures by one way hash function and authentication provided by digital signature algorithm. Public key cryptography was introduced by deffi and helmen [2]. This technique uses two keys(public and private) at both side (sender and receiver). It was build for those communicating parties in which they cannot meet before to start communication. Thus signature generation and
encryption is so costly. Zheng give solution to this problem by contributing signcrypion [3]. It combines both the functionality of digital signature and encryption in the single step. But this is not enough for maximum security. We proposed two tier schemes on the bases of signcrypion using elliptic curve and image steganography for hiding the cipher text. It also assures the security properties like message Confidentiality, message integrity, message non repudiation and also message authentication.

II. PRELIMINARIES

Some basic preliminary are define bellow.

- **Elliptic curve**
  Firstly ECC can be divided into curves one is prime curve (TP) and another is binary curve (ZF (2m)). Prime curve (TP) is to use in software applications, because it not required extended bitfidding operation, which (ZF (2m)) require. But hardware application are required a few logic gates to build a dominant crypto-system used a binary curves (ZF (2m)).
  Secondly, ECC variable and coefficients are limited in a finite field of elliptic curve, this limitation would to increase the efficiency of ECC computational operations.
  In finite field $T_p \mod p$ an elliptic curve is represent as $Ep(a,b): y^2 = x^3 + ax \mod p$ , where $(a,b) \in Tp$ and $4a3 + 27b2 \mod p \neq 0$. The condition $4a3 + 27b2 \mod p$ is essential to certify that $y^2 = x^3 + ax + b \mod p$ has no repeated factors in finite Abelian group in the set of $Ep(a,b)$.
  The point 0 is a zero point of an elliptic curve. This point at infinity is third point of intersection of any straight line with the curve. Points $(x,y), (x, -y)$ and 0 is on any straight line with the curve. Now addition rules, which is denoted by “+” are given below:
  1) $0 + p = p$ and $p + 0 = p$ , where 0 is additive identity.
  2) $-0 = 0$
  3) $+(-p) = (-p) + p = 0$ , where $-p$ is negative points of $p$.
  4) $(p + Q) + R = p + (Q + R)$
  5) $p + Q = Q + p$
  
  For any two points $p = xp, yp$ and $Q= xq,yq$ over $Ep(a,b)$ the elliptic curve addition operation, which is denoted as $P + Q = R = (xr, yr)$, satisfies following equations.
  $$Xr = (\kappa x - xp - xq) \mod P; Yr = (\kappa (xp, xr) - yp) \mod P$$
  Where
  $$\kappa = (yq - yp/xq - xp)$\mod p$, if $P \neq Q$$

Where $\kappa = (3x2p + a/2yp) \mod q$, if $P = Q$

- **Plaintext.** Message before encryption is known as Plaintext. It is the original message that sender want to send the receiver. Plaintext is understandable as well as readable.
- **Cipher text.** Message obtained after encryption is known as Cipher text. The cipher text is readable but not understandable.
- **Cryptology.** The study of both cryptography and cryptanalysis is known as Cryptology. In cryptology both the encryption and decryption phases occurred.
- **Cryptanalysis.** The breakdown of Cipher text to plaintext without knowing key is known as Cryptanalysis. In Cryptanalysis the not understandable text is transform to understandable text (from cipher text to Plaintext).
- **Cryptosystems.** Message encrypted by Computer system for the purpose of secure data transmission and storage known as Cryptosystem.
- **Key.** It is variable values that are used in both in encryption as well as decryption stage.
- **Cover object.** Original object in which we embed secret data or message is known as cover object.
- **Stego object.** After embedding data in cover object stego object is formed.
• **Steganalysis.** The breakdown of stego object into cover object is known as Steganalysis.

• **Hash functions.** It is a function which is used for digest of a message. Hash is a one way function.

### III. RELATED WORKS

For confidentiality and integrity of data two types of techniques are used for data hiding which are steganography and cryptography [4]. In steganography information are being transmitted through a channel through which other kind of information’s already transmitted [5]. The aim of steganography is to hide information inside other “undamaging” digital media in such a way that third party not detects the existence of secret information [6]. The major aim of steganography is to communicate two different parties in such a way that the third party is unaware from transmission of hidden data [7].

In cryptography the text of secret message is visible to third party. The text is readable but not understandable to third party [6]. In cryptography, the format of data is in such a way that the text is worthless and unintelligible way [8]. The cryptography prevents the hacker from reading the message which has been sends by or to sender [9].

For better security we have to combine both of Steganography and Cryptography. The Cryptography encrypts the message while the Steganography hide the secret message which provides more security to secret information [4, 10]. Without viewing the stego object is being transmitted from sender to receiver and vice versa. Whenever, if an attacker detects the message from the stego object, so first he had to decode the message from digital media. Then he had to require the cryptographic algorithm to decipher the encrypted message [11].

The author suggests the designing of strong and secured image steganography based on least significant bit (LSB) insertion technique [12].

In [13] the authors suggest a technique that provides better security by using two tier techniques (cryptographic and steganography) at the same time.

### IV. PROPOSED SCHEME

This section includes details discussion about the proposed two tier scheme. It includes three phases namely called key generation phase, Signcrypion and un-Signcrypion.

#### Key generation phase

In this phase the sender and receiver select their private keys and also generates there public keys.

- **Sender Pick** $S_a$ from $\{1, 2, 3, ..., t - 1\}$ as a private key & Calculate their public key $S_b = S_aS_a \cdot G$.
- **Receiver Pick** $P_b$ from $\{1, 2, 3, ..., t - 1\}$ as a private key & Calculate their public key $d_v = P_v \cdot G$.

#### Signcrypion Phase

In This section the sender first generate the signcryptext of a message $M$ after that then generate the stego image of the signcryptext. Now stego image send to the receiver.

#### Algorithm

1. Generate a random no. $x \in \{1,2,3, .... , t − 1\}$
2. Calculate $K = x \cdot P_v \ mod \ t$.
3. split $K = K1, K2$
4. $C = K1(m)$
5. $d = hide(C)$
6. $r = h(d)$
7. $R = r \cdot G$
8. $S = x/r + S_a$

Send to receiver $(S, r, R, d)$
The block diagram of a Signcryption phase is followed below.

**Block Diagram**

The block diagram of a Signcryption phase is followed below.

**Explanations**

The Signcryption phase consists of following steps. First the secret message is encrypted through Elliptic curve cryptography into cipher text. Than we hide the cipher text through a cover image through steganographic technique. Than we take signature and hash of stego file mean combine hash of cipher text as well as cover image. We get a stego image (d), signature (S) and hash (h) value. Than the sender send stego image (d), hash (h) and signature (S) to receiver side.

**Un-Signcryption Phase**

The un-Signcryption phase consists of following steps which is explained in following algorithm.

**Algorithm**

1. $K1, K2 = S \cdot d_o (S_b + R)$

2. Recover $d$

3. Decrypt $M = DK1(C)$

4. Check $r, G = R$ than Accept otherwise reject.

**Explanations**

The receiver receives the stego image (d), Hash value (h) and signature (S). Than we apply steganographic technique we get the RGB pixel value of stego image and hence we get a cover image and cipher text. Than we takes the elliptic curve cryptographic decryption and hence we get plaintext.

The receiver receives the stego image (d), Hash value (h) and signature (S). Then the receiver gets the LSB of stego image and has to decrypt it through elliptic curve cryptography. By decryption we get cipher text. Than we apply steganographic method to get cover image and plain text. At last we take Hash function of plaintext and cover image we get Hash value new. If the Hash values old are equal to Hash value new than it shows integrity. If the Hash value old and Hash value new became different than it not provide integrity.
V. SECURITY ANALYSIS

The security of our proposed design scheme is based on ECDLP. In security analysis we focus on main security features like integrity, Confidentiality, authentication and non-repudiation.

Confidentiality

The proposed scheme provides the Confidentiality property. If the attacker wants to decrypt the message for that the attacker needs to get x as well as K1 which is the public key of receiver. Finding two unknown parameter from one equation is difficult as well as impossible for attacker. This problem is known as discreet logarithm problem due to which the attacker cannot reveals the original contents of message due to which our scheme provide confidentiality property.

Integrity

Our scheme provides the property of integrity. As in proposed scheme we use hash function which has one way property. Hash provides the irreversibility property due to which our scheme is more secure than existing schemes. The hash function used in our scheme provides the property of integrity.

Authentication

Our proposed scheme provides the property of authentication. When the attacker generate a forge sign, for this it required the random generate number x and private key of sender s, from the mentioned equation. Now calculating two unknown variables from same equation is hard for attacker.

Non repudiation

Our scheme provides the property of non-repudiation. If the sender deny from message which has been send by sender. The third party proves that the message is being sent by sender or not from private key of sender. This property is known as non-repudiation.

VI. CONCLUSIONS

A new and advance two tier secure steganography provide better security to our data. Cryptography and steganography are the techniques used for security of data. Cryptography is technique of secret writing while the steganography hide the secret messages. In this paper we are going to discuss the two tire concept in which both the cryptographic and stenographic techniques are used for security of data. The proposed two tier scheme is more efficient on the basis of security. Our scheme is more secure as compare to the other existing schemes which are discussed in the above literature. The proposed scheme provides the properties of Confidentiality, integrity, non-repudiation and authentication.

REFERENCES


Formal Model of Smart Traffic Monitoring and Guidance System

Umber Noureen Abbas, Farhan Ullah, Nazir Ahmad Zafar

Department of Computer Science, COMSATS Institute of Information Technology Sahiwal
COMSATS Road off GT road, Sahiwal 57000, Pakistan

Abstract—Emergency Services Rescue 1122 and Smart Sticker components of our proposed Smart traffic monitoring and guidance system model are presented in this paper to provide smart emergency services and to identify vehicles to develop advanced transportation system. It involves the Wireless Sensors and actors to communicate with the system. The proposed components require fewer resources in terms of sensors and actors. Further, Sensors component identifies vehicles through Smart Stickers and it is readable through sensors from its barcode and barcode consists of vehicles details in terms of vehicles registration, model, engine and color. Secondly, Emergency Services Rescue 1122 component provides emergency services as it locates the vehicles through sensors and informs the local authority for providing emergency services. Third, violation of rules detects intruders on roads to provide smooth flow of traffic. Fourth, to avoid congestion, traffic signals are configured and communicated with sensors to update the system if congestion occurs. The proposed components of our model are implemented by developing formal specification using VDM-SL. VDM-SL is a formal specification language used for analysis of complex systems. The developed specification is validated, verified and analyzed using VDM-SL Toolbox.

I. INTRODUCTION

Advanced transportation system has the ability to handle complex situations in developed countries. A good transportation system is very important for the development of a country. It does ensure reliability and safety operations on roads. The main objectives of traffic management system are the ability to reduce congestion problems and overcome various diseases caused by traffic pollution. With the growth of population, traffic management is a big problem in Pakistan. Irregular traffic is a big problem in populated cities of Pakistan like Karachi, Lahore, Rawalpindi, Islamabad, Hyderabad, and Peshawar. Intelligent traffic management system is useful to overcome traffic problems and it can contribute a lot to the development of a smart city. Thousands of vehicles are passing through a city and due to poor traffic management system; it causes traffic congestion.

Traffic congestion can cause, accidents, waste of time, reduces trade opportunity, increases energy consumption and negatively affect the education system. It has a big impact on society and thus create problems for everyone [1]. These issues will be solved if we develop smart traffic management system in which sensors are used to gather real-time data about traffic at specific points and then it will communicate with other sensors to replicate information to users. In this system, traffic lights and LED screens will be used as sensors to guide the users about the traffic situations. Smart sensors in traffic signals sense traffic situations to develop an intelligent transportation system [2, 3]. Smart Traffic Monitoring and Guidance System (STMGS) have a basic purpose of maintaining a balance among different types of vehicles. It provides security, road safety, less energy consumption, smooth traffic flow, and better guidance to users. In smart traffic management system sensors will gather real-time data from traffic flow and after analysis, this information will be uploaded on the cloud. Traffic management department will view the information from the cloud and will be able to take necessary decisions to make it better.

We proposed a model for better traffic monitoring and management system to solve congestion problems. The model is called Smart Traffic Monitoring and Guidance System. Formal methods are effective ways to formalize the valid and invalid data [4]. Semi-formal and formal methods are two most important methods to write requirements. We transferred requirements from semi-formal way to formal way. Different types of formal methods like Z notation, B method, and VDM++ [5] are used for formal modelling.

Currently we focused on emergency services rescue 1122, smart sticker, and violation of rules and traffic signals components in our model. We did formal modelling in Vienna Development Method Specification Language (VDM-SL) of emergency services rescue 1122, smart sticker, and violation of rules and traffic signals components in our model. This paper consists of seven sections which are Literature Review, Problem statement, Model of Smart traffic monitoring and guidance system, UML use cases, Formal specification, Formal analysis with results and conclusion.

II. LITERATURE REVIEW

Traffic jam is a big problem in any metropolitan city. Numbers of vehicles are increasing day by day due to rise of standard living. Due to this problem there is a need of advanced research to develop an intelligent traffic system (ITS) which can work automatically to solve a problem or to investigate a problem in traffic. A model is proposed in [6] which uses centrally placed microcontroller and infrared proximity sensors which uses vehicular length to develop an intelligent traffic monitoring system. This system needs real time data to be collected for each situation, in a dynamic situation to gather data about traffic is a time consuming and expensive work. It uses UML (Unified modeling language) diagram to interact between user and system. In addition we
have used VDM-SL (Vienna Development Method-Specification language) to formalize and verify sensors data. A model is proposed in [7] which works on simple algorithm based on length of traffic lane. Time allotter on current lane affects the length of traffic on the other lanes. To determine the length of traffic proximity sensors are used instead of WAN. Intelligent traffic system (ITS) implemented through wireless sensor networks, Radio Frequency Identifier (RFID) and graph theory concepts to find the shortest path. This algorithm does not able to identify a vehicle or to update the driver about traffic situation at specific intersections. We have used smart sticker for each vehicle to identify vehicle and to update the system about the vehicle record. Second we have used Light emitting diode (LED’s) display to show traffic information to drivers at specific points. A new traffic signal control algorithm is proposed in [4, 8] to develop intelligent traffic system. The new traffic signal can measure the individual travel time of a vehicle. The control algorithm calculates the delay and then searches the optimal solution to minimize the total delay based on queuing model. We have used sensors to control the congestion at threshold value, to find the location of vehicles through Global Positioning system (GPS) and update rescue team about accidental situations. In [9, 10], authors proposed a system which used image processing technique to analyze the traffic flow to control the traffic. They used image sensors embedded with web based cameras to capture the movements of vehicles. This system cannot give correct result as image processing is very complex to analyze each situation of the traffic. Second this technique requires expensive hardware for image detection and processing. Unlike this, we have used smart sensors which just collect data about the traffic to update system. We proposed a model for smart traffic and guidance system in which we used sensors as a backbone. Sensors are configured at different places in a city. All sensors collect data from dynamic flow of traffic and update system and then system inform local authorities about the situation. We used VDM-SL for requirements specification to formalize and verified our requirements used in our model [5]. In this paper, author is presented moving block interlocking with its safety characteristics for avoiding collision and derailing of trains at the crucial areas of the network [26]. In this study, author has described the entire state space of critical components of moving block interlocking system by using graphs and in combination with Z notation and also provided the specification of the work [27]. This paper presents a novel approach to model and analyse an important and critical component of moving block railway interlocking system that is railway crossing [28]. Author has explained formal methods as an advance software engineering technique and used Z notation for describing formal specification of critical m X modules of automated train control system [29]. Railway interlocking system is very critical in different ways like safety, environmentally, economically and its nature of distributed system, any failure may risk the human life, environment and money. The author has used formal specification languages such as VDM, Z-notation for its modelling using crisp (two-valued logic) theory [30]. As the traffic system also include all these risks and we have overcome these problems by our proposed system.

Some of the other related work on application of formal method in critical systems can be found in [18-25].

III. PROBLEM STATEMENT

In these days, the major focus of the industry is on smart systems. Smart systems are IOT based systems in which each component acts as a communicable device [2] alarm systems [11] and fire detection [3]. Developed countries are transferring their system on IOT. In Pakistan, there is no as such intelligent IOT system for transportation. As transportation is a major factor for health, education and other aspects of life. However, problem is that building such systems is very difficult because of their complexity [6]. Therefore, this field requires a lot of research and struggle to develop such a traffic management system in which all these issues can be solved. Such system requires real-time data analysis from traffic flow to find better solutions for every problem [12].

The main problem of building such system is requirement engineering. These requirements are not understandable to develop, due to this, we are building a formal model of requirements for smart traffic management system [13].

IV. THE MODEL OF SMART TRAFFIC MONITORING AND GUIDANCE SYSTEM

Traffic monitoring and guidance system is an application of advanced technology to solve the traffic problems and to support smooth flow of traffic. Unbalanced signals and high load of traffic increases the problems in traffic flow.

In our model we have described the main problems of traffic system which are traffic congestion, emergency incidents, vehicle identification through smart sticker, and smooth control of traffic signals, security and users guidance about traffic through Light Emitting Diode (LED) about at different points. Currently we have focused on smart sticker, emergency services rescue 1122 components in our model. Smart sticker has a barcode which consists of owner name, vehicle registration number, vehicle model number, vehicle engine number and color of vehicle. Smart sticker is pasted on front screen of vehicle. Sensors installed at different points will read the smart sticker from vehicles, extract information from it and then update the system about the vehicle. Emergency services rescue 1122 will be activated if any emergency occurs. Sensors will automatically detect miscellaneous activities. The traffic system automatically update through new information. The admin will be quickly informing the rescue 1122. These rescue services provide the medical treatment as soon as possible.

Traffic signals are installed and configured to communicate with the sensors. Traffic signals gather real time data from traffic flow and report congestion to system if it reaches to a threshold value. Then Traffic light will turns to
green automatically. Then system will display updated information on LED’s (light emitting diode) to inform the users. Traffic signals will turn to green immediately if it detects any emergency vehicle which provide social and health services to people.

Users must follow the traffic rules to overcome accidents on roads and to provide smooth flow of traffic. Traffic rules are not only necessary for vehicles but at the same time these are necessary for pedestrian. Sensors will operate on traffic rules and report the system about vehicles not following the traffic rules. There are many rules which are important for traffic flow but after the Second World War there are number of rules implemented to ensure the road safety [16].

Figure 1: shows a high level model of traffic system. We can say, it also represent the work we have done with VDM SL to formalize traffic system. This model is not fully functional traffic system but we tried to cover some important aspects of traffic system and because it is a critical system so we formalized all our work to show it is valid.

V. UML USE CASES

A use case diagram displays the relationship among actors and use cases. Use case diagrams determined the relation between actor and performance action. Interaction between rescue team and system described through use case diagram. In our model we will focus on rescue 1122, smart sticker, Traffic signals and Violation of rules. In rescue 1122 use case has an actor and performs some action [17]. Traffic signal use case shows interaction between vehicle owner and traffic signals.
VI. FORMAL SPECIFICATION OF MODULES

A. Rescue module

The functionality and specification of Emergency is formally modelled by using VDM-SL. Its properties are specified with the help of known modelling and specification language, VDM-SL. Firstly we describe the emergency service and then we will look closely into different functions. This service is designed for attending medical emergency situations on road, caused by traffic collision. Before taking patient to hospital it is necessary to give him first aid if he is serious, and if matter is not very serious then this service can help on road by giving basic medical help.

So to implement this system, we need to know some information about the incident like location that is token type, type of emergency that is quote type. So to store information different variables are used in the specification. Emergency is defined by composite type which has related information about single emergency, different other variables are also involved. All the variables are of global type so all can easily be accessible anywhere in the program.

### types

- id: token;
- emergencyLocation: token;
- emergencyType: <MEDICAL>|<FIRE>;
- isEmergency: token;
- SensorinformationforanyMiscellaneous: < EMERGENCYTYPE>|<EMERGENCYLOCATION>;
- Location: token;
- Sensors: token;

These are the variables, id is used for giving unique id to every emergency, emergency type is defined with quote type because we are considering two type of medical emergencies, one Boolean variable is defined isEmergency to check either is there emergency or not. One variable is for location of emergency and other are sensors that are related to traffic monitoring.

```vdm-sl
Emergency::
eNumber:id
location:set of emergencyLocation
type:set of emergencyType
inv mk_Emergency(-,1,t)== (card(l) = card(t)) and (((<FIRE>) subset t \ (<MEDICAL>) ) or ( <MEDICAL> subset t \ ( <FIRE>)) and ( <FIRE>, <MEDICAL> ) inter t<> {});
```

This is like an object of emergency which have all the related emergency information, in VDM SL it is called composite data type. It have also invariant which verifies its integrity and correct initialization, so no emergency should be call when there is no emergency. It is checking that if there is any emergency then there must be a location and it also checking emergency must be from one of its type either medical or fire.

The next part of specification defines the state of the system. State of the system refers to permanent data that must be stored by the system for its operation. State of the system must have some variables to store data, initialization and invariant conditions that must be satisfied to use this system. As in other programming languages we cannot declare two variables with same name, same in VDM SL we can’t do this, so we have to declare names with modification in the system state. In system state we have used loc for taking locations that are coming from sensors. Moreover System maintain sensors and also it have variable for current location if there are any emergency currently going on.

```vdm-sl
state rescuee of
loc: map Sensors to Location
sensors: set of Sensors
currentlocation: set of Location
getinformationforanyMiscellaneous: map Sensors to SensorinformationforanyMiscellaneous

anyemergency: set of isEmergency
listOfEmergencies: map id to Emergency

init mk_rescuee(\%,\%,\%,\%,\%,\%) == a=\{|\->\} and c={} and an={} end
```

There are different operations involved in the emergency services that provide facilities to users when an emergency occur.

SetSensorOnBridge is the first operation that is very simple, it takes a sensor and a locations. What it does is, it only place that sensor on that location for monitoring. Pre-condition checks that sensor must not already place anywhere else and post conditions finally does sensor placement if pre-conditions returns true. We are using set notation to keep
sensors and for assignment we are mapping sensors to their locations.

```
SetSensorsOnBridge(sensorin:Sensors, locationIn: Location)
```

GetInformation operation gives us information about the location, where the sensor is deployed. Once this method is called, it will return us information of activities happening there so that information can be provided to rescue if there is any accident. Operation have pre-condition that verifies the information of this accident is not already added, and if it return true then post condition will execute and the information of the current accident will be added to system.

```
GetInformationForRescue(getinformationin:Sensors, sensorinformationforanyMiscellaneous, sensorin:Sensors)
```

NewEmergency operation will create a new emergency; it needs some information for creating a new emergency object that is added to system in the list of emergencies. To create a new emergency it needs ID, location of emergency and emergency type.

```
NewEmergency(idIn:id, location:emergencyLocation, type:emergencyType)
```

NumberOfEmergences is a simple method that is returning the total number of emergencies added to system. This operation is working like a central information system that is maintaining how many emergencies are currently registered in system. System is maintaining variable called any emergency in a form of set. So to find how many variables in a set we use cardinality operator, this operator return us total number of elements in a set.

```
NumberOfEmergences() total:int
```

B. Smart Sticker Module

This is another module of traffic system. To identify or sense traffic situation on road we need to deploy wireless sensors on roads, but what sensors will sense? This is worldwide problem many counties tried different things to solve this problem. So we are also giving our idea of smart stickers. We use smart sticker that we will put on every vehicle on road that a sensor can sense, this process will take time but it worthwhile.

First part of the specification is type, in which different variables are declared and defined so when we have to save something for system, we can use these. Smart sticker have String variable that can save sequence of characters. Smart sticker have Sticker variable as composite data type, it will contain all the information about the vehicle and its owner on which it is attached. System has different variables to save sensors data and sensors states also there are a variable to save location.

```
types
String = seq of char;
Sticker :: carnumber:String
    Reg:token
    vehicleModel:String
    engineNumber : String;
Sensorinformation = set of token;
Sensors =set of token;
Location =token;
```

Smart sticker state define the whole system generally, what it will have while running and what its initialization condition is. So the system will have location of the under consideration area, some basic ownership information and a set of stickers. So the invariant and initialization condition validates when this system initialized it will not have any data in it. It is initialized empty and afterward we will fill information.

```
state SmartSticker of
```
First operation of the smart sticker is to set sensors on the road, because we need sensors to sense smart sticker. We can give location and a sensor to deploy it on the road or anywhere in parking etc. precondition will check this sensor is not already in use and if it returns true then that sensor will be deployed on the road by taking union with the set that have already deployed sensors.

To get information from the sensor we need this operation, we just have to give sensor identification from which we want to get information. Pre-condition verify that the sensor that is called belongs to our system sensors. Post condition gets the sensor information is also defined, location to save location of sensor information is also defined, location to save location of sensor information.

This method reflects its functionality by name; compare smart sticker will compare a given sticker from our database and return true or false accordingly. It takes car number, registration no, engine number and vehicle model to query database.

This method is quite useful because of its functionality; this method is used to add more stickers’ information into our system. Because vehicles are growing day by day and we have to add more vehicles to our database so we can sense those cars also and our system work correctly.

Second part is of values but we don’t have any predefined values in our traffic system so this area will remain empty.
values

Third part is state of the system; it is important part because system will be functional if state runs successfully. It allows system to wake up under certain conditions. State also has different variables, we can call them system variables, and these variables are always in the system with some values that are required during runtime. So we have variables like restricted area, current traffic, signal, and location, all these variables are explained earlier. Get information is variable that will save current sensor information. In invariant system is checking current traffic status must be from the defined states, and signals must also be red, green or blue. In first location is empty.

\[
\text{state trafficSystem of restrictedArea : set of restrictedAreas}
\]

\[
\text{currentTraffic : set of trafficSituations}
\]

\[
\text{signal : set of signals}
\]

\[
\text{getinformation : set of sensorinformation}
\]

\[
\text{inv mk_trafficSystem(-,C,S,L,-,-) == (C subset (\\{\\text{<JAMMED>},\\text{<CONGESTION>},\\text{<SMOOTH>},\\text{<ACCIDENT>}\}) and (S subset (\\{\\text{<RED>},\\text{<AMBER>},\\text{<GREEN>}\}) and L <> {})}
\]

Next part of the specification includes operations or functionalities of the system.

operations

Get information from sensors is second method and as name suggests it will collect information from sensors. This method has one parameter that is sensor from which we want to collect information. Pre-condition validates information from the sensor not already save in the system variable, because we don’t want to save duplicate information and then finally post condition return us information.

\[
\text{Getinformationfromsensors(getinformationin :sensorinformation)}
\]

\[
\text{ext wr getinformation: set of sensorinformation}
\]

\[
\text{pre getinformationin not in set getinformation}
\]

\[
\text{post getinformation= getinformation union\{getinformationin\};}
\]

D. Violation of Rules

This operation takes three parameters and checks for violation, if there is any violation it will return true. This operation is necessary for making a challan if any vehicle is violating rule, it will make police representative work easy.

\[
\text{ViolationOfRules(carSpeed:int, currentLoca-}
\]

\[
\text{tion: restrictedAreas,signalCrossing: signals)}
\]

\[
\text{ext rd restrictedArea : set of restrictedAreas}
\]

\[
\text{pre true}
\]

\[
\text{post (carSpeed > 100) or (currentLocation in set restrictedArea) or (signalCrossing = <RED>)};
\]

Next operation is update current traffic situation, it will take number of cars as parameter and return us current traffic situation in quote type. By looking at the current traffic situation any one can understand it and can choose best route. In this method post condition is checking temp traffic, it is either less than fifty or less then hundred or greater than hundred and deciding from smooth, congestion or jammed and update current traffic situation.

\[
\text{UpdateCurrentTraffic(tempTraffic:int)}
\]

\[
\text{ext wr currentTraffic : set of trafficSituations}
\]

\[
\text{pre true}
\]

\[
\text{post ((tempTraffic >= 0 or tempTraffic <= 50) and currentTraffic =\\{\\text{<SMOOTH>}\}) or ((tempTraffic >= 51 or tempTraffic <= 100) and currentTraffic =\\{\\text{<CONGESTION>}\}) or ((tempTraffic >=101) and currentTraffic =\\{\\text{<JAMMED>}\});}
\]

As we are updating traffic situation, same as we have to update traffic signal timings accordingly, otherwise increased traffic on road will lead to congestion or jammed and less traffic will lead to more unnecessary wait on traffic signals. So to update signal timing, this method is looking for current traffic situation and updating signal timings accordingly.

\[
\text{UpdateTrafficSignal(signaltime:int)}
\]

\[
\text{ext wr currentTraffic : set of trafficSituations}
\]

\[
\text{pre true}
\]

\[
\text{post if currentTraffic =\\{\\text{<SMOOTH>}\}
\]

\[
\text{then signaltime=20}
\]

\[
\text{elseif currentTraffic =\\{\\text{<CONGESTION>}\}
\]

\[
\text{then signaltime =10}
\]

\[
\text{else signaltime =5;}
\]

Medical emergency is the most critical situation on roads if there is any incident. So our system is also dealing with this situation, if sensors reports about any accident, system will initialize an emergency call to nearest medical centre so they can help the affected person.
emergencycall() emergency:bool
ext wr currentTraffic : set of trafficSituations
pre true
post if currentTraffic = {<ACCIDENT>}
  then emergency = true
  else emergency = false;

E. Traffic Signals

Signals are important component in traffic management system. The existing methods for traffic monitoring and management are not fully efficient in terms of cost, performance, support and maintenance. In this paper, the idea of more utilization and accurately managing the traffic lights presented.

Formal Specification of traffic signal control system is formally described with the help of VDM-SL. Traffic signals are modelled with the help of wireless sensors network, because sensors are small devices which are used for getting and providing different type of information. All communication links are established through wireless sensor. Traffic signals are important for smooth traffic transaction. Intelligent sensors which is reasonable of vehicles which are passing through signals.

In this paragraph we have described the types and different variables that are first part of formal specification for traffic signals. Signal is defined with quote type which is combination of three colors. Variable color is token type; number of car is integer type.

```
types
String = seq of char;
numberOfCars = nat;
Color = token;
Signal = <RED>|<AMBER>|<GREEN>;
Signalstatus = <RED>|<AMBER>|<GREEN>|<THRESHOLD>;
Location = token;
Sensors = set of Sensors;
```

Second part of the specification is values, either there are any predefined values we are using in our specification or not, if any we have to define those values here. So we have defined different threshold values for different traffic load that we will use in update signal method for checking that in which threshold current traffic relay and will update signals accordingly.

```
values
ZERO_THRESHOLD : nat = 0;
MINTHRESHOLD : nat = 10;
MIDTHRESHOLD : nat = 50;
```

The most important part of specification is state of the system. State of the system permits to initialize and run the system under specific conditions if true, and it also preserve all the values during system running that are required for proper functionality of system. The functions needed for proper initialization are called init and ini, init (invariant) check all the preconditions and ini (initializer) initialize the system with given values. In our system invariant of the system determine that the number of cars should be non-zero and the status of signal should be from given signal colors. The color of signal changes according to predefined timings but with the passage of time and change in traffic flow will lead to update signal timings. Initially all the variables are empty and number of cars are given value of zero.

```
state signalUpdate of 
  Location : map Sensors to sensor
  sensorInformation : map Sensors to Information
  Sensors : set of Sensors
  signals : set of Signal
  numberOfCars : nat
inv mk_signalUpdate(-,-,-,-,N) ==
  N >= 0 and
  (S = <RED>) or
  S = <AMBER>
  S = <GREEN>)
init s == s = mk_signalUpdate({},{}->{),{}(),}(),0)
end
```

Operations defines the main functionality of any system, so in this part different operations and their functionality is described

```
operations
AddSensor is the first operation in which sensors can be placed at different locations. This operation takes two parameters; one is sensor which is to be placed and second is location where the sensors are to be placed. These sensors are specific which have ability to get the traffic condition at any time. Pre-condition checks that sensor must not be already placed anywhere and post condition finally does placement after pre-condition return true.
```

```
AddSensor(sensorin:Sensors, locationIn:Location)
ext wr loc : map Sensors to Location
wr sensors : set of Sensors
pre sensorin not in set dom loc post loc = loc union(sensorin)->locationIn);
```

Sensor Information is the second operation that is necessary to update signal timing and also everyone on system administrator side and user side want to know, what the current traffic situation is. So this method take only one input and give us one output, it take sensor id as an input and gave
us output or information from that sensor in return. This is very simple method but it is very useful. We are giving id to sensor map that returns us a sensor, that sensor further given to information map, that return us the information associated with that sensor, and finally delivered to information Out variable.

\[
\text{sensorsInformation(id:nat) infoOut: Information}
\]
\[
\text{ext rd sensor: map Id to Sensors}
\]
\[
\text{rd information : map Information to Sensors}
\]
\[
\text{pre id in set dom sensor}
\]
\[
\text{post infoOut = information(sensor(id));}
\]

Signal Update is important and critical operation in any traffic control system, all the system depends on the timing of the signals. If signals timings are not updated according to traffic situation on road, it will create problems that lead to road accidents and congestion, and if signals fail to work it will crash whole transportation system. So we have carefully designed all the conditions that update signal timings according to traffic situation on road. This method is using different variables for calculating new signal timing and path is the variable that saves number of roads. Second parameter is numberofcars that will give information about number of cars on each path and also some thresholds are used that are defined by system admin. Threshold gives us information about numbers of cars when we have to update our signal timing, in response each signal will be updated. First we are giving id to that sensor, and finally delivered to information Out

\[
\text{if(numberOfCars >= ZERO_THRESHOLD) and (numberOfCars <= MINTHRESHOLD)}
\]
\[
\text{then (signal1 = <GREEN> and other=<RED>) and time=20 and path=path+1 mod 4}
\]
\[
\text{else if numberOfCars > MINTHRESHOLD}
\]
\[
\text{and numberOfCars < MIDTHRESHOLD}
\]
\[
\text{then (signal1 = <GREEN> and other=<RED>) and time = 20 and path=path+1 mod 4}
\]
\[
\text{else (signal1 = <GREEN> and other=<RED>) and time = 30 and path=path+1 mod 4}
\]
\[
\text{else if path = 2}
\]
\[
\text{then if(numberOfCars >= ZERO_THRESHOLD) and (numberOfCars <= MINTHRESHOLD)}
\]
\[
\text{then (signal2 = <GREEN> and other=<RED>) and time=20 and path=path+1 mod 4}
\]
\[
\text{else if numberOfCars > MINTHRESHOLD}
\]
\[
\text{and numberOfCars < MIDTHRESHOLD}
\]
\[
\text{then (signal2 = <GREEN> and other=<RED>) and time = 20 and path=path+1 mod 4}
\]
\[
\text{else (signal2 = <GREEN> and other=<RED>) and time = 30 and path=path+1 mod 4}
\]
\[
\text{else if(numberOfCars >= ZERO_THRESHOLD) and (numberOfCars <= MINTHRESHOLD)}
\]
\[
\text{then (signal3 = <GREEN> and other=<RED>) and time=20 and path=path+1 mod 4}
\]
\[
\text{else if numberOfCars > MINTHRESHOLD}
\]
\[
\text{and numberOfCars < MIDTHRESHOLD}
\]
\[
\text{then (signal3 = <GREEN> and other=<RED>) and time = 20 and path=path+1 mod 4}
\]
\[
\text{else (signal3 = <GREEN> and other=<RED>) and time = 30 and path=path+1 mod 4;}
\]

VII. **Formal Analysis with Results**

We have formally verified two components of our model emergency services Rescue 1122 and Smart Sticker through VDM-SL. The analysis of formal specification was done with checking of syntax free and type free errors. The details of formal analysis is given in figure 4, figure 5, Table I, Table II, Table III and Table IV.
The model of smart sticker and their properties have verified with VDM-SL tool box.

Table I

<table>
<thead>
<tr>
<th>Operation</th>
<th>Syntax Check</th>
<th>Type Check</th>
<th>Integrity Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetSensorsOnBridge</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GetInformationForRescue</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NewEmergency</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GetEmergency</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NumberOfEmergences</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Table II

<table>
<thead>
<tr>
<th>Operation</th>
<th>Syntax Check</th>
<th>Type Check</th>
<th>Integrity Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetSensorsonLocation</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GetInformationforSmartSticker</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>AddSmartSticker</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>CompareSmartSticker</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Table III

<table>
<thead>
<tr>
<th>OPERATION</th>
<th>Syntax Check</th>
<th>Type Check</th>
<th>Integrity check</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddSensors</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GetInformation</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SignalUPDATED</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
VIII. CONCLUSION

This paper presented Emergency Services Rescue 1122, Smart Sticker, Traffic Signals and Violation of rules of our proposed model. The goal of traffic management system is to identify vehicles, to inform drivers about traffic situation and road conditions. Traffic is monitored remotely through sensors on roads for providing different facilities to users Smart Sticker identifies the vehicles and informs the local authority to update the system about vehicles. Smart Sticker provides security in smart traffic management system to restrict illegal activities in traffic flow. Emergency Services Rescue 1122 provides emergency related services to overcome different incidents like accidents, fire fighting etc. Traffic signals are configured for the purposes of smooth flow of traffic. Violation of rules ensures road safety and provides incidents free traffic flow. Violation of rules also detects intruders on roads not following traffic rules. Sensors are distributed and configured on roads for monitoring different activities of traffic to update the system. Formal methods based technique, i.e. VDM-SL is used to develop formal representation of the proposed model. The proposed model components are validated, verified and analysed using VDM-SL Toolbox.

The proposed model consists of Smart Sticker, Emergency Services Rescue 1122, LED, signal control timing, alternative paths on specific threshold and miscellaneous activities of traffic flow. Smart algorithms can be proposed to control signal timing on specific threshold and make traffic incidents free. LED can be installed on different points on roads to provide information about traffic flow to users. In future this model can be enhanced to provide smart services in traffic management system in the country.

REFERENCES


Anonymous and Secure Routing Protocol for Multi-hop Cellular Networks

Salwa Othmen 1, Faouzi Zarai 1, Aymen Belghith 2, Lotfi Kamoun 1

1 LETI laboratory, University of Sfax, Tunisia
2 Saudi Electronic University (SEU), Computer Science Departement, Saudi Arabia

Abstract—In single cellular networks, the mobile stations cannot communicate directly with each other. All communications are relayed through the base stations. Such topology suffers from many limitations such as congestion problem when a large number of users are communicating in the same time to a base station. In this context, the device-to-device communications have been proposed to overcome the limitations of the conventional cellular architecture. Indeed, a mobile station can allow two nearby stations to communicate with each other without involving a base station. However, security becomes an important challenge that must be taken into consideration as the mobile stations participate in routing data between each other. In this paper, we propose a secure routing protocol for Multi-hop Cellular Networks (MCNs). Our goal is to discover a secure and short route between the source and the destination. To evaluate this proposed protocol, we perform some simulations using Network Simulator (NS-2). The simulation results show that it provides acceptable performance in terms of throughput and routing overhead as comparing with Secure Ad hoc On demand Distance Vector (SAODV).

Keywords-component; single cellular networks, base stations, Device-to-device, secure routing protocol, MCNs, NS-2;

I. INTRODUCTION

In traditional cellular (single hop) networks, the mobile stations can communicate with each other only through the base station (BS). Such architecture suffers from many limitations such as signal attenuation especially when the station is at the edge of the cell. In order to overcome partially some problems, installing a high number of BSs is required. However, increasing the infrastructure of such networks is very expensive at management and deployment phases. Other emerging alternative called Multi-hop Cellular Networks (MCNs) is currently considered as a part of the five Generation (5G) network evolution. It includes the integration of cellular and Ad-Hoc technologies. So, the direct link between mobile nodes and BSs is not required [1]. This alternative has a lower implementation cost in comparison with adding new BSs. Many studies have showed the advantages and benefits of MCNs. Indeed, the coverage area is increased [2] and the interference is reduced as the radiated energy is diminished. Moreover, the transmission rate is increased [3] due the reduction of the signal loss in each node. As the signal covers a small distance, the energy consumption of each node is also reduced. To achieve such objectives of MCNs network, it is necessary to take into consideration some important technological challenges such as design and secure multi-hop routing protocols.

Two cases of communication are distinguished in MCNs. The first case is when the source and the target destination are in the same cell. In this case, the packets are relayed by the mobile terminals and the intervention of the base station is not required. However, when the source and the destination are in different cells, the BSs have to participate in routing process. In MCNs the participation of mobile nodes in routing process, makes security as an important challenge that must be taken into consideration. Indeed, an attacker can trace the paths, infer the source and its target destination and so it can track other users.

In this paper, we propose a new routing protocol for MCNs. This protocol selects a secure and short route that ensures security in terms of confidentiality, integrity and authentication. To prevent the anonymity of the users, we propose that they use temporary identities generated by themselves every session. Moreover, to minimize the computational overhead for a node in verifying the validity of node’s certificate, we use “Weil Pairing” scheme [4]. This scheme can help each node to authenticate implicitly its neighbor with minimum complexity. To secure the exchanged data between them, the source and the destination generate a session key initiated by the source node.

The paper is organized as follows. In section II, we present some related works. In section III, we present some notations and preliminaries. In section IV, we describe our proposed protocol. To evaluate its performance some analysis and simulation results are given in section V. We conclude the paper with the conclusion and some proposed future works in section VI.

II. RELATED WORK

Many routing protocols are proposed for Ad Hoc networks. These protocols can be performed in MCN networks by the source when it is in the same cell as the destination. In [5], Zapata et al. proposed a secure routing protocol named SADV. This protocol has the same steps as AODV protocol, but it integrates some cryptographic techniques to prevent routing messages against attacks. It use hash chain to protect hop count information and digital signature to authenticate the source and destination. The disadvantage of SAODV is the lack of authentication between neighbor nodes. This can leads to some attacks such as impersonation attack.

In [6] Zhou et al. proposed an Optimal and Secure Routing Protocol (OSRP) for Multi-hop Wireless Networks. This proposed protocol satisfies security by selecting secure routes that are resilient to attacks. OSRP relies on a Trusted
Clearance Center (TCC). According to the report behaviors of the nodes, the TCC computes and assigns a trust value for each node based on game theory. The authors prove that the TCC can detect attackers and segregate them from the wireless networks. Therefore, the OSRP can select optimal routes with low false alarm rate and high detection rate. However, this protocol is vulnerable to several attacks such as impersonation attack due to the lack of authentication between the nodes. In [7], K. Sanzgiri et al proposed a secure routing protocol called ARAN. It ensures security in terms of authentication, integrity and non-repudiation. It is based on asymmetric key cryptography and it involves a trusted certification server. The certificate requires the address and public key of the node and a time-stamp of when the certificate is generated and when it is expired. The disadvantage of this protocol is the use of a central authority and it is not secure against wormhole attack. In [8], K.V. Kumar et al. proposed a secure routing protocol which consists of three steps. In the first step, each node exchanges a secret key with its one and two hop neighbors based on its public key. When establishing a shared key, the node participates in routing process in the second step. In the third step, the source and destination share a secret key securely and then data communication is triggered. The disadvantage of this protocol is that the shared secret key between nodes is based on public keys and so attacks are possible to occur.

III. NOTATION AND PRELIMINARIES

A. Weil Pairing

The proposed protocol is based on “Weil Pairing” scheme for cryptographic foundation. Assume that $G1$ is an additive cyclic group over an elliptic curve; $G2$ is a multiplicative cyclic group and these two groups are with prime order $q$.

“Weil Pairing” is the mapping of $\hat{e}: G1 \times G1 \rightarrow G2$, for all $P, Q, R, S \in G1$, we have:

$$\hat{e}(P + Q, R + S) = \hat{e}(P,R) \cdot \hat{e}(P,S) \cdot \hat{e}(Q,R) \cdot \hat{e}(Q,S)$$

B. Smart-Chen-Kudla scheme

The proposed protocol is based on “Smart-Chen-Kudla” scheme for key generation. This scheme has the advantage of providing implicit authentication. It is based on “Weil Pairing” tool. In this scheme, the trust party is in charge of generating and distributing public parameters $(q, H1, P, P_{pub}, G1, G2)$, where $H1$ is a hash function $\{0, 1\}^* \rightarrow G1$, $P$ is a generator of $G1$, $P_{pub}$ is the master public key formed as $P_{pub} = sP$, where $s \in \mathbb{Z}_q$ is the master private key of the trust party. The trust party registers each mobile node $M_i$ and assigns to it a master private key $P_i = s \cdot Q_i$, where $Q_i = H1(ID_i)$ and $ID_i$ is the identity of $M_i$.

When two communicants A and B want to share a secret key, each one generates a random value $a$ and $b$ respectively.

Key generation phase between A and B is performed as follows:

- A sends $T_A = aP$ to B.
- B sends $T_B = bP$ to A.
- A calculates its secret key as the following:

$$K_{AB} = H1(abP || \hat{e}(sQ_A, T_B)\hat{e}(Q_b, asP))$$

- B calculates its secret key as the following:

$$K_{BA} = H2(abP || \hat{e}(sQ_B, T_A)\hat{e}(Q_a, bsP)).$$

Both users A and B share the same secret key:

$$K = K_{AB} = K_{BA} = H2(abP || \hat{e}(bQ_B + aQ_a, sP))$$

Where, $H2$ can be a random oracle or a secure hash function [9].

C. Adversary Model

We assume that the attacker knows network protocol and functions but it does not know the secret keys and parameters. Also, it can observe and collect data packets to analyze the node behavior and reveal its hider identity to break the privacy of this node. The attacker can learn other important information from these collected data such as message content. It can use this information to launch other attack such as impersonation attack or Sybil attack. It can also modify the exchanged messages or broadcast a wrong message to influence the routing behavior.

The attacks that can be launched by an attacker from the collected information are listed below:

Attacker replay: An attacker store a message without authorization and then it retransmits this information in order to trick the destination into unauthorized operations such as duplicate transaction or false authentication.

Sybil attack: The attacker generates a set of unauthorized identities in order to establish a neighbor relationship. The other nodes do not know that these identities are issued from an attacker due to some security problem such as the lack of authentication between them.

Rushing attack: In rushing attack, the attacker transmits the route request packet to a large number of nodes using a high transmission range. The receiver of this false packet may be unable to respond the sender, and so cannot establish the route.

Impersonation attack: The attacker tries to impersonate the identity of a legitimate node in order to become a member of the selected route or to establish a neighbor relationship with other nodes. Therefore, the attacker can receive the routing messages directed to the faked nodes and so it can modify their contents to falsify the network.

IV. PROPOSED ROUTING PROTOCOL

In this section, we present the network model as well as the description of our proposed algorithm.

A. Network Model

In our network model, we are based on Multi-hop Cellular Network that consists of a fixed BS and several numbers of mobile stations (see figure 1). Before deployment, each new mobile station must authenticate to the BS in order to obtain the system parameters $(q, H1, P, P_{pub}, G1, G2)$ necessary to generate secret keys shared with the neighbor nodes. Also, the BS furnished to each node a temporary identity used by this node in its first communication. In this network model, we assume that the time is divided into successive sessions. Also, the BS and mobile stations are synchronized, so we adopt $ID||t$ to compute the private key and the temporary identity.
for each mobile $M_i$ in each session ($t$ is the timestamp). For that purpose, each node must know the beginning of each new session to renew its private key and its temporary identity.

The private key of a mobile $M_i$ is computed as the following equation: $S_i = s Q_i$.

Where: $Q_i = H_1(ID_i||t)$ and $ID_i$ is the real identity of the mobile.

In each session, the mobile have to perform a neighbor discovery phase in an authenticated way. During this phase, each node generates a random value $a_i$ and sends to its neighbor $P_i$ value based on Pairing Discrete Logarithm Problem (PDLP): $P_i = a_i P$.

![Figure 1: Topology of Multi-hop cellular network cell](image)

**B. Proposed algorithm**

We propose a new anonymous on-demand routing protocol which achieves communication between mobile nodes without disclosing their real identities. Indeed, during route discovery process, the nodes use their temporary identities instead of their real identities. Indeed, when a node sends its real identity in plaintext a passive attack can be performed by the attacker by analyzing exchanged packets. Also, the disclosure of real identity makes the attacker able to trace packets backward to the source or forwarded to the destination. This is undesirable because in some case the source or the destination is a critical node. Moreover, when a node uses the same temporary identity for long time, it cannot be protected against many types of attacks, because this temporary identity can be analyzed the same way as its real identity. Thus, each node must use a dynamic identity in each session. These identities are used in data transmission after route selection. So, the route anonymity is achieved and the attacker cannot infer the participating mobile nodes in one session.

To secure routing packets, we are based on a symmetric cryptography based on Weil Pairing tool. This scheme guarantees also an implicit authentication instead of verifying the validity of node’s certificate and involving a trusted certification server. This leads to minimize the expensive cryptographic mechanism in term of time and complexity.

The source and destination share a secret key used to secure data transmission phase. This key is initiated by the source node during route request process since the source and its destination are not neighbor to exchange secret information ($P_s$ and $P_d$) in the neighbor discovery process (see Network Model section).

Our proposed protocol is divided into two phases: route request (see figure 2) and route reply phases.

![Figure 2: Flow chart of route request phase](image)

1) Route request phase

Route request phase is initiated when a source needs to communicate with a target destination for which it has no route maintained in its routing table. To secure route request packet, each mobile station $M_i$ computes a session key shared with its neighbor $M_j$ based on Weil Pairing as the following equation:

$$K_{M1M2} = \hat{e}(S_1, P_2) \hat{e}(Q_2, a_1 s P) = \hat{e}(S_2, P_1) \hat{e}(Q_1, a_2 s P) = K_{M2M1}$$
The route request phase is performed as the following steps:

- **Step 1**: The source S generates and sends to each neighbor an RREQ packet:
  
  **Step 1-1**: S generates a random value \( r \in \mathbb{Z}_q \) to compute a secret key shared with the destination D as the following equation:
  
  \[
  K_{SD} = e(rS_S, H_1(IDD||t))
  \]

  **Step 1-2**: S generates session key shared with each neighbor \( M_i \) as equation (1).

  **Step 1-4**: S encrypts its temporary identity with \( K_{SD} \) shared with D to guarantee its anonymity and so the intermediate nodes cannot know who communicate to whom.

  **Step 1-5**: S sends to each neighbor \( M_i \) the packets RREQs protected by \( K_S \).

  The format of RREQ packet is as follows:
  
  \[
  \text{RREQ: } \{ E(K_{SD}, \text{seq_num} || \text{TTL} || \text{Hop_count} || rH_1(IDS||t) ), E(K_{SD}, XIDS), H_2(*) \}
  \]

  The source adds to RREQ packet the seq-num to prevent the route request against replay attack, TTL is used to limit the propagation area of the route request, Hop_count is the number of hops traversed by the route request and it is incremented by each hop, \( rH_1(IDS||t) \) is used by D to compute the shared key with S, \( E(K_{SD}, XIDS) \) is the temporary identity of S encrypted by the secret key \( K_{SD} \) for anonymity and \( H_2(*) \) is the hashed value of the RREQ packet.

  If S does not receive a route reply in a fixed time period, it sends a new RREQ packet. If it sends \( k \) packets and no response sent by D, it record that this destination is unreachable.

- **Step 2**: An intermediate mobile station \( M_k \) receives a RREQ packet from its neighbor \( M_w \). It performs the following subsets:

  **Step 2-1**: \( M_k \) decrypts the RREQ packet by the shared key with \( M_w \). By this way, \( M_k \) authenticates \( M_w \) because only this node can compute \( K_{in} \).

  **Step 2-2**: \( M_k \) checks the integrity of the RREQ by computing its hash value. If the verification passes, goes to step 2-3. Otherwise, discard this packet.

  **Step 2-3**: \( M_k \) computes the \( K_{Sj} = e(rH_1(IDS||t), S_j) \) in order to checks if it is the destination of this process. If \( M_k \) can decrypt \( XIDS \), so it is the destination, goes to step 3. Otherwise, goes to step 2-4.

  **Step 2-4**: \( M_k \) decrements the TTL value and increments the hop_count by one.

  **Step 2-5**: \( M_k \) computes the new hash value of RREQ.

  **Step 2-6**: \( M_k \) encrypts RREQs packets and sends it to the next neighbors.

- **Step 3**: D receives RREQs packets. It performs the following subsets:

  **Step 3-1**: D decrypts the RREQs packets received through different routes and so authenticates each neighbor.

  **Step 3-2**: D selects the packet comes from the shortest route based on hop_count value.

  **Step 3-3**: D compute \( K_{DS} \) and decrypts the temporary identity of S by its private key. It maintains this key in its routing table to prevent the data exchanged with S after route selection.

  \[
  K_{DS} = e(rH_1(IDD||t), S_D)
  \]

  **Step 3-4**: D checks the integrity of this packet. If this verification passes, goes to Step 3-4. Otherwise, it discards this packet and selects the second one corresponding to the shortest route.

  **Step 3-5**: D lunches the route reply phase.

2) **Route reply phase**

After selecting the RREQ with minimum \( \text{hop_count} \), D performs the following steps:

- **Step 1**: D generates the corresponding RREP,

  **Step 1-1**: D computes its temporary identity:

  \[
  XIDD = H_1(IDD||t)
  \]

  We assume that each node of the selected route compute a temporary identity used in data transmission after route selection to guarantee route anonymity.

  **Step 1-3**: D computes the hash value of RREP packet.

  **Step 1-4**: D sends the RREP encrypted by \( K_{DS} \) toward S through the reverse route. Where \( M_i \) is its neighbor node of the reverse route.

  The format of RREP is as follows:

  \[
  \text{RREP: } \{ E(K_{DS}, \text{seq_num} || \text{TTL} || \text{Hop_count} || rH_1(IDS||t) ), \text{H2(*)} \}
  \]

- **Step 2**: An intermediate mobile station \( M_k \) receives a RREP packet from its previous neighbor.

  **Step 2-1**: It decrypts the RREP packet by the key shared with the sender of the RREP,

  **Step 2-2**: Checks the integrity of the RREP.

  **Step 2-3**: \( M_k \) maintains the temporary identity of the previous node and add its new identity to RREP.

  **Step 2-4**: \( M_k \) re-computes the hash value of RREP packet.

  **Step 2-5**: \( M_k \) encrypts RREP and sends it to the next node of the reverse route.

- **Step 3**: S receives the RREP. It decrypts it and verifies its integrity. Then, it uses the corresponding route to communicate with D. The data transmission phase is protected by the session key shared between S and D.

V. **Security analysis and evaluation of our proposed protocol**

A. **Security analysis**

Our proposed protocol achieves the following security requirement:

**Confidentiality**: The routing packets are protected by the secret keys shared between neighboring nodes. These keys are generated using the Weil Pairing scheme based on several secret parameters such as the private key of the BS. An attacker has to solve the PDLP to find the secret key of the BS and compute the shared keys. Also, the source and the
destination share a session key to encrypt data transmitted after route selection.

**Integrity:** In the proposed protocol, each transmitted packet is concatenated with its hash value to provide integrity. To modify a packet, an attacker must decrypt its content and then computes the corresponding hash value of this modified packet. However, the decryption of such packet needs to learn the secret key shared with the sender. The shared keys and the private keys are generated using “Weil Pairing” scheme. By this way, the attacker cannot learn the correct keys to generate the corresponding hash value. So, the proposed protocol ensures the integrity of transmitted packets.

**Authentication:** In our proposed protocol, we are based on Weil Pairing scheme for key generation. This scheme has the advantage to provide implicit authentication based on several secret parameters.

**Anonymity and Intractability:** In the proposed protocol, each node participates in the route establishment phase using its on-time temporary identity. Based on this identity, an attacker is not able to reveal the corresponding real identity. Also, our anonymous routing protocol does not reveal the information related to the source, destination and the intermediate nodes. Even, these nodes cannot learn with which node the source communicates. An attacker is not able to trace the RREQ packet based on its common parts to discover the source and the destination nodes. In fact the RREQ is encrypted by the shared keys of the intermediate nodes. So, our proposed protocol provides anonymity and intractability.

**Key secrecy:** The proposed protocol ensures perfect forward secrecy because when an attacker compromises the secret keys of all nodes, it cannot reveal the previous session keys. This is because each session key relies on random values.

Our proposed protocol is secured against the following attacks:

**Replay attack:** This attack cannot be realized in our proposed protocol because each session key is relies on random values generated by the two neighbor nodes. So, the new keys will be generated without any links with the previous session keys. Also, using the timestamp in computing a new temporary identity and a sequence number for each new packet prevent our proposed protocol against replay attack.

**Sybil attack:** In our proposed protocol, the BS assigns to each node a private key as function as its identity and the private key $s$. So, to perform the Sybil attack, an adversary has to generate a private key for its false identity. This is not possible for an attacker because it must resolve PDLP problem in order to learn the private key $s$ of the BS. So, the Sybil attack is not possible in our proposed protocol.

**Rushing attack:** In our proposed protocol, when a node receives a request packet, it authenticates the sender of this packet by verifying the encryption key. If the authentication is performed successfully, the node accepts the packet and responds the sender because only a legitimate node can generate a valid key. Otherwise, it drops the received packets. So, if an attacker forwards a packet using a large transmission range, this packet will not be accepted by the receiver. Therefore, the rushing attack cannot be realized in our proposed protocol.

**Impersonation attack:** In our proposed protocol, to perform this attack, an attacker must generate a secret key shared with the nodes to which it will send the message. However, this attacker is not able to solve the PDLP problem to learn the secret key of BS and computes a valid private key corresponding to this impersonated identity. Also, it is infeasible to learn the real identity of a legal node and compute its private key because the request packet does not contain a real identity of any node. Thus, the attacker fails to impersonate another legitimate node.

### B. Simulation results

To evaluate the proposed protocol, a set of extensive simulations is conducted using Network Simulator (NS-2) [10]. We compare it with SAODV protocol. The implementation of the security techniques is performed by applying the Crypto++ library because NS-2 does not support these functions.

The parameters of the simulation are summarized in Table I.

<table>
<thead>
<tr>
<th>Table I: Parameters for simulation evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>Routing Protocol</td>
</tr>
<tr>
<td>Traffic Type</td>
</tr>
<tr>
<td>Simulation duration</td>
</tr>
<tr>
<td>Packet Size</td>
</tr>
<tr>
<td>Simulation Area</td>
</tr>
<tr>
<td>Total number of mobile stations</td>
</tr>
<tr>
<td>Number of malicious nodes</td>
</tr>
<tr>
<td>Queue length</td>
</tr>
<tr>
<td>MAC protocol</td>
</tr>
<tr>
<td>Mobility model</td>
</tr>
</tbody>
</table>

The impact of the presence of malicious nodes is measure based on the following metrics:

- **Throughput:** is the average of data received by the destination among the total number of data delivered by the source during the simulation time.
- **Routing overhead (packets):** is the number of routing packets needed to send in order to deliver the data packets from the source to the destination.
Figure 3: Overhead versus number of source node
Figure 3 represents the routing overhead versus the number of source node. We note that, the value of the overhead increases when the number of source nodes increase for both SAODV and the proposed protocol in the presence of five malicious nodes. However, in our proposed protocol the overhead is less than SAODV because each node sends the routing packets only to the neighbor nodes which share with it a secret key. In SAODV, the route request packets can be sent by the attackers as no authentication between nodes is guarantee.

Figure 4: Throughput versus number of source node
As show Figure 4, the throughput increases for both the SAODV and proposed protocol when the number of source node increases. However, our proposed protocol has a higher value in comparison with the SAODV. This is because during route discovery process the nodes authenticate each other and so the probability that an attacker becomes a member of the selected route to drop data packet is low. This is not guaranteed in the SAODV because the authentication is performed only between the source and the destination.

VI. CONCLUSION
In Multi-hop Cellular Networks, the implementation of a reliable routing protocol which ensures both the network performance and the security requirement is a challenging task. In this paper, we propose a secure routing protocol which selects the shortest path between a source and its target destination. This proposed protocol provides performance both in term of security requirements and network performance. In the protocol design, we aim to fit inexpensive cryptographic mechanism in each phase in order to make it robust against attacks.

In the future work, we plan to extend this protocol to be used when the source and the destination exist in different cells and so other types of relay will be considered in routing the exchanged packets.

REFERENCES
Performance analysis of Heterogeneous Data Normalization with a New Privacy Metric

J.Hyma †, PVGD Prasad Reddy ‡, and A.Damodaram ‡‡

† Department of CSE, GIT, GITAM University, Visakhapatnam, INDIA
‡ Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, INDIA
‡‡ Department of CSE, Sri Venkateswara University, Tirupathy, INDIA

ABSTRACT
Investigation on privacy preserving data mining is in extensive need to the present day technological situation. Storage of the data and its usage through various computational processes is becoming very easy and efficient. At the other end the primary concern or sometimes can be termed as limitation to this extensive data analysis is privacy. There are existing privacy preserving techniques that solve this problem and also guarantee privacy as well as data utility. But these techniques have to be updated in parallel to the expansion of digital technology. In view of this, the part of research in this paper analyses various normalization techniques with heterogeneous data distortion. The experimental consideration is done with the comparison of various statistical measures on the distorted data and their preservation with respect to the original data. We evaluated the performance of heterogeneous data distortion with three types of transformations namely Min-Max Normalization, Z-Score Normalization and Decimal Scaling. The performance is evaluated with various data distortion measures and privacy measures.

Key words: Privacy Preserving Data Mining (PPDM), Data Normalization, Privacy, Data utility.

1. Introduction
Every user of technology can notice the raise in data collection, storage and its usage. This information explosion enables us to extract valid useful patterns using various computational techniques. Data mining is a set of well defined techniques can be applied on these massive amounts of data and can deduce valid hidden patterns [1][2]. Marketing, Sales, Finance, Insurance, Weather, Banking and Health sector etc., are various application fields of data mining. Data sharing and processing among various organizations is an important phenomenon now days with the rapid advance in internet and communication technology.

Privacy stands as a main threat at the apathetic side of this aggressive data mining. The data owners who stay at the low end in the data sharing scenario are becoming victims of this privacy violation. However, we cannot ignore the obvious data sharing and its processing. But one has to take the considerable safety measures to protect the data privacy.

Privacy preserving data mining is one such prominent area used to prevent the data disclosure. Its main focus is that ‘do the data mining in a privacy preserving manner’ [3][4]. Several privacy preserving techniques have been proposed and used in various applications. However, all these techniques follow one level of privacy for all data. In real time it is not applicable because, privacy is an individual choice of data disclosure. In this paper we propose an experimental study of various normalization techniques with heterogeneous data distortion.

The rest of the paper is organized as follows. Section 2 provides related literature in privacy preserving data mining, section 3 elaborates the proposed work with the flow chart. Experimental study is tabulated and also graphically represented in section 4. Section 5 gives the conclusion of the work.

2. Related Literature
Several methods have been proposed in the area of privacy preserving data mining to come across the problems caused by excessive data mining and to protect the privacy. The primary classification of this includes anonymization, perturbation and cryptographic techniques. Anonymization is a process of de-identifying the original data with semantically meaningful substitution. Various techniques K-Anonymity [5][6], L-diversity [7], t-closeness [8], comes under this category. In the perturbation approach the data is being modified by including noise component [9][10]. In [10] random data perturbation technique is proposed and they have also shown the construction of original data distribution and building a data model with acceptable deviation. The existing perturbation techniques follow one-size-fits-all approach which is relatively inflexible. To enhance the existing perturbation methods another work proposed in
[11] has performed the perturbation at two different levels with different intervals.

Privacy preserving techniques can be proposed in accordance with the data mining technique being applied. Privacy preserving data clustering by data transformation is implemented in [12][13]. K-means clustering on vertically partitioned data in a privacy preserving manner is proposed in [14]. Privacy preserving data classification is studied in [15]. First the data transformation is performed and then the classification model is built on the distorted data. Its accuracy is measured with distorted data against original data. Privacy preserving association rule mining is implemented in [16]. These methods illustrate the procedure of hiding the sensitive rules by decreasing association of the extracted rules.

This part of work mainly aims at to study the effectiveness of data modification through perturbation techniques. A proper evaluation of perturbation techniques shows a better performance than other categories in terms of accuracy and computational time. The work proposed in [11] has motivated us to perturb the data values in a heterogeneous manner. The quality of data distortion is measured in terms of various utility and privacy measures [17][18]. Privacy gain and information loss are two important factors have to be maintained with a proper balance. The roles involved in the data sharing scenario can fix their thresholds for data utility and privacy levels. This work performs the data distortion with three different transformation techniques and evaluates their performance with various measures. In addition to the normal way of data transformation the heterogeneity component is also introduced.

3. Proposed Work
In this section we illustrate our work with the flowchart given in figure 1. One privacy level fits for all approach is not suitable for better privacy protection and data utility. In this regard we proposed a new heterogeneous data distortion in our earlier work [19][20]. Our earlier work has categorized the data into three various classes namely High, Medium and Low. In order to perform this categorization we proposed a different privacy analysis approach. In that process it uses the privacy preference of the owner, privacy decision of the collector and existing correlations. Using these validations, the data could be mapped to any of the available classes. Then accordingly the perturbation with various threshold levels is introduced. We recommend the readers to go through our earlier work proposed in [19] to know more about this privacy mapping.

As a part of this research, after the data mapping to privacy classes various normalization techniques are applied to perform the data transformation. We have evaluated the performance of heterogeneous data distortion with Min-Max normalization, Z-Score normalization and decimal scaling. A scaling factor known as privacy threshold is also added accordingly to each of the class. After the data gets transformed it has to preserve some properties to prove its effectiveness in data utility and privacy protection with an acceptable deviation. In order to do this various statistical measures are evaluated on transformed data against original data.

![Flow Chart of Proposed Work](image-url)
3.1 Min-Max Normalization

Min-Max normalization transforms the attribute data to fit into a specific range.
For example, a value $A$ to $B$ which fits in the range $[C, D]$

$$B = \frac{A - \text{minimum value of } A}{\text{maximum value of } A - \text{minimum value of } A} \cdot (D - C) + C$$

Equation 1

3.2 Z-Score Normalization

The Z-score normalization linearly transforms the data in such a way that the mean value of the transformed data equals to 0 and their standard deviation is equal to 1.

The values for an attribute, $A$, are normalized based on mean $\mu_A$ and $\sigma_A$

A value, $x$, of $A$ is normalized to $x'$ using the following transformation formula

$$X' = \frac{x - \mu}{\sigma}$$

Equation 2

Where

- $X'$ - transformed data
- $X$ - data to be transformed
- $\mu$ - Mean of attribute
- $\sigma$ - Standard Deviation of attribute

3.3 Decimal Scaling

Decimal scaling transforms the data into a range [-1, 1]. It normalizes by moving the decimal point of values of attribute A.
The transformation formula is

$$V' = \frac{v}{10^j}$$

Equation 3

where $j$ is the smallest integer such that $\text{Max}(|V'|) < 1$.
The normalization process usually changes the original data quite a bit and we can choose the desired transformation technique depending upon the acceptable deviation.

3.4 Statistical Measures

Every data modification process has to be evaluated carefully. The drastic change may negatively affect the data utility and less change will give the same on privacy. Hence both the properties have to be preserved in a balancing manner. The following properties shown in table [1] are used to perform this evaluation.

### Table 1: List of Measures

<table>
<thead>
<tr>
<th>Distortion Measure</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>$\mu = \frac{\sum X}{N}$</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>$\sigma = \sqrt{\frac{\sum (X-\mu)^2}{N}}$</td>
</tr>
<tr>
<td>Signal to Noise Ratio</td>
<td>$\text{SNR} = \frac{\mu}{\sigma}$</td>
</tr>
<tr>
<td>Mean Square Error</td>
<td>$\text{MSE} = \frac{1}{N} \sum_{i=1}^{N} (\mu - X)^2$</td>
</tr>
<tr>
<td>Mean Absolute Error</td>
<td>$\text{MAE} = \frac{1}{N} \sum_{i=1}^{N}</td>
</tr>
<tr>
<td>Utility Measure</td>
<td>Equation</td>
</tr>
<tr>
<td>Information Loss</td>
<td>$(N-O) / (U-L)$</td>
</tr>
</tbody>
</table>

3.5 Information Loss Metric (IL)

A new metric is proposed to measure the information loss. The basic idea is drawn from the metric proposed in [21]. In the proposed work the data distortion is performed at various classes, hence a variant of existing metric is imposed to measure the information loss in each of the privacy class.

$$\text{II}_{\text{class}} = \frac{(N_h - X_h)}{(U_h - L_h)} \text{ ...Equation 4}$$

where

- $N_h$ - New Distorted Data
- $X_h$ - Original Data
- $U_h$ - Max Value in Class $h$
- $L_h$ - Min Value in class $h$

The amount of data distortion can be performed on the basis of information loss metric value. If the $\text{II}_{\text{attribute}}$ measure returns a ‘0’ then it means that there is no distortion and if it is ‘1’ it implies full distortion. The administrator has to take proper decision to fix this parameter and thus decides to what extent the data utility and privacy can get compromised. This measure hopefully helps us to provide a balancing factor between the data utility and privacy.

![Figure 2 Information Loss Vs Data Utility](https://sites.google.com/site/ijcsis/)

---


ISSN 1947-5500

https://sites.google.com/site/ijcsis/
4. Experimental Consideration

This section gives the detailed result analysis. Our experiment is performed on three different data sets given in table 2. The illustration with sample data is given in table 3.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Attributes</th>
<th>Instances</th>
<th>Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult Data Set</td>
<td>14</td>
<td>32561</td>
<td>2</td>
</tr>
<tr>
<td>Liver Data Set</td>
<td>7</td>
<td>345</td>
<td>2</td>
</tr>
<tr>
<td>Income Data Set</td>
<td>9</td>
<td>100</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 3: Sample Data

<table>
<thead>
<tr>
<th>Original Data</th>
<th>Data with Min-Max</th>
<th>Data with Z-Score</th>
<th>Data with Decimal Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>61.66667</td>
<td>61.71636</td>
<td>67</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
<tr>
<td>20</td>
<td>18.5</td>
<td>21.33601</td>
<td>22.5</td>
</tr>
<tr>
<td>75</td>
<td>77.66667</td>
<td>77.40625</td>
<td>83.5</td>
</tr>
<tr>
<td>25</td>
<td>23.83333</td>
<td>26.68612</td>
<td>28</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
<tr>
<td>36</td>
<td>35.56667</td>
<td>38.45636</td>
<td>40.1</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
<tr>
<td>45</td>
<td>45.16667</td>
<td>48.08655</td>
<td>50</td>
</tr>
<tr>
<td>25</td>
<td>34.5</td>
<td>37.38634</td>
<td>39</td>
</tr>
<tr>
<td>66</td>
<td>68.06667</td>
<td>67.99232</td>
<td>73.6</td>
</tr>
<tr>
<td>76</td>
<td>78.73333</td>
<td>78.45224</td>
<td>84.6</td>
</tr>
</tbody>
</table>

Result analysis is carried on three different transformations and finally checked with various measures. In this work we proposed a new information loss metric for evaluating the amount of data reduction. The administrator can check the value and accordingly can fix the threshold parameter.

Table 4: Metric Evaluation

<table>
<thead>
<tr>
<th>Adult Data Set</th>
<th>Original Data</th>
<th>Data with Min-Max</th>
<th>Data with Z-Score</th>
<th>Data with Decimal Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>59.6</td>
<td>61.0733</td>
<td>61.88</td>
<td>66.39333</td>
</tr>
<tr>
<td>Signal to Noise Ratio</td>
<td>2.80921</td>
<td>2.6715</td>
<td>2.88926</td>
<td>2.817</td>
</tr>
<tr>
<td>Mean Square Error</td>
<td>420.1066</td>
<td>487.785</td>
<td>428.1477</td>
<td>518.43129</td>
</tr>
<tr>
<td>Mean Absolute Error</td>
<td>18.266</td>
<td>19.70678</td>
<td>18.35003</td>
<td>20.31567</td>
</tr>
<tr>
<td>Sum of squared error</td>
<td>6301.6</td>
<td>7316.786</td>
<td>6422.21549</td>
<td>777.46932</td>
</tr>
</tbody>
</table>

The graphical representation given above on three transformations proved that our data preordering technique showed desirable performance with respect to all metrics with different amounts of deviations. The deviation rate is high in decimal scaling followed by Min-Max followed by Z-score.

Table 5: Comparison of original and perturbed data sets on Adult Data Set

<table>
<thead>
<tr>
<th>Adult Data Set</th>
<th>Original Data</th>
<th>Data with Min-Max</th>
<th>Data with Z-Score</th>
<th>Data with Decimal Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>38.57689</td>
<td>38.46562</td>
<td>40.57101</td>
<td>43.14101</td>
</tr>
<tr>
<td>Signal to Noise Ratio</td>
<td>2.82869</td>
<td>2.6366</td>
<td>2.84017</td>
<td>2.83719</td>
</tr>
<tr>
<td>Mean Square Error</td>
<td>185.9812</td>
<td>212.8346</td>
<td>204.04737</td>
<td>231.20159</td>
</tr>
<tr>
<td>Mean Absolute Error</td>
<td>11.18829</td>
<td>12.02336</td>
<td>11.66317</td>
<td>12.52910</td>
</tr>
<tr>
<td>Sum of squared error</td>
<td>6041785.34</td>
<td>6914144.96356</td>
<td>6628862.79591</td>
<td>7510814.71635</td>
</tr>
</tbody>
</table>

Figure 3 Comparison Plot for MAE

Figure 4 Comparison Plot for MSE
Table 6: Comparison of original and perturbed data sets on Liver Data Set

<table>
<thead>
<tr>
<th>Liver Data set</th>
<th>Original Data</th>
<th>Data with Min-Max</th>
<th>Data with Z-Score</th>
<th>Data with Decimal Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>44.74614</td>
<td>46.39698</td>
<td>47.04387</td>
<td>49.92401</td>
</tr>
<tr>
<td>Signal to Noise Ratio</td>
<td>2.76384</td>
<td>2.75789</td>
<td>2.84697</td>
<td>2.76346</td>
</tr>
<tr>
<td>Mean Square Error</td>
<td>261.66111</td>
<td>282.53992</td>
<td>272.58098</td>
<td>325.81152</td>
</tr>
<tr>
<td>Mean Absolute Error</td>
<td>13.31455</td>
<td>13.93772</td>
<td>13.34759</td>
<td>14.95953</td>
</tr>
<tr>
<td>Sum of squared Error</td>
<td>152548.42596</td>
<td>164720.77071</td>
<td>158914.71141</td>
<td>189948.11821</td>
</tr>
</tbody>
</table>

Table 7: Comparison of original and perturbed data sets on INCOME Data Set

<table>
<thead>
<tr>
<th>INCOME Data set</th>
<th>Original Data</th>
<th>Data with Min-Max</th>
<th>Data with Z-Score</th>
<th>Data with Decimal Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>58.57576</td>
<td>59.9202</td>
<td>60.94132</td>
<td>65.20606</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>17.90627</td>
<td>19.36656</td>
<td>17.94544</td>
<td>19.96342</td>
</tr>
<tr>
<td>Signal to Noise Ratio</td>
<td>3.27124</td>
<td>3.094</td>
<td>3.39592</td>
<td>3.26628</td>
</tr>
<tr>
<td>Mean Square Error</td>
<td>317.39578</td>
<td>371.27505</td>
<td>318.78573</td>
<td>394.51239</td>
</tr>
<tr>
<td>Mean Absolute Error</td>
<td>15.75814</td>
<td>17.07966</td>
<td>15.63114</td>
<td>17.60491</td>
</tr>
<tr>
<td>Sum of squared Error</td>
<td>31422.18186</td>
<td>36756.23034</td>
<td>31559.78681</td>
<td>39056.72634</td>
</tr>
</tbody>
</table>

Table 8: Information Loss on Adult Dataset

<table>
<thead>
<tr>
<th>Feature</th>
<th>Privacy Class</th>
<th>Information Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGE</td>
<td>Class 1</td>
<td>0.11764</td>
</tr>
<tr>
<td></td>
<td>Class 2</td>
<td>0.18518</td>
</tr>
<tr>
<td>Hour-per-Week</td>
<td>Class 1</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td>Class 2</td>
<td>0.102564</td>
</tr>
</tbody>
</table>

Figure 5 Graphical Representation on Mean

Figure 6 Graphical Representation on Mean Square Error

Figure 7 Graphical Representation on Information Loss on Adult data
3. Conclusion

In this paper we proposed a comparative analysis of various data transformation techniques with heterogeneous data distortion method. The techniques namely Min-Max, Z-Score, and decimal scaling have been applied to transform the data for privacy protection. These normalizations are applied at various privacy classes. The distorted data is evaluated against various distortion measures and privacy measures. A new privacy measure is implemented to measure the level of data distortion in each of the privacy class. The administrator can take the decision on amount of noise to be added depending upon the information loss metric. All the three transformation techniques have performed in accordance to the data perturbation with different data deviation rates. We conclude that our proposed method for data categorization into various privacy classes can be adoptable to any distortion and thus enhances the privacy protection. Results have shown that proposed heterogeneous data perturbation provides better privacy.

References


Image compression using clustering algorithms

Lale Fathi Ajirlou
Department of Computer
Germi Branch, Islamic Azad University
Germi, Iran

Seyed Naser Razavi
Department of Computer Engineering,
Faculty of Computer,
University of Tabriz,
Tabriz, Iran

Abstract—there is a correlation between pixels in each image so that each pixel value of adjacent pixels can be guessed. By removing these dependencies can be compressed images. Our goal is to reduce the amount of compressed image data needed to display the digital images and therefore reduce the cost of transmission and storage. Compression has a key role in many important applications. These applications include image database, transmission of images, remote sensing, medical imaging, military and space equipment remote control and so on. In addition to the compression, image coding, there's talk. That after quantization matrix should be coded range of conversions. In reconstruction after decoding to achieve our desired image obtained with the difference that the picture is far less than the original image. What we've done in this thesis using a fractal method utilizes a Kohonen neural networks and clustering to increase the compression ratio and reduction coding and decoding the image. We have implemented three methods based on fractal coding. The first method is simple fractal coding. In the second method to create the codebook of multiple tree fractal coding is used. In the second method of vector quantization LBG algorithm for Kohonen neural network-based clustering algorithm and code book for coding image is used. Results in the second method show faster encoding. The method is simple fractal compression rate is higher than other methods.

Keywords: image compression; clustering; vector quantization

I. INTRODUCTION

Image compression is the application of data compression on digital images. In effect, the objective is to reduce redundancy of the image data in order to be able to store or transmit data in an efficient form [1]. Data compression has become requirement for most applications in different areas such as computer science, Information technology, communications, medicine etc. In computer science, Data compression is defined as the science or the art of representing information in a compact form [2].

Image processing systems can compress raw images with the resolution and quality desired. Nowadays and thus to achieve different levels of compression as applicable. The compression ratio can be changed depending on the intended application. This need has always existed. For example, it is possible to transmit real-time images and video via packet-switched networks.

High quality images are obtained from the studio, medical images, satellite imagery and scanned images of manuscripts in order to preserve historical monuments.

They need to compress because of the immense size for storage, maintenance, as well as sending via communications equipment with limited bandwidth. For this purpose, the resolution and bit rate compressed images decrease as much as the eye does not recognize.

Image compression, is processing that eliminates additional information, reduces data into digital signals.

This process depending on the bandwidth required for data transmission and storage, to reduce additional information. Reducing the bandwidth required to transfer more data at the same time.

Compression methods remove duplicate information in the image and with suitable encoding techniques reduce the size of image files. Dhawan et al. (2011) reviewed and discussed about the image compression, need of image compression, its principles, classes and various algorithm of image compression. They mainly worked over gray scale images of Lena and finger print images[3].

Compression methods can be divided into two groups. Lossy compression and lossless compression.

Lossless compression tries to have the least amount of change in image quality

However, in lossy compression due to the loss of parts of the picture finally compressed image will be lower quality. So, according to intended use can be determined compression type.

In this paper compression based on clustering that the purpose of this paper is that the images are divided into several groups, and in this division images, different groups should be as different as possible together and images contained in a group must be very similar.

Clustering method is used to analyze the data relating to distances of between the border and the center of gravity and angles between the distances of the images.

K-means is one of the most used clustering algorithms which word of K in the name of the algorithm refers to the fact that the purpose of this algorithm is to find a fixed number of clusters

According to the data points is near which is based on image compression using the k-means algorithm is implemented. The algorithm has two major drawbacks: First, algorithm is depend on the initial values of the number of the cluster and capitals clusters Second, it is easily trapped in local optimum and therefore does not generate the optimal
solution. The method of fractal is another method which used features of self-similarity in the image.

The advantage of this method is a high compression ratio, good mathematical structure for speed coding and decoding. The drawback of the Fractal method is that the coding time in this method is high. In this paper, vector quantization coding of a clustering algorithm based on Kohonen self-organizing map is used to improve the image. The simulation results on the images, shows that this method of coding time reduced, no significant change in the reconstructed image quality and compression ratio. Simulation in this paper is done using MATLAB software. Using clustering enables us instead of processing massive amounts of images, only image review and analysis that are very similar and this is a big step for simplifying the problem.

The processing is only reducing the coefficients of each block DCT 8 * 8, have proposed according to the objective function to minimize energy consumption and maximize the lifetime of the system, and states image quality[Abou-Chadi, 2011][2].

Analysis of each component of DCT blocks show that image quality and power consumption are two opposite effects, the image is segmented regions of interest, and is expressed to different parts of different sizes[4].

II. MATERIALS AND METHODS

In this paper, three-step simulation done and these steps are separately. The reason for this was to do a comparison between the proposed methods with other methods. Initially, fractal coding method is implemented simple. In the next step, method of fractal coding has been implemented along with algorithm multiple tree. In last method, it was used Fractal coding algorithms with Kohonen self-organizing neural networks based on clustering algorithm implementation. In terms of compression is carried out two operations of coding to compress and decoding compressed image reconstruction. The more we can raise the compression ratio so that the difference between the original image and the coded image is low (better image quality) results will be satisfactory.

Since the method of Fractal coding used to Image Compression, because of the high coding, Fractal coding method makes have more computational cost. The reason for this is that the coding process used for each block, the block area searches for the best ambiguous and finally some parameters of similarity between good block board and similar domain block is used to encrypt blocks.

In the first stage of book, code can be built where each block book, code displayed an index and in the second stage takes place coding, it means which each image block corresponding with a book-index the code. Continue to increase time of coding were discussed Kohonen network clustering.

Implementation of this process is used of a laptop with core i7 processor with RAM 4 GB. Implementations were done Version 2014 in MATLAB environment.

III. THE STUDY OF IMPLEMENTATION RESULTS

Initially, the results of simple fractal coding algorithm have examined. As well as seen in Figure 1-4, image is used of a size of 255 x 258 for image compression.

As expected, coding and decoding time algorithm for operation is fairly long. In addition, the compression rate is higher.

![Original image](https://sites.google.com/site/ijcsis/) ![Reconstructed image](https://sites.google.com/site/ijcsis/)

**Figure 1.** Output from a simple fractal coding method

Running time algorithm take 1046 seconds which is slightly more running time and for the on-line cases can not be a good algorithm. As well as, the of PSNR values is obtained 27.4698 by this method. PSNR value of this method compared to other methods proposed in other research show that this method has better rate of compression.

![Original image](https://sites.google.com/site/ijcsis/) ![Reconstructed image](https://sites.google.com/site/ijcsis/)

**Figure 2.** Output from a simple fractal coding method with a running time algorithm of 540 seconds.

Running time algorithm take 540 seconds which is slightly more running time and for the on-line cases can not be a good algorithm. As well as, the of PSNR values is obtained 34.18 by this method.
Running time algorithm take 240 seconds which is slightly more running time and for the on-line cases can not be a good algorithm. As well as, the of PSNR values is obtained 34.18 by this method. It used multiple trees to solve of problem of a method of simple fractal coding. It is used to the image segmentation and creating a block for coding. This segmentation is important which is presented simple fractal coding method using small blocks with a lower compression ratio, although larger block sizes increase the compression rate and makes the reconstructed image is of lower quality.

Running time algorithm take 244 seconds which shows change quite dramatically compared with fractal coding algorithm. As well as, the of PSNR values is obtained 25 by this method. PSNR value is slightly lower in this method than before. But coding and decoding time is dramatically reduced.

In the next stage, it was used Kohonen self-organizing neural networks in purposing of reducing of coding and decoding time. The results showed that the algorithm can also reduce the time and also maintain image quality.

Running time algorithm takes 30 seconds which shows decreased compared with the previous two method. As well as, the of PSNR values is obtained 24 by this method.

PSNR value is slightly lower in this method than before, but the time of coding and decoding has been reduced.
Figure 8. The output of SOM- method and vector quantization based clustering with a running time algorithm of 120 seconds.

Running time algorithm take 120 seconds which is slightly more running time and for the on-line cases can not be a good algorithm. As well as, the of PSNR values is obtained 33.16 by this method. The results showed which coding time is reduced no significant decrease in the quality of the reconstructed image. The following table show comparison of the methods implemented in this paper.

Table 1. Compares results between techniques implemented

<table>
<thead>
<tr>
<th>Method</th>
<th>Coding Time</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fractal method</td>
<td>1046</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>540</td>
<td>34.18</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>34.18</td>
</tr>
<tr>
<td>Fractal and Multiple trees</td>
<td>44</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>220</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>110</td>
<td>33</td>
</tr>
<tr>
<td>SOM- method and vector quantization based clustering</td>
<td>30</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>120</td>
<td>33.16</td>
</tr>
<tr>
<td></td>
<td>83</td>
<td>30.65</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

In this study, with the aim of increasing the compression ratio, which makes to reduce the image size, is reduced. So that the image quality is not significantly different than the original image and also aims to reduce the time coding and decoding image, it used three different ways to implement. Finally, it was compared them with each other. It was observed that simple fractal coding method image reconstruction time is better quality, although coding and decoding time is very high in this method. This problem makes the changes to the algorithm which maintains the quality reconstructed image, as well as can be reduce the time. Multiple tree algorithms could well reduce this time. This algorithm could with creating of suitable book to well reduce speed in coding and decoding algorithms. In last stage, it was used Kohonen self-organizing neural networks based on clustering algorithm have provided a further reduction of time. While by obtaining a measure of PSNR be able to measure the quality of output image. The results showed which coding time is reduced no significant decrease in the quality of the reconstructed image.

REFERENCES

Abstract—IEEE 802.15.4 standard is widely adapted for Body Area Sensor Networks (BANs) due to its low duty cycle and low power operation. However, IEEE 802.15.4 recommends the use of fixed duty cycle operation which results in high energy consumption and end-to-end delay. Therefore, an efficient algorithm is needed to adapt duty cycle operation to overcome the end-to-end delay and energy consumption. In this paper, we propose a Joint Duty Cycle algorithm (JDCA) for the BAN to enhance the network lifetime, throughput and decrease the end-to-end delay. Dynamic duty cycle can be adapted by the two MAC parameters: Beacon Order (BO) and Super frame Order (SO). However, these parameters are set by the network administrator before the network deployment. During simulation, JDCA algorithm is capable of adapting dynamic duty cycle at run time based on traffic load. Furthermore, simulation results show enhanced network lifetime, network throughput and less end-to-end delay when compared with IEEE 802.15.4.

Index Terms—Dynamic duty cycle, IEEE 802.15.4, Body area sensor networks, Wireless personal area network.

I. INTRODUCTION

The IEEE 802.15.4 [1] is a wireless technology widely adapted for low rate Wireless Personal Area Networks (WPANs). IEEE 802.15.4 based application ranges from: home automation, industrial automation, intrusion detection, agriculture monitoring and body area sensor networks.

Fig 1 shows a WBAN infrastructure for medical and non-medical applications. The nature of data reported by BAN devices can be on-demand, emergency and periodic. On-demand traffic is used by the doctors for the purpose of diagnostic; this traffic is normally requested by the doctor or observer of the patient. This is further divided into Periodic data traffic and continuous data traffic. Periodic traffic can be sent by the sensor after some interval of time, possibly when a node have some data to send (when information is required occasionally). Continuous traffic is sent by the sensor node continuously; such as Continuous Glucose Monitoring. Emergency traffic is totally unpredictable and is initiated by the source nodes when exceeds from a threshold value. Whereas, the normal traffic is generated by source nodes in a routine condition. PAN coordinator collects the normal routine data of a patient and proceed for further processing with no time critical and time bound requirements. The PAN coordinator is further connected to telemedicine, server for relevant recommendations. At the end the data is given to the care giver to monitor the health relevant conditions and then treated accordingly as per the need.
results and critical analysis of JDCA and IEEE 802.15.4, whereas, the last section concludes this paper.

II. IEEE 802.15.4 OVERVIEW

This section discusses the beacon enabled mode of IEEE 802.15.4. IEEE 802.15.4 is a protocol which support Internet of Things (IoT) based applications widely [3].

IEEE 802.15.4 is being widely adapted communication protocol for Internet of Things (IoT) based applications. These application ranges from smart university, home automation, and industrial automation, agriculture monitoring weather monitoring and smart tracking of objects [4]. To form an IEEE 802.15.4 based communication network there are two types of network devices: Fully Functional Devices (FFDs) and Reduced Functional Devices (RFDs). FFDs have more capability in terms of energy, topology maintenance, and communication control and for network organization. Due to their functionality FFDs are also called Personal Area Network (PAN) controllers. Whereas, RFDs devices has less functionality as compared to the FFDs. RFDs can only communicate with the FFDs. These devices together can form star, peer-to-peer or tree topology shown in figure 2. In star topology, the end devices are connected to the one main controller, usually called “PAN coordinator”. The PAN coordinator usually transmits beacons to the connected devices to send data to the PAN coordinator and synchronization.

IEEE 802.15.4 is operated in two modes of communication: Beaconless and Beacon-enabled mode. Beaconless mode is used where we do not need any energy constraints. On the other hand, beacon-enabled mode is used in networks where energy, throughput and delay are the primary concerns. Figure 3 represents the detailed overview of the two modes of communication based on IEEE 802.15.4. A super-frame structure is used by the PAN coordinator in a beacon-enabled mode for the purpose of data communication. Super frame structure is bounded by beacons as shown in figure 6.3. The super frame structure is divided into two main portions: active and inactive portions. The Inactive portion is the time period where nodes and PAN coordinators stay in sleep mode which is usually called the low power mode. Active portion is further divided into two portions i.e. Contention Access Period (CAP) and Contention Free Period (CFP). CAP is the time duration which is divided into 16 time slots of equal length. A single slot duration is equal to 60 symbols. CAP portion is depicted by the super frame duration (SD). SD depends on the value of the super frame order (SO) while beacon order is identified by the Beacon Interval (BI). Whereas, CFP is an optional mode of communication, which uses guaranteed Time Slots (GTSs). GTS is used for those application which requires the guaranteed bandwidth for specific period of time.
The BI, SD, DC and sleep period can be calculated by the below equations.

\[ aBaseSuperFrameDuration = aBaseSlotDuration \times aNumSuperSlot \]  

(1)

\[ BI = aBaseSuperFrameDuration \times 2^{SO} \quad (0 \leq BO \leq 14) \]  

(2)

\[ SD = aBaseSuperFrameDuration \times 2^{SO} \quad (0 \leq BO \leq 14) \]  

(3)

\[ Sleep \ Period = BI - SD \]  

(4)

\[ Duty \ Cycle = DC = \frac{SD}{BI} \]  

(5)

III. RELATED WORK

This section briefly surveys the existing dynamic BO and SO adjustment schemes in the area of body area sensor networks. In existing literature, few efforts are focused at improving the performance of IEEE 802.15.4 based beacon-enabled networks by altering only one of the MAC layer parameters, either BO or SO or both simultaneously.

The Beacon Order Adaptation Algorithm (BOAA) [5] and Individual Beacon Order Adaption Algorithm (IBOAA) [6] use BO adjustment for power saving purposes. These schemes increase the sleep mode of nodes by increasing BI during idle network state. However, by fixing SO at a smaller value, the overall throughput is decreased and latency of information delivery is increased. This is because of greater inactive portion within the super-frame as compared to active portion. Therefore, BOAA [5] and IBOAA [6] does not perform efficiently when the traffic nature is unpredictable.

The Duty Cycle Algorithm (DCA) [7] adjusts duty cycle by fixing BO, so it does not meet real time data requirements. The Dynamic Super-frame Adjustment Algorithm (DSAA) [8] alters only SO parameter, with the primary goal of energy consumption. In [8], the active duration within super-frame is changed when application requirements are not meet by current SO. The PAN coordinator dynamically adjusts the duty cycle by adapting SO whereas, the BO is kept fixed, as a result packet delivery delay is increased. In [9], the coordinator detect congestion by increased contention during the active period and control congestion by dynamically setting SO according to current network conditions. Although, congestion is controlled but the BO and SO values are not considered for decreasing duty cycle. Also, this solution [9] increases the delay of information delivery under certain network conditions.

In [10], the Markov-base theoretical analysis is proposed for energy saving and to meet the application requirements. However, this model is designed by considering fixed network traffic patterns and require fine tuning of different variables. This model [10] is not validated using simulations or test beds.

Duty Cycle Self-Adaptation Algorithm [11] modifies the duty cycle based on adjusting both BO and SO parameters in IEEE 802.15.4. In the DBSAA algorithm [11], the CAP portion is adjusted in a star topology under beacon enabled mode operation. DBSAA is based on the findings presented in [7]. DBSAA algorithm is based on these three steps; firstly, DBSAA estimates network load, secondly it determines changes in the network load, thirdly calculates a factor α which assigns the number of BI that the coordinator should wait before applying the DBSAA Algorithm.

Load Adaptive MAC protocol (LA-MAC) [12] proposed for the body area sensor network based on IEEE 802.15.4 by considering these parameters: traffic load, number of source members participating in communication and network delay. This primary goal of this protocol to adjust the BO and SO in a star topology to enhance the network life time of the network. The algorithm adapts the BO and SO at run time based on the above parameters. LA-MAC [12] shows enhanced network performance in terms of energy consumption, end-to-end delay and network throughput.

In [13, 14], the algorithm goals to adjust both BO and SO based on traffic load to enhance the network throughput. The algorithm works in three major steps: First, TDSA calculates the expected SO based on the data rate generated by source nodes. Secondly, the TDSA waits for three consecutive BI intervals to alter the SO and BO based on the network requirements. Finally, the network delay is checked to further enhance the SO value if the previous SO does not guarantee the maximum network throughput and network delay. However, this algorithm consumes more energy as it achieves its primary goal of network throughput by adjusting both the BO and SO simultaneously.

IV. JOINT DUTY CYCLE AND OPTIMAL ENERGY ADAPTATION ALGORITHM

This section describes the proposed algorithm called joint duty cycle and optimal energy adaptation algorithm (JDCA). The detailed working of JDCA is shown in figure 5.

In this algorithm the PAN coordinator is responsible for the duty cycle and optimal energy adjustment and values of these parameters are calculated after every BI. When the nodes in the network are not communicating and network is in idle state, default values of BO and SO are used (BO\text{Default} = 4 and SO\text{Default} = 2). Smaller values of SO as compared to BO is used to decrease the energy consumption during the idle network time. The detailed working of algorithm is explained in the rest of this section.

Initially the \( S_{\text{Next}} \) is determined for the next BI by the following equation:

\[ S_{\text{Next}} = SN \times \text{NumPkt} \times \text{NumPktSize} \times \text{PktTransmissionTime} \]  

(6)

In the above equation (6) the \( SN \) represents the Number of source nodes. \( \text{NumPkt} \) is the number of packets that a single source node can generate. \( \text{NumPktSize} \) is the size of the single packet \( \text{PktTransmissionTime} \) is the time the time required for a single packet delay from the source node to destination node.
Then the $SO_{Next}$ is checked whether it is equal to zero or not, if it is equals to zero it means there is no network activity. Thus, the communication is carried out with a default $SO = 2$ to conserve less energy whereas, $BO$ is decremented by 1 to decrease the length of BI for the next interval to avoid disassociation of nodes during no network activity.

On the other hand, when $SO_{Next}$ is not equals to zero, then it checks the network load. A suitable $SO_{Next}$ is chosen based on the data traffic and number of source nodes.

Furthermore, the receive ratio is checked with a predefined threshold. Receive ratio is computed based on the following equation:

$$PAN_{RecvRatio} = \left( \frac{NumPktTotal}{SN \times NumPkt} \right) \times 100$$  (7)

In the equation (8) $NumPktTotal$ is the total number of received packets at PAN coordinator.

In case, the $PAN_{RecvRatio}$ is greater than the threshold, then $SO_{Next}$ becomes the $SO_{Cur}$ and $BO_{Previous}$ becomes the next $BO$ for communication. It is because the network requirements are met and both $BO$ and $SO$ does not need to be altered. However, when $PAN_{RecvRatio}$ is less than the defined threshold value, $SO_{Cur}$ and $BO$ is incremented by 1 respectively to increase the super-frame duration for the next interval to meet the network requirements.

V. RESULTS AND DISCUSSIONS

In this section, the detailed performance of proposed algorithm is evaluated against IEEE 802.15.4. Comparisons are based on packet delivery ratio, throughput, energy consumption and end-to-end latency. The simulation analysis is performed using network simulator NS-2 [15].

![Fig 6. Simulation setup](https://sites.google.com/site/ijcsis/)

The network is configured based on star topology and nodes communicate with PAN coordinator in a beacon enabled mode. The simulation setup is shown in figure 6. There are 5 nodes randomly positioned in 15 meter radio range with PAN coordinator placed in the middle. To have more realistic and actual results we used the ATMEL mote [16] for node’s energy model. The rest of simulation setting are shown in table 1.

Throughput of JDCA and IEEE 802.15.4 is shown in figure 7. In figure 7 the overall data rate is 100kbps for both JDCA and IEEE 802.15.4. It is observed that IEEE 802.15.4 performs the same at IFQ length = 10, 20, 30, 40 and 50 but does not reach the performance of JDCA. It is because, the IEEE 802.15.4 uses fixed $BO$ and $SO$ which results in degraded network performance. However, JDCA outperform IEEE 802.15.4 in all cases due its dynamic behavior of duty cycle adjustment regardless of IFQ length.
Figure 8 shows the average receive ratio of JDCA and IEEE 802.15.4. It can be seen from the figure that dynamic duty cycling of nodes results in enhanced performance as compared to IEEE 802.15.4. Therefore, JDCA manages the super-frame structure according to the traffic and increase or decrease the BO and SO values at run time when receive ratio is observed less at PAN coordinator.

End-to-end delay for the JDCA and IEEE 802.15.4 is shown in figure 9 at the PAN coordinator against interface queue length. A decrease in end-to-end delay is observed with the increase of SO from 2 to 5. Therefore, as the super-frame duration is increased the packet delivery of packets are increased as a result decrease in end-to-end latency is observed. However, when the results of IEEE 802.15.4 is compared with JDCA, it outperforms IEEE 802.15.4 because of its dynamic behavior.

Figure 10 shows the per bit energy consumption of JDCA and IEEE 802.15.4. The energy consumption observed decreased with the increase of SO value. This is just because of less duty cycle of nodes. However, the energy consumption at BO=6, SO=2 is high because of frequent beacons transmission. On the other hand, JDCA performs the same in all cases. Therefore, JDCA is capable of adapting optimal values of both BO and SO values for the network to conserve less energy. Furthermore, when no network activity is observed, JDCA shifts BO and SO to its default values to decrease the energy consumption at maximum level.

VI. CONCLUSION

In this research paper, we proposed an algorithm for the body area sensor network which adapts the duty cycle according to the network requirements to decrease the energy consumption, and end-to-end latency of communication and to enhance the network throughput. PAN coordinator is responsible to compute super-frame duration for the next BI based on traffic load. During no network activity JDCA changes the BO and SO to its default values to conserve less energy. Finally, results show that JDCA performs better than IEEE 802.15.4. In future, JDCA algorithm will be implemented in a multi-hop tree topology.

REFERENCES


Performance Evaluation of High Performance Data Transfer in Grid Environment over Broadband Hybrid Satellite Constellation Communication System

Anupon Boriboon  
Vincent Mary School of Science and Technology,  
Assumption University of Thailand  
Bangkok, Thailand

Siriwhaddhanah Pongpadpinit  
Department of Business Information System,  
Martin de Tours School of Management and Economics,  
Assumption University of Thailand  
Bangkok, Thailand

Abstract—This paper presents the evaluation performance of broadband hybrid satellite constellation communication system (BHSCCS) networks which provides high performance data transfer in grid network environment based on TCP protocols. The evaluated hybrid satellite network uses the COMMStellation™ constellation topology on lower orbital. We adopt the GridFTP to improve network performance. GridFTP is a high-performance, reliable data transfer protocol optimized for high-speed Internet to suitable WAN networks. The simulation results show the network performance of GridFTP which different AQMs, TCPs, PERs, over BHSCCS networks.

Keywords: COMMStellation™; GridFTP; Hybrid Satellite; Queue; TCP

I. INTRODUCTION

Satellite is the only choice for long-haul wireless broadband global area network communication. Some countries with large and/or island geographic areas and/or hard-to-reach areas, such as China, India, Indonesia, are likely to benefit the greatest from satellite broadband. There are a huge big data internet accesses by users. [1] Ever-increasing demands in high-end computing and intensive data exchange, together with the cost effectiveness of high performance commodity systems, have led to massive deployment of compute and storage systems on a global scale. In such Grid-based scenarios, bulk data transfer within and across physically separate clusters or data centers has become an inescapable requirement for scientific data set distribution, content replication, remote data backup, and so forth. Generally, File Transfer Protocol (FTP) is used for handling bulk data transfers. Since the earliest FTP implementation based on Transport Control Protocol / Internet Protocol (TCP/IP), many efforts have been undertaken to improve and extend it. GridFTP, designed specifically for high-bandwidth wide area networks, has appeared as the most popular FTP implementation in the Grid environment.

On the other hand, high-performance interconnections such as InfiniBand (IB) and Gigabit Ethernet/iWARP are rapidly gaining momentum for designing high-end clusters and data centers. In addition to providing high bandwidth and low latency, they provide advanced features, such as zero-copy communication and Remote Direct Memory Access (RDMA), which enable the design of novel communication protocols and libraries. The recent introduction of IB WAN (Wide Area Network) router allows us to extend these capabilities across multiple campuses or even across WAN distances.

Hence, it is the most challenging to implement high performance data transfers in the Grid environment over broadband hybrid satellite constellation communication system. For the future generations of the internet, broadband hybrid satellite access and QoS are surrounded by the most significant issues to be solved.

II. BACKGROUND AND RELATED WORKS

In coherence to this research, we have implemented GridFTP, broadband hybrid satellite network, TCP over satellite, and queue management to analyze the performance evaluation based on the Broadband Hybrid Satellite Constellation Communication System (BHSCCS) topology model.

A. GridFTP

GridFTP [1] is a protocol extension FTP and its existing extensions are used to manage large data transfers across computational grids. GridFTP is a high-performance, secure, reliable extension of the standard FTP data transfer protocol, optimized for high-bandwidth, wide area networks. The Globus implementation of GridFTP provides a software suite optimized for a broad range of data access applications, including bulk file transfer and data extraction from complex storage systems. The following are some of the key advantages of GridFTP which are a) Performance: enhanced performance through use of parallel streams and coordinated data transfers b) Security: PKI/X.509 and SSH-based Grid security c) Robustness: restart markers allowing interrupted transfers to restart with minimal delay overhead d) Extensibility: easy-to-use Open/Close/Read/Write (OCRW) interface to users and applications.

https://sites.google.com/site/ijcsis/  
ISSN 1947-5500
GridFTP relies on Transport Control Protocol (TCP) [2], the most widely used TCP for the Internet as well as computational grids. Such grids are often characterized by networks with large bandwidth-delay products (BDP). Currently, however, the default flow-control parameters in TCP are statically tuned to suit networks with small BDPs, and thus perform abysmally over today’s grid networks with large BDPs.

[2] Tuning of buffer sizes is necessary for maximizing throughput with TCP. For any given connection, the optimal TCP buffer size is equal to the BDP of the connection. Often, grid researchers manually tune the buffer sizes to keep the network pipe full by using diagnostic tools to determine the round-trip time (RTT) and bandwidth of the connections.

In addition of GridFTP, to simulate bulk data transfer the three major parameters defined for the GridFTP simulator are Bandwidth, Parallel, and Ratio. The Bandwidth is used to set the total bandwidth of the satellite link. The Parallel is used to set the parallel GridFTP streams. It is set to 4. The Ratio is used to set the throughput ratio among the parallel streams. By default, it is set to 1:1:1:1, which means that each GridFTP stream will transmit packets at an equal speed.

B. Broadband Hybrid Satellite Network

Broadband satellite systems have been an important component of telecommunications networks for many years serving, in particular, long distance telephony, data, and television broadcasting. The involvement of broadband satellite in Internet protocol (IP) networks is a direct result of new trends in a global telecommunications, where Internet traffic will hold a dominant share in the total network traffic. The large geographical coverage of the satellite footprint and its unique broadcasting capabilities, as well as its high-capacity channel combined with readily available Ka-band spectrum will retain broadband satellite systems as an irreplaceable part of communications systems.

The COMMStellation™ [3] is adopting for implementation in this research. COMMStellation™ is a high-power satellite, with the latest in advanced technology, built by Microsat Systems Canada Inc. (MSCI). The COMMStellation™ group deploy and operate a constellation of 72 satellites plus spares divided into six polar, low earth orbit (LEO) orbital planes at an altitude of 1000 km designed to provide high-speed, global business communications. This is a typical Walker constellation, providing worldwide coverage assuming ground contacts. The bandwidth of satellite is 8.8 Gigabits, uplink, and downlink are 1.1 Gigabits. The key parameter concept for implementation into network simulator is [4]. The COMMStellation™ will be capable of providing high-speed data communications for many applications. Some potential uses of this system for communications include a) Strategic communications for government, military, or corporations b) Special purpose low latency communications, and c) High bandwidth burst data transmission from remote sensors, ships, exploration vessels, sites.

C. TCP over Satellite

Transmission Control Protocol (TCP) is a transport protocol used by many Internet applications for end-to-end reliable data delivery. TCP performs well in terrestrial networks. Given the widespread use of TCP based applications and interconnection with the terrestrial Internet, it is likely that broadband satellite networks will transport large amounts of traffic generated by TCP’s algorithms. The desire to utilize satellite capacity efficiently has led to the development of number of optimized for satellite TCP variants, with altered transmission control behavior. They are run between ground terminals across the satellite link, while other TCP implementation are across the terrestrial Internet [5], [6], [7].

TCP Tahoe [8] being the first implementation of TCP to involve a few new algorithms in early TCP implementations likes Slow Start, Congestion Avoidance, and Fast Retransmit.

TCP New Reno [8] includes a change to the Reno algorithm at the sender end with a view to eliminate Reno’s wait for a retransmit time-out whenever multiple packets are lost from a window. This change modifies the sender’s behavior during fast recovery.

TCP Westwood [9] is a sender-side-only modification to TCP New Reno that is intended to better handle large bandwidth-delay product paths, with potential packet loss due to transmission or other errors, and with dynamic load.

TCP over Satellite on Broadband Hybrid Satellite Network

In Figure 1 is shows the TCP flow data transfer packets into client. The network consists of queue model and error model for realistic situation. We are used this figure to implement our simulation in broadband hybrid satellite network model.

D. Queue Management

Queue management in routers is an important role in taking care of congestion network traffics. Two procedures are adopted to solve the problem. Firstly, is congestion avoidance preventative technique, which comes into play before traffic in network is congested by overloading. Lastly is congestion control, which comes into play after the congestion at a traffic network has appeared and the traffic network is overloaded.

DropTail, it is implements FIFO (First In, First Out) scheduling and drop-on-overflow buffer management, which passive queue management. According to passive queue management, packets are dropped only when the buffer is full.

RED [10] is the most well know queue algorithm. It is Random Early Detection (RED) gateway. Stochastic drops allow RED to avoid global synchronization and unfairness against burst traffic when used in conjunction with TCP based...
flows managed. This moderation maintains a moving average of the queue length to manage congestion. If this moving average of the queue length impostures between a minimum threshold value and a maximum value, then the packet is either marked or dropped with a probability. But if the moving average of the queue length is greater than or equal to the maximum threshold then the packet is dropped. Even though, it tries to keep away from global synchronization and has the ability to accommodate transient bursts, in order to be efficient RED must have sufficient buffer spaces and must be correctly parameterized.

BLUE [11] has been shown to perform significantly better in terms of packets loss rates and buffer size requirements in the network. If buffer overflow causes the queue to recurrently drop packets, BLUE increments the making probability, thus augmenting the rate at which congestion notification is sent back. In addition detail, BLUE maintains a single probability, which it uses to mark or drop packets when they are queued. If the queue is continually dropping packets due to buffer overflow, BLUE increments the marking probability, thus increasing the rate at which it sends back congestion notification. Conversely, if the queue becomes empty or if the link is idle, BLUE decreases its marking probability.

III. TRAFFIC SCENARIOS

Traffic analysis and modeling are integral parts of engineering broadband telecommunications network, including broadband hybrid satellite network systems. The analysis is related with getting statistical properties of the traffic and systematical solutions for the evaluating performance of networks, in terms of different measures such as packet delay. We have also established the presence of self-similarity in many scenarios, which is important for predicting network behavior.

The complexity and dynamics of hybrid satellite networks prevent performance evaluation of GridFTP algorithm using high performance data transfer analytic expression. For testing and analyzing various different packet error rates, various different TCPs protocol, and various different queues algorithm, we have, therefore, developed the GridFTP over broadband hybrid satellite network simulation schematically illustrated in Figure 2. In our experiments, four user station links in different areas around Asia are chosen to observe network traffic. The packet size of GridFTP is 1514 bytes excluding the header size. We run simulation for 100 seconds for all scenarios, and have a full run of GridFTP with maximum user stations both of source and destination.

As for the simulation based on the grid traffic model, we are able to build simulator using NS-2 to accurately replicate the characteristics of the applications we are considering. This simulator is useful in validating our network traffic models and is ultimately released publicly so interested parties are able to evaluate different types of grid traffic in BHSCCS [4] networks.

![Figure 2. The network infrastructure for global area bulk data transfer](image)

IV. RESULTS AND DISCUSSION

Simulations have been used to compare the GridFTP performance of different services employing Transport Control Protocol (TCPs) such as TCP Tahoe, TCP New Reno, TCP Westwood, Active Queue Management (AQMs) such as DropTail, RED, BLUE, Packet Error Rate (PERs) such as 1 - 10 percentiles over BHSCCS system.

Throughput is the main performance measure characteristic, and most widely used. This measures how soon the receiver is able to get a certain amount of data sent by the sender. It is determined as the ratio of the total data received to the end to end delay. Throughput is sometimes different from goodput, because goodput consists solely of useful transmitted traffic, where as a throughput may also include retransmitted traffic. Throughput is an important factor which directly impacts the network performance.

End-to-End delay is the time elapsed while a packet travels from source to destination. The larger a value of delay, the more difficult it is for transport layer protocols to maintain high bandwidths. This characteristic can be specified in a number of different ways, including average delay, variance of delay (jitter), and delay bound.

The research has found out that a principal reason for such high expectations from user station is the amount of throughput in simulation time. The total simulation time of the research is 100 seconds. The simulations are done, the throughput results are shown in Figure 3, 4, and 5 (DropTail, RED, BLUE) respectively; in these figures comparison of the TCP variants’ performance. Each TCP variant has its own advantages or disadvantages. But in this research, we will focus on the most balanced of GridFTP for network performance tradeoffs in the BHSCSS scenario.

The experiment shows the comparison of throughput in different AQMs, TCPs, and PERs schemes over time. The TCP scheme results show an average performance of throughput. The throughputs in Figure 3 TCP Westwood case on DropTail queue are the highest TCP New Reno and TCP Tahoe in any PERs. But, the average throughput performance in RED queue in Figure 4 is the lowest in all dimensions when compared with DropTail queue and BLUE queue in Figure 5. Thus, the results from the analysis of GridFTP application in this simulation is highest average throughput in BLUE queue and TCP Westwood all PERs.
Figure 3. Throughput of GridFTP with Droptail queue

Figure 4. Throughput of GridFTP with RED queue

Figure 5. Throughput of GridFTP with BLUE queue

Figure 6. Average end-to-end delay of GridFTP with Droptail queue

Figure 7. Average end-to-end delay of GridFTP with RED queue

Figure 7. Average end-to-end delay of GridFTP with BLUE queue
The research highlighted the fact that average end-to-end delay time owners must be aware of and must implement fair usage policies in order to prevent bandwidth from being depleted to use bandwidth more productively. Figure 6, 7, 8 are show end-to-end packet delay in different AQMs and PERs.

The total simulation time of this research is 100 seconds. It has 3 TCP flows which start at the beginning of the simulation. A comparison of the TCP variant’s performance with different AQMs and PERs, illustrated Figures 6, 7, and 8.

The end-to-end delay will be reflexive with the throughput; its mean being higher throughput equal higher end-to-end packet either. In illustrated below shows an average end-to-end packet delay in different TCPs and PERs over DropTail, RED, and BLUE queue respectively. The graph shows TCP Westwood has higher end-to-end packet time than others, reflecting the highest throughput in the previous graph. The figures show the network with respect to different PERs. The results are analyzed and a comparison on graphs all the transmitted packets being received successfully, the throughput and end-to-end delay were much affected by the rapid change in queuing of the packets during the fast data transfer. The GridFTP transmission of packet has a positive impact on the throughput but a negative impact on the delay.

In addition, an average end-to-end delay is calculated from median point in increasing the errors in scenario. We have counted the total packets that arrive in destination and successfully transfer bulk data. And, we used same method in the throughput for the median point, too.

V. CONCLUSION

In this research, we have simulated the grid environment using high speed data transfer over broadband hybrid satellite constellation communication system by us network simulation tool. As shown in the results, the AQMs, TCPs, and PERs has an obvious impact on the network performance for high performance data transfer in grid environment. The GridFTP load has been implemented for traffic network load of grid network to investigate efficient ways of dynamically changing on broadband hybrid satellite network communications scenario. In addition, we study the behavior grid environment in a hybrid satellite network to prove the impact quality of services on a network performance.

Finally, it is apparent that evaluated the network performance of the GridFTP with active queue management BLUE queue, and TCP Westwood over hybrid satellite results give an expression of the most viewpoint of higher performance data transfer on broadband hybrid satellite network systems.

REFERENCES


A Lasso-LTS Method for DNA Sequence Classification Based on Beta Wavelet Networks

A. Dakhli, Fellow, IEEE, W. Bellil, and C. Ben Amar, Member, IEEE

Abstract—Wavelet Neural Network (WNN) is attracting interest in field of classification system, because they are universal approximations, particularly due to rapid and accurate representation of nonlinear dynamic systems. The satisfying performance of the WNN depends on an appropriate determination of the Wavelet Neural Network structure. In this paper we provide a new method to solve this problem based on the Least Absolute Shrinkage and Selection Operator (LASSO). At first, the scale of WNN is managed by using the time-frequency locality of wavelet. Furthermore, the unconstrained optimization problem (LASSO) is used to solve the structure and learning of the WNN. This optimization problem can be solved efficiently using the iteratively reweighted least squares (IRLS) and the Least Trimmed Square (LTS) methods to enhance the ineffectiveness; they are applied to train the wavelet neural network. The advantage of the method lies in the oracle property of the LASSO can guarantee the optimal structure of the WNN. The proposed method has been able to optimize the wavelet neural network and this method is able to classify the DNA sequences. Our goal is to construct predictive models that are highly accurate. In fact, the proposed method permits to avoid the complex problem of form and structure in different clusters of organisms. The empirical results and their classification performances are compared with other methods. We compared the WNN-Lasso model with the other five alignment-free models, i.e., k-tuple, DMK, TSM, AMI, and CV, on several large-scale DNA datasets on the DNA classifying application by means of the K-means method. The experimental results have shown that the WNN-Lasso model outperformed the other models in terms of both the classifying results and the running time.

Evenly, in this study, we present our approach consists of three phases. The first one, which is called transformation, is composed of two sub steps; binary codification of the DNA sequences and the Signal Processing of the DNA sequences. The second phase step is the approximation; it is empowered by the use of the Multi Library Wavelet Neural Networks (MLWNN). Finally, the third section, which is the classification of the DNA sequences, is realized by applying the algorithm of k-means classification.

Index Terms—LASSO, LTS, Wavelet Neural Networks, DNA sequences, MLWNN, IRLS.

I. INTRODUCTION

The Wavelet Neural Network (WNN) has recently attracted extensive attention for its ability to identify efficiently nonlinear dynamic systems with incoherent information [1-2-3-4-5]. The WNN were introduced by Zhang and Benveniste [1-2-3] in 1992 as combination of the artificial neural network wavelet decomposition. The generalization performance of the WNN trained by least-square approach deteriorates when outliers are present. This training approach involves estimating parameters in the wavelet network to minimize some function costs, a measure reflecting the approximation quality performed by the wavelet network over the parameter space in the network. However, the studies of the WNN have often concentrated on a small dimension [6]. The reason is that the complexity of the Wavelet Neural Network structure will increase exponentially with the input size, i.e. the curse of dimensionality to improve the performance of the WNN in high dimension application. Feed forward neural network such as multilayer perceptrons (MLP) and the radial basis function networks (RBFN) have been used as an alternative approach to function approximation. The network structure has been studied by several researchers. The research effort has been made to deal with this problem over the last decades [6-7-8-9]. The method, referred as Matching Pursuit (MP), was first introduced by Mallat [10]. The Residual Based Selection (RBS) algorithm is used to select the wavelet function for constructing the WNN [10], the Orthogonalized Residual Based Selection (ORBS) proposed in [6] and the Orthogonal Least Square (OLS) suggested in [8] are both the popular approaches. The Wavelet Neural Network (WNN) is attracting interest in field of classification system. Such as classification of the DNA sequences using artificial neural networks [11]. The neural networks have several unique features and advantages. They can build non-linear decision boundaries between the different groups in a non-parametric fashion, and thereby offer a practical approach for solving highly complex pattern classification problems.

Classification of the DNA Sequences using the Wavelet Variance and the Self-Organizing Map with an Application to Mitochondrial DNA[12]. This approach combines the wavelet
analysis and the self-organizing map algorithm. The Wavelets are applied to select variation across various scales in the short sequence of nucleotides patterns of the DNA sequence. The variation is computed by the estimated wavelet variance, which yields a feature vector, which obtained from many genomic sequences, possibly of different dimensions, is then clustered with a nonparametric self-organizing map scheme.

The classification of two types of the DNA sequence studied 20 sample artificial DNA sequence whose types have been known are given to cluster the types of other DNA sequences. The Wavelet analysis is applied to choose the features of the sample DNA sequences [13-31].

The Wavelet analysis of frequency chaos game signal has been used to classify DNA sequences. The results creating from the complex Morlet wavelet analysis of the frequency chaos game signals have shown its accuracy in detection of the DNA structures. Additional, this could provide in discovering unknown domains with potential biological significance in genomes [14].

A neural network classification method [15] has been developed as an alternative method to the search problem of large molecular databases of the DNA sequence. Two artificial neural systems have been implemented on a Cray supercomputer for rapid nucelcic acid sequence classifications. The used neural networks are three-layered, feed-forward neural networks that employ back-propagation learning algorithm.

Since a DNA sequence can be converted into a sequence of digital signals, the feature vector can be constructed in time or frequency domains. Despite, most traditional alignment-free methods, such as k-tuple [16], DMK [17], TSM [18], AMI [19], and CV [20] methods build their feature vectors only in the time domain, i.e., they apply direct word sequences.

The WVF method uses the discrete wavelet transform (DWT) to adaptively decompose and select features of the DNA sequence matching to its length rather than the DNA microarray data. As a result, sequences of distinct length can be converted into the same-sized feature vector [21].

In this study, our approach applies the Least Absolute Shrinkage and Selection Operator (LASSO) to solve the wavelet neural network structure. This approach is a useful tool to solve the shrinkage and the variable selection simultaneously, which was used successfully in COX model selection [22]. The lasso reduces the residual sum of squares subject to the sum of the absolute value of the parameters being less than a constant.

Because the Least Absolute Shrinkage overcomes deficiency of traditional methods, it has been widely educated in statistics, employ mathematics as well as signal processing [22].

This study is structured as follows: section II introduces an overview of our approach. Section III is about the Beta wavelet function theory. This function will be applied to construct the Wavelet Neural Network. Section IV deals with the experimental results of the proposed approach used to classify the DNA sequences and Section V ends up with a conclusion and discussion.

II. METHODS

This paper presents a new approach of classification of the DNA sequences based on the wavelet network, which is constructed by applying the Library Wavelet Neural to approximate f(x) of the DNA sequence. The unconstrained optimization problem (LASSO) is used to solve the structure and the learning of the WNN. This approach is divided into three stages: approximation of the input signal and cluster of the compact signature of DNA sequences using Wavelet Neural Network (WNN) and the k-means algorithm.

A. Conversion of DNA sequence to genomic signal

The proposed cluster of species in class made according to the DNA sequence components, which is composed of four basic nucleotides, A(Adenine), G(Guanine), C(Cytosine) and T(Thymine), where each species is identified by its DNA sequence[25].

Linear feature extraction can be viewed as finding a set of vectors which represent effectively information content of an observation while minimizing the dimensionality. The method of indicator converts the data into digital signal, which can be used for the DNA signal spectrum indicates 1 or 0 for the existence or not of a specific nucleotide at the DNA sequence level. The binary indicator sequence is formed by replacing the each nucleotide with values either 1 or 0. 1 stands for presence and 0 for absence of a particular nucleotide in specified location in the DNA signal [25]. For example, if x[n] = [T T A T G TC ...], we obtain: x[n] = [0001 0001 0001 0001 0010 0001 0100 ...]

B. Fourier Transform and Power Spectrum Signal Processing

After the DNA sequence has been translated into these indicator sequences, they can be manipulated with mathematical models. The discrete Fourier Transform is used to each indicator sequence x(n) and a new sequence of complex numbers, called f(x), is obtained:

\[ f(x) = \sum_{n=0}^{N-1} X_n e^{-j2\pi kn/N}, k = 0, 1, 2, ..., N-1. \]  

It is easier to use with sequence Power Spectrum, rather than original discrete Fourier Transform. The Power Spectrum Se[k] for frequencies k= 0, 1, 2, ..., N-1 is presented as,

\[ S_e[k] = |f(x)|^2 \]  

Se [k] has been plotted (Fig. 1).
Wavelet Neural Network is an approximation of a given signal. The overall response of the network is obtained by connecting one wavelet candidate with weight values to the following layer. The Wavelet Neural Network (Fig. 2) is composed of three layers (an input layer, a hidden layer, and an output layer) with the same structure as the architecture of a radial basis function. The output is obtained by adding the outputs of each neuron. Each neuron is connected to the other neurons in the same layer and to the neurons in the next layer. The Weighted Radial Basis Function (Wn) is used with the gradient descent algorithm to minimize the mean-squared error:

\[
W = \left\{ \gamma; \gamma(x) = \alpha V(a(x-b)), \alpha = \left( \sum_{i=0}^{m} V(a(x-b)) \right)^{1/2}, j=1 \cdots L \right\},
\]

where \( x_k \) is the sampled input and \( L \) is the number of wavelets in \( W \). Then, the best \( M \) wavelet is chosen based on the training data from the wavelet library \( W \), in order to construct the regression:

\[
f_M(x) = y = \sum_{m=1}^{M} \psi(x).
\]

Where \( I \) is a \( M \)-element subset of the index set \( \{1, 2, \ldots, L\} \), and \( M \leq L \).

Secondly, the reduced cost function is defined as:

\[
j_I(w) = \min_{I} \frac{1}{n} \sum_{i=1}^{n} \left( y_i - \sum_{m=1}^{M} w \psi(x_i) \right)^2.
\]

Two heuristic algorithms have been derived by Zhang, namely, stepwise selection by orthogonalization for deciding appropriate wavelet in the hidden units and backward elimination for choosing the number of the hidden units. The number of wavelets \( M \), which are selected as the minimum of the so-called Akaike’s final prediction error criterion (FPE) [2,3]:

\[
j(w) = \frac{1}{n} \sum_{i=1}^{n} \left( y_i - \sum_{m=1}^{M} w \psi(x_i) \right)^2.
\]

Where \( j(w) \) is the real output of the Wavelet Neural Network at the fixed weight vector \( w \).

The time-frequency locality property of the wavelet is applied to give a signal \( f \). A candidate library \( W \) of the wavelet basis can be constructed [35].

There exist constants \( C_{m,n} \) such that:

\[
\left\| f - \sum_{m,n,n} C_{m,n} \psi_{m,n} \right\| = o(\epsilon)
\]

Hence, based on (10), the approximation can be realized by a three-layer network, as shown in Fig. 2.
E. Wavelet Network construction using Lasso-based Method

A given set of training data \( \mathcal{TN} = \{ (x^{(k)}, f(x^{(k)})) \}_{k=1}^{N} \), which is used to adjust the weights on the WNN, and the output of the three layers of the wavelet neural network in Fig.2 can be expressed as:

\[
Y = \begin{bmatrix} y^{(1)} & y^{(2)} & \ldots & y^{(N)} \end{bmatrix} = \Psi C
\]

(10)

Where \( y^{(k)} \), \( \psi_{j}^{(i)} \), \( 1 \leq k \leq N, 1 \leq j \leq r \) is the output of the three layers of the wavelet network and the output of \( j \)th wavelet candidate for training data \( x(k) \) respectively.

The task of Architecture of the wavelet neural networks is to select a subset from \( r \) wavelet candidates as neurons in the hidden layer in three layer wavelet network. This problem is also solved by a model selection.

Furthermore, based on the determinate architecture, the task of the WNN learning is to obtain the sub-vector \( C \). Many researches are used to select a small subset of the wavelet candidates in the library that best matches an output vector, the weights of subset is computed by iterative gradient-descent algorithm or least square method.

The system identification application of the WNN is to represent the nonlinear dynamic system through as few neurons as possible. There is now an extensive literature indicating the wavelet neural network with few wavelets has the better generalization performance.

We propose a new method for estimation in linear models to solve these two problems we present a novel approach to solve these task based on the Least Absolute Shrinkage and Selection Operator (LASSO), which reduces the residual sum of squares subject to the total of the absolute value of coefficients being less than a constant. Besides of the nature of this constraint it tends to create some coefficients that are exactly 0 and hence gives interpretable methods. Our simulation studies suggest that the Least Absolute Shrinkage and Selection Operator (LASSO) enjoys some of the favourable properties of both subset selection and ridge regression [22].

Based on this idea, these two problems can be transferred into below unconstrained optimization problem.

The lasso is a regularization technique for simultaneous estimation and variable selection [22]. The lasso estimates are defined as:

\[
\hat{C}(\text{Lasso}) = \text{Min} \| C \|_0 + \frac{1}{2} \| Y - \psi C \|_2^2
\]

(11)

Where \( \lambda \) is a nonnegative regularization variable. The first term in (11) is so-named “L0 penalty”. One appealing method is the L0 regularized regression which punishes the number of nonzero features in the model directly.

The second term in (11) represents the measurement of the accuracy of model. The L0 penalty is attractive for variable selection because it directly punishes the number of nonzero weights. However, the optimization involved is nonconvex and discontinuous, and therefore it is very challenging to implement and this optimization problem is NP-hard, i.e., the computational time for solving this optimization is non-polynomial. Moreover, its solution we shall attempt to replace the optimization problem (11) with below convex relaxation (Lasso problem).

\[
\hat{C}(\text{Lasso}) = \text{Min} \| C \|_1 + \frac{1}{2} \| Y - \psi C \|_2^2
\]

(12)

The solution of optimization problem (12) is equal to the one of optimization problem (11). Moreover, since the objective of (12) is an unconstrained convex function, we can apply standard approaches to construct a minimizer. The quickly algorithms of optimization problem (12) also exist.

The architecture and learning of wavelet neural networks are considered as searching the position and values of nonzero entries from \( r \) entries in vector \( C \). Suppose \( \Omega \) is the set of optimal positions of nonzero entries and \( C^\Omega \) denote the values. At the same time, assume \( \Gamma = \{ i : \hat{c}^\Gamma_i \neq 0 \} \) is the
position of nonzero entries of solution of the optimization problem (16) and $\hat{C}_T$ denote the values in positions $\Gamma$. H. Zou points out the lasso have the following oracle properties [23]:

- Determines the right subset model,
  $$\Gamma = \{i : \hat{c}_i \neq 0\} = \Omega$$
- Has the optimal estimation rate,
  $$\sqrt{N} \left( \hat{C}_T - C_T \right) \to N \left( 0, \Sigma^* \right),$$
  where $\Sigma^*$ is the covariance matrix knowing the true subset model.

In our approach, we introduce wavelet-based weighted LASSO with different weighting schemes in the penalty term and discuss some screening strategies that can be used to wavelet-based functional linear model. We assume readers have certain familiarity with wavelet transform.

The weights of the Wavelet Neural Network (WNN) are updated rules based on iteratively reweighted least squares (IRLS) algorithm which be proposed. The LTS estimator is used in robust linear parametric regression problem to nonlinear regression problems. The main motivation is that the Least Trimmed Square (LTS) estimator usually has good robustness against outliers for linear parametric regression tasks.

The residual $e_i$ at the ith output node is presented by

$$e_i = y_i - \hat{y}_i, i \in n \quad (13)$$

The LTS estimator is used to select network weights that minimize the total sum of trimmed squared errors

$$E_{total} = \frac{1}{2} \sum_{i=1}^{N} \sum_{t=1}^{N} e_i^2 \quad (14)$$

Appropriate updating rules for minimizing (12), iteratively reweighted least squares (IRLS) algorithm is used to approximate the optimal weights.

To find the parameters $C = (C_1, ..., C_k)^T$ which minimize the L1 norm for the linear regression Lasso problem (12),

$$\min \lambda \left( \| C \| + \frac{1}{2} \| Y - \psi C \|_F^2 \right) = \min \lambda \left( \sum_{i=1}^{N} |c| + \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} e_i \psi_i C_j \right) \quad (15)$$

The IRLS algorithm at step $t+1$ involves the weighted linear least squares problem:

$$\min \lambda \left( \| C \| + \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} e_i \psi_i C_j \right) = \min \lambda \left( \sum_{i=1}^{N} |c| + \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} e_i \psi_i C_j \right) \quad (16)$$

Where $\omega^{(0)}$ is the diagonal matrix of weights usually with all components set initially to:

$$\omega^{(0)} = 1$$

And updated after each iteration to:

$$\omega^{(t)} = \frac{1}{\max(|\psi_i C_j| + \epsilon, \epsilon)} \quad (17)$$

Where $\epsilon$ is the small value, like 0.0001.

Algorithm IRLS-GD

Set $\omega^{(0)} = 1, \epsilon^0 = 1, t = 0$

1: while $\epsilon^t \neq 0$ do

2: Compute $C^{(t)}$ via (16)

3: $\epsilon^{t+1} = \min (\epsilon^{t+1}, C^{(t)})$

4: Compute $\omega^{(t)}$ via (17)

$$a_i^{opt} = \frac{\partial (\epsilon)}{\partial a_i} = \sum_{i=1}^{N} e(x) \psi_i \left( x - a_i^{opt} \right) b_i^{opt} \quad (18)$$

$$b_i^{opt} = \frac{\partial (\epsilon)}{\partial b_i} = \sum_{i=1}^{N} e(x) \psi_i \left( x - a_i^{opt} \right) b_i^{opt} \quad (19)$$

5: end while

F. Approximation of the DNA Sequence Signal

DNA sequence cluster is an NP-complete problem. Indeed, when the alignment is beyond two sequences, the task quickly becomes very complex because the space of comparison becomes very important. The recent advance of the DNA sequence technology has brought about a consequent number of the DNA sequences. We can are to analyze some million sequences and a first phase for this analysis is applied to determine there is a structure of the DNA sequence data in homogeneous groups according to a criterion to be identified.

In this study, a classifier is applied to cluster the dataset of the DNA sequence using the Power Spectrum to process the signal of sequence and the application of the wavelet neural networks as a classification method, which solves the classification tasks of the DNA sequences. Initially, the proposed approach can bring the learning index defined by the signal of sequence and the application of the wavelet neural networks as a classification method, which solves the classification tasks of the DNA sequences. Initially, the proposed approach can bring the learning index defined by the signal of sequence and the application of the wavelet neural networks as a classification method, which solves the classification tasks of the DNA sequences.

In this step, we apply the principle of k-means clustering to classify the characteristics of the DNA sequences.
To approximate \( f(x) \) of the DNA sequences, the optimal wavelet function is chosen to obtain signal representation with minimal error rate. To solve the approximation task, a library wavelet containing a family wavelet is applied. It is called Multi Library Wavelet Neural Network approach (MLWNN) [40,44]. In our approach, the second phase is to construct the library wavelet and approximate the function \( f(x) \) of the DNA sequence.

**G. Learning Wavelet Network Using the Lasso-LTS Method**

In this section, we show how we can learn the wavelet neural networks using the MLWNN [25-26-16-17-43-46].

1. Proposed Learning Algorithm

**Step 1:** The original data of the DNA sequence is divided into two groups: training and testing dataset.

**Step 2:** Convert the DNA sequence to a genomic signal using a binary indicator and Power Spectrum Signal Processing.

**Step 3:** Construct a library \( W \) of discretely dilated and translated version of a given wavelet \( \psi \), according to the available training data set.

- Use the Least Trimmed Square (LTS) estimator for choosing the optimal mother wavelet function from the library wavelet \( (13)(14) \).
- Choose, from the library, the \( N \) wavelet candidate that best matches an output vector.

**Step 3.1:** Initialize the mother wavelet function

library \( \Psi = \{ \psi_i \} \), \( i = 1, 2, ..., m \), \( m = \| \Psi \| \), is the number of the wavelet candidates included. The LST estimator is applied to choose the best and the optimal wavelet functions \( \text{wavelet}_{\text{best}} \).

**Step 3.2:** Randomly initialize \( w_k \) and \( v_i \).

**Step 3.3:** For \( k=1, ..., m \)

\( \begin{align*}
& a) \text{ Calculate the predicted output } \hat{y}_i \text{ via (3).} \\
& b) \text{ Compute the residuals } e_{ik} = y_i - \hat{y}_i \text{ in(13).} \\
& c) \text{ If the stopping criterion is achieved, then stop; otherwise, go to the next step} \\
& d) \text{ Find the ranked values } e_{ik}^2 \leq ... \leq e_{min}^2 \\
\end{align*} \)

Choosing the \( N \) best mother wavelets function to initialize the WNN.

**Step 4:** Use the translation \( b_i \) and dilation \( a_i \) of the \( N \) relevant wavelets as initial values.

**Step 5:** Use IRLS-GD algorithm to compute \( W_{ij} \), \( a_i \), and \( b_i \).

**Step 6:** Construct an empty matrix (Classes_signature_DNA)(\( W_{ij} \), \( a_i \), and \( b_i \)) which has to contain the clusters of DNA sequences.

**Step 7:** Let Classes_signature_DNA = \( s_j \) = \{ \( W_{ij} \), \( a_i \), \( b_i \) \} be the set of data sequences and \( V=\{v_1,v_2, ..., v_c \} \) be the set of centers.

**Step 8:** Randomly select ‘c’ cluster centers

**Step 9:** Compute the distance between each data point and the cluster centers.
Step 10: Assign the data point to the group center whose distance from the class center is minimum of all the cluster centers.

Step 11: Recompute the new class center using:

\[ v_i = \left( \frac{1}{c_i} \right) \sum_{j=1}^{c_i} s_i \tag{20} \]

Where, \( c_i \) represents the number of data points in \( i \)th cluster.

Step 12: Recompute the distance between each data point and new obtained group centers.

Step 13: If no data was reassigned then stop, otherwise repeat from step 10.

H. The Beta Wavelet Family

The beta wavelet is used to construct the wavelet neural network of the proposed approach. The function beta is defined by \( \beta(x) = [x_0, x_1] \) [26-27-28-32-41-45], \( x_0 \) and \( x_1 \) are real parameters.

\[
\beta(x, p, q, x_0, x_1) = \begin{cases} 
\left( \frac{x - x_0}{x_1 - x_0} \right)^p \left( \frac{x - x_1}{x_1 - x_0} \right)^q & \text{if } x \in [x_0, x_1] \\
0 & \text{otherwise}
\end{cases}
\tag{21}
\]

We have proved, in [26-27-28-36-37-42], that all the derivatives of Beta function \( \in L^2(\mathbb{R}) \), are of class \( C^\infty \) (Fig. 4) and satisfy the admissibility wavelet condition.

The general form of the nth derivative of Beta function is:

\[
\psi_n(x) = \frac{d^n \beta(x)}{dx^n} [(-1)^n \sum_{i=0}^{n} \frac{n!}{p!q!(n-p)!(n-q)!} (x-x_0)^{n-i} (x_1-x)^{i}] P_{p,q}(x) \beta(x) + 
\]

\[
\sum_{i=1}^{n} \left[ (-1)^{n-i} \sum_{j=0}^{n-i} \frac{(n-i)!}{p!(n-i-j)!q!(i-j)!} (x-x_0)^{n-i-j} (x_1-x)^{j} P_{p,q}(x) \beta(x) \right]
\tag{22}
\]

where:

\[
P_{1}(x) = \frac{P}{x - x_0} - \frac{q}{x_1 - x} \tag{23}
\]

\[
P_{s}(x) = (-1)^n \frac{n!p}{(x-x_0)^{n+1}} - \frac{n!q}{(x_1-x)^{n+1}} \tag{24}
\]

If \( p = q \), for all \( n \in \mathbb{N} \) and \( 0 < n < p \), the functions \( \Psi_n(x) = d^n \beta(x)/dx^n \) are wavelets [26-27-34-38-39].
III. RESULTS AND DISCUSSION

This paper uses three datasets HOG100, HOG200, and HOG300. Each dataset was randomly selected from HOGENOM[30], which comprehends homologous gene families from microbial species. Table 1 lists the details of these datasets. The HOG* dataset contains families that vary from 100 to 300.

<table>
<thead>
<tr>
<th>Dataset</th>
<th># families</th>
<th>#DNA sequences in the dataset</th>
<th>Average length of a DNA sequence in the dataset</th>
<th>Dataset size(MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOG100</td>
<td>100</td>
<td>9648</td>
<td>1484</td>
<td>15.1</td>
</tr>
<tr>
<td>HOG200</td>
<td>200</td>
<td>22585</td>
<td>1557</td>
<td>37.0</td>
</tr>
<tr>
<td>HOG300</td>
<td>300</td>
<td>27825</td>
<td>1448</td>
<td>42.6</td>
</tr>
</tbody>
</table>

To evaluate the performance of the proposed approach, we have developed different experiments, each consisting of a different subset of test data. The classification comparative analysis is performed using a selection of published empirical datasets and synthetic DNA datasets [30].

Experiment results were performed to prove the effectiveness of our proposed approach. Evaluation metrics namely Precision, Recall and F-measures are used to compare our approach with other competitive methods.

The F-measure combines the precision and the recall metric. We then calculate the recall and the precision of that cluster for each given class. More specifically, for cluster j and class i.

The recall of group j to family i is as follows:

$$R_{ecall}(j,i) = \frac{n_j}{n_i}$$  \hfill (25)  

The precision of (i, j) is given by

$$Pr_{ecision}(i, j) = \frac{n_{ij}}{n_j}$$  \hfill (26)  

Where $n_j$ is the numbers of members of the class i in the class j, $n_{ij}$ is the number of the DNA sequences of the group j and $n_i$ is the number of the sequence of the class i.

The F-measure of the class j and the group i is the given by

$$F(j,i) = \frac{2 \times R_{ecall}(i,j) \times Pr_{ecision}(i, j)}{(P_{r_{ecision}}(i, j) + R_{ecall}(i, j))}$$  \hfill (27)  

For an entire k-means algorithm the F-measure of any group is the maximum value it attains at any node in the tree and an overall value for the F-measure is calculated by obtaining the weighted average of all values for the F-measure as computed by the following.

$$F = \sum_{j=1}^{m} \frac{n_j}{n} \max \{F(j,i)\}$$  \hfill (28)  

Where the max is taken over all groups at all levels, and $n$ is the number of the DNA sequences.

$Z$ denote the number of clusters in the whole grouping result and $m$ denote the number of families in the dataset.

1) Preferred length of the feature vectors

![Fig.5 Clustering results of the wavelet-based feature vector (WFV) model against the length of the feature vector on different datasets.](image)

Fig.5 shows that the wavelet-based feature vector (WFV) model could achieve the best clustering result when the length of the feature vector was 32 for HOG100 and HOG200, and the next best when the vector was 64. However, the difference of classifying results was very small between 32 and 64. Consequently, 32 was the preferred length of feature vectors in our tests. As a result, a longer feature vector may not achieve a better clustering result. A shorter feature vector can reduce computation time, which is very helpful in processing large-scale DNA sequences.

![Fig.6 Clustering results of our method WNN-Lasso against the length of the feature vector on different datasets.](image)

Fig.6 Clustering results of our method WNN-Lasso against the length of the feature vector on different datasets.
The WNN-Lasso model (Our proposed approach) achieves the best clustering result when the length of the feature vector was 128 on different datasets (HOG100, HOG200 and HOG300). The last best when the vector was 32. However, the difference of classifying results was very small between 32(The average F-measures=0.57) and 128(The average F-measures=0.59). Consequently, 32 was the preferred length of feature vectors in our tests. As a result, a longer feature vector may not achieve a better clustering result. A shorter feature vector can reduce computation time, which is very helpful in processing large-scale DNA sequences.

2) Clustering results

We compared the WNN-Lasso model (our proposed approach) and the WFV with the five other alignment-free models, i.e., k-tuple, DMK, TSM, AMI, and CV. The WNN-Lasso model fixed the length of the feature vector to 128 for all the DNA sequences on the three datasets (HOG100, HOG200 and HOG300). For the other five models, the feature vectors were significantly affected by the size of the sliding window. The sliding window for TSM was 2, while for the rest it was 3. Since the length of each codon is three in the DNA, it might be beneficial to retain the genetic information of the DNA sequence.

Figures 7, 8, 9 illustrate the clustering results from all the models in the F-measure on the three datasets (HOG100, HOG200 and HOG300). It is clear that the performance of WNN-Lasso was best. The WFV did not perform quite as well as WNN-Lasso, but was much better than other methods.
The table 3 shows the best classifying results in F-measure of the WNN-Lasso and the six alignment based models, i.e., K-tuple, DMK, TSM, AMI, and CV., on the different datasets (HOG100, HOG200 and HOG300). The six alignment based models are far worse than WNN-Lasso (our proposed approach) and the WFV. However, the alignment methods are designed for finding the most similar the DNA sequences, namely, every sequence in the cluster must have similarity above a given identity threshold.

3) Running time

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Length of feature vector</th>
<th>Time of building feature vector</th>
<th>Time of k-means clustering</th>
<th>Total running time</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOG100</td>
<td>WFV</td>
<td>128</td>
<td>5.3569</td>
<td>75.645</td>
<td>81.0019</td>
</tr>
<tr>
<td></td>
<td>K-tuple</td>
<td>32</td>
<td>8.4857</td>
<td>102.2634</td>
<td>110.7491</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>64</td>
<td>7.9544</td>
<td>763.5223</td>
</tr>
<tr>
<td></td>
<td>DMK</td>
<td>64</td>
<td>30.2172</td>
<td>1550.4054</td>
<td>1580.6226</td>
</tr>
<tr>
<td></td>
<td>TSM</td>
<td>12</td>
<td>32.7890</td>
<td>576.7237</td>
<td>609.5127</td>
</tr>
<tr>
<td></td>
<td>AM</td>
<td>4</td>
<td>167.8232</td>
<td>326.0293</td>
<td>493.8525</td>
</tr>
<tr>
<td></td>
<td>CV</td>
<td>64</td>
<td>24.5168</td>
<td>2715.1169</td>
<td>2739.6337</td>
</tr>
<tr>
<td>HOG200</td>
<td>WFV</td>
<td>128</td>
<td>16.758</td>
<td>350.664</td>
<td>367.422</td>
</tr>
<tr>
<td></td>
<td>K-tuple</td>
<td>32</td>
<td>20.5239</td>
<td>645.8376</td>
<td>666.3615</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>64</td>
<td>19.6306</td>
<td>3010.5426</td>
</tr>
<tr>
<td></td>
<td>DMK</td>
<td>64</td>
<td>32.5273</td>
<td>7210.1629</td>
<td>7284.4712</td>
</tr>
<tr>
<td></td>
<td>TSM</td>
<td>12</td>
<td>82.2772</td>
<td>2144.6954</td>
<td>2226.9726</td>
</tr>
<tr>
<td></td>
<td>AM</td>
<td>4</td>
<td>410.8531</td>
<td>1059.0261</td>
<td>1459.8792</td>
</tr>
<tr>
<td></td>
<td>CV</td>
<td>64</td>
<td>60.3402</td>
<td>9247.3361</td>
<td>9307.9715</td>
</tr>
<tr>
<td>HOG300</td>
<td>WFV</td>
<td>128</td>
<td>15.556</td>
<td>854.656</td>
<td>870.212</td>
</tr>
<tr>
<td></td>
<td>K-tuple</td>
<td>32</td>
<td>24.1259</td>
<td>1349.6459</td>
<td>1373.7718</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>64</td>
<td>22.5723</td>
<td>5560.3319</td>
</tr>
<tr>
<td></td>
<td>DMK</td>
<td>64</td>
<td>85.1456</td>
<td>13785.8160</td>
<td>13870.9616</td>
</tr>
<tr>
<td></td>
<td>TSM</td>
<td>12</td>
<td>92.8571</td>
<td>3329.9724</td>
<td>3422.8295</td>
</tr>
<tr>
<td></td>
<td>AM</td>
<td>4</td>
<td>471.9211</td>
<td>1577.3361</td>
<td>2049.2572</td>
</tr>
<tr>
<td></td>
<td>CV</td>
<td>64</td>
<td>69.3221</td>
<td>16609.7183</td>
<td>16679.0404</td>
</tr>
</tbody>
</table>
The proposed approach (WNN-Lasso) also improves the classification accuracy of the DNA sequences, but also shortens the running time. Table 4 shows the average running time of the all methods on the tree datasets of DNA sequences (HOOG100, HOOG200 and HOOG300).

The WNN-Lasso' feature vector building time was much shorter than the other models. It is more important that the clustering time of WNN-Lasso was the shortest, so WNN-Lasso is more suitable for enormous quantities of the dataset. The models (K-tuple, DMK, TSM, AM and CV) used in these studies range from sequence and structure alignments. A large set of sequences can be simultaneously compared using Multiple Sequence Alignment which is known to be NP-complete problems. However, full the applied models are still computationally very expensive and require significant computational infrastructure. Our goal is to construct predictive models and cluster that are highly accurate and interpretable. This approach can affect the time complexity of the similarity computation between the DNA sequences. So the complexity of The models (K-tuple, DMK, TSM, AM and CV) are higher than the WNN-Lasso and the WFV.

The results show that the time of the training phase. The time depends on the size of the DNA sequence. When the size is equal to 128, the training time is equal to 9.3569 seconds. The results show that the size of the DNA sequence increases the time of the training phase. The time depends on the size of the DNA sequence. When the size is equal to 128, the training time is equal to 9.3569 seconds.

First, during the approximation phase, our proposed approach tried to decompose the input signal for every sequence and then tried to reconstruct the input signal. The estimation of the performance of this phase was measured by the Mean Square Error (MSE). Table 5 shows that the Mean Square Error (MSE) obtained are low (0.002582) and the run-time increases relatively with the size of the DNA sequence. The results show that the size of the DNA sequence increases the time of the training phase. The time depends on the size of the DNA sequence. When the size is equal to 128, the training time is equal to 9.3569 seconds.

The results show that the WNN can achieve very good prediction accuracy. The results of our approach (Wavelet Neural Network (WNN)) tested on empirical datasets show that accuracy outperforms the other techniques in terms of percentage of the correct species identification. Our proposed approach outperforms the other models (K-tuple, DMK, TSM, AM and CV) in terms of both the classifying accuracy of the DNA sequences, but also shortens the running time. Table 4 shows the average running time of the all methods on the tree datasets of DNA sequences (HOOG100, HOOG200 and HOOG300).

The results of our approach (WNN-Lasso) tested on empirical datasets show that accuracy outperforms the other techniques in terms of percentage of the correct species identification. Our proposed approach depends on the Power Spectrum, processing the DNA sequence signal. Applying this k-means classification enables us to group the similar DNA sequences according to some criteria. This classification aims at distributing n DNA sequences characterized by p variables X1, X2…Xp in a number m of subgroups which are homogeneous as much as possible while every group is well differentiated from the others.

In our approach, achieve very good prediction accuracy. The results of our approach (WNN-Lasso) tested on empirical datasets show that accuracy outperforms the other techniques in terms of percentage of the correct species identification. Our proposed approach outperforms the other models (K-tuple, DMK, TSM, AM and CV) in terms of both the classifying results and the running time.

This approach helps to classify organisms into different categories and groups which have significant biological knowledge and can justify the evolution and identification of unknown organisms. Simulation results are demonstrated to validate the generalization ability and efficiency of the proposed Wavelet Neural Network Model. These results have been realized thanks to many capacities listed as;

- The capacity of Library Wavelet Neural Network Model (MLWNN) to construct the Wavelet Neural Network (WNN).
- The capacity of binary sequence indicators Codification, Fourier Transform and Power Spectrum to process the signal of DNA sequences,
- The capacity of the oracle properly of LASSO can guarantee the optimal structure of the WNN,
- The capacity of the networks of wavelets in approximate of the functions real gives a complex,
- Finally, a powerful tool and a pipeline to perform organisms classification are provided to the DNA sequences community.

### IV. CONCLUSIONS

In this paper, we have used a new method of training called Library Wavelet Neural Network Model (MLWNN). It is used to construct Wavelet Neural Network (WNN). The WNN is used to approximate function f (x) of a DNA sequence signal. Our proposed approach depends on the Power Spectrum, processing the DNA sequence signal. Applying this k-means classification enables us to group the similar DNA sequences according to some criteria. This classification aims at distributing n DNA sequences characterized by p variables X1, X2…Xp in a number m of subgroups which are homogeneous as much as possible while every group is well differentiated from the others.

In our approach, achieve very good prediction accuracy. The results of our approach (WNN-Lasso) tested on empirical datasets show that accuracy outperforms the other techniques in terms of percentage of the correct species identification. Our proposed approach outperforms the other models (K-tuple, DMK, TSM, AM and CV) in terms of both the classifying results and the running time.

This approach helps to classify organisms into different categories and groups which have significant biological knowledge and can justify the evolution and identification of unknown organisms. Simulation results are demonstrated to validate the generalization ability and efficiency of the proposed Wavelet Neural Network Model. These results have been realized thanks to many capacities listed as;

- The capacity of Library Wavelet Neural Network Model (MLWNN) to construct the Wavelet Neural Network (WNN).
- The capacity of binary sequence indicators Codification, Fourier Transform and Power Spectrum to process the signal of DNA sequences,
- The capacity of the oracle properly of LASSO can guarantee the optimal structure of the WNN,
- The capacity of the networks of wavelets in approximate of the functions real gives a complex,
- Finally, a powerful tool and a pipeline to perform organisms classification are provided to the DNA sequences community.

### ACKNOWLEDGMENT

We would like to acknowledge the financial support, under the form of grant, from the General Direction of Scientific Research (DGRST), Tunisia.
REFERENCES


[12] Agnieszka E Jach1, Juan M Marín, Classification of Genomic Sequences via Wavelet Variole and a Self-Organizing Map with an Application to Mitochondrial DNA.


https://sites.google.com/site/ijcsis/ ISSN 1947-5500
Abdesselem DAKHLI continued these academic studies to FSEG Sfax, Tunisia. He obtained his teacher’s certificate in data processing applied to management in June 2001. He continued his degree of Masters in ISIMG of Gabes, Tunisia in 2008. In 2010, he received his Master degree in Information system in the same Institute. In August 2005 he was assigned to the ISG Gabes, Tunisia. Currently, he is a teacher at ISG. In 2012, now he prepares a PhD thesis of bioinformatic in ENIS. Abdesselem dakhli he also participated in one international conference. His areas of research are: Tomography, Bioinformatics.

Wajdi BELLIL received the B.S. degree in Electrical Engineering from the National Engineering School of Sfax (ENIS) in 2000, the M.S. and PhD degrees in Electrical Engineering from the National Engineering School of Sfax (ENIS), in 2003 and 2009, respectively. He spent five years at the ISET Gafsa, Tunisia, as a technologic assistant and researcher before joining the faculty of Science of Gafsa, Tunisia, as Assistant. He joined the Higher Institute of Applied Sciences and Technology, Gafsa University, where he is currently an assistant professor in the Department of computer science. He was a member of the REsearch Group on Intelligent Machines (REGIM). He is a junior member of IEEE.aerospace engineering from the University of Virginia, Charlottesville, in 2001 and the Ph.D. degree in mechanical engineering from Drexel University, Philadelphia, PA, in 2008.

Chokri BEN AMAR received the B.S. degree in Electrical Engineering from the National Engineering School of Sfax (ENIS) in 1989, the M.S. and PhD degrees in Computer Engineering from the National Institute of Applied Sciences in Lyon, France, in 1990 and 1994, respectively. He spent one year at the University of "Haute Savoie" (France) as a teaching assistant and researcher before joining the higher School of Sciences and Techniques of Tunis as Assistant Professor in 1995. In 1999, he joined the Sfax University (USS), where he is currently a professor in the Department of Electrical Engineering of the National Engineering School of Sfax (ENIS). He is a senior member of IEEE, and the chair of the IEEE SPS Tunisia Chapter since 2009. He was the chair of the IEEE NGNS’2011 (IEEE Third International Conference on Next Generation Networks and Services) and the Workshop on Intelligent Machines.
Sindhi Morphological Analysis: An Algorithm for Sindhi Word Segmentation into Morphemes

Department of Computer Science, Shah Abdul Latif University, Khairpur Mir’s, Sindh, Pakistan

ABSTRACT—Morphological analysis is the process of constructing and deconstructing the words of a language, the process is based on the basic grammatical units which are stem, prefixes, suffixes and infixes. Sindhi is rich in morphological features with a great variety of affixes. The problem for Sindhi to come into computerization is the large number of variants in its morphology. This complexity is created due to different positions of prefixes, suffixes and stems in the words. The automatic word segmentation system normally faces such embedded hurdles in Sindhi language. An algorithm is required with a capability of dealing with such issues for the segmentation of Sindhi words. In this paper, an algorithm is designed and implemented to resolve the problem of segmenting Sindhi complex and compound words into possible morphemes. The developed words segmentation system has been tested on a list of 109 compound words, 179 prefix words, 1343 suffix words and 50 prefix-suffix words. The cumulative segmentation error rate of 5.02% is calculated. This system can also be used as pre-requisite in various Sindhi language and speech processing applications.

Keywords—Sindhi Morphology; Morphological Analysis; Word Segmentation; Morphemes

I. INTRODUCTION
Each natural language carries its specific and peculiar mechanism for generation of the words and conversion of other words from the root words. Morphology is a branch of linguistics which purely deals with the study of language from scientific point of view, concerning with words and their constructive grammatical units. The breaking or constructing units are prefix, infix, stem and suffix. Two types of words, i.e. basic and secondary are found in Sindhi. The basic words cannot be broken up any more but the secondary words are breakable and devisable into complex and compound words. The complex words are in the class of secondary words and are built by combining prefix/stem/suffixes. Compound words are formed with the combination of at least two words [1].

Sindhi, an Indo-Aryan language [2], bears a high degree of similarity with modern-day Urdu, Hindi and some other languages of northwest Indian sub-continent. There is also a firm relation among Sindhi, Arabic and Persian which is a contact-induced loaning and borrowing of many words from one to the other. The script used for Sindhi in South Asian states like Pakistan and India is purely Perso-Arabic on predominant basis. Apart from these regions, the same script is used by Sindhi migrants who are settled across the world. The Persian is involved in Arabic script for the representation of several letters which are not present in Arabic but are required to represent some implosive, retroflex and nasal sounds. The inflections and derivations in Sindhi script are most frequently found with the use of prefixes and suffixes. This proves the richness of Sindhi in terms of morphology. The issue arises due to a large number of morphological variants in Sindhi which is yet to be analyzed and solved successfully. A compound word is usually formed by coalition of two or more simple words, i.e. دیس گناه (Rose), چینت رات (Day Night). Prefix words which are the part of complex or derivative words are built with the union of prefix and stem or root words like گناه (a sin) is a primary word when combined with prefix ی (a prefix that shows opposite meaning) becomes ی گناه (innocent). In this, گناه (a sin) is a free morpheme and ی is the bound one [1]. Suffix words are the result of the combination of a root word and suffix, such as یسمجه (understanding) is a primary word when combined with suffix ن (a suffix that shows infinitive mood) becomes یسمجه ن (to understand). There are also many words in Sindhi dictionary which carry both the prefix and suffix along the stem or root word. The example of such words is دیس دنی ئین (Country) is a root word, in condition of its combination with prefix پر (a prefix that shows the sense of far), it forms پر دنی ئین (Abroad) and with addition of suffix ن, then it turns into پر دنی ئین N (Foreigner).

The automatic segmentation of words into morphemes through computer is what we call computational morphology. The morphological analysis is of assistance for many Natural Language Processing (NLP) applications working with large vocabularies [3]. For instance, it is traditional to preprocess texts by returning words to their original forms, specifically in text retrieval in morphologically enriched languages of the world. In computational applications, morphological analysis is basically the segmentation of words into tokens morphemes. The analysis separates the stem (core part of word) from the prefix (the letter–addition in the beginning of word) or the suffix (the letter–addition in the end of the word). Moreover, different approaches and methods have been proposed and developed for morphological deconstruction of words. They include statistical language modeling [4] [5], lexeme-based [6] [7], rule-based [8], syllable-based [9] and corpus-based [10].

II. LITERATURE REVIEW
For the past half-decade, many a great works have been published in the field of Sindhi linguistic applications, Rahman has worked Sindhi Morphology and Noun Inflections [1] in which he has discussed the variation of morphemes in nouns
with respect to the dialects used in Sindhi language. He has used addition, subtraction and replacement methods through which the basic morphemes are derived out in different forms due to the difference in the dialects. Apart from the computational perspective of the work, the grammatical discussion is also carried out like the numbers, genders and the cases of certain nouns. The conclusion of the research reveals that morphological construction of Sindhi language is either inflectional or derivational.

Sindhi is a rich language in terms of the characters having various glyphs. Such characters do also change their form within script depending on their position or order in the text. A Sindhi tokenization model is proposed by Mahar [11] having three layers, each layer assigned a separate task. Similarly, Bhatti [12] has worked on the Sindhi tokenization and developed a Sindhi word tokenization model. He has implemented several algorithms processing the tokenization of Sindhi text into individual words. This way, they have built a corpus and a word repository for grammar checking method, Sindhi Spellings and other NLP applications. The issue is dealt with the first encounter of sentence boundaries and extracting each sentence into a separate list form. In this list, each element is a complete sentence. The next step is the segmentation of sentences into words. This segmentation is performed on the basis of hard and soft spaces are taken as a part of word. Thus, the soft spaces are ignored of segmentation. The final step includes the filtration of words, removal of special characters, converting word into a token and saving it after the validation is done.

Sindhi is one of the Arabic script-based languages but its automatic segmentation application through morphological analyzer is yet unavailable. Though, Mahar [13] has developed four algorithms which possess the capability of segmenting the words into the root level, a higher degree of computational complexity regarding space and speed is the lapsing point of all of them. Due to its categorical function, Mahar’s morphological analyzer uses the type of morpheme as its basis in each algorithm. Each algorithm works for a specific type of morpheme only so that process goes lengthy and slow for being an individualistic type. Therefore, a better and new algorithm is proposed for the segmentation of words into morphemes.

III. SINDHI MORPHOLOGY

Each language has its own grammar, foundation, and rules. Relatively, language is unique in its structure, function and application. For creating the awareness about morphology and analysis of words formation, some words are given in Table I. The first Sindhi word in Table I carries two morphemes: ann (اڻن) (Jan). The first morpheme is bound and the second is independent one. The slight change is notice in third word, the stem comes first and the addition at the second part. “پرهم” is the root word whereas the added part Hen is a suffix which is entailed to a word to change its meaning and sometimes word class even [14].

A. Bound and Independent Morphemes

The bound morphemes are those smallest basic grammatical units which form their meaning when included in a word. Independently, they do not bear any meaning. Thus, the term suggests that they are bound with the words and do not stand independently having their meaning as a word. Consider the examples shown in Table II, the morphemes ئ and ژ are the best examples of this type. Table III depicts the examples of Sindhi independent morphemes.

B. Zero Morphemes

There are several English words which are exactly identical in there different forms even. ‘Sheep’, ‘fish’, and ‘deer’ are some nouns which remain same in both plural and singular forms. Same is the case with some verbs like ‘spread’, ‘shut’ and ‘put’. They remain same in their different forms of present and past. They are called homophonous. In both types of such words, whether nouns or verbs the phonological representation is zero. Therefore, these morphemes are known as zero morphemes.

In Sindhi, no such types of morphemes are found [14]. Though, we may find some homographic words in this regard which do not change their structure for changing into past or plural, they change their sound because in Sindhi, some words can make plural just by changing their diacritics with the same set of letters. The examples are shown in Table IV.

| TABLE I: Comparative Morphological Analyses |
|-------------------|-------------------|-------------------|
| **Word** | **First Morphology** | **Second Morphology** |
| جان | ان | ئ |
| اڻن | دم | ژ |
| ژ | پر | هر |

| TABLE II: Bound Morphemes |
|-------------------------|-------------------|-------------------|
| **Derivative** | **Root** | **Suffix/ Prefix** |
| وڌ | وڌ | ئ |
| ژ | پر | هر |

| TABLE III: Independent Morphemes |
|-------------------|-------------------|-------------------|
| **Word** | **Independent Morphemes** | **Stem** |
| پرچار | پر | هر |
| خیال | ن | ژ |

| TABLE IV: Zero Morphemes |
|-------------------------|-------------------|-------------------|
| **Singular** | **Plural** |
| ژ | پر |
| ن | پر |
| ئ | پر |

294
C. Root, Derivatives and Compound Words

Sindhi does also contain the same word types alike English: root words, derivatives and compound words. These types of words are depicted in the Tables V and VI. The first words in the Table 5 show the variation of meaning only with no change in word class of the root word. The changing of the meaning into the opposite of the root word defines the nature of prefix (ب), which is used to attach with the word for making its negation or opposition. The formation of second word suggests the uniqueness of Sindhi morphology in which the only letter (ب) is the suffix of the word. In addition to this, the letter (ب) used as suffix does not affect only the formation and meaning of the word but also changes its word class from verb to a noun. The prefixes of the third and fifth words are also of the same kind as of the first. They all mostly change the meaning of the word into its negative or opposite. The fourth word contains the suffix (نی) which is used for the emphasis only. It does not change the meaning or the class of the word.

<table>
<thead>
<tr>
<th>Prefix/Suffix</th>
<th>Root Word</th>
<th>Complete Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>ب</td>
<td>بوئ</td>
<td>بوئ ب</td>
</tr>
<tr>
<td>ا</td>
<td>بجي</td>
<td>بجي ا</td>
</tr>
<tr>
<td>لا</td>
<td>شيک</td>
<td>لا شیک</td>
</tr>
<tr>
<td>سب</td>
<td>ني</td>
<td>سب نی</td>
</tr>
<tr>
<td>بتر</td>
<td>دیس</td>
<td>بتر دیس</td>
</tr>
</tbody>
</table>

The first word in the Table VI contains two words as usual compound words do. The following words containing the same formation represent another property of such words which is the coalition of adjective and noun. Each of the words in the Table 6 is formed with one adjective and one noun. This endorses that most of the compound words in Sindhi possess the same nature in terms of their formation.

<table>
<thead>
<tr>
<th>Compound Word</th>
<th>First Word</th>
<th>Second Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>زهربیاط</td>
<td>زهر</td>
<td>بیاط</td>
</tr>
<tr>
<td>نهنگیتی</td>
<td>نه</td>
<td>بیتی</td>
</tr>
<tr>
<td>خوش بوئ</td>
<td>خوش</td>
<td>بوئ</td>
</tr>
</tbody>
</table>

IV. DATA COLLECTION

Corpus of language is inevitably essential for the computational exploitation. We have made the use of Sindhi corpus of 1. 05,733 words developed by Mahar [15]. The sample of developed corpus is shown in Figure 1. It subsumes the genres of music, arts, politics, environment, and other texts. The sources for the collection of information were magazines, books of different types and newspapers. The data was collected in HTML and PDF formats. Then, they were converted into the fair equivalent formats of texts. Table VII represents the comprehensive details in figures for Sindhi corpus.

<table>
<thead>
<tr>
<th>Corpus Type</th>
<th>Sentences</th>
<th>Word Tokens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arts</td>
<td>1897</td>
<td>6884</td>
</tr>
<tr>
<td>Sports</td>
<td>1656</td>
<td>7582</td>
</tr>
<tr>
<td>Politics</td>
<td>2590</td>
<td>13351</td>
</tr>
<tr>
<td>Environment</td>
<td>1819</td>
<td>7098</td>
</tr>
<tr>
<td>Music</td>
<td>3822</td>
<td>15412</td>
</tr>
<tr>
<td>Total</td>
<td>11,784</td>
<td>50,327</td>
</tr>
</tbody>
</table>

Table VII: Statistical Information of Sindhi Corpus

A. Word Tokens

For the representation of the statistical information of this corpus, the first step was taken to break the text into the sentences. The second was the segmentation of sentences into words. This way the words were given to the system and it retained 50,327 unique word tokens. These word tokens do not represent the number of words in the given corpus but each word makes a token regardless of how many times it is used in the text.

Tokenization process is the segmentation of input objects of orthographic symbols into tokens [16]. This is the first prerequisite for NLP applications for these word tokens are then supplied to natural language processing applications for more computational processing. The word limits such as white space, digits, special signs and punctuation marks are useful for tokenization process. Apart from being useful, these sometimes also create complications in the process of tokenization. In this research, Mahar’s tokenizer [17] is used which they proposed particularly for Sindhi language only. This model is composed of three layers which works consecutively one after the other as per the requirement. The implementation of the model, as done by Mahar, has also been imitated in this research work.

B. Developed Lexicon

A large lexicon is always required as a key component for the implementation of morphological analysis. It is, in general sense, a repository of words required to test the proposed algorithms. Hence, a lexicon for computational process is built with a collection of morphemes that are prefixes, suffixes and stems.

In print and electronic media, as the most of the Arabic script-based languages are written or typed without a variety of diacritic marks required for exactness of the sense, so is the case with Sindhi. Therefore, the basic limitation is the requirement of a fully diacritized corpus in order to build a lexicon. This may create another issue of the availability of
different versions of the same word with different diacritics in the lexicon. The words, then, may cause a great ambiguity with reference to their vocalization and meaning as well. Therefore, it is crucially essential to save all the words with full diacritics in the lexicon.

A lexicon having 50,327 words is built for the implementation of proposed algorithm. The lexicon is developed to segment Sindhi words into morpheme sequences. It has five tables and each table is used for the storage of separate type of word morphemes. The tables namely are root words, compound words, prefix words, suffix words and prefix-suffix words. The developed lexicon is called Lexicon of Sindhi Morphological Analysis (LSMA). It is peculiarly constructed for proper and exact segmentation of words in Sindhi text. The lexicon contains only secondary type of words taken from the corpus. Table VIII represents the manifestation of secondary words.

<table>
<thead>
<tr>
<th>Word Types</th>
<th>No. of Words</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compound</td>
<td>541</td>
</tr>
<tr>
<td>Prefix</td>
<td>893</td>
</tr>
<tr>
<td>Suffix</td>
<td>6713</td>
</tr>
<tr>
<td>Prefix-Suffix</td>
<td>247</td>
</tr>
<tr>
<td>Total</td>
<td>8394</td>
</tr>
</tbody>
</table>

V. SINDHI WORD SEGMENTATION ALGORITHM

A word is constructed with letters in a particular sequence. The letters first build a morpheme which is the smallest grammatical unit of language. Morphological segmentation is a general method for disintegration of a word into the combination of letters. This combination is a morpheme and cannot be further disintegrated. The development of any word segmentation technique requires one to be well aware of already developed and established techniques in order to bring effectiveness to the system.

A. Word Segmentation Technique

During the literature survey of Arabic morphological analysis techniques, it has been found that three morphological approaches are mostly in use, i.e. Table Lookup Approach, Combinatorial Approach and Linguistic Approach. These approaches can also be used for Sindhi word segmentation into its possible morphemes. Many times these approaches have been used for Arabic, Persian and Urdu languages. As Sindhi language belongs to the family of these languages on the basis of its script and nature so it can be predicted that these approaches can stand useful for Sindhi.

In this paper, Table Lookup Approach is used for the segmentation of Sindhi words into possible morphemes. This approach mainly relies on a considerably large set of tables in which Sindhi words are stored and found in natural texts with their morphemes. Morphemes are set in the forms of stem, suffix and prefix. A variety of words are found in a language, i.e. foreign words, functional words and proper nouns which require a unique place in the table. Multiple entries may also be found with the same structure which is due to the fact of different types of sense relations of words among them. The sense relations include homonymy, metonymy, synonymy, hyponymy and synonyms and antonyms. Few of these relations require a word to be spelt same but meant differently. These entries enable the system to be capable of dealing with multiple analyses of the words. The entries in these tables are stored in alphabetical letter. For the optimization of search through vertical and horizontal order, a hash table stands efficient and effective to be used. In addition to this, a compression or precision technique is also possible to be used effectively for the reduction of storage needs. Thus, it makes the morphological analysis quite simple by accessing hash table.

B. Proposed Sindhi Word Segmentation Algorithm

The lexicon driven approach is used for our proposed algorithm, therefore, a lexicon named LSMA is constructed that stores all possible morphemes, and the lexicon consists on five tables {T1, T2, T3, T4, T5}. The database table T1 is constructed for storing all the possible root words. The database table T2 is constructed for storing the compound words with three column vectors T2= {C1, C2, C3}. The column C1 is used to store the complete compound word, C2 is used for storing first word and C3 is used for storing second word.

In lexicon LSMA, database table T3 is constructed for storing words having prefix morpheme, it has three column vectors T3={C1, C2, C3} where, C1 is used for storing prefix along with primary word, C2 is used for storing prefix morphemes and C3 is used for storing primary word.

The database table T4 is used for storing words having suffixes. It has three column vectors T4= {C1, C2, C3}. Each column is responsible to store the segments of words after its breakage. Thus, C1 is used for storing words having suffix along with primary word, C2 is used for storing suffix morphemes and C3 is used to store primary word.

The database table T5 is used for storing the words having both prefix and suffix morphemes at a time, this table consists of five column vectors T5= {C1, C2, C3, C4, C5}, where C1 is used for storing the complete words having prefix and suffix morphemes, C2 is used for storing only prefix and C3 is used for storing only suffix morphemes, C4 is used for storing primary word and C5 is used for storing the primary word along with suffix morpheme. Prefix and suffix lexicon entries cover all possible concatenations of Sindhi prefixes and suffixes.

Algorithm of Sindhi Word Segmentation

1. Input Sindhi Text
2. Tokenize Input Text
3. Store all word tokens into temporary array WORDTEMP
4. Select words one by one from WORDTEMP
5. Search Selected word from Column 1 of Table T1 //To check that it is a root word or not
6. If search is successful then display message “This is a Root Word” and go to step 16
Else split selected word into characters and store them into temporary array CHTEMP

Search selected word from Column 1 of Table T2 // For Compound Words

If Search is successful then
  a. Repeat until either both words are successfully compared or any word is not found in Table T2
     i. Select characters consecutively from CHTEMP and append into VAR1
     ii. Search and compare VAR1 from Column 2 of Table T2
     iii. If search is successful then
          1. Concatenate remaining characters of CHTEMP and store into VAR2
     iv. Else go to Sub-step a
     v. Search and compare VAR2 from Column 3 of Table T2
     vi. If search is successful then
          1. Display “First Word”, VAR1 and “Second Word”, VAR2
  b. End

Else search selected word from Column 1 of Table T3 // For Prefix Words

If search is successful then
  a. Repeat until both conditions are true or any morpheme is not found in Table T3
     i. Select characters consecutively from CHTEMP and append into VAR1
     ii. Search and compare VAR1 from Column 2 of Table T3
     iii. If search is successful then
          1. Concatenate remaining characters of CHTEMP and store into VAR2
     iv. Else go to Sub-step a
     v. Search and compare VAR2 from Column 3 of Table T3
     vi. If search is successful then
          1. Display “Prefix”, VAR1 and “Root Word”, VAR2
  b. End

Else search selected word from Column 1 of Table T4 // For Suffix Words

If Search is successful then
  a. Repeat until both conditions are true or any morpheme is not found in Table T4
     i. Select characters consecutively from CHTEMP and append into VAR1
     ii. Search and compare VAR1 from Column 3 of Table T4
     iii. If search is successful then
          1. Concatenate remaining characters of CHTEMP and store into VAR2
     iv. Else go to Sub-step 1
     v. Search and compare VAR2 from Column 2 of Table T4
     vi. If search is successful then
          1. Display “Root Word”, VAR1 and “Suffix”, VAR2
  b. End

Else search selected word from Column 1 of Table T5 // For Prefix-Suffix Words

If search is successful then
  a. Repeat until all conditions are satisfied or any morpheme is not found in Table T5
     i. Select characters consecutively from CHTEMP and append into VAR1
     ii. Search and compare VAR1 from Column 2 of Table T5
     iii. If search is successful then
          1. Concatenate remaining characters of CHTEMP and store into VAR2
     iv. Else go to Sub-step a
     v. Search and compare VAR2 from Column 3 of Table T5
     vi. If search is successful then
          1. Display “Prefix”, VAR1
     vii. Split VAR2 into characters and store into array SUTEMP
     viii. Select characters consecutively from SUTEMP and append into SVAR1
     ix. Search and compare SVAR1 from Column 4 of Table T5
     x. If search is successful then
        1. Concatenate remaining characters of SUTEMP and store into SVAR2
     xi. Else go to Sub-step viii
     xii. Search and compare SVAR2 from Column 3 of Table T5
     xiii. If search is successful then
          1. Display “Root Word”, SVAR1 and “Suffix”, SVAR2
  b. End

End

The process of proposed algorithm starts with the input step of the text. The text can be input through two ways: it can be typed and produced to the system and can also be taken from the corpus of the language. Once the text is input, the process has begun. The input text is tokenized at the beginning of the process. The tokenization model of Mahar [18] has been used in this system. The tokenization sends the prepared tokens to an array called WordTemp. This array stored the word tokens so that they can be forwarded forth. The system then takes each token from WordTemp one by one and starts searching the match for the selected word. The first search is carried out in Table1 Column1. If the search is successful, system displays the word as a “Root Word”. The process does not go further for the search is over and the match is found. This is because
we have stored the root words in Table1 Column1 and the successful search witnesses the word as a root one. If the search is unsuccessful and match is not found, the control shifts to the next search step. Before moving to the next search, the system splits the word into separate characters that constitute it and stores them in an array called CHTEMP.

VI. IMPLEMENTATION AND RESULTS

After the details for the familiarization of our developed algorithm, the algorithm is taken into its application in the system. The application process is defined in this section along with the results received after the application. The results are not calculated at a whole but for the acute evaluation of the system, we have categorized the process into different parts. The system has been evaluated through separate classes of words i.e. prefix words, suffix words, prefix-suffix word and compound words.

The performance of algorithm is evaluated by rating the correctly and incorrectly segmented words as given in [19]. Moreover, the segmentation error rate with each word class is calculated so that the vivid and transparent results can be obtained. These separate word class results will also help find the causes and issues that reduce the success rate of the system. This calculation standard is used under the influence of [19], Segmentation error rate (SER) is defined as:

\[
\text{SER} = \frac{\text{Number of incorrectly segmented words}}{\text{total number of word}} \times 100
\]

A. Compound Words

The main algorithm first makes it sure that the word is not a root one then it shifts to the search of the forwarded word in Table2 Column1 for searching if the word if compound one. The successful search shifts control of main algorithm to the Module Compound Words. The process begins by taking in the split letters stored in CHTEMP one by one until VAR1 is formed by achieving a match from Column2 of this table. Once, the match is found and VAR1 is formed, the system generates VAR2 taking the remaining letters from CHTEMP. The forming of VAR1 requires a repetition process by appending letters one by one from CHTEMP. VAR2 is formed and it also requires a condition of must-match in Column3 of the table. When both conditions are fulfilled and VAR1 and VAR2 are formed the system displays the result by showing first word as VAR1 and second word as VAR2.

After the selection of a word, the splitting into separate characters takes place and each character is selected one by one and all these characters are being appended and stored into a temporary generated variable. Then, system compares the contents of this variable with T2-C2. If the characters are matched properly, the concatenation of remaining characters starts and then these remaining characters and fed into another variable and again the comparison starts with T2-C3, in case of successful match, the system displays both words. For example, نینه رات (Day Night), each character is taken into process from right to left like and it is compared with column C2, then ی is selected and both are appended together and again compared with C2. The system consecutively selects third character ث and again all are appended and compared with C2. The successful search leads to the concatenation of remaining characters ن، ن، ي، ذ، ر through the same procedure and comparison takes place with B3. After both conditions are fulfilled, words are displayed as word1 نینه and word2 is رات

In order to scrutinize and verify the system efficiency and performance, we took 109 words randomly for testing. These words were taken from training dataset of 541 words. The number of taken words stands 20% of training data. For experimental purpose, compound words were categorized into two classes; the words having a hard space in between like گل پیلی (Rose) and the words having no hard space like گلاب (Every Moment). The gist of results is given in Table IX. The pictorial representation of word SER is given in Figure 2.

<table>
<thead>
<tr>
<th>Compound Word Classes</th>
<th>No. of Words</th>
<th>Correct (SER)</th>
<th>Incorrect (SER)</th>
<th>Total (SER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Hard Space</td>
<td>82</td>
<td>82</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Without Hard Space</td>
<td>27</td>
<td>26</td>
<td>1</td>
<td>3.7</td>
</tr>
<tr>
<td>Total</td>
<td>109</td>
<td>108</td>
<td>1</td>
<td>3.7</td>
</tr>
</tbody>
</table>

The complication of compound words is observed during the process of morphological analyzer. It is particularly observed with the words having connecting letters in between the compound words. This leads to the erroneous depiction of morphemes in such situations. In addition to this, certain compound words have non-connective letters in between. They lead to another erroneously segmented morpheme for the remaining non-connecting letters in the second word form a word that has an entirely different meaning from the actual sense of the whole compound word. Thus, two erroneous morphemes are segmented by analyzer in this case. The situation leads to an increase in SER of the morphological analyzer. Due to these issues, the SER of the proposed morphological reached 3.7% with the compound words having no hard space in between and 0.0 with those having hard space.

![Fig.2. Word SER using Module COMPOUND](image-url)
B. Prefix Words
The second step of search ends in two conditions; the word is
compound and process shifts by executing Module Compound
Word and second condition is taking the process to a search in
Table3 Column1. The successful search in this table starts the
execution of Module Prefix Words. The PREFIX module
receives a word from main algorithm as input and splits it into
characters, system selects each character one by one and
appends it into temporary generated variable and then
comparer the contents of this variable with T3→C2, if
comparison is successful, then concatenates remaining
characters and stores into another variable and compares it
with T3→C3, if search is successful, then system displays both
morpheors. For example, پریون (unloyal), the system selects
each character from right to left like ب and compares it with
column C2, then selects character ب and appends it as next
character and compares with C2, if search is successful, then
concatenates remaining characters و and compares with
C3, when both conditions are satisfied, then system displays
prefix پریون and root Word.
The appending of letters and searching for a match in Column3
is repeatedly performed till VAR1 is formed and match is
sought out in Column3. The VAR2 is formed by appending the
remaining letters together and the search is performed in
Column3 of the table. Column3 has the root words in it. It is
also understood that formulation of VAR1 extracts the prefix
from the word and leaves the remaining letters which must
form a stem and VAR2 as well. VAR1 is compared with the
words stored in Column2 and VAR2 is compared with the
words stored in Column3. After achieving both matches, the
system shows the result as VAR1 “Prefix” and VAR2 “Root
Word”.
Evaluating the performance of this module, 179 words were
randomly taken from the training dataset containing 893
words. The words having prefixes are classified into three
categories: (1) The prefix words showing the sense of negation
like بد بخت (unlucky) (2) The prefix words showing the sense
of adjective like لاجر طاب (matchless) and (3) The prefix words
showing the sense of antonym بکیرو (abroad). The summary
of results is shown in Table X. The SER of negation, adjective,
and antonym is depicted in Figure 3.

TABLE X: Summary of Results using Module PREFIX

<table>
<thead>
<tr>
<th>Prefixes Classes</th>
<th>No. of Words</th>
<th>Correct</th>
<th>Incorrect</th>
<th>SER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negation</td>
<td>68</td>
<td>67</td>
<td>1</td>
<td>1.47</td>
</tr>
<tr>
<td>Adjective</td>
<td>97</td>
<td>94</td>
<td>3</td>
<td>3.09</td>
</tr>
<tr>
<td>Antonym</td>
<td>14</td>
<td>14</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Total</td>
<td>179</td>
<td>306</td>
<td>10</td>
<td>4.56</td>
</tr>
</tbody>
</table>

The calculated results depict that the SER of Negation and
adjective is higher than that of Antonym. Since the prefixes
used to form a negative or opposite sense to that of the original
meaning of the particular word can stand as a word separately
with their own meaning. Such prefixes are also used as in
individual word in Sindhi text. Therefore, morphological
analyzer segments them as a separate word sometimes and its
SER increases relatively. On the other hand, simple Antonyms
having prefixes are segmented successfully with the SER of
2.3% which is lesser than that of Negation and Adjectives.

C. Suffix Words
The SUFFIX module takes the word given as input and split it
into characters, system selects each character one by one and
appends it into temporary generated variable, and then,
comparer the contents from T4→C3, if comparison is
successful, then concatenates remaining characters and
comparer with T4→C2, if search is successful, then system
displays both morphemes. For example, سیمی (All to all),
the system selects each character from right to left like س and
comparer it with column C3, then selects character پ and
appends it as next character and compares with C3, if search is
successful, then concatenate remaining characters د ی ن و
and compares with C2, when both conditions are satisfied, then
system displays root word سیمی and suffix د ی ن و.
The process of this module begins with the input of separately
stored letters of the selected word in CTEMP. One by one,
the letters are brought in till VAR1 is formed. After the
formulation of VAR1 the module searches for its match in
Column2. Column2 is responsible to store the root words
therefore VAR1 in this module is the formulation of root
words. The appending of letters and searching their match in
Column is repeatedly done till its formulation and final match
in Column2. After VAR1, the module appends all the
remaining letters and forms VAR2 which is a suffix and such
type is stored in Column3. VAR2 is compared with the
combination of letters stored in Column2 to find its match.
After achieving the successful matches of VAR1 and VAR2 in
their respective columns, the system displays result as VAR1
“Root Word” and VAR2 “Suffix”.
The number of words taken randomly for testing from the
training dataset was 1343. The total number of words in
training dataset was 6713. The selected sample was taken in
order to gauge the performance of this module. For
experimental purpose, words with suffixes were categorized
into 5 classes: (1) the suffix words in singular sense like
پکیرو
(Hungry) (2) the suffix words of plurality like (Jewlars) (3) the suffix words showing adjectival meaning like (Boy) (4) the suffix words classed in masculine like (Lucky) (5) the suffix words of feminine like (Wife). The summary of results with the standard of SER is given in Table XI. The graphical representation of results is given in Figure 4.

The depiction of results proves Masculine class to be yielding the least SER in all. On the other hand Feminine class as well as Singular has acceptable level results with 1.79% and 1.85% SERs respectively. The cumulative SER is 8.84%. This is due to the Plural class of suffix words which stands with an SER of 2.94%. Due to this class, the performance of whole system is affected and led to a higher level of SER. The reduction of SER in plural will ultimately improve the performance of the system. Eventually, besides Singular and Plural, the results are considerably better and encouraging as well.

![Graphical representation of results](https://sites.google.com/site/ijcsis/)

**Fig.4. Calculated SER using Module SUFIX**

D. Prefix-Suffix Words

The process of Module Suffix Words begins with the input of separately stored letters of the selected word in CTEMP. One by one, the letters are brought in till VAR1 is formed. After the formulation of VAR1 the module searches for its match in Column2. Column2 is responsible to store the prefix morphemes therefore VAR1 in this module is the formulation of prefix morphemes. The appending of letters and searching their match in Column2 is repeatedly done till its formulation and final match in Column2 is found. After VAR1, the module appends all the remaining letters and forms VAR2 which is the remaining part of the word containing the root and suffix and such type is stored in Column4. VAR2 is compared with the combination of letters stored in Column4 to find its match. After achieving the successful matches of VAR2 in its respective column, the system displays result as VAR1 “Prefix”. After producing the result of VAR1 Prefix, the system concatenates the VAR2 and split it into letters. The split form is stored in another array called SUTEMP. The selection of letters one by one from SUTEMP and appending them again starts till a SVAR1 is formed. After forming SVAR1, the system starts searching the match for SVAR1 from Column4 where primary words are stored. If system succeeds to find the match, it concatenates the remaining letters taken from SUTEMP and forms SVAR2. Then SVAR2 is compared with the words stored in Column3. After finding the match of SVAR2 in Column3, the system displays the result as SVAR1 “Root Word” and SVAR2 “Suffix”. It is noted that the concatenation and appending of the letters from TEMPs are repeatedly done till the search comes successful. The “Else” condition drives the system to jump to the previous step of concatenation and appending of letter and continues it till the match is found in the column. This module is based on two phases: system segments prefix and the stem in first phase and it cuts off suffix from the root word in the second. The word is appointed into the module from the main algorithm as input and concatenates it into separate characters. System takes each character one by one respectively and keeps appending them into a temporarily generated variable. While appending the characters it also keeps on comparing the contents of this variable from T5→C2. As the comparison comes to a successful match, then the remaining letters are concatenated and stored into another variable. Once more, the splitting and appending takes place and storing the characters into variable while comparing them with T5→C4. Till the match comes successful during comparison process, then the rest of the letters are stored and the process repeats itself again undergoing each step that are already described. After the successful match while comparing the contents with T5→C3, the system displays three parts of the word.

For example, پر و سی (Foreigner), the system takes each character from right to left i.e. پر and compares it the contents in C2, it selects سی and appends to the previous character and again compares with C2, after successful search it concatenates the rest of the letters. پر و سی and takes them through the same process. When the stem پر is successfully segmented, it looks for the other characters و and does comparison with the contents of C3, after the fulfillment of all three conditions; system shows a display of prefix پر root word سی and suffix و. A list containing 247 words was prepared for training 50 words. These words were tested through the system in this module. The outcomes are shown in Table XII.

**TABLE XII: Results using Module PREFIX-SUFFIX**

<table>
<thead>
<tr>
<th>No. of Words</th>
<th>Correct</th>
<th>Incorrect</th>
<th>SER</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>46</td>
<td>4</td>
<td>8.0</td>
</tr>
</tbody>
</table>
E. Cumulative Results
The developed morphological analyzer has been gauged in testing 109 compound words, 179 prefix words, 1343 suffix words and 50 prefix-suffix words. The overall results showed the SER of 5.02%. The calculated cumulative word segmentation error rate of different word classes is given in Table XIII. The Figure 5 depicts the cumulative segmentation error rate of the system in graphical form.

TABLE XIII Cumulative SER of Each Word Types

<table>
<thead>
<tr>
<th>Types of Words</th>
<th>Segmentation Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compound</td>
<td>3.7</td>
</tr>
<tr>
<td>Prefix</td>
<td>4.56</td>
</tr>
<tr>
<td>Suffix</td>
<td>8.84</td>
</tr>
<tr>
<td>Prefix-Suffix</td>
<td>8.0</td>
</tr>
<tr>
<td>Cumulative SER</td>
<td>5.02</td>
</tr>
</tbody>
</table>

The results show that compound words have resulted the least SER which is encouraging part of the work. The SER of these words is 3.7% cumulatively. Segmentation of suffix words produces an SER of 8.84% and the reason of its height is already described as the Adjectives with suffixes sometimes stand as completely separate words in Sindhi script. The SERs produced after suffix words and prefix-suffix words are at a little difference of 0.84%.

VII. WORD SEGMENTATION APPLICATION
In spite of all the details given about the developed algorithm, its function, application and results, the need of more clarity remains intact for the understanding the whole research and its processed outcome through the system. The interface contains two boxes that are connected with the process of the given text. The upper box is responsible to show the text that is input into the system. This box not only accommodates the direct typing of the text but has a property of receiving an already developed file as its input. The system processes the text that is directly typed. In otherwise case, it receives the files which are in doc. format only.

After the text is input into the system, the user has to click the Process Menu and a pop-up will appear in a drop-down box. The box has three options i.e. Apply, Data Setting and Clear. As the user will click the Apply button, this will activate the system to take the text for processing. The process ends up by showing the results in the output box of the interface. The depiction of input box and outbox are totally different in terms of the organization of the text. The input box takes the plain text as it is typed. The input and output box depicts the results in six different columns as shown in Figure 6. These columns have been assigned their respective morphemes. Each word from the text is processed and put into its respective column. The columns are given the names of the morphemes found in Sindhi language. Each column receives a particular morpheme taken out of the word after segmentation.

Fig.5. Cumulative Words SER of Proposed Algorithm

VIII. DISCUSSION AND CONCLUSION
Sindhi language has been considered as one the most complex languages when it comes to automatic language applications. The abundance of homographs in orthography of Sindhi and its cursiveness prove the above fact. Such nature embeds the hurdles in the way of word segmentation process. The affixes become rather complex to be segmented due to cursiveness. Thus, the developed word segmentation system is designed in such a way so that it should segment these basic grammatical units as an embarking source to NLP Applications. The proposed algorithm possesses the capability to deal with all the basic grammatical units of Sindhi: Root words, Prefixes and Suffixes and provides the base for segments its words into morphemes.

The two data sets are extracted from our developed lexicon for experimental purpose: the training data set and the testing data set. The testing data set contains 109 compound words, 179 prefix words, 1343 suffix words and 50 suffix-prefix words. After the process of words segmentation, compound words yielded the SER of 3.7%, the prefix words gave an SER of 4.56%, and suffix words did 8.84% and prefix-suffix words 8%. The individual calculation and cumulative segmentation error rates of the proposed algorithm derive out that the results have come up to the acceptable level. Although, 5.02% SER is produced, the correct segmentation supports the effectiveness of the proposed algorithm with an exactitude rate of 94.08%. It is a proven fact that Sindhi word segmentation is an essential for its application in any natural language processing task. The received results have achieved an acceptable level, though; they are not up to the mark as they should be. This
piece of research has paved a way to reach the ultimate accuracy in NLP applications for Sindhi language. The current SER is surely possible to decrease in future; the achieved SER is a little high due to the limited lexicon. The SER can easily be decreased if the lexicon is extended to a great extent. The table lookup approach is used for automatic word segmentation system. If the approached as combined at least two, the algorithm will be more useful for the same task. Hence, in future, we shall also test the combined system of combinatorial and linguistic approaches.

REFERENCES


A new secret sharing scheme using rational interpolation

Ali Nakhaei Amroudi,
Department of Mathematics and Cryptography,
Malek-Ashtar University of Technology,
Isfahan, Iran,

Ali Zaghian
Department of Mathematics and Cryptography,
Malek-Ashtar University of Technology,
Isfahan, Iran,

Mahdi Sajadieh
Department of Electrical Engineering,
Islamic Azad University,
Isfahan (Khorasgan) Branch, Isfahan, Iran,

Abstract—Most of the existing secret sharing schemes are based on polynomial interpolation. In other word, they use polynomial functions in their schemes. In this paper, we solve the problem of creating a secret sharing scheme based on rational interpolations. We show that if \( \kappa \geq \max\{\mu, \nu\} + 1 \) support points have the same width then the rational interpolation of the support points, which is called \( \varphi(\mu, \nu)(x) \), has \( \mu + \nu + 1 - \kappa \) pole points. Finally, we give an example for the accuracy of the proposed scheme.

Keywords-component; Secret Sharing Scheme; Shamir’s Scheme; Polynomial Interpolation; Rational Interpolation, Pole Points.

I. INTRODUCTION

Secret sharing schemes are important tools in modern cryptography. Some of applications of secret sharing schemes are access control, secure key management systems, secure multi-party protocols, electronic voting and etc. [1, 2]. In other word, secret sharing schemes can be used for any situation in which the access to an important resource has to be distributed over several parties. The case of opening bank vaults or launching a nuclear missile are both situations in which a secret sharing scheme can be utilized [20].

A secret sharing scheme is a method to distribute shares of a secret (called shadows) among a set of participants which is called P by giving each participant a share in such a way that only certain pre-specified subsets of P are qualified to recover the secret while any unqualified subset of P cannot do the same thing.

The first \((t, n)\) -threshold secret sharing schemes were introduced by Shamir [3] and Blakley [4] independently based on Lagrange interpolating polynomial and linear projective geometry respectively. Jackson et al. [18] extended the \((t, n)\)- threshold secret sharing scheme to the multi-secret case, named \((k, t, n)\) -threshold multi-secret sharing scheme, which holds the robustness property and confidentiality property. Robustness means that the shared \(k\) secrets can be recovered when \(t\) or more secret shadows are pooled, and confidentiality means that the shared secrets cannot recovered when \(t - 1\) or fewer secret shadows are pooled. In verifiable multi-secret sharing, there are multiple secrets to be shared during a secret sharing process, and any cheating by a dealer or by participants can be detected.

In the generation step of Shamir’s secret sharing scheme the dealer chooses \(f(x)\), a polynomial of degree \(n\), and computes the secret shares

\[ p_i = (x_i, f(x_i)) \text{ for } i = 0, 1, \ldots, n. \]

In this paper, we analyze the plausibility of secret sharing schemes based on non-polynomials with achieving the properties of a perfect secret sharing scheme. Note that we suppose that all devices have the same precision without less than generality.

The outline of this paper organized as follows: In section 2, we present some preliminaries consist of interpolation and Shamir’s secret sharing. Section 3 is devoted to introduce the Shamir’s secret sharing scheme based on non-polynomial interpolation. Finally, we present an example of the scheme in section 4.
II. PRELIMINARIES

A. Interpolation

Interpolation problem is one of the most important topics in applied mathematics.

**Definition 1.** Consider a family of function of a single variable \( x \),

\[
\phi(x, a_0, a_1, ..., a_n),
\]

having \( n + 1 \) parameters \( a_0, a_1, ..., a_n \), whose values characterize the individual functions in this family. The interpolation problem for \( \phi \) consists of determining these parameters \( a_i \) so that for \( n + 1 \) given real or complex support points \( (x_i, f_i) \) the relation

\[
\phi(x_i, a_0, a_1, ..., a_n) = f_i
\]

holds for \( i = 0, 1, ..., n \) where \( x_i \neq x_k \) for \( i \neq k \).

Interpolation problem is called linear interpolation problem if \( \phi \) depends linearly on the parameters \( a_s \), i.e.

\[
\phi(x, a_0, a_1, ..., a_n) = a_0 \phi_0(x) + a_1 \phi_1(x) + ... + a_n \phi_n(x)
\]

where

\[
\phi_0(x), \phi_1(x), ..., \phi_n(x)
\]

are functions of variable \( x \). This class of problems includes the classical one of polynomial interpolation in form of

\[
\phi(x, a_0, a_1, ..., a_n) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n
\]

as well as trigonometric complex interpolation in the form of

\[
\phi(x, a_0, a_1, ..., a_n) = a_0 + a_1 e^{xi} + a_2 e^{2xi} + ... + a_n e^{nxi}.
\]

The class of linear interpolation problems also contains spline interpolation. The class of polynomial interpolation can be solved by Newton’s divided differences. The rational interpolation problem is defined as follows:

**Definition 2.** Consider the rational function

\[
\phi^{(\mu, \nu)}(x) = r(x)/s(x)
\]

such that \( \mu + \nu = n \),

\[
r(x) = a_0 + a_1 x + ... + a_\mu x^\mu
\]

and

\[
s(x) = b_0 + b_1 x + ... + b_\nu x^\nu
\]

are two polynomials of degree \( \mu \) and \( \nu \) respectively. Rational interpolation problem is the determining \( n + 2 \) parameters

\[
a_0, a_1, ..., a_\mu, b_0, b_1, ..., b_\nu
\]

of \( \phi^{(\mu, \nu)}(x) \) such that \( \phi^{(\mu, \nu)}(x_i) = f_i \) using \( n + 1 \) support points \( (x_i, f_i) \), for \( i = 0, 1, ..., n \).

In Definition 2, if \( \phi^{(\mu, \nu)}(x_i) \neq f_i \), then the support point \( (x_i, f_i) \) is called a pole point. Berrut and Mittelmann suggested a method to avoid poles by using rational functions of higher degree [21]. Some mathematician surveyed various aspects of this kind of interpolation and proposed several algorithms. For more details see [22-24].

B. Shamir’s secret sharing scheme

A secret sharing scheme consists of a dealer and \( n + 1 \) participants \( P_0, P_1, ..., P_n \). The dealer computes secret shares and distributes them to the participants such that a qualified subset of participants can recover the secret. In fact, a secret sharing scheme consists of three steps: generation, distribution, and reconstruction. In the generation step, all the necessary data are computed. In fact, the dealer computes the secret shares such that any information about secret does not leak. In the distribution step, the dealer distributes secret shares to participants. Finally, in the reconstruction step, only a qualified subset of participants can retrieve the secret. In a verifiable secret sharing scheme, the participants can verify their shares. In addition, in some schemes the dealer can distinguish malicious participant. Suppose that \( S \) denotes the secret. The Shamir’s \( (k, n + 1) \)-threshold secret sharing scheme is defined as follows:

**Definition 3.** The Shamir’s \( (k, n + 1) \)-threshold secret sharing scheme consists of three algorithms:

- **Generation:** The dealer chooses the integer numbers \( x_0, x_1, ..., x_n \), the prime number \( p \) and a function \( f(x) \) of degree \( k \) such that \( S = f(0) \mod p \). Then he/she computes the secret shares \( s_i = (x_i, f(x_i) \mod p) \) for \( i = 0, 1, ..., n \).
- **Distribution:** The dealer distributes \( s_i \) to \( P_i \) for \( i = 0, 1, ..., n \).
- **Reconstruction:** Any \( k \) members of participants retrieve the secret using polynomial interpolation of their shares.

III. POLE POINTS

In this section, we prove the existence of pole points in the rational interpolations.

**Theorem 1.** Let \( P = \{(x_i, y_i), 0 \leq i \leq n\} \) be the set of support points. Suppose that \( k \) is the number of support points with the same width \( \beta \). Then the rational interpolation function \( \phi^{(\mu, \nu)}(x) \) of \( P \) is \( \beta \), if \( \max\{\mu, \nu\} + 1 \leq k \) where \( \mu + \nu = n \).

**Proof.** It is enough to show that if \( \max\{\mu, \nu\} + 1 = k \), then \( \phi^{(\mu, \nu)}(x) = \beta \). We find the rational interpolation function

\[
\phi^{(\mu, \nu)}(x) = (a_0 + ... + a_\mu x^\mu)/(b_0 + ... + b_\nu x^\nu)
\]

(1)

using \( n + 1 \) support points

\[
\{(x_0, \beta), ..., (x_{k-1}, \beta), (x_k, y_k), ..., (x_n, y_n)\}
\]

where

\[
\max\{\mu, \nu\} + 1 = k, \ y_j \neq \beta \ (k \leq j \leq n) \ \text{and} \ \mu + \nu = n.
\]

We substitute these support points to relation (1) as follows:

\[
\begin{align*}
\beta(b_0 + b_1 x_0 + ... + b_\nu(x_0)^\nu) &= a_0 + ... + a_\mu(x_0)^\mu \\
&\vdots \\
\beta(b_0 + b_1 x_{k-1} + ... + b_\nu(x_{k-1})^\nu) &= a_0 + ... + a_\mu(x_{k-1})^\mu \\
y_k(b_0 + b_1 x_k + ... + b_\nu(x_k)^\nu) &= a_0 + ... + a_\mu(x_k)^\mu \\
&\vdots \\
y_n(b_0 + b_1 x_n + ... + b_\nu(x_n)^\nu) &= a_0 + ... + a_\mu(x_n)^\mu
\end{align*}
\]
The above relation can be written as

\[ AX = 0 \]

in which

\[ A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \]

\[ X = (b_0, \ldots, b_\nu, a_0, \ldots, a_\mu)^T \]

and

\[ A_1 = \begin{pmatrix} \beta \beta x_0 & \cdots & \beta (x_0)^\nu \\ \beta \beta x_1 & \cdots & \beta (x_1)^\nu \\ \vdots & \vdots & \vdots \\ \beta \beta x_{\kappa-1} & \cdots & \beta (x_{\kappa-1})^\nu \end{pmatrix}_{\kappa \times (\nu + 1)} \]

\[ A_2 = \begin{pmatrix} -1 & -x_0 & \cdots & -(x_0)^\mu \\ -1 & -x_1 & \cdots & -(x_1)^\mu \\ \vdots & \vdots & \vdots & \vdots \\ -1 & -x_{\kappa-1} & \cdots & -(x_{\kappa-1})^\mu \end{pmatrix}_{\kappa \times (\mu + 1)} \]

\[ A_3 = \begin{pmatrix} y_0 & y_0 x_k & \cdots & y_0 (x_k)^\nu \\ y_0 & y_{\kappa+1} x_k & \cdots & y_{\kappa+1} (x_k)^\nu \\ \vdots & \vdots & \vdots & \vdots \\ y_n & y_n x_n & \cdots & y_n (x_n)^\nu \end{pmatrix}_{(n-k) \times (\nu + 1)} \]

\[ A_4 = \begin{pmatrix} -1 & x_k & \cdots & -(x_k)^\mu \\ -1 & x_{\kappa+1} & \cdots & -(x_{\kappa+1})^\mu \\ \vdots & \vdots & \vdots & \vdots \\ -1 & x_n & \cdots & -(x_n)^\mu \end{pmatrix}_{(n-k) \times (\mu + 1)} \]

We have three cases: I) \( \nu = \mu \), II) \( \nu < \mu \) and III) \( \nu > \mu \):

I) \( \nu = \mu \): In this case, consider the matrix

\[ C = [A_1 | A_2] = \begin{pmatrix} \beta & \beta x_0 & \cdots & \beta (x_0)^\nu \\ \beta & \beta x_1 & \cdots & \beta (x_1)^\nu \\ \vdots & \vdots & \vdots & \vdots \\ \beta & \beta x_{\kappa-1} & \cdots & \beta (x_{\kappa-1})^\nu \end{pmatrix} \]

and the matrix \( F = (\beta I_{\kappa \times (\nu + 1)}) - I_{\kappa \times (\nu + 1)} \) using elementary row operations. In other words, \( AX = 0 \) is equivalent to \( A \bar{X} = 0 \). The first \( \kappa \) rows of \( \bar{X} \) yield \( a_i = \beta b_i \) for \( i = 0, 1, \ldots, \nu \). Therefore

\[ \varphi^{\nu,\nu}(x) = \frac{a_0 + a_1 x + \cdots + a_\nu x^\nu}{b_0 + b_1 x + \cdots + b_\nu x^\nu} = \frac{\beta b_0 + \beta b_1 x + \cdots + \beta b_\nu x^\nu}{b_0 + b_1 x + \cdots + b_\nu x^\nu} = \beta. \]

II) \( \nu < \mu \): In this case \( \kappa = \max(\mu, \nu) + 1 = \mu + 1 \).

Consider the matrix

\[ C = [A_1 | A_2] = \begin{pmatrix} \beta & \beta x_0 & \cdots & \beta (x_0)^\nu \\ \beta & \beta x_1 & \cdots & \beta (x_1)^\nu \\ \vdots & \vdots & \vdots & \vdots \\ \beta & \beta x_{\mu-1} & \cdots & \beta (x_{\mu-1})^\nu \end{pmatrix} \]

and the matrix \( F = (\beta I_{\kappa \times (\nu + 1)}) - I_{\kappa \times (\nu + 1)} \) using elementary row operations. In other words, \( AX = 0 \) is equivalent to \( A \bar{X} = 0 \). The first \( \kappa \) rows of \( \bar{X} \) yield \( a_i = \beta b_i \) for \( i = 0, 1, \ldots, \nu \). Therefore

\[ \varphi^{\nu,\nu}(x) = \frac{a_0 + a_1 x + \cdots + a_\nu x^\nu}{b_0 + b_1 x + \cdots + b_\nu x^\nu} = \frac{\beta b_0 + \beta b_1 x + \cdots + \beta b_\nu x^\nu}{b_0 + b_1 x + \cdots + b_\nu x^\nu} = \beta. \]

We rewrite \( C \) as \( \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix} \) in which

\[ C_1 = \begin{pmatrix} \beta & \beta x_0 & \cdots & \beta (x_0)^\nu \\ \beta & \beta x_1 & \cdots & \beta (x_1)^\nu \\ \vdots & \vdots & \vdots & \vdots \\ \beta & \beta x_{\mu-1} & \cdots & \beta (x_{\mu-1})^\nu \end{pmatrix}_{(\mu+1) \times (\nu + 1)} \]

\[ C_2 = \begin{pmatrix} -1 & -x_0 & \cdots & -(x_0)^\mu \\ -1 & -x_1 & \cdots & -(x_1)^\mu \\ \vdots & \vdots & \vdots & \vdots \\ -1 & -x_{\nu} & \cdots & -(x_{\nu})^\mu \end{pmatrix}_{(\nu + 1) \times (\mu + 1)} \]

\[ C_3 = \begin{pmatrix} \beta & \beta x_{\nu + 1} & \cdots & \beta (x_{\nu + 1})^\nu \\ \beta & \beta x_{\nu + 2} & \cdots & \beta (x_{\nu + 2})^\nu \\ \vdots & \vdots & \vdots & \vdots \\ \beta & \beta x_{\mu-1} & \cdots & \beta (x_{\mu-1})^\nu \end{pmatrix}_{(\mu-\nu) \times (\nu + 1)} \]

\[ C_4 = \begin{pmatrix} -1 & -x_{\nu + 1} & \cdots & -(x_{\nu + 1})^\mu \\ -1 & -x_{\nu + 2} & \cdots & -(x_{\nu + 2})^\mu \\ \vdots & \vdots & \vdots & \vdots \\ -1 & -x_{\mu-1} & \cdots & -(x_{\mu-1})^\mu \end{pmatrix}_{(\mu-\nu) \times (\mu + 1)} \]

We show that \( C \) is equivalent to

\[ \tilde{C} = \begin{pmatrix} \tilde{C}_1 & \tilde{C}_2 \\ \tilde{C}_3 & \tilde{C}_4 \end{pmatrix}, \]

in which

\[ \tilde{C}_1 = \beta I_{(\nu + 1) \times (\nu + 1)} - I_{(\nu + 1) \times (\nu + 1)} \]

\[ \tilde{C}_2 = 0_{(\nu + 1) \times (\nu + 1)} \]

\[ \tilde{C}_3 = 0_{(\nu + 1) \times (\nu + 1)} \]

\[ \tilde{C}_4 = \beta I_{(\mu + 1) \times (\mu + 1)} - I_{(\mu + 1) \times (\mu + 1)} \]

Since any row of \([C_1 | C_2]\) is a linear combination of rows of \([\tilde{C}_1 | \tilde{C}_2]\), the matrix \( C \) is equivalent to the matrix \( \tilde{C} \) using case I).

Moreover, the matrix \( V = \begin{pmatrix} C_2 & C_1 \\ C_3 & C_4 \end{pmatrix} \) is invertible, because it is Vandermonde’s matrix. Therefore, the matrix \( C \) is equivalent to the matrix

\[ \tilde{C}^{\mu_3} = \begin{pmatrix} \tilde{C}_1 & \tilde{C}_2 \\ \tilde{C}_3 & \tilde{C}_4 \end{pmatrix} \]

in which the matrix \( I_{(\mu-\nu) \times (\mu-\nu)} \) is an identity matrix. The matrix \( \tilde{C}^{\mu_3} \) is equivalent to the matrix

\[ \tilde{C} = \begin{pmatrix} \tilde{C}_1 & \tilde{C}_2 \\ \tilde{C}_3 & \tilde{C}_4 \end{pmatrix} \]

where

\[ \varphi(x) = \frac{\beta b_0 + \beta b_1 x + \cdots + \beta b_\nu x^\nu + 0x^\nu + \cdots + 0x^\mu}{b_0 + b_1 x + \cdots + b_\nu x^\nu} = \beta. \]
Case III) $\nu > \mu$: This case is similar to previous case.

The following corollary shows the existence of pole points in a rational interpolation.

**Corollary 1.** Let $P = \{(x_i, y_i), 0 \leq i \leq n\}$ be the set of support points. Suppose that $\kappa$ is the number of support points with the same width $\beta$.

i) If $\kappa \geq \max\{\mu, \nu\} + 1$ then the rational interpolation of the members of $P$ has at least $n - \kappa = \mu + \nu - \kappa$ pole points.

ii) If $\kappa < \max\{\mu, \nu\} + 1$ then the rational interpolation of the members of $P$ has not any pole point.

This corollary shows that the rational interpolation function $\varphi_{\mu, \nu}(x)$ of the points

$P = \{(x_0, \beta), \ldots, (x_{n-1}, \beta), (x_n, y_n), \ldots, (x_n, y_n)\}$

has not pole points if $\max\{\mu, \nu\} \geq \kappa$.

**IV. THE PROPOSED SCHEME**

We know that the secret $S$ and the values $x_0, x_1, \ldots, x_n, f(x_0), f(x_1), \ldots, f(x_n)$ are integer numbers in Shamir’s secret sharing scheme. Also, the dealer is constrained to choose a polynomial function $f(x)$ in which the degree of function $f(x)$ is $n$. In this section, we use Shamir’s $(n+1, n+1)$-threshold secret sharing scheme to introduce a new $(n+1, n+1)$-threshold secret sharing scheme based on rational interpolation. Suppose that $\varphi_{\mu, \nu}(x)$ is a rational function in accordance with Definition 2. We propose a new $(n+1, n+1)$-threshold secret sharing based on rational function as follows:

- **Generation:** The dealer performs the following steps:
  1. Choose two integer numbers $\mu = 1$ and $\nu = 2$ such that $\mu + \nu = 3$.
  2. Choose $n+1$ integer pairs $(x_i, y_i)$ for $i = 0, 1, \ldots, n$ such that the condition of Corollary 1 is satisfied i.e. $\kappa < \max\{\mu, \nu\} + 1$.
  3. Construct the rational interpolation function $\varphi_{\mu, \nu}(x) = r(x)/s(x)$ using the pairs $(x_i, y_i)$, $i = 0, 1, \ldots, n$ such that $r(x)$ and $s(x)$ are two polynomial of degree $\mu$ and $\nu$ respectively.
  4. Choose and publish the number $w$ where $w \neq x_i$ for $i = 0, 1, \ldots, n$.
  5. Choose and publish the number $a$ where $a = S + \varphi_{\mu, \nu}(w)$.

- **Distribution:** The dealer performs the following steps:
  1. Publish the numbers $\mu, \nu, w$ and $a$.
  2. Distribute the pairs $(x_i, y_i)$ to participant $P_i$ for $i = 0, 1, \ldots, n$.

- **Reconstruction:** If all of participants pool their shares then they can retrieve the secret by and performing the following steps:
  1. Compute the rational interpolation $\varphi_{\mu, \nu}(x)$ of shares.
  2. Compute $S = a - \varphi_{\mu, \nu}(w)$.

Since we use the concept of Shamir’s secret sharing, thus the proof of reconstruction phase is obvious. Note that Shamir’s $(n, n)$-threshold secret sharing scheme based on polynomial functions will be obtain by choosing

$\nu = 0, a = 0, w = 0, \mu = n$ and $S = \varphi_{n,0}(0)$

in the proposed scheme.

**V. EXAMPLE**

Suppose that the dealer want to construct $(4,4)$-threshold secret sharing scheme in which $n = 3$ and $S = 12$. The dealer constructs $(3+1,3+1)$-threshold secret sharing scheme by the following steps:

- **Generation:** The dealer performs the following steps:
  1. Choose two integer numbers $\mu = 1$ and $\nu = 2$ such that $\mu + \nu = 3$.
  2. Choose $n+1 = 4$ integer pairs $(5, -1), (1, -4), (-1, -2), (2, -3)$.
  3. Construct the rational interpolation function $\varphi_{(1,2)}(x) = \frac{-2x - 14}{4 - x + x^2}$ using the integer pairs $(5, -1), (1, -4), (-1, -2), (2, -3)$.
  4. Choose and publish the number $w = -2$ where $w \neq x_i$ for $i = 0, 1, \ldots, 3$.
  5. Choose and publish the number $a$ where $a = 12 + \varphi_{(1,2)}(-2) = 11$.

- **Distribution:** The dealer performs the following steps:
  1. Publish the numbers $\mu = 1, \nu = 2, w = -2$ and $a = 11$.
  2. Distribute the integer pairs $(5, -1), (1, -4), (-1, -2), (2, -3)$ to the participants $P_0, P_1, P_2, P_3$ respectively.

- **Reconstruction:** If all of participants pool their shares then they can retrieve the secret by and performing the following steps:
  1. Compute the rational interpolation function
\[ \varphi^{(1,2)}(x) = \frac{-2x - 14}{4 - x + x^2} \]

using the integer pairs
\((5, -1), (1, -4), (-1, -2), (2, -3)\).

2. Compute the secret as follows:
\[ S = 11 - \varphi^{(1,2)}(-2) = 11 + 1 = 12. \]

VI. CONCLUSION AND FUTURE WORKS

Our purpose was to implement Shamir’s secret sharing scheme using rational interpolation. We define a new \((n + 1, n + 1)\)-threshold secret sharing scheme based on rational interpolation. We showed that the number of pole points depends on the number of support points that have the same width. In other word, it is proved that the rational interpolation function \(\varphi(\mu, v)\) is the constant function \(\beta\), if the number of support points, which have the width \(\beta\), is greater than \(\max(\mu, v)\). We showed the efficiency of our scheme by giving an example. There is still a lot of work to be done in order to improve the capabilities of the scheme: it would be good to find a \((k, n)\) variant of the scheme with \(k \neq n\) and a way to make it multi-secret (to allow sharing several secrets instead of one secret shared on each round).

ACKNOWLEDGMENT

The authors are highly grateful to the Department of Mathematics and Cryptography, Malek-Ashtar University of Technology for providing an excellent research environment.

REFERENCES


AUTHORS PROFILE

Ali Nakhaei Amroudi received his M.Sc. degree in Mathematics from Yazd University, Iran, in 2008. He is currently a Ph.D. student in the department of mathematics and cryptography at Malek-ashtar University of Technology (MUT), Isfahan, Iran. His research interests include cryptography and network security.

Ali Zaghan was born in Isfahan, Iran in 1959. He received his Ph.D. degree in cryptography-mathematics from Tarbiat Moallem University, Tehran, Iran, in 2008. He is currently associate professor at department of mathematics and cryptography in Malek-ashtar University of Technology (MUT), Isfahan, Iran. His research interests include Coding Theory and Cryptography Algorithms.

Mahdi Sajadieh received his Ph.D. degrees in electrical engineering from Isfahan University of Technology (IUT), Isfahan, Iran, in 2013. He is currently associate professor in department of electrical engineering, Islamic Azad university, Isfahan (Khorasgan) branch, Isfahan, Iran. His research interests include coding theory, cryptography, and other related topics.
A novel Face Recognition System based on Skin detection, HMM and LBP

Mejda Chihaoui 1, Akram Elkefi 2, Wajdi Bellil 3, Chokri Ben Amar 4

REGIM: Research Groups on Intelligent Machines, University of Sfax National School of Engineers (ENIS), Sfax, 3038, Tunisia.

1mejda.chihaoui@ieee.org
3wajdi.bellil@ieee.org
2elkefi@gmail.com 4chokri.benamar@ieee.org

Abstract—Although there are various biometric techniques, like fingerprints, iris scan as well as hand geometry, the most efficient and widely-used one is face recognition because it is inexpensive, non-intrusive and natural.

In our paper, we present an approach aiming at implementing a full architecture which represents an efficient system of face recognition. For this, an attempt is proposed for each system stage. At the beginning, we develop a novel approach to detect faces existing in 2D color image. This approach focuses mainly on how to implement a selection of skin color before using neural networks and Gabor filters. This approach represents an improvement of existing approach especially because it aims to minimize the computation time. Indeed, the skin detection step avoids wrong detection and helps the system detect the face in the right areas and minimize the research time and subsequently the Gabor filter will be applied only on the localized skin space. Later, the face features obtained by the Gabor filter represent the input of the neural network classifier to decide whether an input image pixel is a face pixel or not.

For 2D face recognition, we propose likewise a novel approach that we call HMMLBP (a combination of the two tools Hidden Markov Models HMM and Local Binary Pattern LBP). It allows classifying a given 2D face image through utilizing an LBP tool to extract features. In order to validate our whole system performance, we show experimental results obtained when applying our proposed algorithm on benchmark face databases, respectively AT&T, Yale and Feret.

I. INTRODUCTION

The invention of computer which is able to save and read a huge amount of information was behind the emergence of some digital biometric systems [1][2], such as face recognition, a widely-used technique [3][4][5] that has been dealt with by many research studies [6] whose applications contain systems of automated surveillance, reconstruction of faces, access control, monitoring of security, identification of mug shot, designing human computer interfaces, diagnosis of diseases, communication through multimedia tools, suspect versus perpetrator verification, planning of treatment and identifying missing and victim individuals.

As depicted in (Fig. 1), the system of face recognition is divided into three steps: face detection, feature extraction and finally face recognition.

Any system of face recognition starts with detecting faces in a given image. Obviously, it is the method of detection which makes the recognition system efficient. Generally speaking, a face detection system can decide whether the image contains a face or not and returns the location and the extent of each face in the image if one or more faces are present.

Face detection in the image is considered very difficult due to the variation of color, position, orientation, lighting, facial expressions (smiles, anger....) and some morphological features (mustache, beard, glasses...). All these obstacles prevent the system effective detection and result in a decrease in its detection rate [8].

After a face has been detected, the task of feature extraction is to obtain features that are fed into a face classification system. Feature extraction is also a key to the animation and the recognition of facial expressions because the performance of the whole system depends on it. In this step also known as indexing or modeling, is extracted from the detected face image, a characteristic vector (signature) that is sufficiently representative of a given face and which models the much more precise than the raw image departure.

This new representation of the face must have both the uniqueness property for each person and the property of discrimination between different people. Depending on the type of classification system, features can be local features, such as lines or facial features (eyes, nose, and mouth, etc....). Face detection may also employ features, in which case features are extracted simultaneously with face detection. Finally, recognition means the authentication and identification. The latter includes comparing one face with many other ones to fetch unknown identity from a set of known possibilities. The former consists in comparing one face with another to prove the identity claimed. Besides, recognition is strongly linked to classification in which the major issue is the identification some persons having a number of common characteristics.

A. Overview

Our paper introduces an approach dealing with such issues. Its objective consists in implementing a system of recognizing
2D faces tolerating the aforementioned problematic. In order to implement this system, we have proposed many solutions for different face recognition steps. The rest of the paper is a discussion of our face recognition system implementation. It also presents some experimental results. The remaining parts are the following: section 2 illustrates a number of related studies dealing with recognition of face as well as its detection. In the third section, the proposed face system architecture is depicted. Then, in the fourth section, the step of face detection, which relies on Gabor filter, skin detection as well as neural network, is explained. After that, the step of classification and that of decision are presented. The sixth section enumerates some experimental results obtained by utilizing AT&T, Yale and Feret data stores.

II. RELATED WORK

A. Face detection

Face detection approaches aim at automatically locating the position of the face in a given digital image. In this part, we are interested in the major and most essential face detection techniques. The latter permit the detection and localization of the real position of the face. The performance of these approaches relies on the rate of detection. We may distinguish four major categories of face detection techniques:

1) Image-based approaches: Actually, these approaches are methods of classification having an algorithm of training. Generally speaking, they use automatic techniques of learning. Besides, they treat the classification issue as the major detection face problem. The two most famous approaches of detection, involving two important phases: test and learning, are SVM (support vector machine) [9] and neural network [10][11][12]. The latter uses a classifier for the detection of the face various sizes in a given image. Prior to the network input, the image should be pre-processed by means of histogram equalization, and then scanned using an 18 * 27 window. It is obvious that the above-mentioned technique, which can overcome the problem of noise, is a difficult-to-construct classifier. Added to that, considering the algorithm of detection and the methodology, SVM is different from the neural network.

2) Features based approaches: They are utilized to localize the face. They are sub-divided into two categories. The first one, based on detecting the skin[13], uses the color to effectively detect, in the image, the chromatic areas. Thus, it allows solving the problem of scanning the image, and identifying if the pixel represents the color of the skin or not. This method, where the color of the skin gives a clear idea about the scale and variation in orientation, constitutes a so efficient and time-saving technique. As shown in [14][15], the second sub-category relies on the invariant features of the face. It utilizes a hypothesis in order to localize the top of the face, and later on browse it to distinguish the eyes marked with a sudden rise in the contour density computed by a black/white percentage through browsing the horizontal obtained planes.

3) Template Matching approaches: These techniques are normally based on measures of similarities. Generally, the pixels intensities between a predetermined template and many image sub-areas must be analyzed. This approach is based on the computing and measuring of the relation between the template image and the candidate one; that is why, these methods utilized many templates [16][17].

4) Knowledge-based approaches: They deal with features of the face (lips, eyebrow, nose, etc) and determine the correlation between them. Thus, in [18], the author utilized rules in which he located the facial features through the technique of projection introduced in [19]. In [20] the author used face image resolution. It is easy to extract the image facial features and their relationships. However, such techniques are influenced by the variation in pose. Besides, we should take all images from the front.

B. Face recognition

It is a wide and very interesting area of research[11] [1] [14] [21]. The process of face recognition involves 4 main steps as presented in (Fig. 2).

In [22], the author defined coding as the act of taking the face image from the concrete world in which a face is considered as a dynamic identity which changes constantly under several factors influence such as lighting and illumination. In this stage, this image is transformed into presentation of gray level. It is, then, pre-treated. This phase is so important as it ameliorates the quality of the image (elimination, detection, noise, head position, etc ). The analysis, also named the extraction of the image features[23], is the next step. It is. This phase is to extract relevant information which will be stored in the memory. After that, and during the learning step, the realized peoples obtained representations were saved. At last, the whole process finishes with the step of decision. The latter constitutes an estimation of the difference calculated between a couple of images.
During the last 30 years, many face recognition approaches, using 2D images have been introduced [4] [11]. Among these proposed methods, we distinguish 3 main categories: hybrid approaches, global approaches and local ones.

1) Global approaches: Such methods, like Fisherface [24], Eigenface [25], SVM (Support Vector Machines)[26] and LDA (linear discriminant analysis)[27], utilize informations given by the face without being segmented. For these methods, each face image of the database, presented by a matrix of n lines and m columns, is first transformed into a vector (n x m, 1) by concatenating the columns of the matrix. Then, thus vector is an input for the classifier. These methods are generally sensitive to pose and illumination. Furthermore, they necessitate a memory of very large size.

2) Local approaches: The second category, called local methods such as HMM [28], elastic Bunch Graph Matching [29] and [30], are based on models. These methods use prior knowledge taken about the facial morphology and rely on its local characteristic points. They also present other techniques which take into account the non-linearity by constructing a local features space and using the filters of appropriate images. Generally, this category of approaches is less affected by variation in pose, illumination, and facial expression. But, they are more difficult to implement.

3) Hybrid approaches: As example, we may mention Genetic Programming-PCA[31], PCA-Gabor [32], etc. They benefit from the global and the local methods through combining the extracting the features of the local appearance with detecting the geometrical characteristics. Such solution makes possible to rise the recognition performance stability during lighting, the variations in facial expressions and position. Along with the evolution of 2D face recognition field and due to the growing development of 3D information acquisition and applications [33], 3D face recognition [34] is getting more and more attention. Hence, many researches have been exposed [35].

III. OUR PROPOSED DETECTION APPROACH

Now, we will explain our proposed approach relying on the colors of the skin to remove areas without this feature, and the Gabor filter for the extraction of the texture of the image. However, in the classification phase, we apply the neural network. The combination of both Gabor Wavelet[36] and Neural Network is not new [37] but our improvement consists of incorporating skin detection before feature extraction in order to reduce Gabor process to areas likely to be face pixels.

A. Skin areas segmentation

For the detection of faces in the images, we start first by detecting the areas of the skin. That is to say, in this step, we detect the pixels representing the skin. Actually, skin detection is very important regarding the time of computation because areas of the skin can strongly present the face. Such time saving is so important since the skin parts size is smaller if compared with that of faces image.

This test requires an implementation of the belonging conditions of skin pixels. As we apply this test, the pixel value is, thus, kept. Otherwise, the white pixel is returned. As consequence, the obtained image will only contain skin pixels. Obviously, the described technique relies on thresholding in relations to chromatic space.

1) Chromatic space: We can present the color of the skin in various chromatic spaces like HSV, RGB, YCbCr, normalized RGB, etc.

In This section, we detail the space of YcbCr. In fact, the latter can reduce the illumination. It allows also the separation of the chromatic space by the values given in [38].

\[ Y = 0.2999 * R + 0.587 * G + 0.114 * B \] (1)
\[ Cr = R - Y \] (2)
\[ Cb = B - Y \] (3)

The values of Cb as well as that of Cr give the chromatic data. The skin color is used at a given interval of the thresholding order to define the skin areas in the image. We consider the thresholding described below:

\[ YCbCr(1) \text{ with a threshold } ((85 \leq Cb \leq 135) \text{ and } (135 \leq Cr \leq 180)) \] (4)

Our approach aims at minimizing the time devoted for research in a given image. For this reason, detecting the color of the skin is used in order to save time, and do not work on an area having no skin color. The performance time of the proposed approach is essentially relies on two important matters: the time of learning and that of research.

Actually, it is somewhat difficult to minimize the former because it is strongly related to the number of the classified images in the step of learning. Nevertheless, the latter can be reduced when the color of the skin is used. The detection of the skin, applied on image containing many faces, is presented in (Fig. 3).

![Fig. 3. Example of skin detection](image-url)

B. Extraction of features using Gabor filter

In 1946, Dennis Gabor introduced the so-called Gabor filter [39] which is considered so popular tool of analysis. It is strongly linked to Gabor wavelet because the latter shows an orientation and frequency sinusoidal carrier.

The convolution of an image is performed using 8 orientations and frequencies of the sinusoidal carrier. As example, we may mention Genetic Programming-PCA[31], PCA-Gabor [32], etc. They benefit from the global and the local methods through combining the extracting the features of the local appearance with detecting the geometrical characteristics. Such solution makes possible to rise the recognition performance stability during lighting, the variations in facial expressions and position. Along with the evolution of 2D face recognition field and due to the growing development of 3D information acquisition and applications [33], 3D face recognition [34] is getting more and more attention. Hence, many researches have been exposed [35].

Now, we will explain our proposed approach relying on the colors of the skin to remove areas without this feature, and the Gabor filter for the extraction of the texture of the image. However, in the classification phase, we apply the neural network. The combination of both Gabor Wavelet[36] and Neural Network is not new [37] but our improvement consists of incorporating skin detection before feature extraction in order to reduce Gabor process to areas likely to be face pixels.

A. Skin areas segmentation

For the detection of faces in the images, we start first by detecting the areas of the skin. That is to say, in this step, we detect the pixels representing the skin. Actually, skin detection is very important regarding the time of computation because areas of the skin can strongly present the face. Such time saving is so important since the skin parts size is smaller if compared with that of faces image.

This test requires an implementation of the belonging conditions of skin pixels. As we apply this test, the pixel value is, thus, kept. Otherwise, the white pixel is returned. As consequence, the obtained image will only contain skin pixels. Obviously, the described technique relies on thresholding in relations to chromatic space.

1) Chromatic space: We can present the color of the skin in various chromatic spaces like HSV, RGB, YCbCr, normalized RGB, etc.

In This section, we detail the space of YcbCr. In fact, the latter can reduce the illumination. It allows also the separation of the chromatic space by the values given in [38].

\[ Y = 0.2999 * R + 0.587 * G + 0.114 * B \] (1)
\[ Cr = R - Y \] (2)
\[ Cb = B - Y \] (3)

The values of Cb as well as that of Cr give the chromatic data. The skin color is used at a given interval of the thresholding order to define the skin areas in the image. We consider the thresholding described below:

\[ YCbCr(1) \text{ with a threshold } ((85 \leq Cb \leq 135) \text{ and } (135 \leq Cr \leq 180)) \] (4)

Our approach aims at minimizing the time devoted for research in a given image. For this reason, detecting the color of the skin is used in order to save time, and do not work on an area having no skin color. The performance time of the proposed approach is essentially relies on two important matters: the time of learning and that of research.

Actually, it is somewhat difficult to minimize the former because it is strongly related to the number of the classified images in the step of learning. Nevertheless, the latter can be reduced when the color of the skin is used. The detection of the skin, applied on image containing many faces, is presented in (Fig. 3).
depicts a given image according to the periodic structures through its decomposing by a simple periodic functions base. The representations in frequency and orientation of Gabor filter are similar to those of the human visual system. We consider the kernel of the Gabor filter as the product of a complex sinusoidal wave with a Gaussian envelope. The representations in orientation and frequencies, given by Gabor filter and those of mans visual system are almost the same. In this work, the Gabor filter is viewed as a result of a complicated sinusoidal wave having a Gaussian envelope[40]. An example of facial representation using Gabor wavelet is illustrated in (Fig. 4).

C. Neural network

It represents a method of classification applied in various applications. It relies on both the phase of learning and that of test. The former permits to search for producing automatically rules from the data stores of learning which involves examples i.e the training of the network. Nevertheless, in the test phase, we prove the presence of the face in the test image. We also distinguish non-face images from face ones.

![An example of facial representation using Gabor wavelet: response of the amplitude (a) and response phase (b) using 40 Gabor kernels (8 orientations and 5 scales)](image)

Fig. 4. An example of facial representation using Gabor wavelet: response of the amplitude (a) and response phase (b) using 40 Gabor kernels (8 orientations and 5 scales)

IV. OUR PROPOSED FACE RECOGNITION APPROACH HMM-LBP

Here, we aim at determining, from the database, the identity of the corresponding person whose face is called test image. In this phase, information about the face is viewed, by the HMMs, as a sequence variable in time. The flowchart of this approach is given by (Fig. 6).

![Our proposed HMM-LBP approach functioning](image)

Fig. 6. Our proposed HMM-LBP approach functioning

A. Hidden Markov Models (HMM)[29]

In 1975, the HMMs is first used in various fields especially in speech recognition. These methods show a statistic model decomposed by unidirectional transitions and states. This HMM tool is determined by this triplet $\lambda = (A, B, \pi)$ having:

- $A = \{a_{ij}\}$: the state transitions probability matrix as $a_{ij} = P[q_t = S_j | q_{t-1} = S_i]$ with $1 \leq i \leq N$; $j \leq N$; $0 \leq a_{ij} \leq 1$; $\sum_{j=1}^{N} a_{ij} = 1$; $N$ denotes the model states number; $t$ is the time; $q_t$ shows the state of the model at $t$ (a given instant) with $1 \leq t \leq T$; $T$ represents the observation sequence length; $S$ denotes all the states set;
- $B = \{b_j(k)\}$: presents the observation symbols probability matrix with $b_j(k) = P[O_t = V_k | q_t = S_j]$ and $1 \leq j \leq N$.

- The time of learning: this factor is closely related to the numbers of the learning images, the input vector components number. It depends on the characteristics of the learning technique which has a time not easy to minimize.
- The time of research: is intended to be reduced by using the segmentation of region. In fact, to detect a face in an image, we will not scan the entire image but only skin regions.
N; 1 ≤ k ≤ M; M is the various observation symbols number; O_t denotes the symbol of observation at t a given instant; V = {V_1 ... V_K} shows all possible symbols of observation set;
π = {π_i}; denotes the initial state distribution with \( π_i = P[q_1 = S_i] \) and 1 ≤ i ≤ N.

The Hidden Markov Model have efficiently been applied in many fields like speech recognition, features recognition and face recognition, etc For that reason, we use the approach of HMM to recognize 2D face.

For each face image, seven facial regions (hair, forehead, eyebrows, eyes, nose, mouth, and chin) must be placed from the top to the bottom in a natural order even if it is taken under a small rotation. Then, to each region we assign a state in left-right order. The (Fig. 7) shows the face model states and their non-null transition probabilities.

**B. Our approach HMMLBP**

1) Decomposition into Blocks: This step is to divide both the image of the face and that of test into seven different areas (eyebrows, nose, mouth, forehead, and chin). As shown in (Fig. 8), each region is given a state \( q \).

2) Features Extraction: The extraction of data consists in extracting relevant information from the raw data (image of the face, the face main areas). This phase is very important in every method of face recognition. For that reason, we apply an LBP approach for features image extraction.

   - Local Binary Pattern (LBP) [41]

   Computing the value of the LBP is to threshold the eight direct neighbors of each pixel by a determined threshold having as value the gray level of the current pixel. If the value of the neighbors is more than or the same as the current pixel, they will be assigned the value 1. The latter will be 0 if the previously-mentioned value is less than the current pixel.

   Through multiplying the matrix containing the two values 0 and 1 with the weights of LBP powers of two, we will give the current pixel LBP value. Then, we obtain our LBP value by adding all its elements. (Fig. 9) shows an LBP code calculation with a threshold equal to six. Few years later, the LBP code calculation was extended by using neighborhoods having different sizes. The pixel at the center is surrounded by a circle having R radius. The P values represent the set of points grouped on the circle edge. Its values are compared with those of the central pixel.

   \[ (P, R) \rightarrow \text{The pixel P points neighborhood with a radius R.} \]

   Obviously, some neighbors are not directed related to pixels. Therefore, to estimate the gray level value of the neighbor, bilinear interpolation is used. In order to calculate the LBP existing in P pixels neighborhood, in a given radius R, the equation below is followed:

   \[ LBP_{P,R} = \sum_{p=0}^{p-1} s(g_p - g_c)^2 \] (5)

   With:

   - \( g_p \): the neighbor pixel gray level;
   - \( g_c \): the central pixel gray level;
   - \( S() \): a function defined as:

   \[ S(x) = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{else} \end{cases} \] (6)

   As soon as all the image pixels LBP code is computed, the image coded using LBP operator, is than divided into
small regions in order to construct each one histogram. At the end, we obtain a huge histogram representing the features of the face in an image.

![Image of Face Representation using the Histogram of the LBP code](image)

**Fig. 11.** Face representation using the histogram of the LBP code

3) **Probabilities computing and the maximum selection:**
In the database, each image of the face is transformed into a sequence of observations. Besides, for every class of the 40 obtained ones, a learning model is computed through defining the parameters of the HMM (matrix of the initial probabilities, matrix of the transitions probabilities and matrix of the emissions probabilities). Each Hidden Markov Model represents a different individual. In its turn, a test image is transformed into a sequence of observations and an HMM is computed for this type of image depending on the parameters of the Hidden Markov Model.

Then, we recognize the person’s face through establishing a match between the each learning pattern and the test model. After that, we calculate a probability for all registered persons models in the database. The model which has the highest probability corresponds to the searched individual’s identity.

V. **Results**

A. **Face detection**
In this step, we have already presented in [42] some results obtained by applying the proposed methods of face detection on some images having different orientations, lighting, positions, scales, skin colors and different number of faces. For each image, we have shown the results obtained using the face detection approach proposed by Omid Sakhi in [43].

This method, which we have called Gabor-NN, does not use skin color, but only Gabor and neural network (Gb-NN). Then, we have revealed some findings given by our proposed approach applying Gabor filter, skin detection and Neural network. We have called the new introduced approach (Sd-Gb-NN).

If we compare the proposed method detection results with those of another system that does not depend on the color of the skin, it will be obvious that our approach is more efficient.

B. **Face recognition**

The application of the HMMLBP is tested on standard databases Yale [44], ORL [45] and Feret [46].

The ORL database (Fig. 12), called AT&T, contains 40 different individuals having 10 distinct images of faces. Therefore, we will obtain 400 images of the face having 256 gray levels. Their size is 112*92. All these images have a dark and homogeneous background. They were taken with variance in times, angles, details (with and without hair style, glasses, beard) and with different facial expressions (smile, surprised, angry,...) and with roughly 20 degrees in tilt.

![Image of Face Images from the ORL Database](image)

**Fig. 12.** A subset of face images from the ORL database

The second database, Yale (Fig. 13), consists of the frontal grayscale of face images representing 15 persons together with 11 images of the face for each individual, which gives 165 images. In fact, the variations in lighting involve center-light, right-light and left-light. However, the presence and absence of glasses represent the Spectacle variations. Finally, the variations in facial expressions include happy, wink, sad, surprise, normal and sleepy.

![Image of Face Images from Yale Database](image)

**Fig. 13.** A subset of face images from Yale database

The third FERET database (Fig. 14) is bigger and more complex than the two others since it represents variations in pose, illumination, facial expression and occlusions. It contains a face images set collected by NIST from 1993 to 1997. Each image represents a single face. Feret is composed of a set of reference faces called Gallery containing contains 1,196 face images and four different sets of probe images. The probe, called fafb, is a set of 1,195 images of subjects taken at the same time as the gallery images but with different facial expression as same as the gallery set. The duplicateI probe set contains 722 images of subjects taken between one minute and 1,031 days after the gallery image was taken. The duplicateII probe
set is a subset of 234 images of the duplicateI probe set taken after 18 of the gallery image.

Finally, the face probe set contains 194 probe images of subjects with d different lighting conditions. In our paper, we reduce all images resolution of $768 \times 512$ to $56 \times 46$.

![Fig. 14. A subset of different categories of probe set from Feret database](image)

The three tables above represent the results obtained while applying our proposed approach on the three databases mentioned below.

<table>
<thead>
<tr>
<th>TABLE I</th>
<th>COMPARATIVE RESULTS OF OUR APPROACH WITH SOME OTHERS APPLIED ON ORL DATABASE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approach</strong></td>
<td><strong>Recognition rate</strong></td>
</tr>
<tr>
<td>HMM and the gray levels [47]</td>
<td>87%</td>
</tr>
<tr>
<td>HMM-DCT [48]</td>
<td>99.5%</td>
</tr>
<tr>
<td>HMM-SVD [49]</td>
<td>99%</td>
</tr>
<tr>
<td>SHHMM [50]</td>
<td>99.5%</td>
</tr>
<tr>
<td>Pseudo2DHMM [47]</td>
<td>95%</td>
</tr>
<tr>
<td>2DPCA Principal Component uncertainty [51]</td>
<td>97.8%</td>
</tr>
<tr>
<td>Wavelet transform and improved 2DPCA [52]</td>
<td>92%</td>
</tr>
<tr>
<td>Combination of HMM &amp; SVM [53]</td>
<td>100%</td>
</tr>
<tr>
<td>HMMLBP</td>
<td>99.5%</td>
</tr>
</tbody>
</table>

Applying our face recognition approach to the ORL database, it is obvious that the LBP approach is more efficient as its recognition rate is higher than those given by other techniques mentioned in table I. Actually, the results of our HMMLBP method are better than the recognition rates obtained by SVD and the gray level which are respectively 99% and 87%. Besides, if we apply SVM or DCT with the Hidden Markov Model, we will obtain the same results.

<table>
<thead>
<tr>
<th>TABLE II</th>
<th>COMPARATIVE RESULTS OF OUR APPROACH WITH SOME OTHERS APPLIED ON YALE DATABASE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approach</strong></td>
<td><strong>Recognition rate</strong></td>
</tr>
<tr>
<td>SVM-PCA [54]</td>
<td>99.39%</td>
</tr>
<tr>
<td>SVM-ICA [54]</td>
<td>99.39%</td>
</tr>
<tr>
<td>PCA-2DPCA [55]</td>
<td>92.8%</td>
</tr>
<tr>
<td>PCA-LBP [56]</td>
<td>93%</td>
</tr>
<tr>
<td>HMMLBP</td>
<td>99.33%</td>
</tr>
</tbody>
</table>

By applying our approach on Yale, the obtained recognition rate will be 99.33%, while that given by PCA+LBP is 93%. We notice that combining SVM with ICA and PCA will result in 99.39% recognition rate. The latter is better than that obtained while using the proposed HMMLBP method.

Applying our approach to Feret database which represents a bigger and more complex database due to different variations in pose, illumination, facial expression and occlusions we get a rate equal to 95%. This results are better than results obtained with MLBP and GWT-PHMM. However, results obtained by [22] still better than our ones.

VI. CONCLUSION

The face recognition field has been considered as so interesting subject that many researchers have dealt with. In this paper, we have proposed a novel face recognition system in which a solution was presented for each step. For face detection, we have proposed to use skin detection prior to Gabor filter and neural network in order to minimize the execution time by limiting the face research to the image skin regions. Then, we have combined HMM with LBP tool to recognize the detected face. Some results are presented to validate our proposed approach efficiency.

For future work, we propose, first, to apply other classification tools such as SVM and compare them with the obtained results. Also, our futur work will combine the PCA tool to reduce feature vector dimension in order to improve our results.

We propose also to exploit the work that we published in [60] in order to recognize person from a video sequence. For 3D face recognition, as we have proposed two novel approaches for remeshing 3D objects[61] and [33], we propose to develop a uniform remeshing scheme to establish a sampling pattern across 3D faces.

REFERENCES


Energy Efficiency techniques in cloud computing
Altaf Ur Rahman, Fiaz Gul Khan, Waqas Jadoon

Abstract—Cloud computing gaining popularity at enormous rate since from its emergence. CC changed the way that computing services are provided. On demand platform (PaaS), infrastructure as a service (IaaS) and software (SaaS) as a service through internet. Consumer use third party services instead of building his own infrastructure which need up-front investment and expertise. Cloud computing becoming popular for unlimited computing power, availability, nice pricing, on demand services and quality of service. For availability and computing power the service provider expands their resource capacity to handle user requirements. This expansion in resources capacity lead to high energy demand. Two big issues for cloud computing is energy demand and security/privacy requirements. In this survey we will give a review on the latest techniques for energy efficiency in cloud computing. The main focus is on software base energy efficiency techniques in which we will explain the workflow consolidation and resource management in detail.

Index Terms—cloud computing, data center, energy efficiency techniques.

I. INTRODUCTION

Cloud computing is a platform which enable individual users and conglomerates to use infrastructure, platform and software as a service through internet instead of buying managing and developing their own. By using cloud computing (CC), companies reduce their operational cost while increasing their operational efficiency. With the emergence of Internet of Things (IOT) the CC usage will grow, in 2003 connected devices were 6.3 billion. The figure of active devices per person was 0.8. This figure will grow from 6.3 to 7.6 in 2020 and connected device per person will be 6.58 [1]. IOT device will use cloud platform because of low processing power and limited storage.

Every organization and individual use CC in one or other form using online services. Providing and managing such a flexible platform is a challenging task. Provider built data center that consist of hundreds of thousands of servers continuously running to provide uninterrupted services.

Data center are energy hungry station for continuous running it requires a nonstop supply of power for running and cooling. Data center is a resource rich platform and the scheduling of resources is one of the challenging task. Cloud refer to a data centre where all the user requirements like hardware and software are provided in the form of preconfigured resources and remotely hosted applications [2]. Cloud service provider objective is to maximize their profit by efficiently utilizing the data center resources. Consumer of a service aim to be best served in term of cost and quality. Providing QOS provider have to increase the number and capacity of the resources which in turn increase the maintenance expenditure and decrease the profit that can be made possible by the use of virtualization. According to [3] energy consumption in data center can be classified in to two classes computing resources and physical resources. Computing resources consume about 50% while physical resources 40% the remaining 10% by power supply and other miscellaneous things.

Energy efficiency is one of the biggest issue faced by data center. Two percent of the total power produced in USA is consumed by data center. Energy demand double since 2000 [4]. Amazon estimate that energy related cost is forty-two percent of its budget. Data center are not environment friendly and contribute two percent of co2 emission. Energy consumption can be reduced by efficient utilization of data center resources. In a survey conducted in 2010 it is find out that idle server cause of producing 11M ton of co2 emission on yearly basis [5]. Energy efficient data center are not only economical but also environment friendly.

The rest of the paper consist of five section. Section I introduction give a brief overview of cloud computing and energy efficiency challenges in cloud computing. Section II is about the energy efficiency trends in data center. Section III is about the software based techniques for improving energy efficiency in data center. The techniques presented by Belogazo in 2011 is more focused on power management. We will focus on software side because so far both the Hardware and software side is considered and the techniques on virtualization level is not studied in detail. Section four is about comparative analysis of different software base techniques on the basis of their strength and limitations.

Altaf Ur Rahman student of MS program in department of computer science at Comsats Abbottabad Pakistan.

Dr. Fiaz Gul Khan is in Department of Computer Science at COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad.

Dr. Waqas Jadoon is in Department of Computer Science at COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad.
II. ENERGY EFFICIENCY TRENDS AT DATA CENTER LEVEL

Data center is a collection of connected server used by an organization for remote processing and storage. Data center (DC) give flexible platform to customer by hiding platform dependency. User has no need of any special hardware all he need is thin client. Cloud service provider trying to make DC flexible but harder for the service provider and data center manager. To efficiently perform user request DC have a hundred and thousands of servers which should be managed intelligently. Servers in DC consume huge amount of energy which is expensive and cause co2 that is 2% of global co2 emission [6]. Building energy efficient data center is not only benefited for cloud service provider but also environment friendly.

Initially researcher was focusing on the power distribution unit and power management module. They were involved in improving the flow of current and avoiding multiple conversion of alternating and direct current. This research suggests the use of energy star rating IT and non IT equipment in data center and green DC. Cooling requirements of DC resources is one of the prime energy demanding entity. The suitable location of data center can help in minimizing energy consumption in this regard. Location selection is based on the temperature and low-cost availability of hydroelectric power [7]. Using these techniques, no major gain is obtained. Researcher shifted from focusing on designing green DC and trying to find the energy efficient way in the traditional DC. DC operator work on implementing hardware base techniques for energy optimization.

Using the hardware base optimization techniques data center operator did not get the required gain in energy. According to [8] it was poor program and software design. This initiated the trend of writing parallel program that could run parallel. Latter on it was found that resource management play starring role in energy efficiency. This initiated the trend of developing algorithm for energy efficient management of DC resources.

III. ENERGY EFFICIENCY TECHNIQUES AT DATA CENTER LEVEL

At data center level energy efficiency actions can be divided into hardware base, infrastructure base, software base and location based. In [8] author discuss the various power management techniques both at hardware and software level while in [7] author focus more on software level techniques for energy efficiency. Further software based techniques for energy optimization are classified into five group’s resource management, Dynamic voltage and frequency scaling, parallel program and workload consolidation. In this survey we will extend the work of [7] by adding the latest techniques in resource management and workload consolidation.

Figure 1: Energy optimization techniques at data center level

A. DVFS

The process of intentionally limiting the performance of the processor at the time when it consuming too much power while the task can be accomplished processing at lower frequency. Voltage and frequency have a direct relationship. It has been observed that server consume about 70% power when it is idle [3] saving this energy will have great impact on energy reduction. DVFS can handle this problem effectively. DVFS is basically intended and design for energy efficiency in embedded system. But this can be implemented and consider one of the most effective energy efficiency techniques for computation intensive server. However, this is considering not good for input output intensive processes [4].

Methods using DVFS techniques mostly consider homogeneous physical machine while less interest is shown by researcher toward heterogeneity. In [4] Jacob Leverich suggest a method to power on some of the resources and perform work on them while the rest should be in off state to save energy. The difference between consolidation and DVFS is that consolidation is applied as a whole regardless DVFS which is local [9]. But Wilies lang propos that running all the resources will perform the work in less time and more energy will be saved. Energy efficiency achieved through DVFS depend on the type of SLA either strict SLA lead to low energy saving 1.11% while more effective in relax SLA 6.69% [3].

DVFS can be effectively used in CPU intensive task while it is not suitable in memory and Input output intensive task [10]. A history table is maintained when a request is received it is compared against the table to find out whether it is CPU or I/O intensive. After this calculation the frequency is adjusted.

B. RESOURCE MANAGEMENT

Resource management is the process of selecting computer resources such as computing, storage, network intelligently and allocating against the single or set of request received to meet performance objective of the user [11]. Resource management play starring role in energy efficiency. Identifying the type of request assigning the best possible resources in term of performance and price by looking at SLA. Management is basically the scheduling of resource. When a request is received the scheduler identify an optimal resource allocation by looking and analysing the current state of the
system [12]. Scheduling mostly involve with Virtual Machine management. Virtual machine management deals with VM migration. VM migration performed for three things performance, load balancing and energy efficiency. But as our focus is energy efficiency so we will look at the energy efficiency aspect.

![Resource Management Hierarchy](image)

Figure 2: Resource Management Hierarchy

In [13] energy aware VM migration techniques is proposed based on firefly algorithm. This algorithm work using three principle (I) fireflies attracted toward each other without considering his sex because fireflies are unisex (II) less bright will travel toward brighter firefly’s attractiveness decrease as the distance increase (III) the brightness of the firefly is controlled by the setting of the objective functions to be improved. Firefly algorithm perform energy aware virtual machine migration by migrating VM from the most loaded active node to the least loaded active node. The decision of migration consists of four steps: first loaded active node selection, VM selection from the loaded node, destination node where to be migrated and distance update. For selecting loaded node first computational energy is calculated and a list is generated then a node computation time is calculated and values is put in table. In step third attractiveness is measured on the base of CE value the least CE is the first in the list. In step fourth distance is calculated and a list is obtained a node is selected based on CE value which is closest to the calculated distance. Compute load on individual VM and create a list in descending order. Migrate the top VM in VM list to the top node on AI list and update the distance to reinitiate the process.

To improve energy efficiency is to minimize energy intake of resources such as memory, CPU, network and storage. Suggested strategies use the approaches of utilizing limited resources effectively. Turning off or bringing to sleep mode idle resources for saving energy. Network traffic is kept minimum to optimize network energy. To keep network traffic minimum VM which have high traffic are shifted on same PM. Keeping network traffic minimum less number of network element will be in active state this will lead to save considerable amount of energy [14].

VM on pm are not utilized to the fullest of his capacity in [10] author propose a technique called residual resource fragmentation. There are different resources but we are more interested in processing and memory resources. When a resource usage is limited or blocked by some other resource is called resource fragmentation. In this paper author basically combine the fragmented resource in each single pm and combine them by bringing it to the least number of pm. Let suppose we have two pm its CPU utilization is (80%, 60%) and (80%, 95%) if a request is made for creating a new VM of above 40% processing it cannot be served. But we have 85% processing power combinely on two pm if we combine it we can serve a request of creation of new VM above 80%.

In [15] author proposed a scheme based on virtual machine consolidation, reducing the number of active servers by consolidating virtual machines dynamically on a minimum number of servers, and take advantage of the lacking energy proportionality of commonly used hardware. VM consolidation is a methodology to maximize resource usage while keeping low the energy need in a virtualized environment. Most of the paper does not consider network energy consumption and cooling energy consumption of a data center. Consider both the network data structure and cooling energy when consolidating VM. Fever racks and routers are utilized without compromising SLA to improve energy efficiency.

**C. WORKLOAD CONSOLIDATION**

Data center are physically distributed over a geographical area. When a request is received it is put on the nearest geographically located data center. This help to reduce network delay which in turn reduce turnaround time. Inside data center it is tried to fulfill the request using currently active PM to save energy. A large percentage of energy is consumed as high as 50% more than when server performing at the peak power when server in data center are idle [13]. This high percentage is because 70% of the time server are idle mean under loaded [3]. For saving this energy an effective way of choosing the right node for the request processing is needed. A strategy is required to put the under loaded node into low energy state or turnoff. When to turnoff and when to awake these are some of the decision that should be devised in this strategy. Similarly, if a new request comes and no active server can perform then a new server must be turn on or wakeup to fulfill this request. This flexibility is possible by virtualization technology to put more than one request on a single server to improve resource utilization and decrease the resource demand [16] [17] [18].

Putting more than one VM on a single pm to optimize energy consumption is named VM consolidation. The consolidation of VM on fewer number of pm is online bin packing problem. Where pm is a bin and VM is an object and the process is real time so decision has to be quick and efficient both in performance and resource utilization efficiency [19]. VM are of different sizes according to the resource demand and bin have different capacity in term of the resources it has. At the time of assigning VM to pm it is tried to use the active server instead of turning on or waking up a new server. How it will select the pm from multiple on pm to put the request on them. One techniques are to put the request on the pm which have minimum free space to accommodate the request. This technique is used to acquire maximum resource utilization by leaving the large free space on other pm to be used for another request. However, putting a server
into sleep mode and waking up considered an overhead but this overhead is tiny [20]. Aggressive consolidation may lead to performance degradation as well as energy inefficient. Because when a pm performing at the maximum capacity its performance efficiency and speedup is degraded and its cooling requirement rise up.

D. PARALLEL PROGRAMING

Multi core systems improve performance by the cost of increasing computational energy. Handling fastest processing unit in effective way is one of the most complex task in computer system. A large number of techniques are available for improving the energy consumption of these multicore/parallel system. All these techniques improve energy consumption [21] by compromising throughput to optimize performance per watt. Parallel program came under software optimization which is further classified as code optimization and runtime optimization. Parallel program deal with code optimization. For obtaining energy efficiency programmer have a good knowledge of underlying hardware.

IV. COMPARATIVE ANALYSIS OF DIFFERENT ENERGY EFFICIENCY TECHNIQUES

All techniques have some limitation and strength. There is no technique which have good enough up in all aspects. Mostly techniques are focusing on the area which is more responsible for energy usage like server/storage and cooling which is responsible for 50% and 34% power usage of the data center respectively.

<table>
<thead>
<tr>
<th>Technique</th>
<th>General comments/Strength</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DVFS</strong></td>
<td>— Work well for computational intensive tasks.</td>
<td>— Didn’t perform well for i/o intensive task.</td>
</tr>
<tr>
<td></td>
<td>— No overhead of maintaining data center level load information applicable to a single server.</td>
<td>— dependent on SLA not applicable for hard quality of service application/task. Strict SLA lead to low energy saving.</td>
</tr>
<tr>
<td></td>
<td>— effectively save energy while server is idle and server are 70% of the time idle.</td>
<td>— did not consider the priority of the tasks consider only the workload on CPU.</td>
</tr>
<tr>
<td></td>
<td>— turning on a switch off or bringing a sleep node to an active state consume more energy as compared using DVFS.</td>
<td>— quality of service compromised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— no need of data replication because all the servers are active using the least possible energy</td>
</tr>
<tr>
<td><strong>Resource Management</strong></td>
<td>— Resources are not utilized all the time 70% of the time it is idle.</td>
<td>— accurate prediction for resource, resource capacity and resource time for which an application required a particular resource is not known in advance.</td>
</tr>
<tr>
<td></td>
<td>— using efficient management of resources more than 50% power can be saved.</td>
<td>— resources management is possible only on accurate resource demand prediction</td>
</tr>
<tr>
<td></td>
<td>— resource management is the only techniques that have the potential of more power saving as compared to other techniques.</td>
<td>— performance may be degrading depend on SLA</td>
</tr>
<tr>
<td></td>
<td>— profit and utilization maximization of infrastructure is a service.</td>
<td>— chances of SLA violation is higher</td>
</tr>
<tr>
<td></td>
<td>— quality of service is maintained</td>
<td>— data replication for data availability</td>
</tr>
</tbody>
</table>
Workload consolidation

- Avoid overloading
- balancing the load for energy efficiency and performance.
- turning idle node to sleep or turn off state
- increase service provider profit by maximum utilization of active resources

- increase network traffic
- delay involve due to network
- turnaround time increase
- only consider the workload doesn’t consider the priority of the tasks
- overhead of maintain all the records of server’s workload
- take time to bring sleep or turn off server into active state which increase chances of SLA violation.
- using consolidation, we have to replicate data for availability

Parallel program

- Time for processing decrease
- Throughput increase
- Energy efficiency achieved by decreasing the processing time
- component idle time is minimized
- quality of service is maintained
- not dependent on SLA

- Depend on the percentage of code in a program that can be parallelized.
- less energy saving is achieved as compared to resource management and workload consolidation.
- programmer is responsible for code parallelization

Table 02: energy efficiency effectiveness of different paper on the basis of different parameter

<table>
<thead>
<tr>
<th>Ref</th>
<th>Perf consi</th>
<th>Netw Perf</th>
<th>Load balancing</th>
<th>R- utili</th>
<th>Energy efficiency</th>
<th>Exp Setup</th>
<th>Resp time</th>
<th>Fault toleranc e</th>
</tr>
</thead>
<tbody>
<tr>
<td>[11]</td>
<td>yes</td>
<td>No</td>
<td>yes</td>
<td>yes</td>
<td>10%</td>
<td>Cloudsim</td>
<td>Decrease</td>
<td>yes</td>
</tr>
<tr>
<td>[12]</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>NA</td>
<td>NA</td>
<td>Stable</td>
<td>NA</td>
</tr>
</tbody>
</table>

1.11 kwh less than
V. CONCLUSION

In this paper we discuss four major energy efficiency techniques DVFS, resource management, work load consolidation and parallel programing. These four are software base energy efficiency techniques we tried to include the best and latest techniques for energy efficiency in these four categories. In future we will extend this work by deeply studding and analysing the resource management and workload consolidation techniques in detail. Most of the current research based on these techniques. The margin for energy efficiency is high in these techniques as compared to other techniques.

REFERENCES


**Altaf ur Rahman** was born in Dir lower district, in 1990. He received his B.S. computer science degree from SBBU sheringal and M.S. degree in progress from Comsats institute of sciences and technology Abbottabad Pakistan.

**Dr. Fiaz Gul** was born on 22-11-1982, in a beautiful valley Abbottabad of KPK. My graduation and MS is from COMSATS Institute of Information Technology Abbottabad in the field of Computer Science. For specialization master and Doctorate, he won the HEC scholarship under the project UESTP for Politecnico di Torino Italy. Currently he is serving as an Assistant Professor in Computer Science Department at COMSATS Abbottabad.

**Waqas Jadoon** received the Ph.D. degree in Computer Science from Sichuan University China in 2014. Currently, he is an Assistant Professor at COMSATS University, Pakistan. His research interests focus on Pattern Recognition, Image Processing, theory and applications of Machine Intelligence.
Abstract—Cloud computing provides distributed resources to the users globally. Cloud computing contains a scalable architecture which provides on-demand services to the organizations in different domains. However, there are multiple challenges exists in the cloud services. Different techniques has been proposed for different kind of challenges exists in the cloud services. This paper reviews the different models proposed for SLA in cloud computing, to overcome on the challenges exists in SLA. Challenges related to Performance, Customer Level Satisfaction, Security, Profit and SLA Violation. We discuss SLA architecture in cloud computing. Then we discuss existing models proposed for SLA in different cloud service models like SaaS, PaaS and IaaS. In next section, we discuss the advantages and limitations of current models with the help of tables. In the last section, we summarize and provide conclusion.

Index Terms—Service Level Agreement (SLA), Cloud Computing.

I. INTRODUCTION

Cloud computing, is a source for providing an elastic resources. It is an on-demand computing that gives shared resources or applications to the consumer of the cloud [2]. Cloud is an elastic source of applications or resources. Cloud environment attracted many companies to implement cloud environment and make it available for the users to use its elastic availability of applications. A large number of application have been migrated to cloud platform.

Virtual Machine (VM) technology is the core technology in cloud which enable a physical machine to be split down into several VMs. Through virtualization in cloud, operational cost minimized through server consolidation and better use of computational resources [1].

Through advancements in computing world it is nearly possible that computing will become the most necessary utility of daily life. Cloud computing provides elastic applications to the users and to maintain customer-driven service management and computational risk management to assist Service Level Agreement (SLA).

Due to the large number of market participants and vast types of services, market of cloud services are frequently suffer from low liquidity, e.g., The expectation of purchasing or selling of services, so disadvantaging repelling potential customers and new suppliers [5]. Furthermore, there are no general standard exists for service level agreement (SLA) used in market places. Different SLAs have same meaning but their syntax is different accordingly to the requirements of market users.

Usman Wazir is in Department of Computer Science at COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad, Pakistan.

Dr. Fiaz Gul Khan is in Department of Computer Science at COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad, Pakistan.

Dr. Sajid Shah is in Department of Computer Science at COMSATS Institute of Information Technology, University Road Tobe Camp, Abbottabad, Pakistan.
SLAs in cloud consists of different specification regarding security, pricing, performance, customer level satisfaction (CLS) and SLA violation. Before signing SLA make sure that the cloud platform you are selecting for your business is providing all the requirements which you needed for your business. In Section 2, we will discuss SLA regarding issues in cloud and key points which is necessary in SLAs in this survey [3]. In Section 3, Discussion part will be discussed. And in final part Conclusion and Abstract will be added at the end of the paper.

The above is a cloud architecture in Fig 1, which shows the overall procedure of users, broker, SLA Admission, Virtual machines and Physical machines. In this paper we differentiate the SLA models in cloud environment on the basis of parameters like Performance, CLS, Pricing, Security and SLA Violation in cloud service models i.e. SaaS, Paas and IaaS.

II. SLA IN CLOUD COMPUTING

Cloud computing consists of service models i.e. SaaS, Paas and IaaS.

![Diagram of SLA in Cloud Computing]

We will differentiate each model on the basis of SaaS, Paas and IaaS. Furthermore we will expand this tree like what type of parameters provided by each model.

A. SLA in SaaS:

We will discuss models of SLA in SaaS platform of cloud computing and analyze each model on the basis of parameters i.e. Performance, CLS, Pricing, Security and SLA Violation.

![Diagram of SLA in SaaS]

Trying to maximize CLS, in this [6] paper, the author present scheduling and admission control algorithm. This algorithm is used to increase CLS and also to increase income for the SaaS resources providers. The proposed algorithm performed different tasks in different scenarios. The results shows through simulation of that algorithm in different scenarios shows that it performed well trying to achieve CLS. Through simulation results display that proposed algorithm ProfPD saves upto 40% price of Virtual Machine (VM). In comparison with other presented algorithms differentiated through different QoS parameters ProfPD provide high profit to SaaS provider. There are other two algorithms also presented named ProfminVM and ProfRS. These algorithms are proposed in case of when user required a quick response time. In this case ProfminVM and ProfRS provides much better results than other algorithms.

In [14] this paper a model of computerized negotiation framework is proposed which provides automatic negotiation facility. This negotiation framework provide decent bargaining of SLAs. This decent bargaining is established among different SaaS brokers and different companies which aim to achieve their target goals. To achieve CLS and to increase profit they provide technical strategies and individual choice making heuristics mechanism that remember different trade-off parameters, different constraints regarding marketplace, time and other different QoS parameters. The facts used in negotiation heuristics framework is derived through experimental studies which was taken from an actual cloud enterprise. Their proposed algorithm display a limit on cost and also increase CLS in comparison with currently used heuristics. The selection of cloud resource provider is done though broker. Selection of a good provider and communication overhead takes place when parallel negotiation is done.

In [15] there are two policies are discussed which are used to handle the SLAs regarding its relationship with the goals of commercial enterprise and maximizing revenue. To set up the classification of customers is according to the relation between user and provider and measure the other QoS parameters that consumer wants to purchase a low QoS contract or greater QoS contract by paying high price. It is not necessary to consider or accept the policies as a complete set. There are some drawbacks involve in accepted policies.

In an untrusted cloud for dynamic groups, in [20] propose a scheme of secure data sharing known as Mona. In group without revealing identity privacy to the cloud a client is able to share data with others through Mona. Moreover, Mona supports efficient new client joining and client revocation. More especially, before participation a new clients in the cloud can directly decrypt a stored files and through a list of public revocation they achieved efficient user revocation with no updating of private keys for other clients. Additionally, the encryption computation price and the overhead of storage are constant. The large analysis display that their presented method satisfies the desired guarantees efficiency and security requirements very well.

B. SLA in IaaS:

We will discuss models of SLA in IaaS platform of cloud computing and analyze each model on the basis of parameters i.e. Performance, CLS, Pricing, Security and SLA Violation.

![Diagram of SLA in IaaS]
A cloud service provider have argue the profit optimizing dilemma in cloud system and they have an agreement among short term (decreasing the incoming jobs rejection) and long term (maintain SLAs and QoS) profitability. They present SLA aware admission control algorithm for cloud system which don’t affect the cloud service provider’s short term targets and increase the profits of long term. The profit enhance rate is among 80% and 400%. And they also compare his model with ‘M/M/m/m+r’ queuing model of fixed size [7]. In [10] there is a system called Learning Automata (LA) is introduced which deals with different QoS parameters in IaaS cloud platform. Learning Automata is very useful in dealing with computational tasks. LA based system ensures that CSP meets with all the requirements that is mentioned in the SLA agreement. Through various experiments QoS metrics is established. Through LA system that is used to select resources from the cloud in order to achieve QoS parameter is done through parallel execution speedup, job priority and response time.

In [23] they proposed a novel architecture called DeSVi, which is used to detect the SLA violation in cloud platform. The elements involved in their architecture are automated VM deployer, which is responsible for telling that execution of user application is done and LoM2HiS framework, which is used to track packages execution and convert low level SLAs in to high level.

In [24] they try to find out the two different user’s hidden requirements, which are not known to the CSP, in order to achieve CSL. So new method is used to estimate their requirements. Through this technique Cloud provider try to minimize the SLAs violation and to increase customers trust level. They carried out an experiment that during significant situation when resources are allocated, the estimation of resources can help the CSP to known about users requirements and analyze that which user to be served and which can be rejected. This will maximize CSL and CSP profit. This method is introduced to minimize SLAs violation.

C. SLA in SaaS, PaaS and IaaS:

In this paragraph, we will discuss that models which provides services of SaaS, PaaS and IaaS in cloud computing and analyze each model on the basis of parameters i.e. Performance, CLS, Pricing, Security and SLA Violation.

To overcome the issue of resource provisioning in datacenter that execute multiple form of applications workload, specially transactional and non-interactive applications. Here in [8] scheduling and admission control method is presented not only to maximize the profit and resource utilization, but also guaranteed the customer level QoS satisfaction are achieved at SLA. From their experimental result, for better resource utilization and provisioning of datacenters they suggest that this method is very helpful to aware from other multiple kinds of SLAs with mix of workload and appropriate penalties. The presented method decreases the violations of SLA and provides significant improvement over the consolidation of static server.

In [9] a new method is proposed called SLA aware service (SLAaaS) in Cloud computing. In this method QoS is merged with SLA and his goal is to decrease cost and to improve performance. CSLA language is introduced to define the SLA figures efficiently and addressing SLA violation. It ensures the best SLA guarantee and defined SLO (service level objective) as well as the trade off in SLA, priority of resources and weight among them. For this purpose an online algorithm is used in order to achieve the SLOs and to guarantee the service level agreements. They did not focus on other things like throughput of service etc. they did not target the other QoS parameters like privacy in cloud service and security guarantees.

In [11] architecture is proposed that enables Quality of Service (QoS) aware configurations, which enables the system with network federation integration to different types of cloud middle wares. It achieves the Quality of Service through virtualization on cloud based software define networks (SDN). Interface is proposed on the basis of SLA, allocation of network resources by the highest layer on the basis of QoS parameters that is enforced by the bottom layer. That is refer to the model which is “receive which you pay” e.g. allocation of memory and CPU through virtual hosts.

In unreliable resources context like spot instances to balancing the monetary cost versus reliability in [12] effective bid decision making strategy is proposed. The proposed strategy is known as AMAZING. The proposed strategy exploits the intelligence between different Spot Instances about state transition to facilitate decision making throughout the job’s computation course. They formulate the problem of optimizing decision making as a Constrained Markov Decision Process (CMDP). Before the job’s computation is completed for each instance hour optimal bid decision is applied after solving the AMAZING, CMDP. From their analysis results it is confirm that AMAZING give better performance as compare to early works in both terms like monetary cost and execution time.

In competitive cloud market the service provider should select an optimal penalty policy to achieve the maximum profits. In [13] they first survey the methods for penalties calculations of cloud service providers. According to the survey, they present for cloud service providers a correspondent penalty base profit maximization mechanism and a competitive penalty approach. Based on this approach, during the game procedure to achieve the maximum expected profit every cloud service provider would select the better fit penalty policy.

In [16] they proposed an approach called negotiation approach, which is used in order to achieve time utilization and to increase the profit of cloud providers. Through this approach the provider capture the consumer’s choices and strictly managed the deadline restrictions, which leads to increase the reliability on provider. This approach gives...
negotiation model for both parties in order to discuss their SLA efficiently.

In [17] they proposed a multi problem negotiation model. This model is used to facilitate the following figures. 1) Tradeoff among price and time-slot utilities and 2) PTNs (Price and Time-slot Negotiation) among cloud agents. The agent make multiple proposals in the negotiation round which leads to establish similar aggregate utilities, just individual time-slot utility and cost are different. It provide novel tradeoff algorithm, known as the “burst mode”, which is used for resource reservation, resource allocation in different time slots proposal.

In [18] they proposed an algorithm derived from different machine learning algorithms. This algorithm is used to find the semantically equal SLA elements from different SLAs. This technique provide to utilize the resources for the consumer of the cloud by allowing automatic selection of the required best services offers. A framework is developed for automated selection of SLA, its creation and management and simulation based evaluation is performed. Simulation based results provided which tells that their technique is efficient.

In [19] the authors present the analysis of access control requirement with detail for cloud networking and significant gaps discovered, those are not fulfill through traditional access control mechanism. To identifying the access control requirements of cloud they recommend access control model but the authentication mechanism and risk engine are implemented before a proposed model will be evaluated and implemented. They also implement risk engine with its components which deal with dynamic behaviors and also implement authentication approach which deal with large space and high time complexity.

The negotiation method and description mechanism of privacy information is presented in [21]. First, by description logic base they explain property of privacy with Privacy Negotiation Language (PNL). Second, by pre-negotiation among service provider and client they get privacy attribute sequence. Third, to satisfy both parties they achieve privacy policy based on exchanging privacy disclosure assertion. In this paper for client data protection they offers a theory basis and implementation technique in cloud system. At the end, they present an algorithm for privacy policy negotiation.

To facilitate the selection of competent and trustworthy service provider in [22] the authors recommend a new framework which is known as SelCSP. The trustworthiness is estimated by proposed framework in term of reputation feedbacks, context-specific and dynamic trust. The service provider competence is also computed in kind of SLAs transparency by framework. To estimate the risk of interaction the above two entities are combined. In this situation of interaction such estimate makes able a client to select a services provider.

To minimize service level agreement violations and cost of infrastructure for software as a service provider in [25] three cost driver resource allocation algorithms are presented. The presented three algorithms are intended to make sure that software as service providers capable to mapping client request for infrastructure level parameters, handling the virtual machine heterogeneities and manage the customer’s dynamic changes. The proposed algorithms for both software as a service provider’s and clients perspective consider different QoS parameters like a penalty rate, arrival rate and service initiated time. The simulation result shows that their proposed algorithms minimized the cost of the software as a service provider and rate of service level agreement violations in cloud resource sharing environment.

### III. Analysis of Models

In this section we will analyze all the models proposed for SLA in cloud computing. We will analyze the different parameters which are addressed by the different models in order to ensure the CSL, Security, Performance, SLA violation and to increase the provider’s profit.

<table>
<thead>
<tr>
<th>Paper Ref.</th>
<th>Propose model</th>
<th>SLO (service level objectives)</th>
<th>Profit</th>
<th>Customer Level Satisfaction</th>
<th>Performance</th>
<th>Security</th>
<th>SLA violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[6]</td>
<td>Admission control and scheduling algorithms</td>
<td>Profit, Cost, Customer Level Satisfaction</td>
<td>Maximize, save 40%</td>
<td>Maximize</td>
<td>Quick response time</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[14]</td>
<td>Novel automated negotiation framework</td>
<td>SLA negotiation, resource allocation;</td>
<td>50% increased profit</td>
<td>Improve 60%</td>
<td>Availability Improve 60%, Resource allocation</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[15]</td>
<td>Two sets of policies: Revenue Maximization Or Classification of clients</td>
<td>Cost, Profit, Relation between client and provider</td>
<td>Less</td>
<td>Maximize</td>
<td>Cloud provider is to maximize its economic profit and Client Classification</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[20]</td>
<td>Mona scheme</td>
<td>Security, data sharing, privacy-preserving, access control, dynamic groups</td>
<td>High</td>
<td>Guarantees efficiency as well</td>
<td>Nil</td>
<td>High</td>
<td>Nil</td>
</tr>
</tbody>
</table>
### TABLE II
ANALYZING MODELS WHICH PROVIDES IaaS PLATFORM

<table>
<thead>
<tr>
<th>Paper Ref.</th>
<th>Propose model</th>
<th>SLO (service level objectives)</th>
<th>Profit</th>
<th>Customer Level Satisfaction</th>
<th>Performance</th>
<th>Security</th>
<th>SLA violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[7]</td>
<td>SLA aware admission control algorithm</td>
<td>QoS, SLA base admission control, profit</td>
<td>Maximize, ranges between 80% and 400%.</td>
<td>Maximize</td>
<td>Keeping the response delays</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[10]</td>
<td>Learning Automata (LA)-based QoS (LAQ) framework</td>
<td>QoS parameters</td>
<td>Nil</td>
<td>Better response time</td>
<td>Parallel execution speed up, and job priority</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[23]</td>
<td>LoM2HiS framework for resource monitoring</td>
<td>Obligations, pricing, and penalties of violations.</td>
<td>No cost for missing SLA violation detection</td>
<td>Nil</td>
<td>Nil</td>
<td>Monitor and detect SAL violation</td>
<td>Nil</td>
</tr>
<tr>
<td>[24]</td>
<td>New proactive resource allocation approach</td>
<td>Satisfaction level, SLA violation</td>
<td>Gain profitability</td>
<td>Improve users’ satisfaction level</td>
<td>Maintain response time</td>
<td>Nil</td>
<td>Decreasing impact of SLA violations</td>
</tr>
</tbody>
</table>

### TABLE III
ANALYZING MODELS WHICH PROVIDES SaaS, PaaS AND IaaS PLATFORM

<table>
<thead>
<tr>
<th>Paper Ref.</th>
<th>Propose model</th>
<th>SLO (service level objectives)</th>
<th>Profit</th>
<th>Customer Level Satisfaction</th>
<th>Performance</th>
<th>Security</th>
<th>SLA violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[8]</td>
<td>Admission control and scheduling method</td>
<td>Virtual machine migration, Resource management and user require QoS.</td>
<td>Maximize</td>
<td>Maximize</td>
<td>Maximize</td>
<td>Nil</td>
<td>Resource utilization, decreases the SLA violations</td>
</tr>
<tr>
<td>[9]</td>
<td>SLAaaS &amp; CSLA Language</td>
<td>Addressing SLA violations, cost, dependability, response time</td>
<td>Maximize</td>
<td>Higher-level e-commerce service</td>
<td>Quick Response Time</td>
<td>Nil</td>
<td>SLA violation</td>
</tr>
<tr>
<td>[11]</td>
<td>Architecture that enables Quality of Service (QoS)aware configurations</td>
<td>Quality of Service through virtualization on cloud base SDN.</td>
<td>High Profit</td>
<td>Nil</td>
<td>Better response time</td>
<td>Nil</td>
<td>SLA violations</td>
</tr>
<tr>
<td>[12]</td>
<td>Effective bid decision making strategy known as AMAZING</td>
<td>Bidding Strategy, user reliability, cost</td>
<td>Maximize</td>
<td>Nil</td>
<td>Minimize job completion time</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[13]</td>
<td>Competitive penalty model and penalty based profit maximization algorithm for cloud providers.</td>
<td>SLA, availability, penalty degree</td>
<td>Maximize profit,</td>
<td>Maximize</td>
<td>High availability</td>
<td>Nil</td>
<td>Competitive penalty model</td>
</tr>
<tr>
<td>[16]</td>
<td>Time dependent negotiation model</td>
<td>Reliability</td>
<td>More profit for providers.</td>
<td>Nil</td>
<td>Reliable &amp; Availability</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>[17]</td>
<td>Novel tradeoff algorithm, known as the “burst mode” proposal,</td>
<td>Price and time slot</td>
<td>Maximize</td>
<td>Nil</td>
<td>Resource reservation, Resource allocation, different time slots.</td>
<td>Nil</td>
<td>Nil</td>
</tr>
</tbody>
</table>
In this paper, we surveyed various models used for SLA in cloud computing environment. Some of the models can provide high level security measures for consumer’s data, while some of the models provide penalty on SLA violation. Some of them increases user’s trust level while some of them maximize their performance level as compared with other models. To establish SLA between consumer and cloud service provider, we need to understand the role of cloud service provider either the CSP can provide all the required services according to the user’s choice? Because User expecting from cloud service provider to provide all the necessary services for their data. For every CSP, it is very difficult to provide security for user’s data to ensure confidentiality, integrity, reliability, availability and privacy. In this survey, we discuss some of SLA parameters for consumers that must consider these parameters before signing SLA in cloud platform.

IV. CONCLUSION

In this paper, we surveyed various models used for SLA in cloud computing environment. Some of the models can provide high level security measures for consumer’s data, while some of the models provide penalty on SLA violation. Some of them increases user’s trust level while some of them maximize their performance level as compared with other models. To establish SLA between consumer and cloud service provider, we need to understand the role of cloud service provider either the CSP can provide all the required services according to the user’s choice? Because User expecting from cloud service provider to provide all the necessary services for their data. For every CSP, it is very difficult to provide security for user’s data to ensure confidentiality, integrity, reliability, availability and privacy. In this survey, we discuss some of SLA parameters for consumers that must consider these parameters before signing SLA in cloud platform.

REFERENCES


Usman Wazir was born in D.I.Khan city, in 1990. He completed his B.S. in computer science from Gomal University, D.I.Khan, Pakistan, in 2014 and currently doing M.S in the field of Computer Science from COMSATS Institute of Information Technology, Abbottabad, KPK, Pakistan.

Dr. Fiaz Gul was born on 22-11-1982, in a beautiful valley Abbottabad of KPK. He did graduation and MS from COMSATS Institute of Information Technology Abbottabad in the field of Computer Science. For specialization master and Doctorate he won the HEC scholarship under the project UESTP for Politecnico di Torino Italy. Currently he is serving as an Assistant Professor in Computer Science Department at COMSATS Abbottabad, Pakistan.

Dr. Sajid Shah was born on 10-11-1982 in Swabi, KPK, Pakistan. He did BCS from Peshawar University Computer Science Department. He studied in Politecnico di Torino Italy, both his MS and PhD. He is currently assistant Professor in Computer Science Department at COMSATS Institute of Information Technology, Abbottabad, Pakistan.
Blind watermarking algorithm for 3D multiresolution meshes based on spiral scanning method

Ikbel Sayahi, Member, IEEE, Akram Elkefi, Member, IEEE, and Chokri Ben Amar, Member, IEEE

Abstract—3D mesh is a new data type appeared in the last decades. Since its emergence, it has been used in several areas which raise major security problems. As a solution, we propose a blind watermarking algorithm for 3D meshes. For doing spiral scanning method decomposes the mesh into GOTs (a Group Of Triangles). At each time, only one GOT will be uploaded into memory. It undergoes a wavelet transform to generate vector of wavelet coefficients. This latter undergoes modulation then embedding steps using data coded with BCH code. Once watermarked, the next GOT will be uploaded. This process stopped when the entire mesh is watermarked. Experimental tests show that the quality of meshes is kept despite the high insertion rate and that memory consumption is reduced. As for robustness, our algorithm overcomes the following attacks: translation, rotation, smoothing, uniform scaling, coordinate quantization, noise addition, simplification and compression.

Index Terms—Digital watermarking, 3D meshes, Multi-resolution, Wavelet transform, Spiral scanning, Attacks, Compression.

I. INTRODUCTION

During the last decade, the flow of 3D objects is increasingly used everywhere. This is due to the quality and accuracy of 3D models that makes them increasingly indistinguishable from concrete objects. The strengthening of computer graphics and acquisition techniques has generated a variety of areas benefiting from this new data category. Indeed, 3D meshes become ubiquitous in industrial applications such as movies production where 3D models are used in animated movies and live action feature films [1]. Towards the 2000s, the new 3D technology led the gaming industry to move away from 2D and pseudo 3D games (simulating 3D with 2D graphics projections), and to use 3D game engines leading to an abundant use of 3D models. The mechanical environment is another example as it benefit from 3D objects to perform virtual prototypical models. Let us add the use of this data type in architecture (to see the final impact of such a project) and medical visualization (abundant use of MRI, ultrasonographic and radiography) domains. In particular, the idea of multiresolution plays a growing part in the field of geometric modeling and especially scientific visualization. The initial objective, which remains the principal today, is the simplification of complex and dense mesh, particularly those derived from subdivision techniques or acquisition by 3D scanner.

On the other side, the information technology revolution, that has affected mainly the telecommunications and networks, has made its own way. The result being is the emergence of high speed broadband networks allowing the storage and the transfer of digital documents through remote multimedia databases. The 3D models are an example of these documents shared via the net. Sharing 3D meshes between remote users has spawned a huge security problem especially that digital copying does not entail any loss of quality. In addition, in contrast to acts of counterfeiting of analog works, the digital reproduction costs are negligible and counterfeiters can act anonymously without leaving a trace of their passage. All these problems leads that legal protection is no longer sufficient to ensure alone the peaceful management of works transmitted to the public. Hence, the need to use other techniques to strengthen existing legal protections seems necessary. Digital watermarking is then announced as a new technique that aims to limit these “digital abuse” and to preserve the copyrights [2].

In this context, many works have recently appeared to secure meshes ’copyright. The main topic of 3D watermarking is the choice of the embedding strategy (Where can we embed information? and how can we do it?). To answer these two questions, many 3D watermarking algorithms were published. Sharvari et al in [3] and Chao-Hung Lin et al in [4] chose to insert information in spatial domain by modifying geometric information. Zhiyong et al [5], combined spectral and spatial domain during embedding to improve robustness and invisibility. Multi-resolution domain is also present in the proposed watermarking algorithms. To transform host mesh from spatial to multi-resolution domain, there is an application of a wavelet transform. Works published in [6], [7] and [8] are examples that embed information into wavelet coefficients.

Unfortunately, all this diversity of methods does not deny that 3D watermarking is "still far from the level of maturity of other watermarking technologies for audio, video or image [2]". In fact, a perfect solution for 3D watermarking has not yet been proposed. In this context, we propose a new blind watermarking algorithm for 3D multi-resolution meshes. Our goal is no longer to have a good compromise between insertion rate, robustness and invisibility only, but also to minimize the
hardware resources used during the execution of our algorithm. This may facilitate the implementation of our prototype as well as the handling meshes with high definition.

II. RESEARCH STATUS

Since the appearance of the first watermarking algorithm for 3D meshes by Ohbushi et al in [9], many works were proposed in order make improvement in this research axis. The general structure of a watermarking scheme is always the same. In fact, each 3D watermarking scheme must necessarily go through the following three steps: the insertion of data, dissemination of the marked document in a noisy environment and extracting the signature from the watermarked and often attacked mesh [10]. Unfortunately, it is not obvious to correctly extract embedded information. In fact, attacks applied may alter and even destroy the already inserted data. Therefore, 3D watermarking algorithm targeting 3D meshes have continued to appear attempting to make improvements which create a diversification in terms of adopted areas and used techniques during embedding information into meshes. In order to classify these works, we choose to adopt two different criteria: the embedding domain and the type of information to change during insertion.

The first embedding domain used was the spatial one. The idea is to work directly on the mesh without any transformation. At this level, two types of information can be targeted by insertion. The first is the geometric information. In fact, to insert data into the mesh, Xiao et al [11] and Jen-Tse et al [12] used the Cartesian coordinates of each vertex. The watermarking algorithm, too, published by Hintandra et al in [13] worked also on the spatial domain and more precisely on geometric information. The proposed idea was to move a selected set of vertices from their positions depending on the data to be inserted. This selection is based on the principle of IEEE754 floating point representation. The second target is the topological information as in [5] and [4]. Insertion, in this case, aims at changing connections between vertices. Although working in spatial domain is slightly complex, given that no transformation will be applied on the mesh, results show a failure in visibility criterion. Indeed, working directly on geometrical and topological information has a considerable influence on the deterioration of the mesh quality.

Due to improvement attempts, other domains have been adopted, such as frequency area. The idea is to apply transformations to the mesh, before embedding step, to present it in the frequency domain using the so-called "frequency coefficients". Many tools allow ensuring this new representation. Xiangju et al in [14] chose to apply the mesh Radial Basis Functions before embedding. Insertion, in this case, takes place by changing the low frequency coefficients. Manifold harmonics is a tool used by Jinrong et al in [15] to work in the frequency domain. Applying Manifold Harmonics Transformation allows the generation of spectral coefficients. These latter will be modified according to the message to be inserted.

As was the case for image and video [16]–[18], multi-resolution domain is no longer excluded from watermarking works for 3D meshes. Works in [19] and [3] are examples of works operating in this domain. The used tool is the wavelet transform allowing the generation of multi-resolution coefficients called "wavelet coefficients" which are targeted by embedding. Approach Ouled Zaid et al in [7] targeted these coefficients during insertion. The modification is based on QIM algorithm to improve the amount of information to be inserted.

As a conclusion, we can say that there is a diversity of used methods and tools in watermarking algorithms targeting 3D meshes. Unfortunately, despite the efforts to innovate and improve in this field, the security problem of 3D mesh is always posed. As shown in table I, a perfect solution has not yet been proposed. ST reminds the similarity transformation attacks including translation, rotation and uniform scaling. Results presented in I reveal a failure in robustness criterion. Indeed, there is no solution that resists to all attacks targeting 3D meshes. The compression attack, frequently applied to 3D meshes, is absent in results published in recent works. This suggests that compression presents a real challenge for 3D watermarking. In addition, the watermark used during the insertion is relatively short. This limited the number of bits influence on the amount of information to be hidden in the mesh.

The failure already unveiled amounts to two reasons. The first is the complexity of handling 3D meshes compared with other types of data such as sound, image or video. The complexity of representing 3D meshes and the sensitivity of these data allowed concluding that the manipulation of the 3D mesh is a difficult task. This return to the following 3D mesh characteristics:

- The absence of a global parameterization,
- The arbitrary topology,
- The irregular connectivity,
- The non-uniformity of sampling.

The second reason is the difficulty of finding a good compromise between robustness, visibility and insertion rate which can be justified by the strong link between these 3 criteria. In fact, the increase of the amount of data to be inserted causes either a serious deterioration of the mesh quality or reduces the level of robustness.

III. BACKGROUNDS

A. Multi-resolution Analysis

In the 3D world, an object can be defined by a cloud of points having 3 coordinates x, y and z in the Cartesian coordinate system. The surface of a 3D object is presented by a grid. This latter is partitioned into a set of polygonal elements. Polygons composing the mesh can be either triangles, or quadrangles or any other polygons. Especially, triangular meshes are used in this work.

This category is described using a set of triangles. The points of the triangles are called vertices and they are interconnected by the edge forming the triangles. The vertices refer to the geometric information of the grid, and edges refer to the topological information.

A mesh can be mono or multi-resolution. In the case of...
TABLE I
INSERTION RATE, VISIBILITY AND ROBUSTNESS IN RECENT 3D WATERMARKING WORKS.

<table>
<thead>
<tr>
<th>Work</th>
<th>Blind</th>
<th>Insertion rate</th>
<th>Invisibility</th>
<th>S. T</th>
<th>Noise</th>
<th>Smoothing</th>
<th>Quantization</th>
<th>Simplification</th>
</tr>
</thead>
<tbody>
<tr>
<td>[11]</td>
<td>yes</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[3]</td>
<td>No</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[5]</td>
<td>Yes</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[4]</td>
<td>Yes</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[19]</td>
<td>Yes</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[12]</td>
<td>No</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[14]</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[15]</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[13]</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[7]</td>
<td>Yes</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

multi-resolution, a 3D object is represented at different levels of details. It is composed of a coarse mesh and a set of information which refine the coarse mesh to its finest levels version (see figure 1). Multi-resolution meshes are stored in files with a .dat extension. So far, no watermarking work has targeted multi-resolution meshes stored in DAT format files. This is due to the sensitivity of handling this category of data. In fact, the treatments applied to the mesh can easily alter its multi-resolution appearance. Our goal is then to watermark this kind of meshes without influencing either its quality or its multi-resolution appearance.

B. Digital Watermarking

By definition, digital watermarking [20] is a technique that involves inserting a watermark, in the form of a message or logo, in a digital document known as "host document." The appearance of this technique was the result of an intense need to secure the shared flow of digital data. Once inserted, it must be possible to retrieve the watermark after the transfer of this document. Inserted data may contain an identification number to implement a system of copyright or a description of the content in order to indexing and it must be indelible [21]. That is to say that once inserted, it must be impossible to remove watermark without using the key or the insertion method. On the other hand, inserted data must be robust to any attack targeting the host document. The 3 steps composing a 3D watermarking algorithm are the following:

- Insertion: This step uses the host mesh and the watermark to be inserted. Depending on the application which is dedicated to the 3D watermarking, the insertion can be made either in spatial domain (directly on the mesh) or in the transformed domain (frequency, spectral or multi-resolution domain) [22]. Inserting data in the mesh can be made following an additive (add information to the mesh) or a substitute scheme (substitute some components of the mesh).
- Dissemination: Once the mesh is watermarked, it may undergo different treatments. The most frequent being: storing in a database, transferring in a computer network or even a set of treatments to specific improvements. These can give opportunity to attacks to change the watermarked mesh and consequently alter the data being inserted.
- Extraction: Having received the watermarked mesh, the extraction step begins. It involves extracting data from the watermarked and usually attacked mesh. In the case where the extraction uses only the watermarked mesh, the watermarking algorithm is called "blind".

C. Wavelet Transform

The main idea of the multi-resolution analysis is to decompose a mesh \( M_i \) in two sets: a low resolution mesh \( M_{i-1} \) and a set of details \( D_{i-1} \) (see figure 2): the analysis phase. All these details and meshes of different resolution level are then used to reconstruct the original mesh: synthesis phase. Using the formalism of multiresolution analysis, we can write:

\[
M_j = M_{j-1} \oplus D_{j-1}
\]  

Here \( D_{j-1} \) is all the details necessary to rebuild the mesh, \( M_j \) is the higher resolution from the mesh \( M_{j-1} \), and \( \oplus \) is the orthogonal complement operator. The principle of wavelet transform is to decompose the energy of a signal using two basic functions (prediction and update). Thus, applying these functions on a mesh in an analysis step, we obtain a lower resolution mesh and a set of wavelet coefficients needed to reconstruct the original mesh in the synthesis step. All these
coefficients are assembled into a single vector called wavelet coefficient vector (WCV) as shown in equation 2. Especially, this vector will be modified during insertion.

\[
WCV = \begin{pmatrix} D_1 \\ \vdots \\ D_i \end{pmatrix} = \begin{pmatrix} d_{x1} \\ d_{y1} \\ d_{z1} \\ \vdots \\ d_{x1} \\ d_{y1} \\ d_{z1} \end{pmatrix}
\]

(2)

For doing, a lifting schema, which is a wavelet transform of second generation introduced in 1998 by Sweldens [23], should be used. It consists in exploiting the spatial and frequency correlation present in the mesh to reduce its entropy. As shown in figure 3, the lifting scheme is divided into three steps:

- Poly-phase transformed: it is a basic operation that divides the signal to two sub-bands.
- Prediction: This step exploits the spatial and frequency correlation present in the signals. During this step the elements of the first component are used to predict the elements of the second component. The difference between the predicted element and the element present in the same second component is the detail.
- Update: at this stage the first component element represent only a sub-sampling of the original signal. To transform these elements to low frequencies, we apply a low pass filter.

D. Spherical coordinate system

To insert information into a mesh, we should calculate the module of each wavelet coefficient. For this reason, a transition to the spherical coordinate system is necessary. To transform the Cartesian coordinates (x, y and z) of each wavelet coefficient into spherical coordinate system (ρ, θ and φ), formula 3 is used.

\[
\rho = \sqrt{x^2 + y^2 + z^2} \\
\theta = \arccos\left(\frac{z}{\rho}\right) \\
\varphi = \begin{cases} 
\arccos\left(\frac{x}{\sqrt{x^2+y^2}}\right) \\
2 \times \Pi - \arccos\left(\frac{x}{\sqrt{x^2+y^2}}\right)
\end{cases}
\]

(3)

To recalculate the wavelet coefficients, the application of an inverse transformation is necessary after insertion. For doing, formula 4 is applied as follows:

\[
x = \rho \times \sin \theta \times \cos \varphi \\
y = \rho \times \sin \theta \times \sin \varphi \\
z = \rho \times \cos \theta
\]

(4)

E. BCH error correcting code

The BCH code (code of Bose, Chaudhuri, and Hocquenghem) [24] is a block error correcting code intended for binary data. This code allows the correction of t errors with t between \(\frac{n-k}{2}\) and \(\frac{n-2}{2}\). Let n, the codeword length, be equal to \(2^m - 1\). k refers to the number of bits to encode and m is the number of control bits. Abbas et al. affirmed in [25] that the
BCH code is able to correct a number of errors up to 25% of the number of bits transmitted. This encouraged us to involve this code in our watermarking algorithm.

1) Galois Field (GF): For a Prime number q, a Galois field, characterized through defined arithmetic operations, refers to the set of integers modulo q ensuring the following proprieties:

Property 1: Let us consider the irreducible polynomial of degree m, named \( p(x) \), representing GF \((q^m)\). \( p(x) \) does not contain roots in GF \((q)\) but we assume that it has roots elsewhere. We note \( \alpha \) one of these roots. Thus, the set of roots that we can handle is \( \alpha^0, \alpha^1, ..., \alpha^{q^m-1} \).

Property 2: if \( \alpha \) is a root in GF \((q^m)\) then:

\[
\alpha^i \times \alpha^j = \alpha^{(i+j) \mod (2^m-1)}
\]  

2) BCH encoder: To encode a message using the BCH code, we had to use a predefined polynomial said "generator polynomial". The codeword is resulting from a multiplication, in Galois field that owns the code, of the generator polynomial with the message that we aim to code.

3) BCH decoder: The decoding step using the BCH code follows these sex steps:

Step1: Let \( p(x) \) the polynomial that corresponds to the code-word. The syndrome \( S_1 = p(\alpha^1), S_2 = p(\alpha^2), S_{2t} = p(\alpha^{2t}) \) should be calculated.

Step 2: If the syndrome is zero, the received message is correct. The execution of the algorithm stops. If not, the rest of the algorithm is executed.

Step 3: The number of errors that occurred noted \( \delta \) can be calculated. It corresponds to the rank of the following matrix (see formula 6):

\[
\begin{pmatrix}
S_1 & S_2 & \cdots & S_{t-1} & S_t & S_{t+1} & \cdots & S_{2t-1} \\
S_2 & S_3 & \cdots & S_t & S_{t+1} & \cdots & S_{2t-1} \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
S_t & S_{t+1} & \cdots & S_{2t-1} \\
\end{pmatrix}
\]  

(6)

Step 4: Following the number of errors, system in equation 7 is solved.

\[
\begin{pmatrix}
S_1 & S_2 & \cdots & S_{t-1} & S_t & S_{t+1} & \cdots & S_{2t-1} \\
S_2 & S_3 & \cdots & S_t & S_{t+1} & \cdots & S_{2t-1} \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
S_t & S_{t+1} & \cdots & S_{2t-1} \\
\end{pmatrix} \times 
\begin{pmatrix}
\zeta_{\delta+1} \\
\zeta_{\delta+2} \\
\vdots \\
\zeta_{2\delta} \\
\end{pmatrix} = 
\begin{pmatrix}
S \\
S_{\delta} \\
\end{pmatrix}
\]  

(7)

Step 5: The \( \delta \) roots \( \alpha^{-i_1}, ..., \alpha^{-i_\delta} \) of the polynomial \( M(x) \) are determined. \( M(X) = \zeta^\delta X^\delta + ... + \zeta^1 X^1 + 1 \).

Step 6: The errors occurred in positions \( i_1, ..., i_\delta \). These bits should be reversed.

IV. APPROACH DESCRIPTION

We present, in this paper, a new blind watermarking approach for multi-resolution 3D meshes. Our goal is to find a good compromise between invisibility, insertion rate and robustness while minimizing the amount of memory used during the execution of our algorithm. The minimization of memory consumption is due to the decomposition of the mesh while being watermarked using the spiral scanning method which is the main idea of this manuscript. The minimization of memory consumption is due to the decomposition of the mesh while being watermarked using the spiral scanning method. As shown in Figure 5, our work is based on the use of a watermarking buffer. This refers to the maximum amount of memory reserved for watermarking. Decomposition of the mesh into GOTs depends on the watermarking buffer size. For each GOT overloaded in memory, watermarking which can be either an insertion or an extraction step is applied. Once treated, the next GOT is overloaded. This process ends when the entire mesh is treated.

A. Embedding

Embedding involves inserting data in the host mesh while keeping its quality. This step requires then the presence of a multi-resolution mesh and a watermark in the form of a binary sequence. As already mentioned, embedding is applied to each GOT saved in memory. To further detail this step, we present figure 6 which shows a zooming of the watermarking part in figure 5. The steps necessary for watermarking a GOT are:

1) Spiral Scanning acquisition: To treat an object during its acquisition, we must break it down into parts and send the necessary part to memory each time. Contrary to semi-regular mesh, decomposition of image into blocks or video into image looks very simple. The problem that arises during the decomposition of a mesh is the choice of the starting point and the direction chosen to browse the mesh. It is then essential
to answer the following two questions: from which triangle can we begin decomposition? And how do we ensure that we scanned the entire surface and that the entire mesh was processed?

To answer these questions, we based our approach on spiral scanning method proposed to ensure a progressive compression in [26]. The use of spiral scanning method during compression gives very good results in terms of minimizing the amount of used memory during compression. We will readopt this method for 3D watermarking. Our objective is to ensure that the watermarking process has swept the whole mesh and that there is no untreated part, which is tricky, as the topology of the object is varied. The choice of course affects directly the memory size used.

Our idea is, then, to take a low frequency triangle as a unit and to provide a tool for scanning the mesh as shown in figure 7. The step of calculating the neighborhood is very costly in terms of the number of operations. To solve this complex problem, instead of searching the neighbors throughout the mesh, we proposed a procedure for locating the smallest area covering them using the following properties:

Property 1: The neighbors of a central triangle Tc are among the sons of the father of Tc.

Property 2: Of the sons of the father of a triangle T, the only one that is central is a neighbor. Other neighbors of T are among the neighbors’ son of the father of T.

Property 3: If two triangles T1 and T2 are adjacent then one of them is central. Once this is known, it facilitates the search for other neighbors according to property 1.

Property 4: Of the son of the father of a triangle T, the only one that is central is a neighbor. Other neighbors of T are among the neighbors’ son of the father of T.

As shown in figure 8, the acquisition follows an oriented movement so that the scanning of the 3D mesh does not leave untreated portions. To do it, we follow, as a reference, the list L0 = \{a, c, b\} for acquiring the triangles Ai, Bi and Ci, respectively colored in yellow (near the point a), green (vicinity of the point c) and blue (vicinity of the point b). This represents a complete initialization turn. When detecting a new triangle, we send it to the watermarking buffer and we update the new reference list. The second round will reference the newly created list being L1 = \{r0, r1, ..., ri\} and so on. The end of transmitting triangles to the watermarking buffer corresponds to a new empty reference list. To explain in a clear and simple way, we propose Algorithm 1.

\[\text{Algorithm 1: Spiral Scanning Method}\]

Vertex St = “a”  // Initialization
// Ed is the third vertex triangle containing ”a” and ”b” and
which is not in the StartingList.

Vertex Ed = ThirdVertexOf(CurrentTriangle,a,b)  
StartingList=a,b,c  // Definition of Lists L0 (StartingList).
EndingList=Ed     // And L1 (EndingList).
while(EndingList!=Null)  // The algorithm remains in the loop until the ”EndingList” generated is empty.
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // Loop on the entire “starting” vertex to find the triangles of the entourage.
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // On all the ”Ending” vertices. If the third vertex
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // ”temp” is the first element of the ”EndingList”
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // Then we move on to the next item in StartingList.
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // (temp) != First (EndingList)
   Add Temp in EndingList  // Update of EndingList.
   Stat(T)=MarcTriangle (St, Ed, Temp)  // Mark visited triangle T.
   Ed = temp
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // Move to the next element in the StartingList. St = Next
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // The current startingList is recorded in ”List” that will
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // contain the list of all the points covered spirally.
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // List=List + StartingList;
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // // switch the Starting List with the Ending move to the next
   Temp=ThirdVertexOf(CurrentTriangle,St,Ed)  // round.
   StartingList = EndingList  // StartingList = EndingList
End.

The application of this method leads to the division of the mesh into four parts (see figure 8):  
Part 1: treated and cleared (1).
Part 2: treated and stored in memory (2).
Part 3: during treatment (3).
Part 4: not yet treated (4).

2) Wavelet transform: The application of the spiral scanning method has decomposed the mesh into GOTs. For every GOT, we apply a wavelet transform to generate the vector of wavelet coefficients. This vector then undergoes amendment during embedding. Inserting data in the multi-resolution domain leads to the increase of the amount of embedded information, better preservation of the mesh quality and the improvement of the robustness of our algorithm.
3) **BCH encoder:** To protect information against any type of alteration and to be able to correct the eventual errors that may occur [27], we used BCH error correcting code. This latter encode data before being inserted. As a result, a codeword containing the initial information and a set of control bits, is generated. This new data will be embedded into a host mesh.

4) **Embedding information:** The vector generated from each GOT will be presented in the spherical coordinate system. Only the $\rho$ component, which refers to the module of each wavelet coefficients, will be modified during embedding. This first component undergoes a modulation. It will be multiplied by a modulation coefficient determined experimentally to obtain a modulated coefficient that we call $C'$. Insertion occurs then according to the bit of data as seen in formula 8.

$$
C' = \begin{cases} 
C = 0.3 & \text{if } bit_i = 0 \\
C = 0.7 & \text{if } bit_i = 1 
\end{cases}
$$

(8)

Once watermarked, we apply a demodulation to $C'$ and we present coefficients again in the Cartesian system. Finally, the watermarked GOT will be released from memory to upload the next one. Our approach relies then on the use of the spiral scanning method. At each time $t$, only a portion of the mesh is saved in memory to be watermarked. Once this part is watermarked and as long as there is untreated parts, the execution of our watermarking algorithm restarts. When the whole mesh is treated, an inverse wavelet transform occur to rebuild the watermarked mesh.

### B. Extraction

This step allows the extraction of the inserted information from the mesh. Unfortunately it is not always possible to extract all data correctly. This is due to treatments (also called attacks) applied to the watermarked mesh. The aim of our watermarking algorithm is to retrieve information correctly in spite of any kind of attack: the robustness criterion.

We propose in this part, the extraction step of our approach. Our primary goal is to extract all the information correctly. To achieve this objective, we decompose the mesh into GOTs using spiral scanning method. For each GOT, a wavelet transform is applied to have a wavelet coefficient vector. For each coefficient presented in a spherical system, we apply modulation. Finally, we extract the inserted bit depending on the results of modulation (see figure 10). After that, we move to the next coefficient. Once this part of the mesh is processed and the watermark is extracted, the following GOT is loaded into memory to be treated in its turn. Once the entire mesh is processed and the totality of the watermark is extracted, collected data will be decoded using a BCH decoder. This treatment allows the correction of wrong bits. As shown in figure 10, only the watermarked mesh is used during extraction. Our watermarking algorithm is then said “blind.”

### V. Evaluation tools

To evaluate this approach, we have to study firstly the influence of our algorithm on the mesh quality. This allows calculating the difference between the original and the watermarked mesh. As for tools, we resorted to calculating MSQE and PSNR.

Secondly, we must focus on the extraction of information. Our goal is to recover correctly all the information from the watermarked and attacked mesh to reach the decision-making step. During this step, we have to compare the difference between the information inserted at the beginning and that extracted in order to conclude on the robustness of our algorithm. This amounts to calculating the correlation values between the inserted information and the extracted one.

### A. MSQE and PSNR

Embedding a watermark in a host mesh should not affect the mesh quality. To evaluate this criterion, we should find differences between watermarked and original meshes by computing Mean Square Error (MSQE, MSE or MSDM) [28]. The MSQE is then calculated using formula 9. The main idea is to evaluate the distance between the two meshes. It represents the distance between a point $x$ from the first mesh and a surface from the second one [28].

$$
d(M, \tilde{M}) = \left( \frac{1}{\text{area}(M)} \int_{x \in M} d(x, \tilde{M}) dx \right)^2
$$

(9)
The MSQE is then calculated using formula 10.

\[ MSQE = \max(d(M, \hat{M}), d(\hat{M}, M)) \]  

(10)

Another comparison tool we can also use is the PSNR (Peak Signal to Noise Ratio) measured in decibels (dB). This parameter calculates the ratio between the signal dynamics and the error of the watermarking.

\[ PSNR = 20 \times \log_{10}\left(\frac{Bounding\ Box}{MSQE}\right) \]  

(11)

B. Correlation

To evaluate the robustness criterion of our algorithm, we chose to calculate the correlation value between the inserted information I1 and that extracted I2. This allows measuring the intensity of the link between the two latter (see formula 12)

\[ C = \frac{(\sum_{i=1}^{n} I_1 - \bar{I}_1) \times (\sum_{i=1}^{n} I_2 - \bar{I}_2)}{\sqrt{\sum_{i=1}^{n}(I_1 - \bar{I}_1)^2 \times \sum_{i=1}^{n}(I_2 - \bar{I}_2)^2}} \]  

(12)

n refers to the size of information. We can say that we were able to extract correctly all the information when the correlation value obtained is close to 1.

VI. APPROACH EXPERIMENTATION

For evaluating our watermarking algorithm, two criteria must be taken into consideration. The first one is visibility. It aims at measuring the impact of our algorithm on mesh quality. The second one is the robustness criterion. It focuses on the ability of our approach to extract data correctly from watermarked and attacked mesh.

To test our approach, we used multi-resolution meshes stored in multiresolution files having variable sizes. Table II summarizes the different meshes used during tests.

<table>
<thead>
<tr>
<th>Name</th>
<th>Triangle numbers</th>
<th>Vertex numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feline.dat</td>
<td>516096</td>
<td>258046</td>
</tr>
<tr>
<td>Horse.dat</td>
<td>225280</td>
<td>112642</td>
</tr>
<tr>
<td>Venus.dat</td>
<td>81920</td>
<td>40962</td>
</tr>
<tr>
<td>Rabbit.dat</td>
<td>70658</td>
<td>35329</td>
</tr>
</tbody>
</table>

A. Visibility criterion

The objective of this section is to test the effect of our algorithm on the quality of watermarked mesh. To do this, we watermarked several 3D meshes and each time we calculated the MSQE and PSNR. We aim at finding a compromise between watermarking strength and invisibility criterion (see table III). Results presented in table III show that even with a large insertion rate (watermark=250000 bits), our algorithm does not affect the quality of the mesh. We can conclude, from an MSQE equal to \(1.2 \times 10^{-6}\) and a PSNR value equal to 126.35, that our algorithm preserves the visual appearance despite the important size of inserted information.

TABLE III

<table>
<thead>
<tr>
<th>Watermark length (bits)</th>
<th>5 \times 10^4</th>
<th>15 \times 10^4</th>
<th>25 \times 10^4</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSQE</td>
<td>0.7 \times 10^{-6}</td>
<td>10 \times 6</td>
<td>1.2 \times 10^{-6}</td>
</tr>
<tr>
<td>PSNR</td>
<td>130</td>
<td>124</td>
<td>126.35</td>
</tr>
<tr>
<td>Correlation</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

TABLE IV

<table>
<thead>
<tr>
<th>Modulation coefficients</th>
<th>MSQE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.1</td>
<td>45</td>
<td>1</td>
</tr>
<tr>
<td>100</td>
<td>10^{-4}</td>
<td>60</td>
<td>1</td>
</tr>
<tr>
<td>1000</td>
<td>0.2 \times 10^{-5}</td>
<td>95.5</td>
<td>1</td>
</tr>
<tr>
<td>10000</td>
<td>1.2 \times 10^{-6}</td>
<td>126.35</td>
<td>1</td>
</tr>
<tr>
<td>100000</td>
<td>0.5 \times 10^{-6}</td>
<td>130.7</td>
<td>1</td>
</tr>
</tbody>
</table>

TABLE V

<table>
<thead>
<tr>
<th>Approach</th>
<th>Insertion rate</th>
<th>MSQE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our approach</td>
<td>250000</td>
<td>1.2 \times 10^{-6}</td>
<td>126.35</td>
<td>1</td>
</tr>
<tr>
<td>[11]</td>
<td>765</td>
<td>0.004</td>
<td>–</td>
<td>1</td>
</tr>
<tr>
<td>[3]</td>
<td>–</td>
<td>–</td>
<td>68.78</td>
<td>1</td>
</tr>
<tr>
<td>[5]</td>
<td>12732</td>
<td>0</td>
<td>84.47</td>
<td>1</td>
</tr>
<tr>
<td>[4]</td>
<td>39707</td>
<td>0.0</td>
<td>84.13</td>
<td>1</td>
</tr>
<tr>
<td>[19]</td>
<td>–</td>
<td>–</td>
<td>92.45</td>
<td>1</td>
</tr>
<tr>
<td>[28]</td>
<td>1045515</td>
<td>5 \times 10^{-6}</td>
<td>–</td>
<td>1</td>
</tr>
<tr>
<td>[12]</td>
<td>32</td>
<td>–</td>
<td>–</td>
<td>1</td>
</tr>
<tr>
<td>[13]</td>
<td>21022</td>
<td>2.7 \times 10^{-5}</td>
<td>–</td>
<td>1</td>
</tr>
<tr>
<td>[7]</td>
<td>10650</td>
<td>0.2 \times 10^{-3}</td>
<td>–</td>
<td>1</td>
</tr>
</tbody>
</table>

The \(\rho\) component of each wavelet coefficient, before being modified, is multiplied by a modulation coefficient determined experimentally. This coefficient is related to the strength of our algorithm and the visibility criterion. The higher the value of coefficient is, the more affected the mesh quality becomes. In order to study the influence of this coefficient on the watermarked mesh quality, we present table IV. Results show that, with a coefficient equal to 10000, we obtain an MSQE equal to \(1.2 \times 10^{-6}\) and a PSNR value of about 126db. Working with a modulation coefficient equal to 10000, there is almost no difference between the original and the watermarked mesh. We will maintain this value for other applied tests.

To locate our algorithm relatively to existing work, we compared our results with recently published results in terms of insertion rate, MSQE, PSNR and Correlation. Table V summarizes the results found during comparison. Although the number of bits that we can insert makes the insertion rate of other approaches insignificant (250000 bits in our works and about 39000 in others works), we still present best PSNR and MSDM values. Our approach is consequently able to insert
the highest number of bits in host mesh while keeping mesh quality.

B. Attacks

Evaluating the robustness criterion need the application of attacks after watermarking the host mesh. According to Kai Wang et al [29], attacks which threaten correct retrieval of information from a watermarked mesh can be classified as follows:

- Geometry attacks: This category of attack tends to change coordinates of vertices without modifying the topological information (connectivity). Similarity transformation, Noise addition, smoothing and coordinate quantization are examples.
- Connectivity attacks: This kind of attack modifies the connections between vertices without changing their positions. Only the topological information is targeted. We cite simplification as example of connectivity attacks.

1) Similarity transformation: This category, which is made up of three attacks: translation, rotation and uniform scaling, does not cause any alteration on the form of the mesh (see figure 11). Results, present in table VI, assert that our algorithm is robust against similarity transformation attacks. Indeed, the application of translation, rotation and uniform scaling to watermarked meshes, has not prevented the correct extraction of data.

![Fig. 11. Similarity transformation Attacks.](image)

![Fig. 12. Noise Addition Attack.](image)

2) Noise addition: The main idea of this attack is to modify the coordinates of vertices using a pseudo-random generator. This modification follows formula 13:

\[
\begin{align*}
\hat{x}_i &= x_i + \alpha \times d \\
\hat{y}_i &= y_i + \alpha \times d \\
\hat{z}_i &= z_i + \alpha \times d 
\end{align*}
\]  

With \(d\) is the distance from the center of gravity of the mesh and \(\alpha\) a pseudo random number. In order to study the robustness of our algorithm against noise addition, we carried out several tests. Each time, we apply this attack to a watermarked mesh, we extract data and we calculate the correlation value. Results, depending on the noise level and the proportion of vertices affected by noise are presented in tables VII and VIII. As shown in Table VII, correlation value is acceptable for a noise level down to \(10^{-4}\). Correct retrieval of information is possible in this range of values. By comparing the correlation values of our approach to recently-published results, we note that our approach is an outstanding improvement over existing approaches. Changing the number of vertices affected by noise has not led to a large drop in the value of correlation. In fact, we kept values close to 1. Results in [8] and [3] show a significant decline in correlation values.

3) Smoothing: To apply a smoothing attack to a mesh, formula 14 should be used:

\[
\begin{align*}
\hat{x}_i &= x_i + \text{DFactor} \times \bar{d}_x \\
\hat{y}_i &= y_i + \text{DFactor} \times \bar{d}_y \\
\hat{z}_i &= z_i + \text{DFactor} \times \bar{d}_z 
\end{align*}
\]  

DFactor is a manually initialized parameter. \(d_x\), \(d_y\) and \(d_z\) should be calculated as shown in formula 15.

\[
\begin{align*}
\bar{d}_x &= \frac{\sum_{j=1}^{\text{vertex}} \sum_{i=1}^{\text{vertex}} x_j - x_i}{\text{vertexNumber}} \\
\bar{d}_y &= \frac{\sum_{j=1}^{\text{vertex}} \sum_{i=1}^{\text{vertex}} y_j - y_i}{\text{vertexNumber}} \\
\bar{d}_z &= \frac{\sum_{j=1}^{\text{vertex}} \sum_{i=1}^{\text{vertex}} z_j - z_i}{\text{vertexNumber}} 
\end{align*}
\]

To study the effect of smoothing during extraction we did many tests. Found results are presented in table IX. For
a dFactor value less than \(10^{-7}\), we obtained a correlation value near 1. Comparing these results with those of previous published work published [8], we note that with our present approach we have reinforced the robustness against smoothing attack.

### TABLE IX

<table>
<thead>
<tr>
<th>Quantization Level</th>
<th>10^{-5}</th>
<th>10^{-6}</th>
<th>10^{-7}</th>
<th>10^{-8}</th>
<th>10^{-9}</th>
<th>10^{-10}</th>
</tr>
</thead>
<tbody>
<tr>
<td>C in [8]</td>
<td>–</td>
<td>–</td>
<td>0.18</td>
<td>0.31</td>
<td>0.43</td>
<td></td>
</tr>
<tr>
<td>Obtained C</td>
<td>0.034</td>
<td>0.2</td>
<td>0.848</td>
<td>0.968</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

4) Coordinate quantization: This attack aims at quantifying vertex coordinates using two previously calculated factors according to the maximum and minimum values along x, y and z called \(x_{\text{max}}, x_{\text{min}}, y_{\text{max}}, y_{\text{min}}, z_{\text{max}}\) and \(z_{\text{min}}\). Ql refers to the quantization level which is initialized manually (see equations 16 and 17).

\[
\begin{align*}
\text{Step}_x &= \frac{x_{\text{max}} - x_{\text{min}}}{Ql} \\
\text{Step}_y &= \frac{y_{\text{max}} - y_{\text{min}}}{Ql} \\
\text{Step}_z &= \frac{z_{\text{max}} - z_{\text{min}}}{Ql}
\end{align*}
\]

\[
\begin{align*}
\text{Factor}_x &= \left\{ \begin{array}{ll}
\frac{x - x_{\text{min}}}{\text{Step}_x} & \text{if } \text{Factor}_x > 0.5, \\
\text{Factor}_x + \text{Step}_x & \text{Otherwise}
\end{array} \right.
\end{align*}
\]

Previous factors are then used to quantify vertex coordinates.

\[
\hat{x}_i = \begin{cases} 
\text{Factor}_x \times \text{Step}_x - x_{\text{min}} & \text{if } \text{Factor}_x > 0.5, \\
\text{Factor}_x + \text{Step}_x & \text{Otherwise}
\end{cases}
\]

5) Simplification: The main idea is to present the mesh with a number of triangles less than the original representation. Removing triangles from the mesh can alter the inserted mark and even destroy it. The main idea of this attack is to remove triangles from the mesh. Deleted triangles may be carrying the information which threatens the extraction phase. Applied tests, whose results are presented in table XI, show very well that we were able to extract all the information inserted despite the application of simplification in various levels.

### TABLE XI

<table>
<thead>
<tr>
<th>Iteration Number</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>C in [30]</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>0.46</td>
<td>0.31</td>
<td>0.15</td>
</tr>
<tr>
<td>C in [13]</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>0.79</td>
<td>0.68</td>
<td>0.61</td>
</tr>
<tr>
<td>C in [7]</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>0.99</td>
<td>0.97</td>
<td>0.92</td>
</tr>
<tr>
<td>C in [31]</td>
<td>–</td>
<td>0.6</td>
<td>0.45</td>
<td>0.25</td>
<td>0.1</td>
<td>0.05</td>
</tr>
<tr>
<td>Obtained C</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

6) Compression: The compression method shown in Figure 16 includes two parts: a wavelet transform and a coding [32]. The input is a watermarked 3D mesh. This compression method processes the host mesh sequentially. Each time, the spiral scanning sends a GOT of coarse triangles with all its details to the memory of wavelet transform. The block of the wavelet transform calculates the wavelet coefficients and sends the result to be encoded. Coding Buffer has four steps: binary allocation, quantization, entropic coding and coding of connectivity.

Obviously, compression should not alter the information already inserted. Unfortunately, this type of attack presents a challenge for watermarking algorithms targeting 3D meshes. This justified the absence of experiments focusing on compression in the recently published algorithms. In this paper, we aim to concentrate on this type of attack. In order to conclude
The approach proposed in this paper is based on the use of spiral scanning method. It consists in decomposing the host mesh into GOTs. Each time, a GOT will be sent to memory to be treated. Treatment includes the application of a wavelet transform in order to generate the vector of wavelet coefficients. Components of this vector undergo modulation to be watermarked according to binary data. Finally, a demodulation phase and an inverse wavelet transform will be performed. Once this treatment is finished, the next GOT will be sent into memory. This process is stopped when the entire grid is watermarked. During extraction, the same sequence of steps will be executed using the watermarked mesh. Our algorithm is then said to be blind. The particularity of this work is the application of spiral scanning. This method of decomposition allowed a huge gain in memory adopted (reducing memory reached 24%). Indeed, we are able to control the memory amount used during the execution of our algorithm. Our algorithm can then work even with a very small memory space.

Applied tests prove that our algorithm preserves mesh quality. It does not cause quality degradation of the mesh despite the large number of bits to be inserted (250000 bits). Previous displayed results, which present a considerable improvement compared to the results of recent works, assert that our algorithm is robust against several attacks such as similarity transformation, random noise addition, coordinate quantization, smoothing, simplification and compression.

Concerning our future work, we think of changing the method of wavelet transform used to further reduce the amount of memory used. As for the criteria of robustness, we strongly believe in changing techniques used to improve the results already presented.

## VII. Conclusion

In this paper, we propose a new watermarking approach for 3D meshes. The main idea is to apply spiral scanning method to split the mesh (decomposition into GOTs). At each time, a GOT will be sent to memory to be treated. Treatment includes the application of a wavelet transform in order to generate the vector of wavelet coefficients. Components of this vector undergo modulation to be watermarked according to binary data. Finally, a demodulation phase and an inverse wavelet transform will be performed. Once this treatment is finished, the next GOT will be sent into memory. This process is stopped when the entire grid is watermarked. During extraction, the same sequence of steps will be executed using the watermarked mesh. Our algorithm is then said to be blind.

The particularity of this work is the application of spiral scanning. This method of decomposition allowed a huge gain in memory adopted (reducing memory reached 24%). Indeed, we are able to control the memory amount used during the execution of our algorithm. Our algorithm can then work even with a very small memory space.

Applied tests prove that our algorithm preserves mesh quality. It does not cause quality degradation of the mesh despite the large number of bits to be inserted (250000 bits). Previous displayed results, which present a considerable improvement compared to the results of recent works, assert that our algorithm is robust against several attacks such as similarity transformation, random noise addition, coordinate quantization, smoothing, simplification and compression.

Concerning our future work, we think of changing the method of wavelet transform used to further reduce the amount of memory used. As for the criteria of robustness, we strongly believe in changing techniques used to improve the results already presented.

## References


Towards the Development of an Efficient and Cost Effective Intelligent Home System Based on the Internet of Things

A. Imtir Chaudary  
Dept. of Computer Science  
CIIT, Sahiwal  
Sahiwal, Pakistan

Muhammad Usman  
Dept. of Computer Science  
CIIT, Sahiwal  
Sahiwal, Pakistan

Arshad Farhad  
Dept. of Computer Science  
CIIT, Sahiwal  
Sahiwal, Pakistan

Wajid Ullah Khan  
Dept. of Computing and Technology, Abasyn University  
Peshawar, Pakistan

Abstract—Internet of Things (IoT) is an emerging technology which is covering everyday things from industrial machinery to consumer goods in order to exchange information and complete tasks while involved in other work. IoT based smart home automation system is a system that uses PCs, mobile phones or remote devices to control basic operations for home automatically from anywhere around the world using internet. The proposed intelligent home automation system differs from existing systems as it allows the user to operate the system from anywhere around the world by using internet connection along with intelligent nodes that can take decisions according to the environmental conditions. We implemented a home automation system using sensor nodes that are directly connected to Arduino microcontrollers. Microcontroller is programmed so that it can perform some basic operations on the basis of sensors data. e.g. fan is controlled on basis of temperature value and light is controlled on the basis of occurrence of motion in the room etc. Furthermore Arduino board is connected to the internet using Wi-Fi module. An extra feature this system provides is to monitor power consumption of different home appliances. The designed system provides the user remote control of numerous appliances locally as well as outside the home. This designed system is expandable, allowing multiple devices to be controlled. The objective of the proposed system is to provide a low cost and efficient solution for home automation system by using IoT. Results show that the proposed system is able to handle all controlling and monitoring of home.


I. INTRODUCTION

Now a-days home and building automation systems are taking place of manual systems. They provide increased comfort when employed in private homes [1]. On the other hand they contribute an overall cost reduction and energy saving, which is today’s major issue. A typical home automation system allows to control house hold appliances from a centralized control unit. These appliances include fan, lights, air conditioners, etc. For mostly commercial home automation systems, all devices should be compatible with centralized control unit [2].

The capabilities offered by the IoT make it possible to develop various IoT based applications. All the applications are build using many more smart things like sensors, actuators, microcontrollers etc. Figure 1 demonstrates that IoT applications are classified into three major categories as:

- Society
- Environment
- Industry

On the basis of classification the term “Things” can be distinguished in a different way and depends on the application domain in which it is used.

In industry, IoT activities involve financial or commercial transactions between companies, manufacturing process of industries, service sector, banking security, and intermediaries etc. As a whole the thing may be product itself, the equipment used or transportation means used, or we can say everything that participates in product lifecycle. In environment, applications are based on activities like security, protection, monitoring and development of all natural resources such as energy management, agriculture, human body monitoring etc. Lastly in the whole society the thing may relates to devices used with in public places or devices used for assisted living. For example smart homes, smart cities and smart campuses etc.

The proposed system can be easily integrated into the home’s electrical system and allows one to wirelessly control...
appliances that are plugged into specially designed wall smart sockets. The designed system consists of Arduino Nano board, Arduino Mega 2560, NRF module, CC3000 Wi-Fi module, relays, keypad and sensors. Sensors are directly connected with Arduino microcontroller board in order to perform automated functions on the basis of data provided by sensors. Firstly data is processed by sensors and then forwarded to Arduino mega for further processing. Wi-Fi module is attached to Arduino mega to connect the whole system with internet. Sensors used in our system are DHT11 temperature and humidity sensor, PIR motion sensor, Current sensor, electromagnetic door sensor and MQ5 gas sensor.

The system is capable of detecting when the user enters or leaves the room. Electromechanical relays are used to control light, fan and sockets on the basis of sensor’s data or commands received. Number of relays depends on number of appliances to be controlled. A remote is made using NRF module with Arduino Nano. The remote is used to control the smart socket locally. Current sensor is used to monitor the power consumed by home appliances to whom it is attached. The power consumption can be monitored using internet and is shown on LCD attached to the system as well. Electromagnetic sensor is used to monitor the door status, either the door is open or closed.

The main challenges faced by smart home systems are high ownership costs, poor security, poor management, and inflexibility. Some systems provide complete solutions but those are very costly. These complex systems usually need to be integrated when the building is constructed and must be planned in advance. They are also difficult to upgrade or replace once installed. The overall investment adds up considerably and is financially infeasible in most cases. These drawbacks hinder the popularity of such systems. Secondly, world is in the grip of serious power crisis since many years. A reason behind these severe crisis is the wastage of energy. Normally it is seen that the electricity load shedding increase in busy hours. Therefore, our designed system is able to overcome all the above mentioned problems efficiently and cost effectively.

The remaining part of this paper is organized as follows; related works is discussed in section II, section III outlines the internet of things. Prototype of proposed system is presented in section IV. Section V describes the components of IoT based home system. The results and its analysis is discussed in section VI, whereas last section concludes this paper.

II. RELATED WORKS

This section presents the existing techniques of smart home system based on IoT, ZigBee, Bluetooth and smart phones.

In [3], smart homes are described to introducing the technology in your home environment for comfort, security, convenience and to provide energy efficiency to its occupants. In [4], author describes that with advancement in sensor networks there comes a rapid increase in automation. Everything going to be automated rather than manual. Due to rapid increase in internet users a technology named Internet of things (IOT) emerged. IOT is an emergent network of daily objects. Smart home system using IOT is monitoring and controlling basic home functions automatically or through internet using mobile or PC. Intel Galileo board is capable of integrating wireless communication, cloud networking and to remotely control various devices and appliances. System is flexible depending on the type of sensors.

In [5], the author states that by making your home environment intelligent enough we can make life easy for disabled and elderly personals. In last few years there is much increase in home automation because of rapid increase in smart phone usage. Introduction of Internet of Things boosted up the research and implementation of smart homes. In [6], the author suggests his idea that In order to make smart home low cost and flexible mobile web server based on Arduino Ethernet, hardware interface modules and android based application is used. Using this system authorized users can remotely control and monitor home devices connected through 3G/4G or Wi-Fi.

In [7], the main objective of the author is to provide Home automation system by integration of smart phones, cloud computing, wireless and power line communication (PLC). The system will be capable of providing the remote access to switch on and switch off various home appliances with in home. This system facilitate the user by consolidating hand held wireless remote, PC based application and android application. In [8], the author explains a system which is based on standalone embedded system Arduino Mega Android Accessory Development Kit. ADK acts as intermediary between home appliances and android mobile or tablet as ADK put forwards the coming signal from the mobile/tablet to the devices. The author proposes the design and implementation of the system that is capable of monitoring and controlling the home devices.

In [9] the author suggests to design and implement a flexible and secure cell phone based home automation system. The design is based on a standalone Arduino BT board and the home appliances are connected to the input/ output ports of this board via relays. The communication between the cell phone and the Arduino BT board is wireless. This system is intended to allow a number of devices to be controlled with minimum changes to its core. Only authorized users are allowed to access the system as system is password protected.

In [10] the author suggests an innovative, detached and flexible ZigBee based smart home system. The system is flexible and scalable that allows extra home appliances designed by multiple vendors to securely add to the home network with the minimum amount of extra work. The system allows its owners to monitor and control the connected devices locally, through multiple controls like any Wi-Fi enabled device which supports Java or using ZigBee based remote control. Moreover, in this system a common home gateway is used to integrate ZigBee based home automation system and Wi-Fi network. The network is interoperable, simple and flexible due to common home gateway that provides user interface, and remote access to the system.

[11] Come up with an idea to control the home using Bluetooth technology. System provides convenient access and monitoring to the home appliances with in short range. AT89C51 single chip microcontroller is used to control the
designed circuit. Different functions are performed based on programming of the circuit. The system is suitable only for ordinary household applications. Only short range control of different devices is provided in this system. In [12] the author proposed a Bluetooth based energy management system in which devices communicate with energy management system. The devices communicate using Bluetooth low energy technology. The proposed approach elaborates that devices automatically goes to stand-by state in peak hours while small devices remain in working condition. This saves energy as well as reduces the electricity bills.

In [13] the author introduced the emerging technology of IoT for the purpose of environmental monitoring in smart homes. The system is designed by integrating wireless sensor network and internet of things. Sensor nodes are responsible for sensing the provided environment and send the data to central node. Central node is connected with Wi-Fi router acting as a gateway in this system. The user monitors the data through webpage. In [14] the author proposed a smart home system based on Wi-Fi technology and IoT technology. In this system a low cost Wi-Fi module is used with different sensors and home appliances in order to monitor and control them. Power line communication is used to control the devices. System can be locally accessed through mobile phone or tablets. For remote access of the system, the system comes up with home proxy and remote server. They are communicating with the smart device using XMPP protocol. Remote server is capable of controlling and communicating different smart homes.

In [15] the author designed a system in order to minimize transmission delay and to handle large data. A new protocol is used to assist living in smart homes. The protocol used is named as wellness sensor networks. This protocol was used in early smart homes in nineties. A local database server is used for building statistics of data and data is sent to webserver for remote access. In [16] the author proposed an IEEE 802.15.4 based smart home and energy monitoring system by using CC2430 on chip technology. Main focus of this paper was to design a hardware which is capable of doing automatic load balancing and load prioritization results in bill saving. In [17] the author proposed to design a system based on ZigBee based wireless sensor network. The system can be remotely accessed via home gateway designed based on a LM3S9B96 chip and a RF CC2520 chip. The gateway software uses real time operating system free RTOS embedding both TCP/IP and ZigBee protocol stack on it.

III. INTERNET OF THINGS

In this section, we briefly discuss the IoT which is an emerging network of daily objects from industrial machinery to consumer things that can exchange information and complete tasks when you are busy in other activities. A basic example of such objects is smart home automation which uses mobile devices or computers to control home devices using internet from anyplace around the world. An automated home is sometimes called a smart home. It is intended to save the human energy and electric energy. The proposed home automation system differs from other existing systems as it allows its users to control the system from anywhere across the world using internet connection along with intelligent nodes which can take decisions according to the environmental situation. There are other domains e.g. healthcare, industrial automation, transportation, and natural and other disasters where IoT can play incredible role and can help us to improve quality of our lives.

IoT elements help us to better understand the real importance and functionalities of the IoT. In IoT Identification of each object helps to identify the objects uniquely. Objects may use public IP addresses instead of private for identification. For providing a clear identity to objects within the network different identification methods are used e.g. IPv4 and IPv6. Sensing includes collection of information from different objects in the network and to send that information on the cloud, local server, or database. Then the gathered data is analysed in order to take particular actions based on services and data. In IoT data can be gathered from smart sensors, wearable sensing devices and actuators. In IoT heterogeneous objects are connected with each other to provide specific smart services. IoT objects communicate on lossy and noisy links because of the low power operation. Communication in IoT takes place using protocols IEEE 802.15.4, Bluetooth, W1-Fi, Z-wave etc. In IoT data is processed using dispensation units e.g. microcontrollers and software applications e.g. cloud services. The processing units and software applications specifies the computational ability of the IoT. Hardware platforms used for IoT are i.e. Arduino, Raspberry Pi, Intel Galileo, UDOO etc. The other important calculation part of the IoT is Cloud platforms which facilitates different objects in order to send their collected information to the cloud. The received data on cloud is then processed in real-time and helps the user to benefit from the knowledge extracted. IoT services are important for improvement of our life-style; these services include Identity related services, Information aggregation services, Collaborative aware services and Ubiquitous services. These services are improving our daily lives by providing Smart home systems, intelligent transportation systems, Industrial automation, Smart health care, Smart grid and Smart city. In IoT semantics refers to the ability of extracting knowledge from different objects for the provision of required services. Semantics recognize and analyse the information to take decision in order to provide exact services.

![IoT elements](image)

In IoT sensors are capable to sense, think and perform actions by having them communicate together, to share records and information to make decisions. The general IoT elements are shown in figure 2. The general idea behind IoT is that each domain precise software is interrelating with domain unbiased submissions while in each area devices and actuators interconnects with each other without delay. IoT is projected to be used in smart homes as it allows its users to routinely open their garage when reaching at their gates, turn on the fan when temperature is getting high, notify the users if there is a gas leakage in the kitchen, and control their appliances when away from home using internet.
The architecture of IoT is consisted of three basic layers, first is Perception layer which signifies the physical objects such as sensors and actuators to perform different actions or to monitors objects such as motion, temperature, humidity, energy, etc. Second is Network layer which is responsible for the transfer of data produced by the sensors by means of Wi-Fi, Bluetooth, Infrared, GSM, ZigBee, etc. This layer allows the IoT applications to work with various types of objects with different kind of specified hardware platform. Other processes handled by this layer are data management process and cloud-computing. Network layer is mainly used to collect data from perception layer and processing the data for application layer. Third is the Application layer which directly interacts with the user to which it offers the requested services. For example, this layer can provide gas and temperature measurements to the user who demands for such data. The last layer has significant importance in IoT because it provide high quality intelligent services to the users they need. This layer covers various marketplaces such as smart HealthCare, smart homes, industrial automation, smart grid, etc.

IV. METHODOLOGY

A. Prototype of Intelligent Home Systems

The designed IoT based intelligent home system comprises of four major portions as follows,

Automation: In this portion sensors are connected with the controller (Arduino Mega) and automates different objects as; the light will automatically turned on when someone enters the room, the alarm will notify you when there is a gas leakage in the kitchen and the alarm will also notify you when the main gate remained open for certain time.

Energy monitoring: In this portion temperature and current sensors are connected to the controller (Arduino Mega) temperature sensor is used to automates the fan in the room as the fan will automatically turned on when the temperature rises to certain value and the fan speed will gradually increase with the increase in temperature. Current sensor is used to monitor the energy consumption of the appliances at home. The Wi-Fi module is used to send the data to the internet and is accessed at web page. The values of energy consumption and temperature are shown on web page and the control of the appliance is also connected on the web page which can be accessed globally.

Smart Socket: In this portion we designed a remote in which keypad and wireless module (NRF) working as sender are connected with controller (Arduino Nano). On the other hand socket is comprised of controller (Arduino Nano) which is connected with wireless module (NRF) working as receiver and relay. Remote is used to control the socket locally.

Smart Meter: In this portion smart meter is designed which comprises of current sensor and LCD connected with controller (Arduino Mega). Smart meter is designed to calculate the energy consumption and number of units consumed in a smart home.

The detailed working of IoT based intelligent home system is shown in figure 3.
B. The designed architecture is comprised of four folds:

Automation part is built by using following components as following: Arduino mega is used for controlling the whole automation part of the project. It is connected with the other modules used in automation as shown in figure 4. It actuates different devices on the basis of sensors data. Sensors attached to Arduino Mega are following: Temperature and humidity sensor, Motion Sensor, Electromagnetic door sensor, Gas Sensor, Electromagnetic Relays are used to control and automate the electrical appliances on the basis of sensors data. We used 5 Volt to power supply for micro-controller.

Energy monitoring part is used to monitor and control the energy consumption of home appliances especially heavy appliances by using web page as shown in figure 5. This part consists of following modules: CC3000 Wi-Fi module is attached to Arduino mega; we used this to send data to the internet and to receive commands through web page.

Smart meter is used to monitor energy consumption of home, is shown in figure 7. This circuitry is used to measure electrical energy consumption in your home. It measures voltage with an AC to AC step down transformer acting as adapter and current with CT013 clamp sensor. This makes the system pretty safe as there is no interaction needed with high voltages.

Smart socket is designed to remotely control the appliances within the room by a specially designed remote. This part consists of following modules: Arduino Nano is connected with NRF module and electromagnetic relays in order to automate the home appliances like light, fan etc. It also controls the specially designed smart socket using remote. NRF module is used at both ends to wirelessly control socket using remote. Keypad is attached to the microcontroller on remote side in order to control the socket.

This circuitry can be used to measure the power consumption of different home appliances. It measures voltage with an AC to AC step down transformer acting as power adapter and current by using a CT013 clamp sensor. This makes the system pretty safe as no high voltages are used in this circuit. This designed portion can calculate real power, apparent power, root mean square voltage and root mean square current. Arduino digital domain is used to make all calculations for this portion. LCD display is attached to Arduino mega, we used it for energy monitoring locally. Arduino mega is controlling the Wi-Fi module and other circuitry used in this part of the project. It gets the data from current sensors, calculates desired values and shows these values on web page and LCD as well.

Figure 4 represents the flow of smart socket. Smart socket is designed to remotely control the appliances within the room by a specially designed remote. This part consists of following modules: Arduino Nano is connected with NRF module and electromagnetic relays in order to automate the home appliances like light, fan etc. It also controls the specially designed smart socket using remote. NRF module is used at both ends to wirelessly control socket using remote. Keypad is attached to the microcontroller on remote side in order to control the socket.
The energy meter can calculate real power, and the units consumed in KWH. Arduino digital domain is used for calculating values for this smart meter. LCD display is attached to Arduino mega, which displays power consumption at home and the unit’s consumed. It gets the data from current sensors, and calculates desired values.

V. COMPONENTS OF IoT BASED INTELLIGENT HOME SYSTEM

This section briefly describes the components of IoT based home system.

1. Automation

The components used in automation part of this system are PIR motion sensor, DHT11 temperature and humidity sensor, MQ5 gas sensor and electromagnetic door sensor as shown in figure 8. On the basis of data coming from sensors different functions are performed like fan speed is controlled according to temperature values and light turns on when someone enters the room. Their statistics is also build.

Figure 8. Home automation

2. Energy Consumption Monitoring

The components used in energy monitoring part are CT013 current sensor, a step down transformer, LCD, cc3000 Wi-Fi module, capacitors and resistors are shown in figure 9. Current sensor clamped on the positive wire of the appliance whose power consumption we want to monitor. The values are shown locally on LCD and remotely on the web page.

Figure 9. Energy consumption monitoring

3. Smart Socket

Smart socket is comprised of Arduino Nano microcontroller boards with electromagnetic relay and NRF transceivers. Remote is also build of same components, the only differentiation is that relay is replaced with keypad in order to send the commands to the socket. It provides easiness to elders in order to control any device with in the room as NRF communicates with in eight to ten meters. Figure 10 shows the smart socket.

Figure 10. Smart socket

4. Smart Meter

Figure 11 shows the smart meter. Smart meter is designed with almost same components as used in energy monitoring part of the system. Only Wi-Fi module is not used in this part of the system. It is programmed so that it cannot only show us power consumption at home but also calculates the units consumed.

Figure 11. Smart Meter

https://sites.google.com/site/ijcsis/
VI. PERFORMANCE EVALUATION

This section represents the performance evaluation of our intelligent home system based on IoT. The results are only shown for energy consumption, voltage monitoring, and temperature monitoring.

The designed system is tested by installing it in home environment. Interconnecting with the home router using IPv4 such that router worked as IoT application gateway for the designed system. Integrated system is continuously used and generated real time graphical representation of the sensed data. The rest of this section presents the results.

Figure 12 shows the energy consumption of a 100W bulb from 9am to 11am. Power is calculated by using ampere and voltage as under:

\[ \text{Power} = \text{Voltage} \times \text{Current (amperes)} \]

Both these values are graphically represented on IoT webpage working on the embedded static IP of the Wi-Fi module. If some appliances is consuming more power and exceeding the threshold (a maximum limit), the user can control the appliance through IoT webpage.

The real time temperature observed on the webpage against time is shown in figure 13. Thus, on the basis of temperature data the fan speed is automatically controlled. On the other hand the user can control the socket from the IoT webpage to turn the air conditioner ON or OFF after getting temperature values.

Figure 14 shows the input voltage fluctuation for a 100 watt electric bulb from 9am to 9pm. It is observed that in busy hours the voltage drops to the minimum limit. As voltage vary, the power consumption of the appliances also vary.

Figure 15 shows the power consumption of 1.5 Ton air conditioner from 9am to 11 am. The power consumption varies as voltages fluctuates, this is because the power is calculated as a product of voltages and amperes it consumes. Results are verified by taking these values using multi meter.
VII. CONCLUSION

The designed system overcomes almost all the existing highlighted problems. This system not only monitors the sensors data but also actuates a process according to the requirement. This system highlights almost all important scenarios of smart home systems like: smart security, alarming, smart metering and energy monitoring. This efficient and cost effective model can be implemented in a real environment. In future, this work can be extended to monitor and control the home on a cloud.

VIII. REFERENCES


Areeb Imtar Chaudary currently pursuing his bachelor’s degree in Telecommunication and Networking from COMSATS Institute of Information Technology, Sahiwal, Pakistan. His research interests include Internet of Things, smart sensors and sensing technology, performance evaluation of communication protocols for wireless ad hoc networks, and wireless sensor networks. His work includes design and implementation of sensor networks, microcontrollers programming and IoT website development.

Muhammad Usman currently pursuing his bachelor’s degree in Telecommunication and Networking from COMSATS Institute of Information Technology, Sahiwal, Pakistan. His research interests include Internet of Things, smart sensors and sensing technology and wireless sensor networks. His work includes sensor programming and IoT website development.

Arshad Farhad currently working as Lecturer in department of computer, COMSATS Institute of Information Technology, Sahiwal, Pakistan. He has completed his MS degree in Telecommunication and Networks from Bahria University, Islamabad, Pakistan in 2015. He received his BS degree in Information Technology from University of Peshawar, Peshawar, Pakistan in 2012. His research interests include design and performance evaluation of communication protocols for wireless ad hoc, wireless body area networks and sensor networks.

Wajid Ullah Khan currently working as Lecturer in department of Computing and Technology, Abasyn university Peshawar campus, Pakistan. He has completed his MS degree in Telecommunication and Networking from Abasyn University, Peshawar, Pakistan in 2015. He received his BS degree in Information Technology from University of Peshawar, Peshawar, Pakistan in 2012. His research interests include mobile ad hoc network, wireless body area networks and sensor n
A Threshold-Based Predictive Scheme for Mobile Subscribers in Publish/Subscribe Systems

Fatma Abdennadher #1, Maher Ben Jemaa #2

# National School of Engineers of Sfax, University of Sfax, RedCAD Laboratory
B.P.1173, 3038 Sfax, Tunisia
1 fatma.abdennadher@redcad.org
2 maher.benjemaa@enis.rnu.tn
1 corresponding author

Abstract—In this paper, we present our strategy adopted to deal with the mobility into publish/subscribe. Specifically, we focus on the management of the mobile users from one broker to another. In fact, the topic of mobility into publish/subscribe systems may cause many problems such as the increasing of the traffic into the network and the messages loss. To overcome these problems, we have created a selective scheme on the basis of an accurate selection. In fact, a threshold value is devoted to be the criterion for the selection of caching points. On the basis of this principle, we apply various network settings to explore the effectiveness of our approach. Hence, we extract the improvement of our approach on the messages loss, the caching cost and the propagation cost in function of buffer size, publication rate, period of disconnection and connect time.

Keywords—Distributed Networks; Mobile Computing; Publish/Subscribe; Prediction Management; Performance Efficiency.

I. INTRODUCTION

Nowadays the propagation of the pervasive computing devices, with the emergence of network access technologies (mobile wireless, wireline, and Internet), has led all kinds of devices to access networks. So, all these facts has given rise to the mobile computing paradigm. In this paradigm the users can be assumed stationary while on-line, but change the physical access points to the network. So, the users may temporarily disconnect from the network. Then, upon their connection, they expect to recuperate the data disseminated while their disconnection occurs. This demands a flexible middleware infrastructure, based on a scalable interaction style, to cope with the dynamic nature of mobile computing. In this context, the publish/subscribe model can be very promising.

The publish/subscribe paradigm shown in Fig. 1 consists of a set of distributed nodes elaborating the communication into the network. Two types of clients are existing based on their roles which are subscribers and publishers. The subscribers are information consumers. The publishers are information producers. The messages are passed from publishers to interested subscribers through the brokers. The route from publishers to all interested subscribers is coordinated by brokers for assuring the matching.

The potential of the publish/subscribe communication model consists of the full decoupling of the interacted parties in time, space, and flow [1], [2], [3]. This decoupling makes the publish/subscribe systems flexible and scalable. Also, the brokers remove all explicit dependencies between publishers and subscribers. In fact, the multicasting mechanism implemented by brokers decouples publishers from consumers. This makes the publish/subscribe system a good candidate for mobile computing by inducing three important effects. The first effect is that a client can operate in the system without being aware of the existence of other clients. So, the client only know the structure of the event notifications for issuing its interest in the form of subscriptions. In practice, the publish/subscribe approach could be easily exploited by a PDA to advertise its presence in a room and receive the services published there. The second effect is the ability of the client to connect and disconnect without affecting the other components. The third effect is the suitability of the publish/subscribe communication to cope with unannounced disconnection of clients, which characterizes mobile networks.

Given the strength of this paradigm, a large number of publish/subscribe middleware have been developed. These systems differ along several dimensions. Two main dimensions are usually considered fundamental which are the expressiveness of the subscription language and the architecture of the event dispatcher.

The expressiveness of the subscription language classifies the publish/subscribe systems into three categories which are topic, type and content systems. The first two categories [4], [5], [6] are limited in the expressiveness. In the content-based systems [7], [8], [9], subscriptions contain expressions that permit sophisticated matching on the event content. In our work, we have applied our approach into a publish/subscribe middleware providing a content-based subscription language.

Two types of architecture are proposed for publish/subscribe systems. In the centralized architecture a single component acts as event dispatcher. So, the publish/subscribe system could not be scalable enough. Also, the risk of a single point of failure may occur. In the distributed architecture [10], [11], [12], a set of interconnected brokers coordinate in collecting subscriptions coming from clients and in routing events. This architecture contributes to the reduction of network load and
the increase of scalability. The topology of the distributed brokers differs from system to system. Most existing publish/subscribe systems are implemented for fixed environments. So, several extensions are needed to make these systems able to cope with mobile subscribers.

In recent years, more importance is accorded to the performance issues induced by the mobility of the users [13]. To solve these issues we propose to predict the mobility of subscribers. This prediction is based on a dynamic selection of the most probable locations that the subscriber moves to during its run. Our approach aims at forwarding the required information for the mobile users at their new locations upon their connection while minimizing the caching cost, the propagation cost and the messages losses.

![Publish/Subscribe Model](image)

**Fig. 1.** The publish/subscribe Model

The rest of the paper is formulated in this way: We give an overview of the management of subscriber mobility into publish/subscribe systems in section II. Then, we present the principle of our approach and the strategy that we have followed in section III. After that, we explore the adequacy of our approach by applying various network settings and compare it to the standard proactive scheme in section IV. Finally, section V concludes the paper.

## II. RELATED WORK

The mobility is an issue examined in many fields [14], [15], [16], [17]. Precisely, in this section we give an overview of studies which propose approaches for the management of mobile subscribers into publish/subscribe systems. In fact, the mobility of the subscribers is managed by three types of approaches. The first type is the durable subscriptions [18], [19], the second type is the reactive approaches [20], [21], [22], and the third type is the proactive approaches [23], [24], [25]. Each type differs from the other by the time and the manner that the transmission of the cached publications is realized.

### A. Durable Subscription Approaches

The approaches classified in the category of durable subscription are limited to the operation of disconnection and connection to the same broker. As an example of approaches adopting this type of approach we find Elvin [19]. The followed strategy is realized on the basis of proxies used for the buffering of publications. Indeed, these proxies play the role of the disconnected subscriber in order to transmit to it the desired interest upon its reconnection. Thereby, two roles are attributed to this proxy according to the state of the subscriber whether it is connected or not. Hence, when the subscriber is disconnected, the proxy is considered as a subscriber expressing the interest of the disconnected subscriber. Consequently, when the subscriber reconnects, the proxy is transformed into a server transmitting to it its cached publications.

The same category of strategy was adopted into JMS [18]. In fact, we remark that this approach causes a considerable loss of messages when the subscriber does not reconnect to the same broker. In addition, this induces a significant load on the network by the fact of storing infinitely the interest of the disconnected subscriber into the old broker. In fact, the operation of caching is stopped only when the subscriber reconnects to the old broker. Hence, a serious degradation is induced on the performance of the system.

### B. Reactive Approaches for Mobile Subscriber

Many systems have deployed the reactive strategy to handle with mobile subscribers. Rebeca [30], [31] is one of those systems. In fact, its strategy is elaborated on the basis of virtual counterparts related to the old broker. The reconfiguration of subscriptions is accomplished as soon as the subscriber detects the change of the broker. In fact, the junction broker between the old and the new broker transmits the buffered messages. Hence, the junction broker is the only responsible for the handoff requests. So, a significant increase in the handoff latency is induced. In addition, the junction broker risks to be overloaded by the massively quantity of messages moving through it. Therefore, the performance of the system is affected.

The same type of strategy [21] was developed into SIENA [26], [27]. Indeed, this strategy is handled by the proxies related to the brokers of the publish/subscribe system. Unfortunately, the massive use of proxy components affects the performance of the system. Also, many duplicated messages are overloading the network and are not deleted due to the expensive operation of elimination.

Reds [28] is another publish/subscribe system that implements a reactive approach [22]. The basic idea of the adopted strategy was founded on the selection of each broker as a caching point for the publication as long as it has a subscriber in its subscription table interested on this publication. This approach suffers from the overload on the client.

Another reactive approach [29] was presented into Jedi[20]. The adopted approach runs as follows: The retransmission of subscriptions is first of all elaborated by the new broker. This retransmission is required for tracing the new routes for the publications. So, the publications matching the interest of the mobile subscriber are cached into the new broker. Consequently, the buffering is stopped in the side of the old broker. A major inconvenient in this approach is its limited scalability.
Another reactive approach based on the event mediators was proposed in [32]. The event mediators play the role of the buffer for the publications of the mobile subscriber. Hence, the event mediator sends the stored publications to the mobile subscriber upon its reconnection. The implementation of this approach is not clear and it suffers also from the limited scalability.

In the same category of approaches, we find the strategy proposed in [33]. As the previous approaches, the old broker buffers the publications for the mobile subscriber. As a drawback, this strategy suffers from the invocation of a high handoff latency in the large network.

C. Proactive Approaches for Mobile Subscriber

The main objective of proactive approaches is the minimization of the transfer delay of the cached publications. Thereby, these approaches are most times used for streaming and real-time applications. As a result of this minimization of delay, an increase in the network load is induced.

As an example of proactive approaches, we find the strategy used in [25]. In fact, this approach is based on the exploitation of the neighbor graph. This latter represents the list of the brokers that will be visited by the mobile subscriber. Indeed, this graph is constructed upon the reconnection request and the context transfer request invoked after the movement of the mobile subscriber. Thereby, all the brokers in the graph receive the subscriptions of the mobile subscriber before its movement. As a consequence of applying this approach, the network will be overloaded.

Another proactive approach was applied in [23], [24]. This strategy employs a layer of replicators between publish/subscribe system and clients. The replicators serve for the positioning of virtual clients at the possible brokers that may be visited by the mobile subscriber. A drawback of this approach is that the same subscription can be expressed by different subscribers related to the same broker. So, this broker risks to cache similar publications. This is due to the fact that the caching is invoked per subscriber. The major inconvenient of this approach is the huge load on the network and the incapacity to cope with the failures or long time disconnection of subscribers.

This section has demonstrated that the reviewed works have accomplished the support of mobility with distinct rates of success. In fact, the management of mobility in these works poses different technological problems. Hence, these strategies are not yet effective and efficient for the management of mobility with no loss of messages. Also, they are characterized by their limitation in the performance metric. The main goal of our approach is the management of mobility in a transparent manner by assuring high performance. As mentioned before, the architecture of the publish/subscribe system can be distributed. In such cases, the management of mobility may affect the performance of the system due to the high traffic. Hence, it is primordial to create a new strategy with a reduced traffic. Also, our strategy requires to be flexible and scalable. To achieve such goals, our approach is based on the analysis of the most probable brokers to be next visited by the mobile subscriber. Next, we will perform an evaluation of our approach to extract its gains comparatively to the standard proactive approach.

III. Proposed Approach

The attention for extending publish/subscribe systems to mobile applications was little. In fact, the most extensions were based on a reactive strategy. This type of strategy suffers from the increase of network traffic and high handoff latency. In our work, we tend to manage subscriber mobility efficiently. The main idea relies on the selective predictive caching of messages prior to the movement of the mobile subscriber by the use of an intelligent mechanism.

Recently, the users in real scenarios of mobility are moving according to repeated routines. Indeed, we can offer a multitude of repeated movements every day for example from home to office, from home to school, from home to market and vice versa. So, we can rely on the probability of movements between brokers to extract dynamic calculations of probabilities on run time movement in order to offer an efficient management of mobility into publish/subscribe.

Our selective scheme follows a predictive strategy and has proved its capacity to handle mobility with effectiveness. This effectiveness is assured through a clever selection of a set of brokers serving for the caching of published messages during the disconnection of the mobile subscriber. This predictive strategy in managing mobility contributes to the improvement of system availability. In fact, the past and actual states of the movement of the client are the key information for a correct prediction. Thereby, we use the information extracted from the actual movement of the subscriber in order to anticipate the future movements. So, the different movements between brokers are analyzed for the future prediction.

As we have said, our strategy is based on the probability of movements between brokers. Hence, two important values are calculated dynamically which are the handoff weights and the threshold value. The handoff weight from broker $A$ to broker $B$ is obtained by fractionating the total sum of handoffs from broker $A$ to broker $B$ by the total sum of handoffs from broker $A$ to all the other brokers. Hence, the threshold weight of broker $A$ represents the average of weights from this broker. We obtain the weight threshold by fractionating the total sum of weights by the number of caching points. Hence, the selected caching points will require to have a handoff weight equal or greater than the threshold value. Thereby, a significant gain in the network traffic is approved by our approach through the elimination of the useless caching points. The following formulas clarify the two values with $W$ is the weight, $X$ is the number of handoffs, and $nb$ is the number of caching points.

$$W_{AB} = \frac{X_{AB}}{\sum_{N in caching points A} X_{AN}}$$  \hspace{1cm} (1)
The previous approaches do not consider any criterion for the selection of caching points. Thereby, a considerable traffic on the network is induced in large networks. Therefore, the criterion of weight becomes essential to eliminate the useless caching points. So, the selected caching points are characterized by a weight value greater or equal than the threshold value. Hence, the calculation of different weights in a dynamic manner is recommended to obtain the updated values.

In order to maintain the values updated, we apply upon each movement a function named Update-Weight. For the broker from which the movement is invoked. In fact, for each movement the new broker notifies the old broker about the reassociation. So, the construction of caching points is elaborated correspondingly to the movements of the subscriber between brokers.

The storing operation in the caching points begins when the mobile subscriber disconnects from its broker. To avoid a loss of messages into the caching points, the old broker is charged to send to the set of caching points the buffered messages published until the operation of caching begins. Hence, when the new broker to which the mobile subscriber connects is among the caching points, it will send directly the messages to the mobile subscriber upon its reconnection.

The efficiency of the system is ameliorated since the caching points with a low probability to be visited are eliminated. Indeed, the caching points are selected intelligently by comparing accurately the weights values to the threshold value. Hence, the caching points subscribe in advance and store the published messages instead of the mobile subscriber during its disconnection. A great major in our approach is its adaptability to all subscription language and to all general overlays topologies.

The construction of the caching points is elaborated on the basis of changes occurred into the network. According to the movements of clients between the brokers, the values of weights and threshold are updated. Thereby, the set of caching points is dynamically varied. Indeed, the update of values is invoked for each movement. Hence, new brokers are added to the set of caching points and others are deleted. Therefore, we obtain a selection of caching points presenting the most probable brokers to be visited. Table 1 exhibits the selective dynamic behavior of our approach. Thus, a considerable load on the network is avoided. Added to that, we have tend to select always the closest caching points from which the mobile client recuperate its messages upon its reconnection when the new broker is not among the caching points.

The quality of our approach can be measured by the fact that the new broker visited by the mobile subscriber belongs to the set of caching points. So, this indicates the exactitude in predicting the movement of the mobile subscriber. Hence, the recuperation of messages will be occurred directly from this new broker. So, the exactitude value can be expressed by the following equation:

$$ E_{x(t_0,t)} = \frac{\text{number of handoffs to a caching point}(t_0,t)}{\text{number of handoffs}(t_0,t)} $$

This metric explores the adequacy of our approach in succeeding the prediction of the next accessed brokers. Hence, when the value of $E_{x(t_0,t)}$ is close to 1 that means that the selected caching points are useful enough for the prediction.

IV. Evaluation

We achieved all our experiments on a prototype implementation of a distributed publish/subscribe system (PADRES)[34] to which we extend our approach and the standard proactive scheme. For all the experiments the same mobility model is applied. The evaluation of our approach is elaborated around the propagation cost, the caching cost and messages losses. The results of these evaluations are elaborated according to the buffer size, the publication rate, and the period of disconnection. Through these different parameters, we extract the gain of our approach compared to the standard proactive scheme.

A. Propagation cost

The propagation cost is the cost induced by the propagation of the subscriptions emitted by the mobile subscriber($c_i$) on the set of caching points. This propagation is occurred during the disconnection of the mobile subscriber which can be defined by the following equations with $nb caching points(B_i)$ is the number of the caching points of the old broker $B_i$ from which the mobile subscriber ($c_i$) disconnected, and $nb sub$ is the number of subscriptions of the mobile subscriber emitted before its movement and not yet matched.

$$ \text{Prop cost}(c_i) = nb sub(c_i) * nb caching points(B_i) $$

We have varied the frequency of movement from the high to the low as shown in Fig. 2. We have used 30 and 120 seconds as average duration of connection. In the scenario of high frequency of movement, the mobile subscriber connects for a short period of time, then it moves to other brokers. This results in triggering the propagation process in each movement. The number of propagated subscriptions depends on the subscription rate applied during the connection time. So, when the connection time is low, the number of propagated subscriptions is proportionally low. But, the high frequency of movement induces the increase of the propagation process. In contrast, when we have a long connection time, we risk to have an increased number of propagated subscriptions and a reduced propagation process as the frequency of movements will be reduced.
Table I

<table>
<thead>
<tr>
<th>Mobility Model</th>
<th>B</th>
<th>C</th>
<th>B</th>
<th>C</th>
<th>B</th>
<th>D</th>
<th>B</th>
<th>A</th>
<th>B</th>
<th>D</th>
<th>B</th>
<th>C</th>
<th>B</th>
<th>C</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caching points of A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caching points of B</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C.D</td>
<td>C.D</td>
<td>C.D</td>
<td>C</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Caching points of C</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Caching points of D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 2. Propagation cost

Fig. 3. Caching cost

B. Caching cost

The caching cost is induced by caching the publications during the disconnection of the mobile subscriber (ci). This cost is calculated by the following formula with nb cach pub(ci) is the number of cached publications, Cach cost(ci) is the caching cost, nb caching points(Bi) is the number of brokers at which the caching is occurred for the broker Bi from which the mobile subscriber disconnects.

The selection of the caching points by eliminating those with a weight value under the threshold value permits to decrease considerably the caching cost. We varied the period of disconnection from 60 to 240 seconds. The increase in the period of disconnection induces an increase in the caching cost. By reducing the period of disconnection and the publication rate, the caching cost will be reduced.

\[
\text{Cach cost}(c_i) = \text{nb cach pub}(c_i) \times \text{nb caching points}(B_i)
\]  

Fig. 3 shows the impact of our approach in reducing the caching cost on the network. The mobile subscriber moves between the brokers while varying the period of disconnection for different values of publication rates. The obtained results highlights the scalability of our approach and its capability to reduce the caching cost even for increased period of disconnection and publication rates.

C. Loss of messages

The loss of messages is a very important metric to consider in the evaluation of the performance. In our experimentations, we have used two values of buffer size 200 and 500, and we have varied the publication rate for different period of disconnections. Fig. 4 shows that the loss of messages increases proportionally to the increase of the publication rate. In fact, as more the publication rate is important, as more the number of stored messages will be important. Thereby, when the buffer becomes full, the cached messages will be
lost. So, as our approach presents a selected set of caching points, the number of cached publications will be considerably reduced. Consequently, our approach reduces significantly the loss of messages. This observation is confirmed by Fig. 5 when the publication rate is increased. So, for publication rate=27 pub/min the loss of messages is minimized by 1350 messages. Thus, our approach permits to minimize notably the loss of messages especially for higher publication rate.

The performed tests examined how much our approach can reduce the loss of messages and the traffic of messages in a distributed environment under different values of publication rates and period of disconnection. The obtained results showed that a considerable reduce is assured by our approach for higher publication rate. Hence, these tests have allowed us to compare exhaustively the behavior of our approach and the standard proactive scheme under the same conditions.

V. CONCLUSION

In this paper, we evaluated our strategy for the management of mobile subscribers into publish/subscribe networks. Various network settings are used to explore the adequacy of our approach compared to the standard proactive scheme. The obtained results show how much our approach can reduce considerably the loss of messages, the caching cost and the propagation cost in function of buffer size, publications rate and period of disconnection. In fact, our approach implements an efficient service for mobile subscribers. The efficiency is realized through a dynamic prediction for the next location of the mobile subscribers. The information for the prediction is extracted dynamically from the past and actual states of the mobile subscribers.

REFERENCES


A Novel Protocol Stack for Improving QoS in Vehicular Networks

Mohammadreza Pourkiani  
Department of Information Technology  
Science and Research Branch, Islamic Azad University  
Tehran, Iran

Sam Jabbehdari  
Department of Computer Engineering  
Tehran North Branch, Islamic Azad University  
Tehran, Iran

Ahmad Khademzadeh  
Department of National and International Cooperation  
Iran Telecommunication Research Center  
Tehran, Iran

Abstract—Intelligent Transportation Systems are defined as those systems utilizing synergistic technologies and systems engineering concepts to develop and improve transportation systems of all kinds. Vehicular Ad-hoc Network (VANETs) which is an application of Mobile Ad-hoc Networks (MANETs) play an important role in ITS and emerged to provide Vehicle to Vehicle, Vehicle to Roadside and Vehicle to Infrastructure communications, aiming to improve safety on roads, exchange data between vehicles and provide different services to the users. According to special characteristics of VANETs like bandwidth limitation, high mobility, signal fading and real-time data communications, QoS provisioning in these networks is a challenging task.

In this paper, we introduce an architecture for vehicular networks and a protocol stack which aims to reduce the processing overhead, make routing easier and provide Quality of Service in vehicular networks. Finally, after designing protocols and headers of the mentioned protocol stack, we will simulate our proposed idea in a vehicular environment and after simulation process, we will compare the achieved results with another scenario in which regular TCP/IP protocols are used.

Keywords-component; VANETs; ITS; QoS; Protocol Stack

I. INTRODUCTION

A. Intelligent Transportation System

The Intelligent Transportation System (ITS) is a system which is able to exchange different kinds of information of its moving objects. ITS converges remote sensing and communication technologies to improve safety of transportation and make journey more enjoyable. As the objects are moving, wireless communication technologies play an important role in this system. ITS integrates information, communications, computers and other technologies and applies them in the field of transportation to build an integrated system of people, roads and vehicles by utilizing advanced data communication technologies [1]. ITS also includes a broad variety of usage scenarios and user preferences and interests.

B. Vehicular Ad-hoc Networks

The typical ITS scenario is land traffic on roads and the most common examples of ITS applications are the exchange of traffic information to provide roadside assistance, warning in case of emergencies and traffic jam. These services deal with data as, e.g. road condition, traffic light status and position of the single vehicle [2].

There are four typical ways of transportation, on the land by car or train, in the air or water. The most common traffic coming into our mind in combination with intelligent transportation systems is traffic on land. Among the means of transportation, the most prominent are cars, at the present time cars and other private vehicles are used daily by many people. The biggest problem regarding the increased use of private transport is the increasing number of fatalities that occur due to accidents on the roads. In recent years traffic congestion and accidents, as well as environmental pollution caused by road traffic and fuel consumption have become important global issues [3].

Vehicular networks are proposed to provide information exchange via Vehicle to Vehicle (V2V), Vehicle to Roadside (V2R) and Vehicle to Infrastructure (V2I) communications. A Vehicular Ad-hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network and it turns every participating vehicle into a wireless router or node [4]. VANET is also capable of enhancing driving safety by exchanging real-time transportation information and it should upon implementation, collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger, before they actually face it [5].

VANETs have their own characteristics when compared with other types of MANETs. Authors in [6] describe the unique characteristic of VANETs as follows:

- Predictable mobility
- Providing safe driving, improving passenger comfort and enhancing traffic efficiency.
- No power constraints.
- Variable network density
- Rapid changes in network topology
The key role that VANETs can play in the realization of ITS has attracted the attention of major car manufactures and they continue to incorporate more and more technological features into their vehicles [4]. It is reported that over 50% of interviewed consumers are highly interested in the idea of connected cars, 22% of whom are willing to pay $30-65 per month for value-added connectivity services while on the road [7]. However, there are lots of challenges in this field. Authors in [6] list the issues as follows:

- Signal fading
- Bandwidth Limitation
- Connectivity
- Small effective diameter
- Security and privacy
- Routing

Because of the challenges, limitations and new requirements in VANETs, the idea of Heterogeneous Vehicular Networking has emerged recently.

C. Heterogeneous Vehicular Networks

Heterogeneous Vehicular Networks (HVN) integrates cellular networks with Ad-hoc networks which is a potential solution for meeting the communication requirements of the ITS. Although there are a plethora of reported studies on either DSRC or Cellular Networks, joint research of these two areas is still at its infancy.

Emerging heterogeneous networks not only have the ability of providing wide-area coverage to all vehicles in large-scale networks, but also supports real-time safety messages distribution in local areas in order to reduce traffic accidents.

Therefore, Heterogeneous Vehicular Networks may well support the communication requirements of the ITS. It is clear that a car that takes part in such a network is equipped with a WLAN and cellular communication device [3].

The rest of this paper is organized as follows: In section II we present some proposed architectures for vehicular networks while in section III QoS concepts are described. In section IV we review previous works and in section V the proposed architecture and protocol stack are given before the conclusion in section VI.

II. VANET ARCHITECTURE

This part describes the system architecture of VANETs. We first introduce the main components of VANETs architecture from a domain view. According to [27] and [28] we are able to achieve the VANETs system by entities which can be divided into three domains: the mobile domain, the infrastructure domain, and the generic domain [29]. Authors in [6] describe the main system components as follows: Application Unit (AU), On Board Unit (OBU) and Road Side Unit (RSU).

An OBU is a wave device usually mounted on-board a vehicle used for exchanging information with RSUs or other OBUs. The OBU connects to the RSU or to other OBUs through a wireless link based on the IEEE 802.11 p radio frequency channel, and is responsible for the communication with other OBUs or with RSUs.

The AU is the device equipped within the vehicle that uses application provided by the provider using the communication capabilities of the OBU.

The RSU is a wave device usually fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11 p radio technology, and can also be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network (Fig. 2-4). Typically the RSU hosts an application that provides services and the OBU is a peer device that uses the services provided. The application may reside in the RSU or in the OBU; the device that hosts the application is called the provider and the device using the application is described as the user. Each vehicle is equipped with an OBU and a set of sensors to collect and process the information, then send it on as a message to other vehicles or RSU through the wireless medium [6]. The main functions and procedures associated with RSU are:

- Extending the communication range of the Ad-Hoc network by re-distributing the information to other OBUs and by sending the information to other RSUs in order to forward it to other OBUs.
- Running safety applications
- Providing internet connectivity to OBUs
However, this architecture could not support all requirements and applications, therefore to remedy the drawbacks of existing vehicular networks, new ITS network architecture is needed in order to support various services under dense vehicular environments. Authors in [3] describe the framework of Heterogeneous Vehicular Networks (HVN) as follows:

As illustrated in Fig. 5, a HVN is composed of three main components, namely a Radio Access Control (RAN), A Core Network (CN), and a Service Center (SC). Service providers can often supply a variety of services to vehicular users through the SC. The CN is a key component of the HVN because it provides many important functions, such as aggregation, authentication, switching and so on.

Authors in [4] present an overview of integration of VANET and WiMAX. Architecture of VANET based on WiMAX consists of several logical network entities including subscriber station (SS) or Mobile Station (MS), Access Service Network (ASN) and Connectivity Service Network (CSN) [9], [10]. As it is illustrated in Fig. 6, the SS is for fixed device terminal and it is not required to support handover capability. The MS providing handover function is installed or embedded in car for VANET and it should support handover. ASN is a set of network functions to provide wireless connection and WiMAX system profile. These functions are including media access control for MS, transfer of authentication, authorization and accounting (AAA) messages by RADIUS or diameter preferred network discovery and selection, radio resource management and IP connectivity.

III. QUALITY OF SERVICE

Quality of Service (QoS) is the ability of a network to provide improved service to selected network traffic over various underlying technologies, including frame relay, ATM, Ethernet, SONET, and IP-routed networks and it offers
flexibility, scalability, efficiency, adaptability, software reusability, and maintainability. QoS is also defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [12], in fact it is the measure of how good a service is as presented to the user [13]. QoS provisioning often requires negotiation between host and network, call admission control, resource reservation, and priority scheduling of packets [14]. QoS can be rendered in network thorough several ways: per flow, per link, or per node [14]. Characteristics of network such as lack of central coordination, mobility of hosts, and limited availability of resources make QoS provisioning very challenging [15]. In particular, QoS features provide improved and more predictable network service by providing the following services [16]:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

As it is mentioned, QoS is quantitatively defined in terms of guarantees or bounds on certain network performance parameters. The most common performance parameters are the bandwidth, packet delay, jitter, and packet loss [17]:

- **Bandwidth**: The term bandwidth defines the transmission capacity of an electronic line. Theoretically, it describes the range of possible transmission rates, or frequencies. In practice, it describes the size of the pipe that an application program needs in order to communicate over the network. The significance of a channel bandwidth is that it determines the channel capacity, which is the maximum information rate that can be transmitted.

- **Delay**: Network delay is an important performance characteristic of a computer or telecommunication network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. Although users only care about the total delay of a network, engineers need to perform precise measurements. Thus, engineers usually report both the maximum and average delay, and they divide the delay into several parts; propagation delay, transmission delay, queuing delay and processing delay.

- **Jitter**: Jitter is defined as a variation in delay of received packets. The sending side transmits packets in continues stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant [18].

- **Packet loss**: Packet loss is another important QoS performance measure. Some applications may not function properly, or may not function at all, if the packet loss exceeded a specified number or rate. For example, when streaming video frames, after certain number of lost frames, the video streaming may become useless, this number may be zero in certain cases. Therefore, certain guarantees on the number of rate of lost packets may be required by certain applications for QoS to be considered. Packet loss can occur because of packet drops at congestion points when the number of packets arriving significantly exceeds the size of the queue. Corrupt packets on the transmission wire can also cause packet loss [17].

There are numerous levels of QoS and those levels have been grouped into three main categories:

- **Best Effort Services**: Best Effort is a single service model in which an application sends data whenever it must, in any quantity and without requesting permission or first informing the network. For best-effort services, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput [16].

- **Integrated Services**: Integrated services is a multiple service model that can accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. The request is made by explicit signaling; the application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile. [16].

- **Differentiated Services**: In this QoS level, no absolute guarantees are given. Rather, different priorities are assigned to different tasks. Hence, applications are grouped into different classes of priorities. Many application traffics work very well with this policy when absolute guarantees are not needed. For example, network control traffic should always be given higher priority over other data communications to ensure the availability of, at least, the basic connectivity and functionality at all times [17].

Providing QoS support in ad-hoc networks is a dynamic research area. These networks have certain inimitable characteristics that facade several intricacy in QoS provisioning. The characteristics that affect QoS provisioning in these networks are: dynamic varying network topology, inaccurate state information, lack of central coordination, error prone shared radio channel, hidden terminal problem, limited resource availability and insecure medium [14]. There are approaches designed for QoS provisioning in MANETs but they are not suitable for VANETs, because they do not consider the high mobility constraints and large scale node population [19]. QoS parameters such as throughput, latency, jitter, and packet loss are key requirements in VANETs [20]. Each application in VANETs has its own requirements, for example; safety warning applications should have minimum End to End (E2E) delay, because if a warning message receives at destination with high
delay, that message could not be helpful for preventing an accident. Accordingly, packet loss and throughput are two other factors that are very important in active safety applications [13].

IV. PREVIOUS WORKS

A. Improving QoS in VANET Using MPLS

Authors in [13] divide vehicular communications into two categories, Vehicular Ad-hoc Networks which includes V2I and V2V communications and Roadside Network which consists of Roadside Access Network (RAN) and Roadside Backbone Network (RBN). RBN represents the backbone network of RSUs, in which RSUs communicate with each other and with the internet [21]. They assumed that each vehicle is covered by a base station, which has its own domain of service, and base stations are connected with a wired network named RBN and then, they used MPLS in wired domain. MPLS is a forwarding method which can assign packets to different forwarding equivalent class (FEC) for receiving the required service from the network to support QoS. MPLS is considered as layer 2.5 protocol [21] and it is compatible with any layer 2 technology, like Ethernet and ATM. They also used AODV as a wireless ad-hoc routing protocol, because AODV imposes less overhead to the network. Finally they used SUMO [22] to design Manhattan mobility model and then they exported the output of SUMO to NS2.34 for the main test. Results show that with the help of the proposed idea in [13], better performances in terms of E2E delay, packet loss and throughput is achieved.

B. Utilizing Mobile IP and MPLS to Improve QoS in VANET

Mobile IP is the current standard for supporting IP mobility of mobile nodes in wireless networks with infrastructure [23]. Mobile IP enables the mobile node to access internet and changes its access point without losing the connection [23]. Mobile node (MN), Home Agent (HA), Foreign Agent (FA) and Care-of-Address (CoA) are main components of Mobile IP. When the MN moves away from HA to the foreign network, a CoA is assigned to it in order to inform the HA of its current location. This operation enables MN to send and receive at any location without going through HA [24]. Authors in [24] used Mobile IP, MPLS based backbone and AODV routing protocol to improve the QoS in VANET. They used city which was simulated in [13] with SUMO [25] and then exported the outputs of SUMO to NS2.34 to implement the communication network. Their results show that using Mobile IP (in comparison to the proposed idea in [13]) doesn’t have positive effect on delay but, better performances in terms of packet loss and throughput are achieved.
C. Improving QoS in VANETs by detecting and Removing Unused Messages

Authors in [26] tried to increase the performance of VANETs by removing the useless or unused packets. They considered the following scenarios:

Scenario 1: Consider a highway that has at least two lines for car traffic (Fig. 14). Suppose that car 1 brakes abruptly. In this vehicle, emergency electronic brake light application sends a message in its area. In this way other vehicles that receive the message must have a proper reaction. Vehicles that are in the same line and are behind the car 1, such as 4 and 5, after receiving and processing of the received message from car 1, they must reduce their speed [26]. Although cars 3, 6, 7, 8, and 2 receive these messages and after receiving the safety message they can remove it. In this special safety application, the position of vehicles has influential effect on their reactions [26]. According to this scenario if car 3 brakes and sends a safety message, car 1, 4, and other cars receive this message, but according to their position, they do not have to do any reaction. So all cars which receive this message do not need to process it and without any processing, they can drop it. If we do not have this idea, each car which receives the safety message should process it and according to the type of that message, each car should do a reaction [26].

Scenario 2: In this scenario as shown in Fig. 15, suppose that car 1 brakes abruptly and sends a safety message over its area.

Each car which receives the sent message will be forced to react and send a safety message according to its condition. If we review the scenario, we will see that the received safety message for vehicles far from the source, vehicles such as 4 and 5, is less important than closer ones [26]. In this scenario all of the cars are in the same lane and according to the previous scenario, all of them must process the message after receiving and then show a proper reaction according to the type of the received message [26]. But we know that when car 1 brakes, car 2 which is the nearest car behind it, must react quickly. Car 3 which is so far away from car 1 does not need to do any reaction because of its distance to car 1. In this idea each vehicle must be able to compute the distance between itself and another [26].

Simulation results show that with the help of the proposed idea in [26], better performance in terms of Message Expiration Ratio is achieved.
V. PROPOSED ARCHITECTURE AND PROTOCOL STACK

A. Proposed Architecture for Vehicular Networks

In this section we are going to introduce our proposed architecture for vehicular networks. As it is illustrated in Fig. 18, in our proposed architecture, geographical regions are divided into 25 unique areas and in each area there are 9 WiMAX base stations which provide wireless services to the vehicles and they are connected together with a wired network. These WiMAX base stations operate as a wireless switch for in-cell communications and a gateway for out-of-cell communications. Cars communications is also restricted, each car could communicate only with other cars and base stations in other 24 areas around it (Fig. 18).

B. Proposed Layer 3 Protocol

VCNP (Vehicular Communication Network Protocol) is our proposed layer 3 protocol for vehicular communications. VCNP header is illustrated in Fig. 20. There are some differences between VCNP and Internet Protocol (IP). As we know, there are four octets for each of source and destination address fields in IP but in VCNP we propose to use 3 octets instead of four. The first octet represents the area, the second octet represents the base station and the third octet represents the vehicle, so any node will have a unique layer 3 address and according to the restricted communication domain, we will be able to reuse layer 3 addresses several times in other areas. There is a one-bit field, M, which shows the last packet of the stream, whenever M is set to 1, it shows that there are more packets to come and when M is set to 0, it means that the stream is finished. We also eliminated the Fragment Offset and Flag fields, because according to layer 2 technologies and Maximum Segment Size (MSS) we could estimate a constant size for layer 3 packets, therefore routers do not have to fragment packets and both header and packet size will be constant. Version field is also eliminated and the QoS field is reduced to 3 bits. Other fields of VCNP are the same as IP header fields.
C. Proposed Layer 4 Protocol

Vehicular Communication Transport Protocol (VCTP) is our proposed transport protocol for vehicular communications. TCP and UDP have their own advantages and disadvantages. According to special characteristics of VANETs, we propose a new transport protocol aiming to provide better rates in terms of throughput, delay and packet loss.

TCP is a connection-oriented protocol and is suited for applications that require high reliability and less transmission rate. TCP is also a heavy-weight protocol and does error checking, handshaking and flow control, therefore it is not a suitable transport protocol for VANETs with those mentioned characteristics. On the other hand, UDP is suitable for applications that need fast and efficient transmission. UDP is faster because it is a light-weight protocol and there is no error checking, flow control, etc. and it is a small transport layer designed on top of IP.

In this paper we propose a new transport protocol aiming to provide the high throughput of UDP, as well as the packet loss rate of the TCP. VCTP is similar to UDP in terms of source port, destination port and checksum fields but in contrast to UDP, there is a recovery option as well as a handshaking process. VCTP also guarantees that the sent packets will reach to destination. VCTP header is illustrated in Fig. 21.

D. VCTP Algorithm

Application layer sends the produced data to transport layer and then according to MSS, transport layer divides the whole data into segments and sends them to the destination. We assume that application layer produces some data and transport layer wants to send these data in 1000 segments.

VCTP operates as follows:

1- At first, source sends a segment to the destination, in this segment “Syn” is set to “01” and “Seq#” is set to “0111101000” or “1000” in decimal system. It shows that source wants to establish a connection and send 1000 segments.

2- If destination is ready for data exchange, it will send a segment to source. In this segment “Syn” is set to “10” and “Seq #” is set to “0111101000”. It shows that destination is ready to exchange data and knows that 1000 segments will be sent (Fig. 22).

2-1- If destination did not catch the segment that was sent in part 1, after a while, source sends that again.

3- Source starts to send data, when each segment is sent, the “Seq#” will be increased in the next segment. For example in the first segment, “Seq#” is set to “01”, and in the second segment “Seq #” is set to “10”.

4- When source finishes sending data, it sends a segment to destination. In this segment, “Fin” is set to “01” and it shows that source has finished sending data.

5- If the destination node, receive this segment:

5-1- Destination will check if it has all one thousand segments. If yes, a segment will be sent to the source by destination and in this segment “Fin” is set to “11” and it shows that destination has received all the 1000 segments and is ready to finish the connection (Fig. 23).

5-2- If the destination node finds that some segments are lost, it will send some segments to inform the source about the lost segments. In these segments “Fin” is set to “10”. For example if destination do not receive #200 and #201, it will send two segments to source, in both of them “Fin” is set to “10” but “Seq#” in the first one is set to “11001000” and in the second one is set to “11001001”. It means that, destination has not received segments with mentioned sequence numbers.

5-3- Source will send #200 and #201 segments to the destination immediately, and repeats the finishing process which is explained in part 4 (Fig. 24).
E. Simulation Results

We used OMNET++ to simulate our proposed idea. OMNET++ is an open-source, component-based simulation package built on C++ foundations. Simulation parameters are depicted in table 1.

Table 1: Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Area</td>
<td>1000 * 1000 m</td>
</tr>
<tr>
<td>Channel Type</td>
<td>Wireless</td>
</tr>
<tr>
<td>Radio Range</td>
<td>500 m</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>Visualization</td>
<td>OMNET++</td>
</tr>
<tr>
<td>MAC</td>
<td>IEEE 802.16</td>
</tr>
<tr>
<td>Routing</td>
<td>Static</td>
</tr>
<tr>
<td>Number of Vehicles</td>
<td>20</td>
</tr>
<tr>
<td>Number of Base Stations</td>
<td>4</td>
</tr>
<tr>
<td>Vehicles Speed</td>
<td>40-80 Km/h</td>
</tr>
<tr>
<td>Packet Size</td>
<td>1000</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>VCTP</td>
</tr>
<tr>
<td>Duration</td>
<td>60 s</td>
</tr>
<tr>
<td>Radio Propagation</td>
<td>Two Ray Ground</td>
</tr>
<tr>
<td>Queue Type</td>
<td>Drop Tail</td>
</tr>
<tr>
<td>Addressing Type</td>
<td>Hierarchical 3 level</td>
</tr>
</tbody>
</table>

In the simulation scenario, there are 20 vehicles and 4 base stations. Vehicles communicate with each other via base stations, so the communication type is Vehicle to Roadside to Vehicle or V2R2V.

After the simulation process we compared the achieved results with another scenario in which TCP/IP protocol stack was used. Simulation results show that better performance in terms of throughput is achieved. Packet loss rate and delay are also improved.
VI. CONCLUSION

In this paper we presented a short overview of vehicular networks architecture, QoS concepts and QoS provisioning in vehicular communications. We proposed a novel architecture and protocol stack, aiming to improve QoS and security in vehicular networks. Finally we simulated our proposed idea and compared the achieved results with a similar scenario in which TCP/IP protocol stack was used. Results show that our proposed protocols provide better rates in terms of delay, packet loss and throughput. The type of communication that was used in our simulation was Vehicle to Roadside to Vehicle (V2R2V). Moreover, we did not use any specific routing protocol. Therefore, in the future works a routing protocol will be used and we will implement our proposed idea on other types of vehicular communications like V2V and V2I communications.

REFERENCES


Performance Analysis of VoIP over IPV4, IPv6 and 6-to-4 Tunneling Networks

Muhammad Fawad 1, Syed Irfan Ullah 2, Haseena Noureen 3, Arbab Wajid Khan 4, Zar Khitab 5, Shahab Khan 6, Abdus Salam 7, Muazzam A. Khan 8

1,2,4,6,7 Department of Computing & Technology, Abasyn University Peshawar KP Pakistan
3 Faculty of Computer Science & IT, University of Malakand Dir(L) Malakand KP Pakistan
5 Faculty of Electrical Engineering, APCOMS Rawalpindi, Pakistan
8 NUST College of EME, National University of Sciences & Technology, Islamabad Pakistan

Abstract—Transition from IPv4 to IPv6 is a cumbersome process because of their irreconcilability with each other and coexists during the transition period. This work examines the behavior of transition mechanisms that involve communication among IPv4 and IPv6 in various scenarios and traffic conditions. A network analyst faces variable traffic and data rates at different nodes in such a heterogeneous network, that requires more attention to make it able to work with stable network flow and data rate. We analyse an end-to-end delay of VOIP data packets in IPv4 and IPv6 homogeneous and heterogeneous networks using 6 to 4 tunneling techniques. This work shows that IPv6 has better performance than IPv4 and IPv6-to-IPv4 tunneling. The tunneling technique improves the network throughput and queuing delay over the intermediate nodes of the heterogeneous network.

Keywords: IPv4, IPv6, VoIP, 6-to-4 tunneling, DSTM

I. INTRODUCTION

Routing devices are needed for traffic exchange in interconnected networks. In case of dynamic routing the router makes its tables by broadcasting informative messages. Routing protocols determine the shortest path to destination. Based on traffic and routes availability, the routers are updated accordingly.

Internet Protocol shortly IP is a transmission technique for data on internet. Its current address space is 32 bit. Often other protocols are used to complement with it in making sure that data has been transferred to its required destination, as every device is uniquely identified by IP-address in a network. IP is a connectionless protocol and is not concerned with the delivery and order of data. Also it doesn’t give any information about packet loss during transmission. In future internet will face a problem of limited addresses and no new host will get a chance to be connected with the internet. The increasing usage of internet through different devices i.e. mobiles, PC, tablets etc. require large number of IP addresses. IPv6 not only replaces IPv4 to achieve a large address space of 128 bits, but also provides extra facilities like high security, QOS, Mobility, Simple header formats. The new version of Internet protocol i.e. IPv6 is getting importance due to scalability, multimedia transmission and elimination of NAT requirement. Most of the networks are based either IPv4 or IPv6 and connecting both the networks is the hard issue of today’s communication systems.

Section II discusses the objectives of the research. Section III discusses the proposed and its analysis. Section IV summaries and concludes this work.

II. LITERATURE REVIEW

The digital world is switching over rapidly from IPv4 to IPv6 due to the shortage of IPv4 addresses, huge routing tables, security issues, mobility and Quality of Service that over the Internet. High speed networks and extra IP addresses are required to every person to become a part of the globally connected network. New protocols are designed to fulfill the end user demands and face new challenges of the digitally communicated world. Internet protocol IPv6 has the improved features over IPv4 that overcome IP address shortage and numerous IP addresses are available to assign them to each individual node [1]. A number of applications still support IPv4 only and require communicating with other applications over IPv6 enabled networks.

Abrupt migration from IPv4 to IPv6 is not possible and still it may take years to completely replace IPv4 over the Internet. Various migration techniques like Dual Stack, Translation and Tunneling Mechanisms are used to make IPv4 functional with IPv6. IPv4 is compared with IPv6 in [4] which shows that in low traffic load IPv4 perform better than IPv6. The impact of IPv6 transition mechanism is discussed in [6] which show that the performance overhead is minimal but the translation packet degrades its performance. VoIP is compared on LAN using Background UDP that shows IPv6 has more packet loss than IPv4 in high congestion and have poor voice quality [8]. Dual Stack Transition Mechanism(DSTM) provide better reliability and low data loss as compared to IPv4 having a longer queue delay due to encapsulation and de-capsulation overhead at the end points of the channel.

Combining Tunneling and Dual Stack Mechanism improves reliability and reduce packet loss. Increasing the packet size (>1000 bytes) the queuing delay increases which results in overall low through put in DSTM, in that case IPv4 networks performance is better. The transition 6 over 4 mechanisms using IPv4 multicast tunneling and their constraints are...
discussed in [7]. This mechanism is suitable for small networks but having scalability issues in large networks. Internet uses both IPv4 and IPv6 addresses which require frequent translation of the IP addresses wherever required. NAT-PT translates IPv6 addresses to IPv4 [3]. NAT-PT uses different ports for the hosts which increase its limit to 63K hosts to overcome the IPv4 address shortage. NAT-PT is limited to TCP and UDP connections and does not support DNS and FTP that has been resolved by using Application Level Gateway (ALP). The VoIP data traffic on FTP using translation technique face problems highlighted in [3] and degrades integrated network performance [6]. In the first phase of tunneling networks use IPv4 protocol and small island of IPv6. In second phase IPv4 is encapsulated with IPv6 tunnel that migrate IPv4-to-IPv6, which makes IPv6 network able to communicate with IPv4 networks. Various tunneling techniques are discussed in [5].

**Table 1: Results collected from the Designated Model at Different Modes**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Point-to-Point Throughput (Packets/sec)</th>
<th>Point-to-Point Queuing Delay</th>
<th>Packet End-to-End Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>41.7</td>
<td>0.000017628</td>
<td>0.060191</td>
</tr>
<tr>
<td>IPv6</td>
<td>114.51</td>
<td>0.00001401</td>
<td>0.06009</td>
</tr>
<tr>
<td>6-to-4 Tunneling</td>
<td>123.06</td>
<td>0.00001387</td>
<td>0.060185</td>
</tr>
</tbody>
</table>

IV. PERFORMANCE EVALUATION

The model is evaluated from different angles; their results are collected at different levels. Here we analysed collected information in different ways.

**4.1 Throughput, Queuing Delay and End to End delay**

Table 1 shows that the throughput of 6 to 4 tunneling is three times to IPv4 and almost similar with IPV6. Tunneling increases the throughput and it is obvious that Queuing delay for workstation ‘B’ in 6-to-4 tunneling router is least delayed because it is connected to a relay router. Workstation ‘D’ in IPv6 environment which is connected to IPv6 backbone has the second lowest delay as compared to other two stations i.e. workstations ‘A’ and ‘C’ which is connected to IPv4 backbone. IPv6 has least delay as compared to IPv4 and hence IPv6 perform better than IPv4. Relay router further reduces the queuing delay in 6-to-4 tunneling network. Packet end-to-end delay and throughout is stable and well in limits.
Workstations connected to their respective routers observe similar results are graphically represented in Figure 3, 4 and 5. Workstations connected to IPv6 networks has better throughput utilization as compared to the workstations connected directly to IPv4 networks as can be seen in the given figure.

4.2 Investigating Relay Router

From above results since relay router is producing excellent results for throughput and queuing delay, it is important to further investigate this router. Throughput and queuing delay of relay router to IPv6 router is better than towards IPv4 router. The point to point utilization between the IPV6 network and IPv4 network is same.

4.3 Voice calls made to workstation D

Now let’s break up the packet delay variation graph for voice calls made to workstation D. The packet delay variations for voice calls made to workstation D from workstation A, B and C.

From above graphs workstation C has much lower throughput then workstation D (three times lower), but the queuing delay for D is same as station C. The reason for same queuing delay for C and D is that they are inside their networks.
It is obvious that the packet delay variations for voice call coming from IPv4 networks (i.e. from workstation A and C) are much higher. Since Workstation B is connected to a relay router and making call to D station in IPv6 environment, it has the least packet delay variations.

<table>
<thead>
<tr>
<th>Workstation VoIP Call</th>
<th>Packet End-to-End Delay (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C to D</td>
<td>0.060191</td>
</tr>
<tr>
<td>A to D</td>
<td>0.060185</td>
</tr>
<tr>
<td>B to D</td>
<td>0.06009</td>
</tr>
</tbody>
</table>

Table 2: End-to-End Delay (sec) in Voice Calls

We observe the overall network jitter and packet delay variation. Results show that the network has presented an acceptable jitter and packet delay variations for VoIP as per international standards.

Figure 11: Voice Jitter

Figure 12: (voice packet delay variation)

Figure 11, 12 shows that jitter becomes almost predictable and stable gradually when a load is applied over the networks.

V. CONCLUSION

We analyze the performance of IPv4-only and IPv4/IPv6 integrated networks by using the framework of the 6-to-4 tunneling. The behavior of IPv4 and integrated IPv4/IPv6 is analyzed by different angles i.e. throughput, queuing delay, jitter and mean end-to-end delay. The 6-to-4 tunneling better performance than IPv4 networks in all these tests and the overall end-to-end delay is reduced to a significant level in heterogeneous network. Other tests on jitter and packet end-to-end delay prove that IPv6 has better performance than IPv4 enabled networks.

REFERENCES


Muhammad Fawad graduated from Islamia College Peshawar in 2006. Currently he is doing his MS degree from Abasyn University Peshawar. His research interests include IPv4 to IPv6 transitions and tunneling. Currently, he is acting as computer Lecturer in GPGC Dargai and supervising IT Projects at graduate level.

Syed Irfan Ullah received his master degree from University of Peshawar and received his MS and PhD from Islamic International University Islamabad. His field of research is Data and Network Security, Secure algorithm Design, Securing data on Private and public channels, Secure Communication, Cryptanalysis and Breaking code. Currently, he is doing his job as Assistant Professor in Abasyn University Peshawar and is supervising MS and PhD research Projects.

Arbab Wajid Ullah Khan currently working as Lecturer in department of Computing and Technology, Abasyn University Peshawar campus, Pakistan. He has
completed his MS degree in Telecommunication and Networking from Abasyn University, Peshawar, Pakistan in 2015. He received his BS degree in Information Technology from University of Peshawar, Peshawar, Pakistan in 2012. His research interests include mobile ad hoc network, wireless body area networks and sensor networks.
Investigation of Collusion Attack Detection in Android Smartphones

M. Kireet
Research Scholar, Dept of CSE
JNTUH
Hyderabad, India

Dr. Meda Sreenivasa Rao
Professor
JNTUSIT
Hyderabad

Abstract—Today as Android is used by majority of the smartphone users it has become one of the effortless platform for the malware-writers to introduce their malicious activities into smartphone world through this android mobile applications. The main loophole in Android applications is permission based security control. The User unawareness of accepting every permission as a mandatory requirement by an app is making more and more convenient for the hackers to extract the users private data. In this paper we have analysed all the leakages which are done by using permissions required by an app. We carefully made an investigation to detect collusion attacks. We analyzed the present detection methods of inter-permission leaks especially on Collusion attacks and mentioned the areas where the enhancements are needed with limitations that existed in present detection methods.

Keywords—Collusion attacks, inter-permission leaks

I. INTRODUCTION

The Excaberation of smartphones has extended the use of mobile apps. At around 2.6 billion users are using the smartphones and as per analysis and estimation of various surveys the mobile usage may raise by 6.1 billions by 2020[5]. As a result there is an instantaneous increase of mobile apps in different app play stores. At present Google play store has 1.6 million android apps and Appstore of Apple has 1.5 million apps [4] [5]. All the Android apps follow the classical and traditional permission based access control as a centralized control mechanism. For an app to be installed into a Smartphone user should accept all of the required permissions mandatorily, this mandatory acceptance of each and every permission creating an opportunity to intruders to introduce the malware. As per statistics given by appvigil analysis reports [16] 98% of the present apps in different app stores are pregnable as these apps require the permissions which are inexpedient to the app functionality. This permission adoption is giving an entry to the intruders to launch intrusions through mobile apps by which most of the private user data is released.

This immensive explosive growth of apps became a channel for the introduction of many types of attacks by which most of the mobile users private content is revealed. The intruders find the inadequacy in the accepted permissions in the existing apps or with their own strategies they are developing their own apps with permissions insignificance to the apps functionality and finally the user’s sensitive data from the Smartphone’s is extracted. This type of problem is pointed as data Leakage done by using permissions or “Permission leakage “ which is one of the most dangerous attacks by which
legally extraction the Smartphone user’s private/sensitive information is done.

The Permission leakage attacks [2] are of three types known as Confused deputy attacks, Intent Spoofing and Permission collusion. Confused deputy attacks completely depend on misconfigured applications. Intent spoofing [2] is a form of confused deputy attack which affects applications that are not meant to communicate with other applications. Collusion attacks [2][10] uses overt and covert channels and aggregates the permissions from different apps and releases user sensitive data. These type of collusions attacks are difficult to detect and causing a great deal of research in the mobile applications. We analyzed some of the methods that detects the colluding applications and we enhanced the present detecting models of colluding applications.

There are many attacks through apps of which collusion attacks, confused deputy attacks and intent spoofing attacks are the permission leakage attacks. At present there are different tools and methods to avoid these types of attacks but the existing classical permission model in smartphone needs to be intensified and give the user necessary indications to the user on the acceptance of each and every permission required by the app.

To give appropriate directions to the mobile users on classical permission model we proposed a framework that investigates the app and its permissions and finally points out if the app requires a pertinent permissions based on its functionality or not.

The rest of the paper is organized as .In section-2 we presented the problem of application collusion in smartphones along with examples. In Section-3 we presented the inference on collusion attacks .In Section-4 we presented the analysis of collusion attacks by using present detectors and their limitations. In Section-5 we presented the future scope in the detection of collusion attacks and finally we draw conclusions on the collusion attacks detection and scope.

II. APPLICATION COLLUSION IN SMARTPHONES

Colluding applications are those applications that collaborate in breach of some security policy of the system. These applications legally do not individually break any security permissions or pervert software vulnerabilities. They alternatively use existing channels or new channels are constructed for communication to perform malicious actions or try to access the unauthorized resources.

![Diagram](https://sites.google.com/site/ijcsis/)

Figure 1. The ContactsOptimizer application on the left and the News application on the right colluding through a covert communication channel. The ContactsOptimizer does not have access to the network, but has access to user’s contacts. The News application has no access to user’s contacts but can access the network. The ContactsOptimizer leaks the user’s contacts to the News application, which then sends this information to a third party.

The attack of colluding applications is viable be-cause modern present security mechanisms are not focusing on controlling the channels where two applications can make a route to communicate. Rather, most of the efforts have been made to achieve application sandboxing or containment. This is most likely due to the fact that there is little concern on tight information flow control i.e with overt or covert channels typically of personal computers OSs, by which many smartphone operating systems are based.
A. Covert and overt channels on smart phones

Covert channel is a channel that is deliberately used by applications to make communication while it was not meant to be used for communication[2]. Covert Channels, uses non data objects to transfer information from one source application to another. Source manipulates system state, such as file lock or busy flag to signal information to the Sink. Sink is nothing but application that receives data.

Overt channel is a channel by which application uses a data container such as a file or a buffer to hide information [2]. Overt Channels uses data objects which are normally used as data containers such as buffers, files, and I/O devices to transfer the communication from one source application to another.

Overt channels could be controlled by strictly enforcing the access control policy while covert channels could be controlled by implementing dedicated methods.

The Covert and Overt channels can be found at different levels of abstraction in a system which are as follows

At the highest level, the level of API that an operating system provides the developers forms a channel as an example android uses java API this can be taken as the highest level, this is the simplest level where the channels can be closed. At Intermediate level the OS is considered. This is the level of the operating system which is revealed by using native calls that will extract the data present in the operating system. This level can be closed but causes severe damages. At the lowest level hardware level which forms channels for exploitation using the smartphone hardware functionalities. This level is completely dependent on hardware functionalities and channels may not be closed easily. The Covert and Overt channels can be found at different levels of abstraction in a system which are as follows

At the highest level, the level of API that an operating system provides the developers forms a channel as an example android uses java API this can be taken as the highest level, this is the simplest level where the channels can be closed. At Intermediate level the OS is considered. This is the level of the operating system which is revealed by using native calls that will extract the data present in the operating system. This level can be closed but causes severe damages. At the lowest level hardware level which forms channels for exploitation using the smartphone hardware functionalities. This level is completely dependent on hardware functionalities and channels may not be closed easily. The Covert and Overt channels can be found at different levels of abstraction in a system which are as follows
Figure 2. The Figure showing visualization of the Broadcast Intent overt channel.

```java
Context ctx = this.getSystemService(Context.BROADCAST_SERVICE);
Intent intent = new Intent("com.something.action");
setReceiver(ctx, intent);
intent.putExtra("key", "value");
ctx.sendBroadcast(intent);
```

Figure 3. The above figure showing the java code that is required for communication between source and sink in which the communication contains the private data.

D. Example of Covert channel

The Figure 4 shows the Java code needed to exchange communication through the number of running services. By using this method the sink counts the number of services that the source application is using and will infer information from that, the source for a given amount of time t, either precipitate an extra service or not. The Sink requires one more extra permission i.e GET_TASKS to utilize the Java API and to list the running service

```java
public class Service extends BroadcastReceiver {
    public void onReceive(Context context, Intent intent) {
        service = intent.getStringExtra("key");
    }
}
```

Processes Enumeration from native code: Figure 5 shows the concept of how the sink finds the no. of forked processes of source using the native (C) code. In this covert channel the sink application counts about how many processes have been forked by parsing the /proc/ file system. Source application forks its process from a native JNI function by fork() call. A similar type approach can be used by using pthread_create() from the native code as a substitute to forking the process on the source side. In this case sink could read the file /proc/<PID>/status to count the no. of spawned threads. This allows information to be exchanged between the sink and source applications

```java
Intent svc = new Intent(Intent.ACTION_MAIN);
svc.setPackage("com.example.package");
startService(svc);
```

III. INFERENCE ON COLLUSION ATTACKS

Most of the collusion attacks are done using the intent-filters. Intent filter mechanisms do not provide any guarantee of security so it is considered as loose binding between Activity (components built for interfaces of mobile devices) and intents. Intents are used for communication between activities of same application or for inter-application communication [2]. In the application manifest which is Android XML manifest file the components of application and their
encapsulation and permissions required are specified. Most of
the developers by mistake or by knowing specify the intent
filters in their way which leads to permission leakage attacks
like collusion attacks. Considering two points (i)If the Intent-
filter specified is declared and exported attribute is not set to
true or false, default value is true which makes the Activity to
be accessible by any application ,in the same way(ii) if an
intent-filter is not declared ,the exported attribute is not set ,by
default Activity accessible though intents whose source is
from the same application. Until and unless the developer
specifies sharedUid in the manifest file exception is not
allowed in the above two points.

IV. ANALYSIS OF PRESENT INTER-PERMISSION LEAK
(COLLUSION ATTACK) DETECTORS

The permissions leakage attacks detection and prevention in
android mobiles is one of the most seriously considered
research areas as the majority of the smartphone users are
utilizing the services provided by android. Most of the
contemporary methods intensify on detection and prevention
of Collusion attacks by static and dynamic analysis detection.
The analysis of different inter-permission leaks along with
their limitations as follows

A.MockDroid[13], familiarly known as modified version of
the Android operating systems permits user to `mock' an
application's access to a resource. The system of MockDroid
aims on faking the information that is utilized by the
application so that the user data not to be divulged and that
forms a major security of users data. In case of Broadcast
intsents problem as per MockDroid specified in [13], “if the
permission required to send a broadcast intent from a package
is mocked”, the broad-cast intent is never sent; likewise, “if
the permission required to receive a broadcast intent by a
package is mocked, it is never received”. In this way
Collusion attacks are protected using Mockdroid by giving
notifications to user as “Mocks permissions for applications”. There
are limitations in MockDroid as hiding the notifications
for applications which use fullscreen and mocking the source
used by a background service .

B.Fire-Droid[18], familiarly known as a policy-based
framework which makes use of interleaving system calls to
implement security protocols. FireDroid introduces FireDroid
Application Monitor(FDAM) by using ptrace() which is
considered as policy tracing, so everytime when the target
process executes a system call, the kernel suspends the target
process and notifies the FDAM. FDAM maintains policy
enforcement policy(PEP) within it and checks the required
information of the target process execution of system call.
PEP takes and forwards this information to policy decision
point(PDP) that will retrieve policies from policy repository
within FDAM. Finally based on the policy evaluation is done
to kill the process or accept the process and this is notified to
user to take his decision based on the evaluation from
FDAM.In this way collusion attacks are detected using
FireDroid. There are few limitations in FireDroid if the
policies were not designed and implemented there could be
allowance of applications to collude and moreover there is no
proper steps or policies given to the applications which are
developed by same developers as a result collusion may
happen.

C.TaintDroid[19], is used for dynamic taint tracking to
identify the information flows that reach sinks. TaintDroid
assumes that third-party applications downloaded, are not to
be trusted and monitors in real-time how these kind of
applications access and manipulate user’s private data.Still
better handling in control flow is needed to further detect
collusion attacks.

D.ScanDroid[20] is the tool for android and can detect
information flow violations but it is not extensible with new
taint propagation rules as a result of that collusion attacks
detection is not effectively monitored.
 PermissionFlow [2] is a static analysis-based technique for automatic identification of permission-protected information sources in permission-based systems. PermissionFlow identifies APIs whose base execution leads to permission checking and tracks the flow of APIs. The limitations are PermissionFlow is unable to trace of malevolent attacks performed by the top Android Market applications; when most applications correctly configure internal Activities by not supplying an exported="true" attribute or an intent-filter. As it fails to detect some of the traces of intent filters and sharedUid collusion attack detection is not effectively done by using PermissionFlow.

There are several other tools which are used for detection of Collusion attacks but we considered the most effective methods which are track the information flow as it makes much easier for detection of interpermission leaks.

V. FUTURE SCOPE

Most of the present methods and tools track the flow and if it leads to permission leakage it informs the user that the app is malicious and recommends the users to uninstall the app. As Android in present versions has given an option of only removing a permission where by disabling the required permission the user can run the app so there is a scope to track the malicious permissions and notify the user that malicious permissions should be disabled. We have also analyzed that there are identifying risky permissions out of present 135-140 permissions is easier. There are several methods by which the risky permissions can be given ranking so that if high risky permissions can be asked at installation user can directly disable that option once it is installed. There is also a scope to use RecDroid tool[14] where user recommendations are used for ranking the permissions and also disabling the malicious permissions. There is also a scope to categorize apps and based on the categorization the best possible permissions for a particular category of app should be given as per rating based on this user can know for which category of app which permissions should be treated as defailty needed permissions and which permissions are asked extra and take a decision of disabling or enabling that extra permission asked other than specified in category relevant permissions. These are the different methods by which have scope to detect Collusion attacks.

VI. CONCLUSION

The substantial increase in the usage of Android mobiles has made the malware writers to choose this as a base platform for introducing the malware. The easiest way to introduce malware into smartphones is done by using the loophole of permission control. The attacks that are done through permissions are called as inter-permission leaks. In this paper we carefully analyzed how inter-permission leaks will happen and mentioned the inter-permission leaks as one of the inter-permission leaks of collusion attacks are still difficult to detect we analyzed how collusion attacks takes place ,with our analysis we mentioned the collusion attacks with examples. As per our analysis we took the different efficient existing tools which detects the inter-permission leaks, we analyzed them and mentioned the areas where the existing tools lack detection the collusion attacks. Finally we draw to a conclusion that there is lot of scope for research in this area of detection of inter-permission leaks especially Collusion attacks as most of the android mobiles are releasing the private content of user.

REFERENCES


[16] https://appvigil.co/vulnerability-scanner/#/
A Hybrid Machine Learning Model for Selecting Suitable Requirements Elicitation Techniques

Nagy Ramadan Darwish
Department of Computer and Information Science
Institute of Statistical Studies and Research
Cairo University, Egypt

Ahmed Abdelaziz Mohamed
Department of Information Systems
Higher Technological Institute
Cairo, Egypt

Abdelghany Salah Abdelghany
Department of Information Systems
Higher Technological Institute
Cairo, Egypt

Abstract—Requirements elicitation is the first and the most critical phase of Requirements Engineering (RE). Many techniques have been proposed to support the elicitation process. Each technique has its strengths and weaknesses. This variety makes the selection of technique or combination of techniques for a specific project a difficult task. Mostly techniques are selected based on personal preferences rather than on attributes of project, technique, and stakeholders. In this paper, the researchers propose a three-component approach for elicitation techniques selection. First, a literature review is conducted to identify the attributes affecting techniques selection and common elicitation techniques. Second, a multiple regression model is built to analyze these attributes in order to find the critical attributes influencing techniques selection. Finally, an Artificial Neural Network (ANN) based model for selecting adequate elicitation techniques for a given project is proposed. The ANN model helps reduce the human involvements in this process. It was implemented using Neural Network Fitting Tool in MATLAB. The network has accuracy of 81%. The ANN model was empirically validated by conducting a case study in a software company.

Keywords: Requirements Engineering, Requirements Elicitation, Multiple Regression Analysis, Neural Network.

I. INTRODUCTION

Requirements Engineering (RE) is the process of formulating, documenting and managing software requirements. RE process is composed of various sub phases: requirements elicitation, analysis, specification, validation and management [1]. Requirement Elicitation is the first and the most important phase in the process of requirement engineering. It is the process that deals with seeking, uncovering, achieving, and detailing requirements for computer based systems [2]. Most of the software projects fail just because of the problems of requirements elicitation process.

Many surveys have been conducted to explore the projects failure statistics. A survey conducted by Standish Group showed that 13.1% of projects fail due to incomplete requirements and 8.8% of projects fail due to changing requirements. Another survey found that 12.7% out of 1027 projects were successful and the main reason for the failure was unclear and imprecise requirements [3, 4]. According to these various surveys, it is clear that poor requirements elicitation process is the most critical factor for the failure of software projects.

The success of requirement elicitation process depends mainly on knowing which requirement elicitation technique to apply to a particular project. There are a variety of elicitation techniques such as interviews, observation, brainstorming, etc [5]. Each technique has its strengths and weaknesses. This is due to the fact that there is no one technique that can satisfy all situations. They work best at different situations and problems. Moreover, they can work in a complementary manner where the weakness of one technique can be compensated by the strengths of some other techniques [6].

Using a variety of techniques ensures discovering most of the requirements, and thus leads to effective requirements elicitation process. This variety makes the selection of a technique or a combination of techniques for a specific project a challenging issue. Selecting inappropriate techniques has negative effects on the quality of the elicited requirements. Mostly the selection of requirements elicitation techniques is based on personal preferences rather than on the basis of characteristics of project, technique and stakeholders.

Software engineers tend to select a particular technique for any combination of the following reasons [7]: it is the only technique that they know; it is their favorite technique for all situations; they follow a methodology that specifies a particular technique; or they guess that the technique is effective in the current circumstances. This subjective decision can bias the elicitation process and decrease the quality of elicited requirements. It is clear from the above analysis that an efficient approach for requirement elicitation is required which can be helpful for the selection of elicitation techniques.

In this paper, the researchers propose a three-component approach for elicitation techniques selection. First, a literature review is conducted to identify the contextual attributes that may affect techniques selection process and common elicitation techniques. Second, a multiple regression model is built to analyze these attributes in order to find the critical attributes influencing techniques selection. Finally, a neural network based model for elicitation techniques
selection process is proposed which reduces the human involvements in this process.

The rest of the paper is organized as follows: Section 2 provides a background overview about the main concepts related to the research topic. Section 3 presents the related work focusing on elicitation techniques selection. Section 4 describes the proposed approach and its main components. Section 5 presents a case study to validate the proposed model. The last section concludes the paper with final remarks.

II. BACKBOARD OVERVIEW

This section consists of three parts. The first part presents the requirements elicitation process and its tasks. The second part provides an overview of artificial neural network. The final part gives an analysis of the multiple linear regression model.

A. Requirements Elicitation Process and Its Tasks

Requirements elicitation is one of the important phases in the RE process. It is the process of collecting the requirements from stakeholders using different techniques [8]. Requirements elicitation process includes tasks that must allow for communication, prioritization, negotiation, and collaboration with all the relevant stakeholders [9]. Typical tasks of this process can be grouped into five types as shown in Fig. 1 [10].

B. Artificial Neural Networks (ANN)

ANN is a system that is inspired by the way biological neural networks work. In other words, it is an imitation of biological neural system [11]. ANN is composed of a network of interconnected processing units (known as neurons). Fig. 2 shows the neuron model. In this model, various inputs to the neuron are represented by \( x_1, x_2, x_3, \ldots, x_n \). Each line that connects these inputs to the neuron is assigned a weight. These weights are represented by \( w_1, w_2, w_3, \ldots, w_n \) [12].

![Neuron Model](image)

Our paper focuses on the task of selecting techniques for elicitation process because it is a difficult task for software engineer to decide which technique or combination of techniques is the most suitable for a given project. There are a range of techniques for eliciting requirements including interviews, surveys, Joint Application Development (JAD), prototyping, etc.

Regression analysis is a standard statistical technique for determining the relationship between two or more variables which have reason and result relation. The simple regression analysis estimates the relationship between a dependent variable and one independent variable and formulates the linear relation equation between dependent and independent variable. Regression models with one dependent variable and more than one independent variable are called multiple regression analysis [15].

According to McClave and Benson [16], the multiple regression model, assuming that there are \( n \) independent variables, is formulated as follows:

\[
y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + \epsilon
\]

(2)

In this model, \( y \) represents the dependent variable and \( x_1, x_2, \ldots, x_n \) are the independent variables, and \( \beta_l \) is the regression coefficient, and \( \epsilon \) is the random error component. The value of the coefficient \( \beta_l \) determines the contribution of
the independent variable $x_i$, given that the other (n-1) independent variables are held constant and $\beta_0$ is the y-intercept [17].

III. RELATED WORK
There are many studies conducted to describe elicitation techniques and provide some guidance on their use and some others comparing elicitation techniques. However, little research has focused on selecting the right technique or combination of techniques for a specific project. For example:

- Carrizo, Dieste and Juristo [7] proposed a framework to help requirements engineers in selecting elicitation techniques at any time. To do this, they determined the contextual attributes of the elicitation process. Then, they established the adequacy values of each technique for each attribute value.

- Tiwari, Rathore and Gupta [18] developed a framework based on project’s contextual information to select elicitation techniques for a given project. One of the limitations of this approach is that the mapping function used by the approach is theoretical one.

- Masooma, Asger and Bokhari [19] presented a systematic approach for selecting the appropriate elicitation techniques based on various factors such as system type, requirements type, time, budget, stakeholder involved, technique maturity, available expertise, etc.

- Anwar and Razali [20] provided a practical guide for selecting the right RE techniques for a given project. This guide consists of a set of factors indentified from a field study including stakeholder characteristics, technique features, project environment, etc.

- Muqeem and Rizwan [21] proposed a framework that helps elicitor to select elicitation methods. The framework components consist of the following: Pre-Domain Development, Stakeholders Management, Technique Selection, and Prioritization.

- Jiang, Eberlein and Far [22] proposed a knowledge-based approach that helps in RE techniques selection. This approach integrates advantages of knowledge representation schemata and reasoning mechanisms.

- Kheirkhah and Deraman [23] identified important factors in RE technique selection from different viewpoints including technique attributes, project and organizational and classified them based on RE tasks.

- Hickey and Davis [24] proposed a model for the elicitation technique selection and identified a set of factors that should be considered during technique selection.

One of the problems related to all presented approaches or models is that they have human involvement during technique selection. This human involvement may bias the technique selection process. Another problem is that they consider few attributes that can influence the technique selection and therefore they are not greatly useful. Unlike these researches, our work tries to:

- Identify the most critical attributes that influence the process of elicitation techniques selection.

- Automate the process of elicitation techniques selection by developing a neural network based model.

- Reduce the human involvement in the process of elicitation techniques selection.

IV. THE PROPOSED APPROACH
This section describes the proposed approach that helps in the selection of appropriate elicitation techniques for a specific project. The step by step stages of the proposed approach is shown in Fig. 3. The steps of the proposed approach are described below:

- **Step 1:** Review the related literature reporting contextual attributes that may affect requirements elicitation techniques selection.

- **Step 2:** Analyze the identified attributes using a number of criteria to define a preliminary list of influential attributes.

- **Step 3:** Conduct a web survey with Likert-type scale questionnaires to measure the importance of candidate attributes in elicitation techniques selection process.

- **Step 4:** Analyze the collected data using a multiple regression model to find out which attributes can positively impact the elicitation techniques selection.

- **Step 5:** Propose an ANN model that is based on the selected attributes for selecting adequate elicitation techniques.

- **Step 6:** Train the ANN based on training and test data sets.

- **Step 7:** Evaluate the ANN model accuracy and performance.

The proposed approach consists of three main components. These components are discussed briefly in the following subsections.
As specified in the proposed approach and illustrated in Fig. 3, the first step is to determine a set of attributes influencing techniques selection and common elicitation techniques. As shown in Fig. 4, this step includes the following procedures:

1. Review the related studies directly defining attributes that may affect elicitation techniques selection process and/or proposing elicitation techniques.
2. Categorize the identified attributes into factors describing the contextual elements that influence elicitation process.
3. Analyze each candidate attribute by a number of criteria to decide whether it should be included or removed.
4. After analyzing the attributes, an action can be taken with each attribute in order to define the preliminary set of attributes that may influence techniques selection.

1) Identifying Influential Attributes: To identify the influential attributes, two types of studies were examined: framework proposals and empirical studies. The framework proposals define attributes or factors that were proposed by the authors to have an impact on the techniques selection process. The empirical studies involve experiments that show how a variation in some attributes changes the effectiveness of some techniques. From these sources, a preliminary set of 25 possible influential attributes was identified. These attributes can be classified into four categories:

- **Elicitor**: Requirements engineer or analyst who is responsible for eliciting information related to requirements form stakeholders.
• **Stakeholder**: Stakeholders are persons who have a stake in the project. Stakeholders can be customers, users, managers, etc.

• **Project characteristics**: Each project has some attributes that distinguish one from another based on goal of domain project.

• **Elicitation process**: It is the process of gathering requirements from stakeholders using different techniques.

Inclusion of an attribute in the preliminary list of attributes influencing techniques selection process is based on a number of criteria. Each candidate attribute was analyzed according to these criteria to decide whether it should be selected to be part of the preliminary list. These criteria are:

• **Unambiguity**: Whether the attribute is well explained and defined. The possible values include: yes (Y) and no (N).

• **Measurability**: Extent to which ratings can be defined for the different values of the attribute. The possible values include: low (L), medium (M) and high (H).

• **Practicability**: Possibility of assigning a value to the attribute at any time for a real project case. The possible values include: low (L), medium (M) and high (H).

After analyzing and assessing all the candidate attributes according to these criteria, an action can be taken with each attribute. Table 1 shows a summary of this analysis. The actions that can be taken with respect to an attribute are as follows:

- **Include (C)**: Include the attribute in the preliminary list of influential attributes
- **Remove (R)**: Remove the attribute from the preliminary list of influential attributes.
- **Merge (M)**: Merge with another attribute because they are identical.
- **Modify (F)**: Change the attribute name.

As a result of this analysis, 17 out of 25 candidate attributes were selected to be included in the preliminary set of influential attributes, 4 of 17 selected attributes were renamed, and 4 of 25 were merged. Additionally, one attribute was added based on the researchers' practical and theoretical experience. These totaled 16 attributes: 3 related to the elicitor factor, 6 related to the stakeholder factor, 6 related to the project characteristics and two related to the elicitation process factor.

Table 2 shows the preliminary set of selected attributes for the elicitation process along with their descriptions. Each attribute was expressed in terms of low, medium and high levels in order to determine its role in the techniques selection process. Furthermore, these levels were expressed numerically on a 0-10 scale to use them effectively in techniques selection.

### Table 1: The Summary of Attributes Analysis

<table>
<thead>
<tr>
<th>Factors</th>
<th>Attributes</th>
<th>Proposing Authors</th>
<th>Unambiguity</th>
<th>Measurability</th>
<th>Practicability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elicitor</td>
<td>Requirements engineering experience [25, 7, 26, 27]</td>
<td>[25, 7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Technical knowledge of elicitation methods [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>Knowledge of (familiarity with) domain [27, 28, 29]</td>
<td>[27, 28, 29]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Experience with elicitation techniques [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Cognitive problems [7, 26]</td>
<td>[7, 26]</td>
<td>N</td>
<td>M</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>Number of users [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Number of experts [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>User involvement [25, 30, 31, 32, 33]</td>
<td>[25, 30, 31, 32]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Location/accessibility [7, 26]</td>
<td>[7, 26]</td>
<td>N</td>
<td>L</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Availability of time [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Expertise [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Articulability [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Personality variables [7, 26, 34, 35]</td>
<td>[7, 26, 34, 35]</td>
<td>N</td>
<td>L</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Cognitive problems [p2, r10]</td>
<td>[p2, r10]</td>
<td>Y</td>
<td>M</td>
<td>M</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Knowledge and skills [31, 33]</td>
<td>[31, 33]</td>
<td>Y</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>Communication Skills [31, 34, 35]</td>
<td>[31, 34, 35]</td>
<td>Y</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Project characteristics</td>
<td>Project complexity [36, 37, 38]</td>
<td>[36, 37, 38]</td>
<td>Y</td>
<td>M</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Requirements size [36, 37, 38]</td>
<td>[36, 37, 38]</td>
<td>Y</td>
<td>M</td>
<td>M</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Cost available [36, 37]</td>
<td>[36, 37]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Time constraints [37, 39, 38]</td>
<td>[37, 39, 38]</td>
<td>Y</td>
<td>H</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Requirements volatility [37, 39, 38]</td>
<td>[37, 39, 38]</td>
<td>Y</td>
<td>M</td>
<td>M</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Clarity of project scope</td>
<td></td>
<td>Y</td>
<td>M</td>
<td>H</td>
<td>+</td>
</tr>
<tr>
<td>Elicitation process</td>
<td>Purpose of requirements [7, 26]</td>
<td>[7, 26]</td>
<td>N</td>
<td>L</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Process time [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>H</td>
<td>M</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Development methodology [7, 26]</td>
<td>[7, 26]</td>
<td>Y</td>
<td>M</td>
<td>H</td>
<td>F</td>
</tr>
</tbody>
</table>
TABLE 2 PRELIMINARY LIST OF THE SELECTED ATTRIBUTES

<table>
<thead>
<tr>
<th>Factors</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elicitor</td>
<td>Requirements engineering experience</td>
<td>Number of previous projects in which the elicitor has performed RE activities.</td>
</tr>
<tr>
<td></td>
<td>Understanding domain knowledge</td>
<td>Number of previous projects in the domain executed by the elicitor.</td>
</tr>
<tr>
<td></td>
<td>Experience with elicitation techniques</td>
<td>Previous experience or training acquired by the elicitor with each elicitation techique.</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>Number of individuals in the process</td>
<td>Number of users that can participate in the elicitation process.</td>
</tr>
<tr>
<td></td>
<td>Stakeholder interest</td>
<td>Stakeholder’s motivation to participate in the elicitation process.</td>
</tr>
<tr>
<td></td>
<td>Availability of time</td>
<td>Time that the stakeholder has to spend on the elicitation process.</td>
</tr>
<tr>
<td></td>
<td>Expertise</td>
<td>Stakeholder’s experience in the problem or work domain.</td>
</tr>
<tr>
<td></td>
<td>Articulability</td>
<td>Stakeholder’s skill at analyzing and explaining his or her knowledge.</td>
</tr>
<tr>
<td></td>
<td>Stakeholders conflicts</td>
<td>Level of agreement among stakeholders.</td>
</tr>
<tr>
<td>Project characteristics</td>
<td>Project complexity</td>
<td>Complex of project based on its structure, requirements needed and functions.</td>
</tr>
<tr>
<td></td>
<td>Requirements size</td>
<td>Number of requirements of the project.</td>
</tr>
<tr>
<td></td>
<td>Cost available</td>
<td>Budget constraints on the project.</td>
</tr>
<tr>
<td></td>
<td>Time constraints</td>
<td>Time that is available for eliciting requirements.</td>
</tr>
<tr>
<td></td>
<td>Requirements volatility</td>
<td>Change in requirements during software project developments.</td>
</tr>
<tr>
<td></td>
<td>Clarity of project scope</td>
<td>Clarity of project goals and scope.</td>
</tr>
<tr>
<td>Elicitation Process</td>
<td>Process time</td>
<td>Stage at which the elicitation process is prior to the session.</td>
</tr>
<tr>
<td></td>
<td>Development methodology used</td>
<td>Methodology used to develop the system.</td>
</tr>
</tbody>
</table>

2) Selecting Elicitation Techniques: A variety of elicitation techniques has been presented in the literature to address different requirements problems. These techniques can be classified into four categories with respect to means of communication: classic, cognitive, group elicitation or contextual. In this paper, the focus is on the techniques which are commonly used most cited. At least two techniques were selected from each of the above categories. Table 3 shows the techniques that were selected for this research.

B. Multiple Linear Regression Analysis

This section presents the multiple linear regression model which can be used to identify the most critical contextual attributes that affect the process of elicitation techniques selection. The model was implemented using Microsoft Excel. This section consists of four sub sections which are described below.

1) Data Collection: To gather the data a web survey method was employed. The targeted population was professionals working in different software houses. As Likert scale is the most commonly used scale in quantitative research, a web survey with Likert-type scale questionnaires was distributed to the targeted population. The survey consists of four sections. The first section includes both of the respondent’s details as well as the software project information. The second section includes candidate attributes that influence techniques selection. To measure the importance of candidate attributes, a 10-point Likert scale was used. The third section includes degree of influence on techniques selection process. To measure this degree, a 10-point Likert scale was also used. The last section allows respondents to give any additional comments. After a five-week survey period, a total of 300 people responded by accessing the online survey.

TABLE 3 COMMON ELICITATION TECHNIQUES

<table>
<thead>
<tr>
<th>No</th>
<th>Technique</th>
<th>Literature Support</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interviews</td>
<td>[5, 40, 41, 42, 43]</td>
<td>Classic</td>
<td>It helps get the holistic view of the entire system.</td>
</tr>
<tr>
<td>2</td>
<td>Task Analysis</td>
<td>[5, 41]</td>
<td>Classic</td>
<td>It is used to manage tasks between user and system.</td>
</tr>
<tr>
<td>3</td>
<td>Card Sorting/Laddering</td>
<td>[5, 40, 41, 43, 44]</td>
<td>Cognitive</td>
<td>They are used to prioritize stakeholders’ needs.</td>
</tr>
<tr>
<td>4</td>
<td>Questionnaires</td>
<td>[40, 41, 43]</td>
<td>Classic</td>
<td>They help get large data from large number of stakeholders in lesser time and with low cost.</td>
</tr>
<tr>
<td>5</td>
<td>Protocol Analysis</td>
<td>[5, 41]</td>
<td>Group/Elicitation</td>
<td>It helps in understanding the processes of the system being developed.</td>
</tr>
<tr>
<td>6</td>
<td>Repertory Grid</td>
<td>[40, 41]</td>
<td>Cognitive</td>
<td>It helps identify various characteristics among different domain units.</td>
</tr>
<tr>
<td>7</td>
<td>Brainstorming</td>
<td>[5, 40, 41, 43]</td>
<td>Group/Elicitation</td>
<td>It helps generate innovative ideas.</td>
</tr>
<tr>
<td>8</td>
<td>Observation</td>
<td>[40, 41, 42]</td>
<td>Contextual</td>
<td>It is used to conduct an assessment of users’ work environment.</td>
</tr>
<tr>
<td>9</td>
<td>Prototyping</td>
<td>[5, 40, 41, 42]</td>
<td>Group/Elicitation</td>
<td>It is used to get early feedback from stakeholders.</td>
</tr>
<tr>
<td>10</td>
<td>Focus Group</td>
<td>[5, 41, 45]</td>
<td>Group/Elicitation</td>
<td>It is very effective to handle conflicts between different stakeholders.</td>
</tr>
<tr>
<td>11</td>
<td>JAD</td>
<td>[5, 40, 41, 46]</td>
<td>Group/Elicitation</td>
<td>JAD helps in making rapid decision and mostly used in business analysis.</td>
</tr>
<tr>
<td>12</td>
<td>Surveys</td>
<td>[40, 41, 47, 48]</td>
<td>Classic/Elicitation</td>
<td>They are used to collect data from large number of population.</td>
</tr>
<tr>
<td>13</td>
<td>Workshop</td>
<td>[5, 41, 48]</td>
<td>Group/Elicitation</td>
<td>It is a small meeting between stakeholders for capturing large and complex requirements.</td>
</tr>
<tr>
<td>14</td>
<td>Ethnography</td>
<td>[40, 41, 43, 49]</td>
<td>Contextual</td>
<td>It is useful in capturing contextual factors such as usability.</td>
</tr>
</tbody>
</table>
2) Building a Multiple Linear Regression (MLR) Model:
As this study is an exploratory study to find out which attributes can positively impact the elicitation techniques selection process, it is appropriate for a multiple regression analysis, where the relationship between multiple independent variables (attributes influencing technique selection) and the dependent variable (degree of influence on techniques selection process) is determined. Based on the Eq. (2), the multiple linear regressions model can be expressed as follows:

\[ y (DITSP) = \beta_0 + \beta_1 CT_1 + \beta_2 CT_2 + \cdots + \beta_{12} CT_{12} \quad (3) \]

Where:
- \( y (DITSP) \): is Degree of Influence in Techniques Selection Process (dependent variables)
- \( \beta_0 \): is the y-intercept
- \( \beta_i \): is the regression coefficient
- \( CT_i \): is the Candidate Attribute

3) Data Analysis and Results: In this basic analysis, there were only three main tables presented to provide useful information about the model and the contribution of each explanatory variable. The first table of interest is the Model Summary table (Fig. 5). This table provides the multiple correlation coefficient (R) which is 0.997, coefficient of determination (R²) which is 0.994, and finally adjusted R square (R²) which is equal to 0.819. This indicates that 81.9% of the variance in the dependent variable (DITSP) can be explained by the independent variables (selected attributes), while the rest (18.1%) is explained by other causes. In other words, the elicitation technique selection process is strongly related to the selected attributes of elicitor, stakeholders, project, and elicitation process.

ANOVA table (Fig. 6) shows an analysis of variance that provides information about levels of variability within a regression model and its explanatory power. The F value and the associated significance value in the ANOVA table indicate the statistical significance of the multiple regression model. For this model, the p value for F statistic is lower than 0.05 (p=0.014). This means that the multiple regression model is generally acceptable and statistically significant to determine the most important attributes that influence elicitation techniques selection.

![Figure 5: Regression Statistics](https://sites.google.com/site/ijcsis/)

<table>
<thead>
<tr>
<th>No.</th>
<th>Attribute ID</th>
<th>Attribute Name</th>
<th>Coefficients</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CT12</td>
<td>Cost available</td>
<td>1.767400</td>
<td>Project</td>
</tr>
<tr>
<td>2</td>
<td>CT2</td>
<td>Understanding domain knowledge</td>
<td>1.674401</td>
<td>Elicitor</td>
</tr>
<tr>
<td>3</td>
<td>CT13</td>
<td>Time constraints</td>
<td>1.640012</td>
<td>Project</td>
</tr>
<tr>
<td>4</td>
<td>CT15</td>
<td>Clarity of project scope</td>
<td>1.621395</td>
<td>Project</td>
</tr>
<tr>
<td>5</td>
<td>CT7</td>
<td>Expertise</td>
<td>1.547981</td>
<td>Stakeholder</td>
</tr>
<tr>
<td>6</td>
<td>CT9</td>
<td>Stakeholders conflicts</td>
<td>1.547654</td>
<td>Stakeholder</td>
</tr>
<tr>
<td>7</td>
<td>CT11</td>
<td>Requirements engineering experience</td>
<td>1.516518</td>
<td>Elicitor</td>
</tr>
<tr>
<td>8</td>
<td>CT4</td>
<td>Number of individuals in the process</td>
<td>1.200577</td>
<td>Stakeholder</td>
</tr>
<tr>
<td>9</td>
<td>CT6</td>
<td>Process time</td>
<td>1.151091</td>
<td>Elicitation Process</td>
</tr>
<tr>
<td>10</td>
<td>CT6</td>
<td>Availability of time</td>
<td>1.057823</td>
<td>Stakeholder</td>
</tr>
<tr>
<td>11</td>
<td>CT10</td>
<td>Project complexity</td>
<td>0.993972</td>
<td>Project</td>
</tr>
</tbody>
</table>

![Figure 6: NOVA Analysis](https://sites.google.com/site/ijcsis/)
4) **The Proposed Algorithm of the MLR Analysis:** This section presents an algorithm for identifying the critical attributes that influence the process of elicitation techniques selection by a multiple regression analysis. Fig. 8 shows the flow chart of the proposed algorithm. The steps of the proposed algorithm are as follows:

1. Start

2. Determine the dependent variable (degree of influence on techniques selection process) and the independent variables (attributes influencing techniques selection).

3. Build the multiple linear regression model based on the general equation of MLR.

4. Estimate the MLR model.

5. Check the value of the adjusted R square ($R^2$) to measure how much of the variability in the dependent variable that is accounted for by the independent variables.

6. Test whether the regression model is statistically significant to determine the critical attributes influencing techniques selection by an analysis of variance (ANOVA).

7. If significance $F > 0.05$
   
   ```
   
   - Update the explanatory variables
   - Estimate the model
   ```
   
   Else
   
   ```
   
   - Accept the model
   ```

8. Check the P-values for each variable to identify which attributes are significant.

9. If P-Value > 0.05
   
   ```
   
   - Reject the attribute
   ```
   
   Else
   
   ```
   
   - Include the attribute in the critical list of influential attributes
   ```

10. End

---

**Figure 8: Flow Chart of the Proposed Algorithm for MLR Model**

---

**C. Artificial Neural Network Based Model for Elicitation Techniques Selection**

This section presents a neural network based model for selection of requirements elicitation techniques. The ANN model was implemented using Neural Network Fitting Tool in MATLAB. The data collection, ANN architecture, training the network, evaluating its performance and proposed algorithm of ANN model are described in the following sub sections.
1) Data Collection and Preprocessing: Data Collection and preparation is the first step in designing ANN model. The research’s targets were software engineers in different software development companies. For this study, the data was gathered by a survey sent out via e-mail from February to May 2016. About 300 surveys were sent to the companies. The returned questionnaires were 160, which indicated a response rate of 53.33%. After data collection, the data preprocessing was conducted to train the ANN.

All the data was normalized using min-max normalization to speed up the training phase. Min-max normalization performs a linear transformation on the original data values. Suppose that \( \min_T \) and \( \max_T \) are the minimum and maximum values of an attribute \( T \). It maps value \( v \) of \( T \) to \( v' \) in the range [0.0-1.0] using the following formula [50]:

\[
v' = \frac{v - \min_T}{\max_T - \min_T}
\] (4)

2) ANN Modeling: In this paper, a feed-forward back propagation network is proposed to predict suitable elicitation techniques for a given project. It consists of three layers: the input layer, one or more hidden layers, and the output layer. The inputs to the neural network are influential attributes presented in Table 4. The output is a combination of appropriate elicitation techniques. The properties of ANN proposed in this paper are presented in Table 5.

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Hidden Layer</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hidden Neurons</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Input Neurons</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Output Neurons</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td>Levenberg-Marquardt</td>
<td></td>
</tr>
<tr>
<td>Training Function</td>
<td>TRAINLM</td>
<td></td>
</tr>
<tr>
<td>Transfer Function</td>
<td>TANSIG</td>
<td></td>
</tr>
</tbody>
</table>

3) Network Training: The neural network was trained by 160 data records. For this research, 100 out of 160 records were considered for the training set, 30 for the validation set and the remaining 30 for the test set. The network was tested by investigating different numbers of neurons (i.e., 12, 20, 25, 28 and 32) in hidden layer(s) in order to select the best structure of the network. The best results were obtained from the network with 11 inputs, 20 neurons in the hidden layer and 14 outputs as shown in Fig. 9.

4) Performance Evaluation: In order to assess the model accuracy, it is necessary to use some quantitative measures of learning. In this study, the Mean Squared Error (MSE) and regression analysis were used to evaluate the model performance. MSE is a useful measure of success for numeric prediction and is calculated using Eq. (5). It is worth mentioning that small values of MSE indicate better performance of the ANN model. It was found that the optimum performance of the model is at 25 neurons with MSE 0.1481. The accuracy of the model with different neurons is presented in Table 6.

\[
MSE = \frac{1}{N} \sum_{i=1}^{P} (t_{ij} - y_{ij})^2
\] (5)

Where \( P \) is the number of output possessing elements, \( N \) is the number of observations, \( t_{ij} \) are the target outputs and \( y_{ij} \) are the actual outputs.

<table>
<thead>
<tr>
<th>Neurons in the Hidden Layers</th>
<th>MSE Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>0.3263</td>
</tr>
<tr>
<td>20</td>
<td>0.1652</td>
</tr>
<tr>
<td>25</td>
<td>0.2672</td>
</tr>
<tr>
<td>28</td>
<td>0.2870</td>
</tr>
<tr>
<td>32</td>
<td>0.6301</td>
</tr>
</tbody>
</table>
Fig. 11 shows the regression analysis of targets and outputs for Levenberg-Marquardt algorithm during training and testing process. The best fit lines in Fig. 11 demonstrate the relationship between the desired value and actual value. As shown in Fig. 11 the R value of ANN model is 0.8134 which indicates that LM algorithm has high ability to train data for the model. Overall, the network has an accuracy of 81%.

Figure 11: Neural Network Regression Analysis

5) The Proposed Algorithm of Neural Network Based Model for Elicitation Technique Selection: This section presents an algorithm of neural network based model for selection of requirements elicitation techniques. Fig. 12 shows the flow chart of the proposed algorithm. The steps of the proposed algorithm are as follows:

1. Start
2. Normalize the input data using min-max normalization in the range [0.0-1.0].
3. Divide the data set into training, test, and validate.
4. Create the neural network initially with $N$ inputs, $H$ neurons in the hidden layer(s) and $O$ outputs.
5. Train the neural network using Levenberg-Marquardt algorithm.
6. If MSE is small
   
   - Save the neural network
   
   Else
   
   - Update the weights and bias between input and hidden layers.
   - Modify the number of neurons in the hidden layers.

7. Test and validate the network to check out the model accuracy.
8. Use the trained and verified network for predicting suitable combination of elicitation techniques for a given project.

Figure 12: Flow Chart for the Proposed Algorithm of ANN Model

V. CASE STUDY

In order to empirically validate our ANN model a case study in a software company X was conducted. One project was selected for the case study. One of the problems of the selected project is that the techniques selection procedures are based on elicitor experience. The aim of this case study is to check whether the proposed ANN model predicts more effective techniques than the current requirements engineering methods. The contextual situation of the selected project that is the particular values for the influential attributes is shown in Table 7. Table 8 shows the normalized values calculated using Eq. (4) for each attribute. These normalized values are considered the input data for the ANN model.
The goal of the project was to develop an Android mobile application that enables users to scan their physical documents using their smart devices camera, then crop, enhance, sync, share, store and manage these documents as needed.

The result of ANN model is shown in matrix R. The result is analyzed as ‘1’ in the output vector corresponds to the elicitation technique that is selected for the elicitation process while ‘0’ in the output vector corresponds to the elicitation technique that is rejected to use in the elicitation process. As a result, the ANN model recommended the following techniques: interviews, task observation, card storing/laddering, questionnaires, repertory grid, focus group and ethnography.

VI. CONCLUSION AND FUTURE WORK

This paper proposed an approach to help requirements engineers in selecting the most suitable elicitation techniques for a particular project. To do this, the literature review was conducted to identify the attributes which are relevant to the context of the elicitation process and influence techniques selection. Then, these candidate attributes were analyzed using a multiple regression model to find the most important attributes that influence techniques selection and eliminate the less critical ones. Finally, a neural network based model for elicitation techniques selection was developed. In order to empirically validate our ANN model a case study was conducted. The results showed that the proposed ANN model has proven its effectiveness in selecting more effective techniques than the current requirements engineering methods. It is recommended as a future work to integrate other machine learning techniques such as fuzzy logic with the proposed ANN model in order to enhance the model accuracy.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
R = \begin{bmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}
\]

The references are as follows:


Abstract—Proxy Re-Encryption has been used since the need for forwarding an encrypted message to a party for whom it was not encrypted was highlighted in the form of delegation rights by Blaise, Bleumer and Strauss. Various Proxy Re-Encryption schemes have been introduced till today mainly focusing on demonstrating features like transitivity and collusion-resistance to ensure minimal trust on the proxy and maximum key-privacy. This survey highlights some major schemes introduced, classifies them based on their directionality, brings to light their major advantages and disadvantages, and provides a detailed comparative study based on the key features a Proxy Re-Encryption Scheme must possess in order for its widespread. 

Index words—bilinear maps, CCA secure, collusion resistance, CPA secure, delegation rights, Diffie-Hellman key exchange, DBDH assumptions, Proxy Re-Encryption; transitivity.

1. INTRODUCTION

Considering the direction of development from traditional sequential systems towards distributed systems, cloud computing where different computational infrastructures are available to the users as services (infrastructure as a service, platform as a service, software as a service etc), IOT; security and privacy of data has become the primary concern of organizations and users worldwide because these developments require an unavoidable sharing of resources, personal and confidential data over the network. Although network security schemes have been implemented and provide access and authorization controls, need still remains of further improvement. Proxy re-encryption is a relatively new data encryption technique devised primarily for distributed data and file security. The goal of proxy re-encryption is allowing the re-encryption of one cipher text to another cipher text without relying or trusting the third party that performs the transfer. In situations where one user wishes for another user to decrypt a message using its own or a new secret key instead of the first user’s secret key, one technique involves the assistance of a proxy. An easily implemented re-encryption scheme is one in which the proxy is given possession of both Users’ keys so the message can be converted to plaintext and then re-encrypted for the second user but this is comparatively weak. User1’s secret key decrypts the cipher-text to plaintext, while User2’s secret key encrypts it. But this is a violation of the primary goal of security; the purpose of proxy re-encryption schemes is to prevent the revelation of the keys involved in re-encryption and the plaintext that needs to be re-encrypted to the proxy. In this context the method mentioned above is not ideal. So for these scenarios where trust cannot be placed in a proxy, the requirement here is to convert messages encrypted under User1’s public key to messages encrypted under User2’s public key without the proxy being able to decrypt the message. The scheme that ensures this arrangement is known as proxy re-encryption. Even though Proxy re-encryption schemes are basically a version of existing encryption schemes consisting of selection of text, generation of keys, sharing or transmitting of keys between concerned parties, conversion from plaintext to cipher-text on one end and conversion from cipher-text to plaintext on the other end, the difference arises with the introduction of two more properties.

Directionality

If the re-encryption scheme is reversible—that is, the same re-encryption key is used to translate messages from User1 to User2, as well as from User2 to User1 the scheme is classified as a bi-directional scheme. In these schemes if a user forwards a message to another, it automatically gives rights to the receiver to communicate with the sender. Such re-encryption keys are hence generated with the keys of both sender and receiver and with their mutual trust and consent. A unidirectional scheme is one-way in this context; giving a higher level of security and making it a feasible option in non-trusted setups where message conveying is essential but not to an extent where receiver should be given rights to respond to it. So if a message is re-encrypted from User1 to User2 with a key, it cannot be used for re-encryption from User2 to User1. Moreover uni-directional schemes are more useful since they can be converted to bidirectional scheme at any time simply by running it in both directions, i.e. from User1 to User2 and from User2 to User1 [14].

Transitivity

Fig.1. Representation of Proxy Re-Encryption
Transitivity in proxy re-encryption schemes is defined as the number of re-encryptions allowed by an algorithm. A transitive PRE scheme would allow a cipher text to be re-encrypted from User1 to User2, and then again from User2 to User3 and so on. While a non-transitive scheme would allow a cipher text to be re-encrypted for a single time (or a pre-defined limited number). This implies that in non-transitive schemes the proxy does not have the authority to assign delegation rights to others beside the pair of communicating users. Besides the above mentioned properties, some more of the security properties demonstrated by existing proxy re-encryption schemes are [3] the inability of the proxy to view plaintext irrespective of the scheme. The secret keys are generated at the data owner’s end, and the proxy in no way can derive the secret keys of the sender or receiver from the re-encryption key. The transitivity and delegation level of an applied scheme depends on the trust matrix of the involved parties, on the fact level of security at each party’s end and the priorities of the involved parties (security, confidentiality, integrity, etc). The need of PRE schemes was first highlighted when Mambo and Okamoto in 1997 mentioned the concept of delegating decryption rights to improve efficiency instead of the conventional decrypt-and-then-encrypt approaches. [2] This work was enhanced by Blaze, Bleumer, and Strauss (BBS) in 1998 when they proposed an application called atomic proxy re-encryption. In their proposed scheme a partially-trusted proxy was allowed to perform conversion from a cipher-text for one user into a cipher-text for another user but was not allowed to access the underlying plaintext. [1]

Although efficiently computable, flexible and applicable the adoption of BBS re-encryption over a larger application domain for managing encrypted file systems has been hindered by considerable security risks. [4] These methods are still under process of maturity and require fine tuning before being adopted in every organization.

II. CLASSIFICATION AND ANALYSIS OF PROXY RE-ENCRYPTION SCHEMES

Fig. 2. Classification of Proxy Re-Encryption Schemes Based on Directionality
A. Type and Identity Based Proxy Re-encryption Scheme

This scheme has thrown light on the problem of multiple delegations of decryption rights. Suppose the delegator wants two different users to view different sub parts of his message. The solution would be to place trust in the proxy to re-encrypt the selective parts of the cipher-texts using this method. This fails if the proxy is corrupted. A better but unrealistic alternative is choosing a separate pair of keys for each delegate. The type-and-identity-based proxy re-encryption scheme is based on the Boneh-Franklin Identity Based Encryption scheme [19] enabling implementation of different access control policies for cipher-texts against multiple receivers. The messages are categorized into different types according to the decryption rights of the intended receivers. The main benefit of this scheme is the single pair of keys which provides re-encryption capability to the proxy for his cipher-texts against his receivers. But the proposed scheme works only for the cipher-texts generated by the sender.

The method is described as follows:

Users categorize their messages into different types

Setup and Encrypt are the same as in the Boneh-Franklin scheme

Re-Encrypt(msg,type,msg_id) : the algorithm outputs the cipher-text ‘sub_msg’ = (msg1,msg2,msg3) based on the message and the type given by user. Each sub message is meant to be decrypted by the respective receiver and no one else.

Decrypt(sub_msg,skid) : Given a cipher-text ‘sub_msg’ = (msg1,msg2,msg3), the algorithm outputs the message ‘msg’ based on the ‘skid’ of the receiver. Hence every receiver gets the sub message intended for him and nothing more. [7] Another scheme and its construction is discussed in [15] based entirely on type of the user is also discussed and its various versions are implemented.

B. Conditional Proxy Re-encryption Scheme

In situation where fine-grained delegation is required requiring fulfillment of a predetermined condition, the notion of conditional proxy re-encryption (or C-PRE) was introduced, whereby only cipher-text satisfying one condition set by Sender is allowed to be transformed and then decrypted by receiver. The scheme is proven to be CCA-secure. The scheme is now improved to work based on multiple conditions rather than one as was its initial version. The conditions can be anything specified by the involved parties and the construction of the algorithm. They can be a set of pre-defined integers, the sending or receiving conditions of the parties, the physical location of the sender or the receiver. The message to be sent is encrypted using the receiver’s public key and the condition. Similarly to decrypt the message the receiver should meet the pre-defined conditions.

The challenge now remains to construct CCA-secure C-PRE schemes with anonymous conditions rather than known predefined conditions. [10]

C. Attribute Based Proxy Encryption Scheme

The Attribute based proxy re-encryption schemes provide a better option especially when impersonating a user is an active issue. Moreover the problem of authentication of a user is easily solved by this. Attribute based PRE involves various user attributes like city, country, street number, GPS coordinates, or any other set of attributes that are predefined while encryption. When a user possesses these attributes only then is the decryption of a message possible and allowed. The identification of these attributes is based on a certain threshold i.e. if the attributes of the receiver match the required attribute set by a certain degree or level, the decryption access is granted and the message can be decrypted by only using these attributes and the secret key. So even if a single attribute doesn’t meet the threshold the whole decryption fails. This is a general scheme whose various modifications exist, namely Cipher-Text policy attribute based encryption and Key policy attribute based encryption which are widely implemented. This mechanism is joined with the proxy re-encryption and implemented in various categories.

D. Key Private Proxy Re-encryption Scheme

Key Private Proxy Re-Encryption also known as Anonymous Proxy Re-Encryption introduces the notion of keeping the keys private such that even the proxy that performs the transformation of message cannot identify or differentiate between the involved users. None of the early PRE schemes provided key security. This scheme is CPA-secure but work is still in progress regarding CCA-safe key private PRE schemes. If a proxy communicates with multiple users it should not be able to reveal to a user what other parties are communicating with it from the message being transmitted or the set of re-encryption keys available. This information should not lead to the users. The necessity and benefit of a key private scheme is that nobody can detect who has access to a certain message i.e. complete anonymity of the users involved in a communication. [9]

E. Ciphertext-Policy Attribute based Proxy Re-encryption:

Ciphertext-Policy ABPRE is a joint construction of attribute-based encryption and traditional proxy re-encryption scheme. It is proven to be secure against CPA. It is a type of ABE where the key is associated
with an access structure namely a group of attributes defining the type of user that should be given access and decryption rights. This solves the issue of multiple users and key distribution over a large audience. Key management creates an overhead in such situations and this algorithm is beneficial in this context. Recent variations of this algorithm are proven secure against chosen ciphertext attacks under decisional q-parallel BDH assumption [11]. This algorithm has widespread applications in medical domains where patient records are continuously being transferred and referred from one doctor or facility to another. It provides a fine grained access control to the user over the delegates enabling it to specify who can decipher the data or message by setting with it a set of attributes [13]. CP – ABPRE scheme is a collusion resistant uni-directional scheme and is associated with a monotonic access structure. A CCA secure version of CP-ABPRE is also constructed in [16].

F. Time/Clock Based Proxy Re-encryption Scheme
A cloud environment is composed of several independent servers communicating to provide services. In a time based re-encryption scheme, each cloud server is allowed to independently re-encrypt data automatically in contrast to the previous methods where the data was encrypted only after receiving a command from the sender [18]. This allows an automatic re-encryption of data based on the internal time of the cloud servers rather than by manual commands. The data is associated with a control structure for defining access and a time for which the access is granted [18]. Hence every piece of data stored in the cloud is associated with a set of attributes that define the type of user the data is meant for and a time structure which basically specifies the time limit for which the data will be accessible to the user. The receiver is issued keys that become effective during the specified access times, implying that the receiver can decrypt the message using only those keys which match the access time. The data owner and the Cloud Service Provider share the secret key. This key is later used to create sub-keys for the users and when re-encrypting the data along with the clock time of the system. This combination of access structure facilitates user revocation and distribution of delegation rights. The algorithm is based on the Bilinear Deffie-Hellman assumption like most proxy re-encryption schemes. The algorithm operates in the following mechanism. First the algorithm is setup by generating the master key, public key and defining a universal attribute set from which the individual attributes will be late selected. Then the CSP identifies all its users and generates secret keys for them based on their attribute sets. The data is then encrypted based on the above mentioned access structure. Now when a user requests for a certain data, it is re-encrypted with the internal time of the system, hence setting up a valid access time for decryption by the user. Therefore a user satisfying the access structure i.e. the attribute set can successfully attempt decryption if the time hasn’t expired [6].

G. Threshold Proxy Re-encryption Scheme
There are three problems in a decentralized cloud storage system. First, high level of traffic between the user and storage servers leads to more computation by the user. Second, key management becomes a problem for the user because security is broken if the user’s keys are compromise. Thirdly, directly forwarding a user’s messages to another one is not feasible.

The proposed system is constructed around the proposed scheme named Threshold Proxy Re-Encryption. In the beginning the cloud storage system stores user details in some database. The user needs to get registered in the database, by entering his data like user_name, user_gender, user_location, user_password, user_birthdate, and user_e-mail address. The user then logs into the system using his credentials that were initially registered. The file is forward contained in a folder along with the user and recipients name, a security question for decryption access, the file containing the key for decryption and the status of the message. The file is transferred using the receiver’s email and public key. After the file is received by the receiver, the selected file is downloaded. But before downloading the file, he has to download the key file that was sent in the same folder. In order to download the key file, receiver has to enter the following details like file name, the secure question and its answer. Now the key is revealed to the receiver with which the message can be downloaded and decrypted. [8]

ANALYSIS
Type Based PRE provides semantic security and cipher-text privacy control but on the other hand encoding operations over encrypted messages is not possible limiting its widespread use. Key-Private PRE provides security against Chosen cipher-text Attack but the privacy proof of this scheme is more difficult than Chosen plaintext attack. Identity-based PRE is secure against an adaptive CCA but it is difficult to find such constructions for the algorithm that are multi-use, efficient and CCA secured.
Ciphertext Policy Attribute-Based PRE provides a fine grained access control over data by limiting the decryption writes based on various attributes of the
receiver but it has an average efficiency and flexibility compared to the other schemes. Conditional PRE schemes provide a very efficient mechanism against CCA but it is very difficult to design C-PRE schemes that are CCA secure. Time based PRE is a more recent modification of PRE schemes which provides a scalable user revocation and reduces the workload of data owners. The major disadvantage of this scheme is that it requires the effective time period to be same for all attributes associated with the user. Threshold PRE enables data forwarding efficiently but it requires very high access control which becomes difficult to provide.

III. APPLICATIONS OF PRE

Proxy re-encryption has many exciting applications in addition to the previous proposals [Blaze et al. 1998; Dodis and Ivan 2003[5]; Jakobsson 1999; Zhou et al. 2004] for performing cryptographic operations on storage-limited devices, law enforcement and most commonly in email forwarding. In particular, proxy cryptography has a natural application to secure network file storage:

Secure File Systems: A secure file system is the most obvious application of proxy re-encryption because we always assume that a storage system will be non-trusted and in PRE the goal is to use a non-trusted or partially trusted party for re-encryption but avoid any harm to data.

Outsourced Filtering of Encrypted Spam: The filtering of encrypted emails performed by freelancing contractors which is a requirement due to spamming and hoaxing performed by hackers and trouble makers is an application of proxy re-encryption that is equally applicable but less known. The amount of such emails has overwhelmed the filtering capacity of many small businesses. This has lead to a potential market for email filtering outsourcing. The advancement in techniques used by these hackers has rendered basic filtering measure useless. With the help of proxy re-encryption, incoming encrypted email can be forwarded to an external contractor for filtering at the first email gateway, without any risk of exposure of the underlying plaintexts. [4] This survey discusses in detail the various PRE schemes introduced till now starting from Mambo and Okamoto [2], their pros and cons and applications of each in respective fields.

IV. COMPARATIVE STUDY

The following table shows a comparative study of the PRE schemes discussed above based on the properties of directionality, multi-use, transitivity, interactivity, security, key-privacy, collusion resistance, and the assumption on which the algorithm is built:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unidirectional/Bidirectional</td>
<td>Bi</td>
<td>Uni</td>
<td>Uni</td>
<td>Uni</td>
<td>Uni</td>
<td>Bi</td>
<td>Uni</td>
</tr>
<tr>
<td>Multiple-use</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Transitivity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Non-Interactive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Key-private</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Collusion-resistant</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fine-grained delegation</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ciphertext-private</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key-pairs</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Secure against</td>
<td>CPA,CCA</td>
<td>CPA(if multi-use), CCA(if single use)</td>
<td>CPA</td>
<td>CCA</td>
<td>CPA</td>
<td>CPA</td>
<td>CPA, CCA</td>
</tr>
<tr>
<td>Assumption</td>
<td>DBDH, Co BDH</td>
<td>DBDH</td>
<td>DBDH</td>
<td>3-quotient BDH</td>
<td>BDH</td>
<td>-</td>
<td>Decisional q-parallel BDH</td>
</tr>
</tbody>
</table>
V. CONCLUSION

This paper briefly discusses various proxy re-encryption schemes, their general mechanism and implementation. They are then broadly classified based on directionality and a comparison is given after analyzing the schemes for traits that should be a part of every successful proxy re-encryption algorithm.

Future work on proxy re-encryption should include features of key-privacy and transitivity. Since most schemes are collusion resistant and key-private but an efficient mechanism also providing transitivity is missing.

REFERENCES


Anum Khurshid was born on 11th February 1992 in KPK, Pakistan. She did her BS in Computer Science from COMSATS Institute of Information Technology, Abbottabad. She is currently a student of MS in Computer Science in COMSATS Institute of Information Technology, Abbottabad.

Dr. Fiaz Gul was born on 22-11-1982, in a beautiful valley Abbottabad of KPK. He did graduation and MS from COMSATS Institute of Information Technology Abbottabad in the field of Computer Science. For specialization master and Doctorate he won the HEC scholarship under the project UESTP for Politecnico di Torino Italy. Currently he is serving as an Assistant Professor in Computer Science Department at COMSATS Abbottabad, Pakistan.

Dr. Abdul Nasir did PhD, University of Malaya, Kuala Lumpur, Malaysia, 2014. His Field of Specialization: Wireless Network, Cloud Computing, and Mobile Computing Security and Privacy. He is currently assistant Professor in Computer Science Department at COMSATS Institute of Information Technology, Abbottabad, Pakistan.
Owais Khan, Fiaz Gul Khan, Babar Nazir, Usman Wazir

Abstract—WSN is an evolving technology since last ten years. As wireless nodes work have less power supply in the form of a battery, it is necessary for the nodes to work for maximum time. Different techniques are adopted to achieve better energy optimization. This paper presents a survey on energy efficient routing techniques, which will help in understanding the factors which affect energy efficiency and other performance parameters and will help to analyse the techniques for further optimizations.


I. INTRODUCTION

The great advance and inventions in computer hardware and software technology has the industry to create very small components, chips and this advancement created small sensor nodes which operate on low cost batteries. They have computational, sensing and transmitting components which capture data from vast environment and send it to a master node or sink node. This network is called wireless sensor network. The nodes have the ability to communicating with each other and also directly with BS. Sensor networks are gaining popularity since last decade and a lot of research work is going on in different WSN domains i.e. routing, scalability, network life time, data integrity and security etc. WSNs are largely adopted by industries and organizations like health care, agriculture and environment, military operations, safety and security, transport systems etc. WSNs are useful because of its low cost deployment and energy consumptions. However, energy consumption is considered to be the main problem as there are certain constraints on energy saving and computation in nodes.

In WSNs, nodes are deployed in an environment to gather data. The node deployment, number of nodes to be deployed depends on the kind of application for which WSN is being used. Nodes are either deployed in a specific order and position or they are deployed accordingly [2]. WSNs adopt different techniques to optimize energy consumption. Some of these techniques are radio optimization, data reduction, sleep/wake up schemes and routing protocols, battery replication [1]. This paper will present a survey on routing protocols. Routing can be optimized in so many different manners to optimize energy. Lots of work has been done in routing protocols for WSN. The main area or task in WSNs which consumes energy is the transmission phase. Routing can be manipulated in different ways to decrease energy consumption. This paper will present a survey on hierarchical routing protocols. Hierarchical approach use clustering of nodes which decrease communication distance, aggregate data, increase network life, minimize number of transmissions, thus decreasing energy consumption [3]. Let’s discuss some main challenges in routing protocol of WSNs. Node deployment either random or in specific order, data collection (time-driven, event driven or query driven), integrity of data while consuming minimum energy, network life [1]. Hierarchical protocols are further divided into sub categories which are grid based, chain based, tree based and area based. Different hierarchical techniques, their advantages and disadvantages will be studies in section 2. The composition and format of overall paper is as follows. In section 3, these techniques will be compared and their comparative analysis will be done against some parameters. In this section 4, the techniques will be analyzed in such a way that which technique is most suitable for a certain category of application. This section will also present trade-offs between different performances parameters. In 5th section, the problems addressed in section 2, will be given with some possible solutions, the section may also include some future work regarding the field. Section 5, will present some related work and in section 6, the paper will be concluded.

The paper will present an analysis of these techniques in section 1. Some problems in these techniques will be discussed. E.g. coverage and nodes heterogeneity problem in LEACH protocol, network-life problem in PEGASIS, some hybrid techniques will be discussed through which more energy consumption can be optimized along with performance improvement of other parameters like convergence time, scalability etc. The
classification of routing protocols in WSNs are shown in fig 1 and 2.

**Fig: 1. Overall Routing Techniques in WSNs**

**Fig: 2. Hierarchical Routing Techniques**

**DIFFERENT HEIRARCHICAL ROUTING TECHNIQUES**

1. **Cluster-based Routing**
   In routing protocols of this category, the nodes form groups, with each group having a master node called cluster Head i.e. CH which is responsible for collecting data from all its group members, aggregate it and send it to the sink node where as in common method, the nodes either transfer the data directly to sink or send to other nodes along the path to the sink. This clustering has an advantage of less range of transmissions as nodes does no communicate with a distant Base Station (BS) or sink node but they communicate with their respective CH which in turn sends data to the sink, Thus reducing the length of transmissions for most of the node. The following are some of the widely used cluster-based protocols used in WSNs.

1.1 **LEACH (Low-energy adaptive clustering hierarchy) and LEACH-C**
   This is the most popular of all hierarchical routing algorithms. In this protocol, the nodes form a cluster with a master node as described above. But if a node remains master node for a long time, its battery will deplete very quickie which will reduce network life, for this purpose, the CH is changed randomly for each round. A round means when a CH collects data from all nodes and send it to BS. In this manner, the power consumption is distributed and balanced. It minimizes energy efficiency by reducing transmission range as the node communicate with CH, instead of directly communicating with BS. Similarly data is aggregated which results in more energy optimization. The process of formation of cluster and CH selection is carried out in the following manner. When a round starts, every node compete for CH. CH is selected on certain criteria, which is (i) how many CHs are required for this system i.e. how many groups need to be created (ii) how many time a node has been selected as CH before. For this, the nodes use the following equation.

\[
T(n) = \begin{cases} 
\frac{p}{1 - p \left( \frac{r \mod \frac{1}{p}}{p} \right)} & \text{if } n \in G \\
0 & \text{other wise}
\end{cases}
\]

Where G represents all nodes, each G chooses 1 or 0, if the selected number is less the above threshold, it is selected as CH. After selection of CH, the nodes connect themselves to the nearest CH, depending on the signal power of CH and thus forms a cluster. This s technique has the benefits of less range of transmissions, load balancing and data aggregation, however it suffers from some problems i.e. in nodes distribution, if one CH has more nodes than the other, this CH will consume more energy comparatively. For this, the clusters need to be almost uniform with respect to number of nodes. This problem can be solved easily for applications with fixed topologies but for other applications, it is comparatively difficult to make the clusters uniform. Another problem is, when there are CHs very near to each other i.e. coverage problem, if these two cluster act as a single cluster, they will consume less energy as compared to two clusters, in other words, we can say that the CH should have some minimum distance in order to create minimum clusters in the system. For above given problems, some possible solutions are discussed in section 3 of this paper.

A variation of LEACH is LEACH-C (Centralized LEACH) which solves the problem of CH selection and coverage in its own way. The BS is selected by BS in the start. This is a proactive approach for topology creation. In the start, BS receives location and residual energy information of all nodes.
BS calculates average energy for a set of nodes and the node having lower energy than the average is removed from nominated list of CHs. BS uses annealing algorithm for cluster formation y minimizing sum of squared distance between nodes and CH. As in LEACH and LEACH-C, CHs have to communicate with all of the nodes, so they use TDMA scheme for communication with all of the nodes [2].

1.2 TEEN (Threshold sensitive energy efficient protocols) and APTEEN (Adaptive TEEN)
This is another cluster-based routing protocol and forms cluster by the mechanism mentioned in LEACH. But unlike LEACH and LEACH-C, this is a reactive protocol. The nodes in this technique are almost in sleep mode and whenever there is a sudden change in the parameters of sensed data, the nodes become active and collect data. TEEN and APTEEN uses some threshold parameters to make the nodes active. Two types of thresholds are used, hard threshold, in which there is a specific limit for the value change and when that change occurs, the node must become active. Another is soft threshold, in which a little change in value attributes cause the nodes to become active. The threshold attributes are provided to all nodes by the CH once it is selected [2].

TEEN is having a problem, as TEEN only send data whenever any of the above threshold is met, otherwise the nodes will remain in the state of sleep and there will be no information about network condition or topology. Similarly, one cannot find out if the system is up or not. This problem was solved in APTEEN which uses the above thresholds for node activation, as well as it periodically sends data to the BS, giving a snapshot of the network. In this manner, it works as a proactive as well as in reactive manner. TEEN and APTEEN also uses TDMA just like LEACH and LEACH-C.

TEEN and APTEEN can be combined used with some other protocols and performance of multiple parameters can be achieved [2]. Some suggestions are given in section 3 of the paper.

1.3 Energy Aware routing Protocol (EAP)
This technique provides another way for CH selection and area coverage. Its uses address tables with each node to know about their neighbors. Every node broadcast E-message to other nodes and calculate distance from each other. Apart from this, the residual energy is also considered before the selection of CH. This method uses inter-cluster and intra-cluster information to achieve better energy optimization.

2. Chain-Based Routing

In Chain-Based Routing, the nodes form chain or chains in the network with a leader node at random position for each round. The data from nodes travels along the chain to the leader node which aggregate and sends the data to BS or sink node. The main advantages of this topology is that its topology is very easy to construct, similarly, as the data is transmitted to neighbor nodes. So transmission distance is less, thus consuming less energy. The main drawback in chain-based routing is that if a single node in the chain fails, the whole network fails. Following are the some chain-based routing techniques with some problems mentioned.

2.1 PEGASIS (Power Efficient Gathering in Sensor Information System):
In this technique, chain is formed and data travels along the chain as mentioned above. The leader nodes position changes for each round, so energy consumption is divided among all the nodes. However, PEGASIS is suffer from the following problems:
(i) What if a node with lesser energy remaining is selected as leader node. (ii) If a leader node with maximum distance from BS is selected, causing delay [4]. Selection of node with minimum residual energy may reduce network life. Some of the possible solutions are proposed for above problems in section 3.

A hybrid technique is also proposed to increase network life time and consume lesser energy. For leader nodes, it is necessary to communicate directly with BS. So PEGASIS is more suitable for applications with fixed topology.

2.2 Concentric Clustering Scheme (CCS)
The topology of CCS is incredibly good and it also solves many problems of PEGASIS in its own way. CCS forms logical circular chains around BS, just like orbits around a nucleus of an atom. Each chain has a cluster head (CH), which gathers data from its member nodes. The nearest chain to BS is called level 1 chain, 2nd level is level 2 and so on. The distance problem between CH and BS in PEGASIS is solved in a way that the CH of higher level sends data to the lower level’s CH and so on. Data to BS is transmitted by the nearest CH, thus consuming less energy. However, it will also suffer a great transmission delay as data travels from higher level CH to lower level CH and then to BS. Also the nodes are nearest to BS suffers more energy depletion, as the whole data goes through these nodes to BS.

2.3 Energy-Balanced Chain Cluster Routing (EBCRP)
In this routing technique, the nodes are divided into rectangular clusters, the nodes in each rectangle or clusters form chain with CH. This CH collects data from all nodes and send it to BS. The energy is balanced in such a way that each CH will remain CH until all of its energy is depleted. This technique has three phase, (i) Cluster formation (through ladder algorithm) (ii) CH selection and (iii ) The steady state phase. Once a CH is selected and remains CH until it dies, this state is called steady state phase. After steady state phase, a new round is started and another node become CH.

This technique is suffer from transmission delay because of two reasons, if there are nodes (successive) far from each other. The other reason is the direct communication between CH and BS. A possible hybrid solution for this problem is given in section 3. (Multi-layered just like CCS).
2.4 Chain-based Hierarchical Routing Protocol (CHIRON)

It consists of four phases (i) group creation in which nodes are divided into fan-shaped areas. BS has the information about all the nodes and their residing groups (ii) chain-formation, this is done as follows, the farthest chain from BS is selected as start of the chain and the successive node connect to it and the successive node to second node attach to the next node and so on, creating a chain of nodes in each group (iii) leader selection, in the start, the farthest node is selected as chain leader, and then in the next round, the node with high residual energy is selected as chain leader. (iv) This is the data transmission phase, the data is first sent to chain leader which then forwards it to the next chain leader and then to the BS. In this way, CHIRON follows multi-hop and short haul transmission because the aggregated data flows through several chain leaders up to the BS. However, it the chain leader nearest to the BS will suffer from quick energy depletion and that is the drawback of CHIRON. The groups are also divided uneven which cause uneven energy consumption resulting in reducing network life.

3. Tree-Based hierarchical routing protocols

The topology of the nodes in this category form a tree like structure (logical). Data from leaf node goes up to parent nodes and then to their parents and son up to the root. This reduces data flooding and unnecessary data retransmissions as the data follows the same route. The energy consumption is minimized in a way that there is no such long distance communication as data is transmitted to immediate neighbors as in chain-based protocols. However this method also suffers from some drawbacks i.e. the topology is not robust, as data follows the same route or there is a single path from one node to root node. If a node in the path crashes, the overall network topology will have to be changed which will increase convergence time. It also suffers from uneven energy consumption and scalability problems. Some of tree-based hierarchical routing protocols are discussed below.

3.1 EADAT (Energy-Aware data Aggregation Tree):

The technique focuses on the issue of energy consumption considering energy aware data centric routing. The tree is created keeping the residual energy of every node in consideration. The tree construction is performed in the following manner, initially the sink node, which is also considered as root node, sends control message to every other node. Each node has a timer associated with it, lower the value of the timer, higher its residual energy is. A leaf node selects a node with higher residual energy and its shortest path to the sink and make that node its parent. This process continues up to sink until a full tree is constructed. When a node’s energy becomes less than some pre-determined threshold, it broadcasts help message to all other nodes and the shutdown, now the nodes attaches to it either as parents or child will create a new topology according to above mechanism [9].

The protocol is data centric in a way that the nodes with higher residual energy and shortest paths become more responsible and more data flows through them as compared to others, this increases network life as well as energy consumption is even around the system. But the mechanism described above for creating tree sometimes create a longer path than the real minimum path which causes transmission delay as well as more energy is consumed.

3.2 BAT (Balance Aggregation Tree)

In this technique, a balanced tree according to energy consumption of each node. This is created in such a way that initially the BS is considered as root node and it is assumed that it has information about the positions of all nodes. In the start, a minimum weighted edge is selected and as much as child nodes are connected to it, the new node is connected to tree, if a neighbor node is found, the node is called leaf node. In short, this technique creates a minimum spanning tree in which weight parameter for edges is the “energy dissipation” as cost. This technique achieves a good energy efficiency, however it does not consider the residual energy of nodes while creating tree, which can reduce network life [10].

3.3 ETR (Enhanced Routing tree)

This a modified and enhanced version of TR (Tree Routing) whose objective is to introduce balance between performance and cost.in this technique, a minimum cost path is created up to the sink for each node. This is done by using a table called “Neigh our Information Table” which has addresses of successive neighbors. Each node has this updated table. For path selection, ETR uses a parameter called “Network Depth” which is the hop-count from one node to the sink or sink to node. The value of “Network Depth” is 0 for root node and for the rest, it increases as a node comes in path. ETR selects shortest path i.e. minimum network depth value for each node to the sink. This protocol has many advantages as less range of transmission, shortest path selection but just like BATR, it also ignores residual energy which is great drawback in ETR.

4. Grid-Based Routing Protocols

In grid-based routing, the nodes the nodes are dispersed in given area on the basis of some geographical constraints that is why this is also called location-aware routing. The advantages of this category contain efficient data delivery as each node has a deterministic set of nodes to which it transfers data. However it suffers from load balancing as there may be more data in one grid than the other. Another problem is almost fixed routing is used in this type of routing, having no alternate routes, ignoring traffic or load considerations. Some of grid-based routing protocols are discussed below.

4.1 PANEL (position-based aggregator node election)

As its name suggests, it selects some data aggregators on the basis of some position information criteria. The nodes are
divided into geographical clusters. An aggregator is selected for each cell, with respect to the lower left corner of the cluster. The communication formats re of two type, inter-cluster in which data is sent to a single cluster closer to BS and intra-cluster in which data is sent or aggregated to an aggregator and then the data is sent from aggregator to sink or BS. PANEL provides load balancing as aggregators are changed after sometime or after each round. However the selection of aggregators based on geographical locations need extra complex technology on both hardware and software side, thus may be considered cost-effective.

4.2 TTDD (Two-Tier Data Dissemination)
In this approach, nodes are divided into different grids with several dissemination nodes for spreading or sending queries to source node. This approach also has a multiple mobile sinks. When a sink needs some data, it sends queries to dissemination nodes which forward queries to source nodes. The sink can move from one grid to another and broadcasts queries to all nodes of the grid. When a sink moves from one grid to another, it selects a reference node called bridge node which forward data to sink which has moved to another cell or grid. This is a good technique for event-driven and on-demand data applications [11].

4.3 HGMR (Hierarchical geographic multicast Routing)
This protocol is a hybrid of GMR and HRPM. The objective of GMR is to enhance forwarding while that of HRPM is reducing encoding overhead. HRPM divides nodes into cells with an AP (Access Point) which has destination information about all nodes in the cell. The Aps are managed by a rendezvous point. Two types of trees are constructed for communication, source-to-AP and AP-to-member tree. The data is transferred to different Aps at different levels until it reaches the lower level AP which is then forwarded to BS or sink. In HGMR, the nodes are given different tasks with different responsibilities and loads, thus less energy is consumed.

5. Area based Hierarchical routing protocols
In this type of routing, some of the nodes are selected as master nodes or act as high tier node. These are responsible for collecting data from other nodes and to forward data to sink node, this is a useful approach for mobile WSNs. The advantages of area based routing is that a specific area is selected so topology implementation is easy comparatively and high tier node can be selected very easily. Another advantage is that just like other cluster and chain topologies, the data is transmitted locally avoiding large distance communication, thus less energy is consumed. However, this approach also suffers from some drawbacks which include: scalability because for large reason the data broadcast may result in high energy consumption. As this approach is largely used for mobile WSNs, so cost is high for their implementation because some extra technologies are needed for the deployment.

The following are some of the routing techniques based on this category.

5.1 LBDD (Line-based Data Dissemination)
In this method, the nodes are divided into two parts creating a fence called vertical strip or line of nodes. This line acts as a storage area and all the data is sent to this line or inline nodes before sending it to the sink the nodes within the area of line are called inline nodes. The operation is performed in two phases, in first phase, a node generates new data and send it to the nearest inline node. In the second phase, the sinks sends query to the vertical strip and the query is flooded to all the nodes of the strip, upon receiving the query, the nodes having some data received from other nodes send data to the sink node [12]. This technique experiences the problem of load balancing because the strip nodes are responsible for data transmission, if there are less number of nodes on the strip line, they will deplete energy very quickly, resulting in reduced network life [14].

5.2 VLLD (Virtual Line-based Data Dissemination)
This topology works on Virtual Line Structure (VLS). This is a specific region with nodes in a chain form. The data is gathered on this line and then sent to sink. If a node wants to send data to VLS, it calculates entry point or node to VLS, the shortest path is selected and data is sent to that node, this data is transferred to the neighbor node of VLS until it reaches the exit point. Now the sink sends query for data to VLS, unlike LBDD in which query is broadcast to all nodes of strip line, the query is sent to entry point of VLS. If VLS has data on its exit point, it notifies the sink by creating a flag with value = false, otherwise the data is taken from other nodes of VLS and sent to sink [13]. The techniques provides good energy efficiency by avoiding flooding, however the exit point of VLS may suffer more from energy depletion.

5.3 Ring Routing
In ring topology, nodes form a ring for collection of data from nodes and transmission of data to sink. After the formation of nodes, the neighbor nodes attach to the ring and transmit data to different nodes in the ring. The ring nodes change time to time, therefore the problem of network failure is minimized. The ring acts as a rendezvous for the tasks and Execution queries. The sink gets data from the ring by sending queries and its location. The topology implementation also easy in ring topology just like in LBDD [14].

5.4 Railroad:
This is a proactive technique in which a topology is created with a specific area which contains Meta data for the actual data. This is called rail and is located in the middle of the network. Whenever a query is generated by the sink for data, it is sent to rail, the rail looks up for Meta data of that query and informs the source node, the source node delivers that data to sink node. The difference between LBDD and railroad is that sin LBDD, the sink node sends data to all nodes of strip line while in railroad, it unicasts the query [60].
COMPARATIVE ANALYSIS OF HIERARCHICAL ROUTING PROTOCOLS AGAINST SOME PARAMETERS

In this section, the above categories and their mention techniques will be analyzed and compared on the basis of the following parameters: Energy Efficiency, Transmission Delay, Scalability, Load balancing, Network Life, Data aggregation and criteria for CH selection. Each technique follows a different topology and mechanism. One topology favors scalability but suffers network life problem, some topologies provides better data aggregation while others are good for convergence time. This section will give us a general and broad idea about how a topology achieves certain performance parameters and how it suffers from some drawbacks. In the next section, keeping this discussion in view, we will suggest a suitable topology or technique for specific application areas. This section will discuss the performance evaluation on the basis of above of parameters category-wise. Data aggregation is common to almost all of the protocols, as data is gathered by a single or multiple master nodes and then sent to sink. The performance analysis is presented in the form of table in Table 1.

Cluster-Based Routing protocols: The network topology of cluster-based routing i.e. LEACH, LEACH_C, TEEN and APTEEN suggests that the nodes can be dispersed in a wide area so scalability can be achieved efficiently, because the group formation can increase the area for network. However, as the farthest CH may cause transmission delay, so there should be a limit regarding scalability[3], but normally data delivery is good in cluster routing. Energy efficiency is also good for these protocols but lesser as compared than those of tree and chain based topologies. The BS is almost fixed for all of these protocols. Load-balancing is good. Network life is enhanced by considering residual energy, similarly convergence time for cluster-based routing is very little which is a very good feature [4].

Chain-Based Routing Protocols: energy efficiency is very Low for chain-based as compared to others. This is because of the reason that sometimes the CH is too far from the BS that it has to consume more of the energy to transmit data to BS. But as CHIRON uses multi-layered mechanism for data transmission, so it has comparatively good energy efficiency as compared to other chain-based protocols. Scalability in chain-based protocols is very less because the nodes form long chains, so it is not scalable to a large extent. Chain-based protocols suffer greatly from the problem of transmission delay because of long chains as well as multiple level of chains, so data delivery rate is high for these protocols, even CHIRON suffers from this problem. Load balancing is good because the data transmission burden is transferred to each node in turn. The algorithm complexity of PEGASIS is more because it acquires the global knowledge of all nodes while algorithm complexity for CHIRON and others is less comparatively as they do not need global information of all nodes. Data aggregation in almost all types of chain-based protocols.

Tree-based routing protocols: Energy efficiency for is better compared to chain and grid based because the transmission distance is very little, as the nodes communicate with immediate neighbors, however it may result in delayed data transmission from leaf node to root node if the leaf node is too far from sink node. Load balancing is also greatly achieved because in the tree construction, the nodes with more residual energy has more responsibility for delivery of data up to the sink. The data in tree-based protocols travel through so many nodes causing delay, so it also limits the scalability of the network. Network life is also good because load is balanced across the network. Tree-based topology suffers from data delivery time if data has to be sent from leaf node to sink or root node. In some techniques of this category, spanning tree is created, which makes its algorithm complex as compared to others. Convergence time varies and depends upon the node’s level, convergence time is greater for nodes of levels nearer to the root node.

Grid-based Routing Protocols: As the topology of grid-based is multi-hop or multi-layered, the energy efficiency is good but lesser than tree and area based routing techniques. In this techniques, aggregator s are responsible for data gathering and transferring and each node has equal chances to become aggregator, so the load is balanced in the system but some of the techniques suffer from imbalanced load problem, so the overall load balancing can be considered moderate. Network life is also moderate. Scalability is good because the data passed through less number of hops, favoring scalability. Transmission delay is moderate, the farther nodes suffer from great delay as data has to travel through many levels. Convergence time is good as compared to tree and area-based routing. Cluster and grid-based routing protocols are almost equal in convergence time of network.

Area-based routing techniques: The Topology of area-based routing is almost the same as grid-based routings. Area-based routing achieves certain performance parameters, these are discussed as: area-based routing performs flooding which results in large energy consumption, but this can be minimized if the network is not too much large. Load is imbalanced in the system because the nodes on the line strip have more responsibility as compared to others. However, railroad and ring protocols achieve some load balancing. Area-based routing suffers a lot from the problem of transmission delay because of flooding. Algorithm comlexity is low as compared to other categories. Convergence time is less because lesser nodes are dependent upon each other.
<table>
<thead>
<tr>
<th>Category</th>
<th>Protocol</th>
<th>Data aggregation</th>
<th>Energy efficiency</th>
<th>Scalability</th>
<th>CH selection</th>
<th>Load balancing</th>
<th>Complexity</th>
<th>Network life</th>
<th>Convergence Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLUSTER</td>
<td>LEACH</td>
<td>yes</td>
<td>moderate</td>
<td>good</td>
<td>proactive</td>
<td>good</td>
<td>moderate</td>
<td>moderate</td>
<td>moderate</td>
</tr>
<tr>
<td></td>
<td>LEACH-C</td>
<td>Yes</td>
<td>Moderate</td>
<td>Good</td>
<td>Proactive</td>
<td>Good</td>
<td>high</td>
<td>Moderate</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td>TEEN</td>
<td>Yes</td>
<td>Good</td>
<td>Good</td>
<td>Proactive    &amp; Reactive</td>
<td>Good</td>
<td>Moderate</td>
<td>Good</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>REAP</td>
<td>Yes</td>
<td>Moderate</td>
<td>Good</td>
<td>Proactive    &amp; Reactive</td>
<td>Good</td>
<td>High</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAIN</td>
<td>PEGASIS</td>
<td>Yes</td>
<td>Very low</td>
<td>Very low</td>
<td>proactive</td>
<td>Moderate</td>
<td>High</td>
<td>Moderate</td>
<td>Less</td>
</tr>
<tr>
<td></td>
<td>CCS</td>
<td>Yes</td>
<td>Very low</td>
<td>low</td>
<td>Proactive</td>
<td>Bad</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Less</td>
</tr>
<tr>
<td></td>
<td>EBCRP</td>
<td>Yes</td>
<td>Very low</td>
<td>low</td>
<td>Proactive</td>
<td>Moderate</td>
<td>Good</td>
<td>Less</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHIRON</td>
<td>Yes</td>
<td>Moderate</td>
<td>Low</td>
<td>Reactive</td>
<td>Moderate</td>
<td>Good</td>
<td>Less</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TREE</td>
<td>EADAT</td>
<td>Yes</td>
<td>Moderate</td>
<td>Low</td>
<td>Proactive</td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>BATR</td>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>Proactive</td>
<td>Bad</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>ETR</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Reactive</td>
<td>Bad</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRID</td>
<td>PANEL</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Reactive</td>
<td>Good</td>
<td>High</td>
<td>Moderate</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td>TTDD</td>
<td>Yes</td>
<td>Very low</td>
<td>Moderate</td>
<td>Reactive</td>
<td>Good</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>HGMR</td>
<td>Yes</td>
<td>low</td>
<td>High</td>
<td>Proactive</td>
<td>Bad</td>
<td>Low</td>
<td>Moderate</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AREA</td>
<td>LBDD</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Reactive</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td>Ring</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Proactive</td>
<td>Good</td>
<td>Moderate</td>
<td>Low</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td>RAILROAD</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Proactive</td>
<td>Good</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>VLDD</td>
<td>Yes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Proactive</td>
<td>low</td>
<td>Moderate</td>
<td>low</td>
<td>good</td>
</tr>
</tbody>
</table>

**TABLE 1. PERFORMANCE ANALYSIS OF HIERARCHICAL ROUTING PROTOCOLS**
II. DISCUSSION
The above discussion and analysis can help us to determine which technique is most suitable for a certain domain of applications. This section is composed of two main points: (i) which of the routing category achieve most performance features, this can help us understand the importance and use of each category and (ii) on the basis of discussion in section 3, we will determine domain of applications for each technique. By analyzing the above discussion and given tables, we can see that area-based routing can achieve more performance parameters as compared to others for small networks, however it suffers from scalability and energy efficiency issues a lot in large networks. Tree and grid-based algorithms lie almost on the same line regarding performance parameters achievement. Cluster-based routing has poor performance achievements comparatively and the reasons are given in the discussion of section 3.

Cluster-based routing is suitable for small-scale applications like agriculture because it is scalable up to some limit. Chain-based routing protocols are suitable for short-range networks such as health monitoring and Bluetooth applications. Tree-based routing can be efficiently used in small-scale networks and data-centric networks like smart home applications. Grid-based routing protocols are best for QoS and multicast applications. Area-based routing protocols use mobile sink nodes so they can be best utilized for large area networks. Here are some of the trade-offs between some performance parameters. Scalability normally suffers when data has to pass through multiple tiers and is also suffered form multiple hops. Similarly, load-balancing increases network life. The more the load is balanced among the nodes, the lesser network fails.

III. FUTURE DIRECTIOS
WSNs have been evolving since last decade and research has been going on in its different domains as was discussed in first section. WSNs are now collaborating the newly evolving technology “Internet of Things” and it can provide many challenges for the researchers to make both the technologies more efficient and useful for users. Similarly, work can also be done on different problems in above discussed routing protocols e.g. LEACH protocol has the problem of coverage and uniformity in clusters creation, this can be solved if there is determined some minimal distance between cluster heads, this will also result in more energy optimization because we have concluded that the lesser the CHs, the more is energy optimization. Similarly hybrids of different protocols can be proposed in order to achieve multiple performance parameters e.g. LEACH and REAP. QoS applications are rapidly increasing, so there is a need to work on this performance parameter. Another challenge is mobile sinks. This area also has lots of challenges for researchers.

IV. CONCLUSION
Above was a brief survey about WSN energy efficient routing protocols. Work can be done in different areas of WSN. Routing is also considered to be a major area which can effect energy utilization. The paper will provide some opportunity to grab basic knowledge about different routing techniques and future challenges.

REFERENCES
Owais Khan was born in Mingora Swat, in 1990. He completed his B.S. in computer science from University of Peshawar, Pakistan, in 2014 and currently doing M.S in the field of Computer Science from COMSATS Institute of Information Technology, Abbottabad, KPK, Pakistan.

Dr. Fiaz Gul was born on 22-11-1982, in a beautiful valley Abbottabad of KPK. He did graduation and MS from COMSATS Institute of Information Technology Abbottabad in the field of Computer Science. For specialization master and Doctorate he won the HEC scholarship under the project UESTP for Politecnico di Torino Italy. Currently he is serving as an Assistant Professor in Computer Science Department at COMSATS Abbottabad, Pakistan.

Dr Babar Nazir is Assistant Professor, Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, K.P.K, Pakistan. He is specialized in the fields of Wireless Sensor networks, resource management and job scheduling in Cloud Computing, Grid Computing, and Cluster Computing and has many prominent publications in above fields.

Usman Wazir was born in D.I.Khan city, in 1990. He completed his B.S. in computer science from Gomal University, D.I.Khan, Pakistan, in 2014 and currently doing M.S in the field of Computer Science from COMSATS Institute of Information Technology, Abbottabad, KPK, Pakistan.
Improved Face Recognition Rate Using Face Partitioning in Eigen And Fisher Feature Based Algorithms

Harihara Santosh Dadi, Gopala Krishna Mohan Pillutla

Abstract— Face partitioning technique is presented in this paper. Instead of directly giving the face to the face recognition system, first the face is partitioned in to different face parts using face partitioning technique. The face parts are namely mouth, left eye, right eye, head, eye pair and nose. Eigen and Fisher features based algorithms are considered for experimental purpose. These face part features are given to the SVD classifiers individually. The outputs of the classifiers are again given to the decision making algorithm. Based on the maximum likely hood principle, this decision making algorithm outputs a face. ORL data base is used for evaluating the performance of this new technique. The first two faces of all the 40 people in the data base are considered for testing and the remaining eight faces are used for training purpose. Results are separately calculated with and without face partitioning technique. Results show that face recognition rate is increased by using the combination of face partitioning technique and basic face recognition algorithm. The new algorithm is also verified on 8 different data sets. Experimental results show that this face partitioning is improving the face recognition rate both Eigen and Fisher feature based algorithms.

Index Terms—Face Partitioning, Facial features, Recognition engine, Support Vector Machine, Decision making algorithm.

I. INTRODUCTION

Face recognition aims at identifying the person’s distinctiveness by comparing the facial features with the available face data base features. The face data base, with known characteristics, is referred as the face gallery and the input face requiring determining the identity is the probe. One of the problems in face recognition is identification, and the other is the authentication (or verification). Of the two, face identification is more tricky as it cross verifies the gallery completely for minimum variance.

Numerous algorithms are developed on face recognition particularly in the last two to three decades. Improving the Face recognition rate is always the challenge ever since the first algorithm was developed. In 1991, Alex Pentland and Matthew Turk [1] applied Principal Component Analysis (PCA) which was invented in 1901 to face classification. This has become the standard known as the Eigen face method and is today an inspiration for all face recognition algorithms evolved. Nan Deng et. al. [2] introduced face recognition algorithm for occluded faces. This method is based on dictionary learning for sparse representation and sub classifier fusion (LSSRC). The advantage of this method is its ability to conduct fusion recognition based on different identification contributions of sub-classifiers. For more robust face recognition algorithms refer [18] – [19]. Le An et. al. [3] introduced face recognition in multi camera surveillance videos. They developed unified face image (UFI) by fusing face image from different cameras. This is more effective as it uses multi cameras for face feature extraction from different orientations. This algorithm needs a high experimental setup.

As the facial features are more localized, the algorithms are becoming more insensitive to the common challenges like facial expressions, occlusions, illumination and pose variations. This is the inspiring force for us to develop this algorithm.

In this paper we propose a novel approach for developing face recognition algorithm. Here, we divided the face in to face parts like head, nose, right eye, mouth, left eye, and eye pair. Paul Viola et. al. developed face parts detection algorithms [4] – [6]. The features like Eigen are extracted for these parts and given to the classifiers. The classifier compares the features of the probe and the features of the gallery in the database. Each classifier outputs the face part. All these face parts are again given to the decision making algorithm which finally generates the matched face. We compare our algorithm’s results with Eigen face feature algorithm. Finally we compare our algorithm with the standard face recognition algorithm, PCA.

While numerous face recognition algorithms are being developed, the authors are comparing them with the existing ones very superficially and few simple comparisons are presented. Given that large set of techniques and the theories that are applicable for face recognition, it is evident that the detailed analysis and bench marking these algorithms is very crucial. Effort done by Universities and research laboratories in developing the data sets pushed the comparisons of face recognition algorithms to the higher level. CMC and ROC curves were introduced for comparisons. Apart from finding the recognition rate, these curves become the basis for showing the superiority of the author’s developed algorithms.
The contributions of this paper are as follows:

- We develop a novel face partitioning algorithm based on localizing the facial features. This works well for finding out the face parts and is more insensitive to the illumination, pose and facial expression variations. As the features are more localized, the variations become substantially reduced when we see for individual face parts.
- We presented a decision making algorithm which accepts different face part outputs from different classifiers and generates a face output.
- Extensive comparisons are made by taking the performance metrics curves namely CMC and ROC and showed that the curves are effective for proposed algorithm compared with Eigen and Fisher feature based algorithms.

The remainder of this work is prepared as follows. Section II reminds the related work. Section III presents methodology of extraction of Eigen features and about SVD classifier. Section IV Face partitioning algorithm is presented. Section V shows the experimental results. Conclusions are finally stated in Section VI.

II. RELATED WORK

Face recognition methods mainly deal with images which are of large dimensions. This makes the task of recognition very difficult. Dimensionality reduction is a concept which is introduced for the purpose of reducing the image dimensions. PCA is the most widely used dimensionality reduction and also for subspace projection. PCA can supply the client with a lower-dimensional picture, a projection of this object when seen from its informative view point. This can be achieved by taking only the starting few principal components in such a way that the dimension of the transformed data is minimized. The linear combination of pixel values here in PCA are called Eigen faces.

Two performance metrics curves are considered. Cumulative Match Score Curves (CMC) is the curve between the rank on the x-axis and face recognition rate on the y-axis. Receiver Operating Characteristics (ROC) is the graph between false acceptance rate and verification rate. ROC curves are more informative

III. FACE RECOGNITION ALGORITHM

A typical face recognition algorithm is presented in this section. For any face recognition algorithm, there are two phases. One is training phase and the other is the testing phase. In the training phase, the features of all the faces in the gallery are found and stored in the data base. Eigen features are taken in the sample face recognition algorithm shown below in the figure 1. In the testing phase, the features of the probe are calculated. These features and the features of the gallery are given to any of the classifier. SVD classifier is taken as example in the figure. The Eigen features of the probe and the Gallery are taken by the SVD. The classifier looks for the closest feature matching face from the gallery with the probe and gives that face as output. Figure 1 shows the sample face recognition algorithm block diagram.
2) **Gallery images**

![Fig. 2. First face image of all 40 people in the ORL database](image)

Fig. 2. First face image of all 40 people in the ORL database

![Fig. 3. Face partitioning algorithm in the training phase which partitions the face into head, right eye, mouth, nose left eye and eye pair.](image)

Fig. 3. Face partitioning algorithm in the training phase which partitions the face into head, right eye, mouth, nose left eye and eye pair.

![Fig. 4. Face parts shown in different colors. Head in red, right eye in magenta, nose in blue, left eye in black, mouth in purple and eye pair in green.](image)

Fig. 4. Face parts shown in different colors. Head in red, right eye in magenta, nose in blue, left eye in black, mouth in purple and eye pair in green.

---

a) **Head Images**

![Fig. 5. Head parts of all 40 people from ORL database.](image)

Fig. 5. Head parts of all 40 people from ORL database.

b) **Mouth Images**

![Fig. 6. Mouth parts of all 40 people from ORL database.](image)

Fig. 6. Mouth parts of all 40 people from ORL database.

c) **Eye Pair Images**

![Fig. 7. Eye pair parts of all 40 people from ORL database.](image)

Fig. 7. Eye pair parts of all 40 people from ORL database.
d) **Left Eye Images**

Fig. 8. Left eye parts of all 40 people from ORL database.

e) **Nose Images**

Fig. 9. Nose parts of all 40 people from ORL database.

f) **Right Eye Images**

Fig. 10. Right eye parts of all 40 people from ORL database.

3) **Probe Image**

The face images of the first person in the AT&T Database.

Fig. 11. All 10 images of first person from ORL database.

Fig. 12. Face parts shown in different colors for the first person from ORL database.

Fig. 13. Face partitioning algorithm which partitions the face image into different parts in the testing phase.

a) **Head Image**
In the training phase, all the face part gallery features are extracted and individually trained by using any classifier. Here we extracted Eigen features and used SVD classifier. Figure 20 shows the training of all the face parts in the training phase. Figure 21 shows the overall training phase of our proposed method. This way of igniting the recognition engine is introduced in this section.
5) Testing Phase

In the testing phase, the probe image is given to the face partition algorithm. The Eigen features of the face parts are extracted individually. Figure 22 shows how the Eigen features of first image of first person in the ORL database are extracted in the testing phase. Figure 23 shows the overall testing phase of the proposed algorithm. Figure 24 shows the face partitioned face recognition algorithm. The training and the testing phases are separately shown.

B. Decision making algorithm:

Let there are ‘n’ classifiers for different face partitioned datasets. Each classifier compares the features of the gallery and the features of the probe. The classifier outputs the nearest face part from the gallery with the probe. The input to the decision making algorithm are the outputs from the SVM classifiers. Decision making algorithm compares all the face parts. The face with more number of face parts is produced as output. Here in our algorithm the face with more than two face parts is considered as the output of the decision making algorithm. Figure 25 shows the complete face partitioned face recognition system.

Algorithm Decision Making Algorithm (DMA)

1. Let the total number of persons in the gallery be ‘p’.
2. Let ‘a’ be the head part from the gallery which is matched with the probe $F_{PH}$, ‘b’ be the left eye part from the gallery which is matched with the probe $F_{PL}$, ‘c’ be the right eye part from the gallery which is matched with the probe $F_{PR}$, ‘d’ be the eye pair part from the gallery which is matched with the probe $F_{PE}$, ‘e’ be the nose part from the gallery which is matched with the probe $F_{PN}$ and ‘f’ be the mouth part from the gallery which is matched with the probe $F_{PM}$. 
3. Let ‘a’ belong to F₁ face in the gallery, ‘b’ belong to F₂, ‘c’ belong to F₃, ‘d’ belong to F₄, ‘e’ belong to F₅, ‘f’ belong to F₆. Where 1<i,j,k,l,m,n<p. /*Equals function outputs the total number of equals with the first argument among the other arguments*/
4. (i,01)=Equals(i and j,k,l,m,n) 
5. (j,02)=Equals(j and i,k,l,m,n) 
6. (k,03)=Equals(k and i,j,l,m,n) 
7. (L,04)=Equals(l and i,j,k,m,n) 
8. (m,05)=Equals(m and i,j,k,l,n) 
9. (n,06)=Equals(n and i,j,k,l,m) 
10. Output face image=Max(01,02,03,04,05,06) 1<Output<p. /* Max function generates that face which corresponds to the Maximum of O₁ to O₆ as output*/.

V. EXPERIMENTAL RESULTS

Experiments have been conducted on proposed algorithm by taking ORL AT&T data base [11]. For training phase the first eight face images are taken and for the testing purpose the last two face images are taken. The face database is first divided in to six separate databases namely head, eye pair, left eye, mouth right eye and nose. Eigen features are extracted in the training phase for all the data sets. And in the testing phase, the Eigen features of these parts are taken and given to the SVD classifiers parallel. The outputs of these classifiers are again feed to the decision making algorithm. The output of decision making algorithm is the output of the proposed system.

The individual results are shown for both the test images in table I and table II. The results for different data sets are shown in different columns. The last column is the proposed method. The green color indicates that the proposed algorithm is generating the correct output where as the original PCA algorithm is giving the wrong result. The red color indicates that even by using the proposed algorithm still some of the face images are not showing the correct output. There are 80 test images and 320 train images. Out of 80 test images, 64 images are correctly recognized by the PCA algorithm. Whereas by using the proposed algorithm, 76 test images are correctly recognized. There is an improvement of 15% in face recognition rate when compared with the PCA algorithm on ORL database.

Figure 26 and 27 shows the 3-D graphs between testing versus training of test face image 1 and 2 respectively.
The proposed recognition engine is also verified on different seven data sets available. The improvement in face recognition rate for all these data sets is listed in Table II.

The performance metrics for different algorithms shown below are with ORL database. All the performance curves show that irrespective of the algorithm, by changing the way of igniting the recognition engine, the performance of the algorithm is optimized. The proposed algorithm performed well and is shown in all the performance curves in blue lines.

**Performance curves of PCA Algorithm**
Fig. 28. (a) CMC and (b) ROC Curves of PCA Algorithm for Face, Mouth, Eye pair, right eye, left eye, nose and head data sets. The proposed algorithm is shown in blue.

Performance curves of LDA Algorithm

Fig. 29. (a) CMC and (b) ROC Curves of LDA Algorithm for Face, Mouth, Eye pair, right eye, left eye, nose and head data sets. The proposed algorithm is shown in blue.

VI. CONCLUSIONS

In this paper, we have formulated a face partitioned algorithm and the decision making algorithm. A new and powerful way of igniting the recognition engine is introduced. This technique is verified on 8 different datasets. This partition based ignition outperforms other face recognition algorithms. Here, the face is divided into seven different face parts. Some of the face parts are redundant like right eye, left eye and eye pair for example. This redundancy is purposefully included in order to face the challenges like pose and illumination variations. Instead of dividing the faces into face parts, the Eigen faces can be divided without any redundancy compromising the pose and illumination changes. Therefore, one of our future works will be developing more efficient way of igniting the recognition engine by dividing the Eigen faces in to either 4 or 9 or 16 parts by dividing the face image in to 2X2 or 3X3 or 4X4 matrices.

ACKNOWLEDGMENTS

Portions of the research in this paper use the FERET database of facial images collected under the FERET program, sponsored by the DOD Counterdrug Technology Development Program Office.

| TABLE III | DIFFERENT DATASETS AND THEIR TOTAL NUMBER OF IMAGES AND PERSONS |
|---|---|---|
| Data base | Total number of persons | Pose, illumination and facial expression variations | Total number of face images |
| Yale Database [9] | 15 | 11 | 165 |
| Yale Face Database ‘B’ [10] | 10 | 64 illumination 9 poses | 5760 |
| Georgia Tech [14] | 50 | 15 | 750 |

| TABLE IV | DIFFERENT DATASETS AND THEIR TOTAL NUMBER OF IMAGES AND PERSONS USED ON PCA ALGORITHM |
|---|---|---|---|
| Database | Total number of people considered | Total number of faces per person | Faces considered for testing | Face recognition rate (in %) |
| PCA Algorithm | Proposed Algorithm |
| Color FERET | 40 | 9 | 8 | 1 | 61.0 | 70.26 |
| Yale Database | 15 | 11 | 9 | 2 | 88.26 | 91.02 |
| Yale Face Database ‘B’ | 10 | 10 | 8 | 2 | 80.01 | 85.56 |
| BioID | 20 | 20 | 16 | 4 | 66.36 | 69.58 |
| Georgia Tech | 50 | 15 | 13 | 2 | 81.63 | 91.02 |
The face recognition rate is calculated by taking the average of the face recognition rates of all the testing images.

<table>
<thead>
<tr>
<th>Database</th>
<th>Total number of people considered</th>
<th>Total number of faces per person</th>
<th>Faces considered for testing</th>
<th>LDA Algorithm</th>
<th>Face recognition rate (in %)</th>
<th>Proposed Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color FERET</td>
<td>40</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>2</td>
<td>63.11</td>
</tr>
<tr>
<td>Yale Database</td>
<td>15</td>
<td>11</td>
<td>9</td>
<td>2</td>
<td>12</td>
<td>85.69</td>
</tr>
<tr>
<td>Yale Face Database ‘B’</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>2</td>
<td>12</td>
<td>81.16</td>
</tr>
<tr>
<td>BioID</td>
<td>20</td>
<td>20</td>
<td>16</td>
<td>4</td>
<td>10</td>
<td>69.68</td>
</tr>
<tr>
<td>Georgia Tech</td>
<td>50</td>
<td>15</td>
<td>13</td>
<td>2</td>
<td>12</td>
<td>80.05</td>
</tr>
<tr>
<td>FEI</td>
<td>50</td>
<td>14</td>
<td>12</td>
<td>2</td>
<td>12</td>
<td>81.15</td>
</tr>
<tr>
<td>Labeled faces in the wild</td>
<td>40</td>
<td>10</td>
<td>8</td>
<td>2</td>
<td>12</td>
<td>59.16</td>
</tr>
</tbody>
</table>

In case of testing images taken are more than one, then the face recognition rate is calculated by taking the average of the face recognition rates of all the testing images.

REFERENCES


Mr. D. Harihara Santosh obtained his B. Tech. and M. Tech degrees from JNT University, Hyderabad in the year 2005 and 2010. Presently he is pursuing Ph.D, in Video Processing at JNTU, Hyderabad. He is presently pursuing his Ph.D. under the Guidance of Dr. P.G. Krishna Mohan. He has 9 publications in both International and National Journals and presented 24 papers at various International and National Conferences. His areas of interests are Image and Video Processing.

Dr.P.G.Krishna Mohan presently working as Professor in Institute of Aeronautical College of Engineering, Hyderabad. He Worked as Head of ECE Dept. , Member of BOS for ECE faculty at University Level, Chairman of BOS of EIE group at University level, Chairman of BOS of ECE faculty for JNTUCEH, Member of selection committees for Kakitya, Nagarjuna University, DRDL and convener for Universite a Hidian committees. He has more than 48 papers in various National and International Conferences.
various International and National Journals and Conferences. His areas of interests are Signal Processing, Communications.
Elastic Extension Tables for Multi-tenant Cloud Applications

Haitham Yaish\textsuperscript{1,2,3}, Madhu Goyal\textsuperscript{2,3}, George Feuerlicht\textsuperscript{3,4,5}

\textsuperscript{1} Faculty of Engineering, American University of the Middle East, Kuwait
\textsuperscript{2} Centre for Quantum Computation & Intelligent Systems
\textsuperscript{3} Faculty of Engineering and Information Technology, University of Technology, Sydney
\textsuperscript{4} Faculty of Information Technology, University of Economics, Prague, Czech Republic
\textsuperscript{5} Unicorn College, Prague, Czech Republic

Abstract—Software as a service (SaaS) is a Cloud Computing service model that exploits economies of scale for SaaS service providers by offering a single configurable software and computing environment for multiple tenants. This contemporary multi-tenant service requires a multi-tenant database that accommodates data for multiple tenants using a single database schema. In general, traditional Relational Database Management Systems (RDBMS) do not support multi-tenancy and require schema extensions to provide multi-tenant capabilities. This paper proposes a multi-tenant database schema called Elastic Extension Tables (EET), which is highly flexible in enabling the creation of database schemas for multiple tenants by extending a preexisting business domain database, or by creating tenant business domain database from the scratch at runtime. The empirical results presented in this paper indicate that the EET schema has potential to be used for implementing multi-tenant databases for multi-tenant SaaS applications.

Index Terms—Cloud Computing, Software as a Service, Multi-tenancy, Elastic Extension Tables, Multi-tenant Database.

I. INTRODUCTION

Cloud Computing has recently emerged as a new computing paradigm that transforms the IT industry, making the computing software and hardware more appealing to use as a service over the internet [17], [26]. This new computing paradigm has been gaining popularity for two reasons. First, the internet has become affordable and its speed has significantly increased [29]. Second, rapid growth in computer usage, in areas such as businesses, governments, health services, education, social media networks, mobile applications, and other computational aspects [17]. This increase in internet speed and the computer usage resulted in the need to maximize the use of computational resources and to minimize the cost. Cloud Computing offers a solution to this need by moving applications and their data from desktop and portable Personal Computers into large data centers [16]. Cloud Computing is rapidly evolving, with the prospects that it will be one day the fifth used utility after water, electricity, gasoline, and telephone [5], [15], [19]. Cloud Computing includes a number of service delivery models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [16], [18], [24], [27]. Multi-tenancy is a fundamental characteristic of Cloud Computing services that allows SaaS vendors to run a single application that support multiple tenants using the same software and hardware infrastructure [13], [25], [28]. It is a common practice in SaaS applications to use a multi-tenant database architecture with a single database schema shared among all tenants [4], [21]. Cloud database service providers regard such a database as an effective resource sharing storage as it reduces the costs by co-locating multiple tenants’ databases into a single database schema. It also reduces the total cost of ownership of the service. Such data architecture consists of two types of data: shared data and tenant’s private isolated data. Combining these two types of data provides tenants with a complete view of data that fits their business requirements [7], [9].

Most modern Relational Database Management Systems (RDBMS) have been designed to manage data for a single tenant. However, single-tenant databases do not support the unique requirements of individual tenants and this can lead to incorrect assumptions and query plans [1], [21]. Various multi-tenant database schema techniques have been studied and implemented to overcome this challenge, including Private Tables, Extension Tables, Universal Table, Pivot Tables, Chunk Table, Chunk Folding, and XML Table [2], [8], [12], [14], [22], [21]. These multi-tenant schema techniques are based on traditional RDBMS [4], [7]. However, these multi-tenant schema techniques suffer from various limitations that still need to be addressed [5], [11], [21], [23], and overcoming
these limitations in the context of SaaS applications has received a lot of attention, both from academic and industry-based researchers.

In this paper, we propose a novel multi-tenant database schema called Elastic Extension Tables (EET) that consists of Common Tenant Tables (CTT), Extension Tables (ET), and Virtual Extension Tables (VET). This multi-tenant schema enables tenants to build their own virtual database schema by creating the required number of tables and columns, creating virtual database relationships, and assigning suitable data types and constraints for table columns during multi-tenant application run-time execution. It also gives tenants the opportunity to address their individual business requirements by choosing from three database models: (1) Multi-tenant Relational Database, (2) Integrated Multi-tenant Relational Database with Virtual Relational Database, and (3) Virtual Relational Database. In addition, it allows tenants to store different data types, including structured, semi-structured, and unstructured data. In this paper, several experiments are performed to evaluate the feasibility and effectiveness of EET multi-tenant database schema by comparing it with Universal Table Schema Mapping (UTSM) [2], which is commercially used by Salesforce. Significant performance improvements obtained using EET when compared to UTSM, makes the EET schema a good candidate for implementing multi-tenant databases and multi-tenant applications.

The rest of the paper is organized as follows: section 2 discusses the related work of multi-tenant database schema designs. Section 3 proposes the Elastic Extension Tables multi-tenant database schema. Section 4 proposes three Elastic Extension Tables database models. Section 5 presents an example to compare other multi-tenant database schema designs with the Elastic Extension Table design. Section 6 presents a set of experiments that compare the performance of Elastic Extension Tables with Universal Table Schema Mapping. Section 7 concludes this paper and discusses future work.

II. RELATED WORKS

A number of multi-tenant database schema designs and techniques have studied and implemented to address multi-tenant database challenges. This section presents seven multi-tenant database schema techniques, including Private Tables, Extension Tables, Universal Table, Pivot Tables, Chunk Table, Chunk Folding, and XML Table [2], [8], [12], [14], [22], [23]. All of these multi-tenant database schema techniques are based on traditional RDBMS [4], [7].

A. Private Tables

The Private Tables technique allows each tenant to have his own private tables, which can be extended and changed [22], [23]. Using this multi-tenant query technique can be transformed from one tenant to another by renaming tables, and metadata without using extra columns like ‘tenant_id’ to distinguish and isolate the tenants’ data. In contrast, many tables are required to satisfy each tenant needs. Therefore, this technique is suitable only for a small number of tenants to ensure sufficient database load and good performance [23].

B. Extension Tables

The Extension Tables are separated tables joined with the base tables by adding tenants’ columns to construct logical source tables [22], [23]. This technique adapted from the Decomposed Storage Model that splitting up n-columns table into n 2-column tables joined using surrogate values [22]. Multiple tenants can use the base tables and the extension tables [7]. It is regarded as a better design when compared to Private Tables described above. Using this design, the number of tables grows with the number of tenants, and variety of their different business requirements [22].

C. Universal Table

A Universal Table contains a large number of columns that enable tenants to store their required columns. It is structured with two main columns ‘tenant_id’ and ‘table_id’, and other generic data columns, which have a flexible VARCHAR data type in which different data types with different data values can be stored in these columns [2], [22]. A flexible technique that enables tenants to extend their tables in different ways according to their business needs. However, the rows of the universal table can be too wide with an overhead in the number of NULL values, which the database has to handle [22].

D. Pivot Tables

In using the Pivot Tables technique, the application maps the schema into generic structure in the database, in which each column of each row in a logical source table is given its own row in the Pivot Table. The rows in the Pivot Table comprise of four columns, including tenant, table, column, and row that specifies which row in the logical source table they represent. It also includes a single data type column that stores the values of the logical source table rows according to their data types in the designated pivot Table [8], [21]. For example, the Pivot Tables can include two pivot tables, the first table ‘pivot_int’ to store INTEGER values, and the second table ‘pivot_str’ to store STRING values. The performance benefits are achieved using this technique by avoiding NULL values and by selectively reading from smaller numbers of columns. Pivot Tables technique, which partitions data vertically performs better when it allows selectively read in columns to improve the performance, when it compared with others multi-tenant database schema techniques that partition data horizontally (e.g. Universal Table) [22].

E. Chunk Table

The Chunk Table is another generic structure technique that is similar to Pivot Table, except it has a set of data columns with a mixture of data types that replace the column ‘col’ in the Pivot Table with ‘chunk’ column in the Chunk Table [22]. This technique partitions the logical source table into groups of columns. Each group is assigned a chunk ID and is mapped into an appropriate Chunk Table. This technique has four advantages over Pivot Table, including (1) Reducing metadata storage ratio, (2) reducing the overhead of reconstructing the logical source tables, (3) reducing the number of columns, and
(4) providing indexes. This technique is flexible, but it adds complexity to database queries [22].

F. Chunk Folding

Chunk Folding is a schema mapping technique that partitions logical source tables into chunks vertically [8], [22]. These chunks are folded in different physical tables and joined together, where a chunk of columns is partitioned into a group of columns and each group has a chunk id [8]. Aulbach et al. [22] performed experiments to measure the efficiency of Chunk Table and Chunk Folding techniques, and they found that Chunk Folding technique outperform the Chunk Table technique. In addition, they state that the performance of this technique is enhanced by mapping the most used tenants’ columns of the logical schema into conventional tables, and the majority of tenants does not use the remaining columns in the Chunk Tables. However, the main limitation and weakness of the Chunk Folding technique is that the common schema that is used by multiple tenants must be known in advance, which is not a practical solution for multi-tenant databases. This issue is also present in Extension Tables, Pivot Tables, and Chunk Table multi-tenant schema techniques.

G. XML Table

The XML Table database extension technique is a combination of relational database and Extensible Markup Language (XML) [8], [12], [23]. The tenants’ extension columns can be provided as native XML data type, or storing the XML document in the database as a Character Large Object (CLOB) or Binary Large Object (BLOB) [23]. XML data type facilitating the creation of database tables, columns, views, variables and parameters, and isolating the application from the relational data model [12]. This technique satisfies tenants’ needs because their data can be handled without changing original database relational schema, and XML data type can be supported by several relational database products [8], [12]. However, this technique reduces the data access performance [23], and Heng et al. [14] state that this technique has the poorest performance (e.g. highest response time), when compared to Private Tables, Universal Table, Pivot Tables, Chunk Table and Chunk Folding techniques.

Heng et al. [14] conducted a number of experiments to evaluate retrieving data from five different multi-tenant schemas used in multi-tenant SaaS applications, including Private Tables, Universal Table, Pivot Tables, Chunk Table, Chunk Folding, and XML Table. The results of these experiments show that retrieving data from Universal Table is faster than the other schema techniques, except the Private Tables schema. Aulbach et al. [23] conducted experiments to compare Private Table schema and the Universal Table (Sparse Columns) schema. The results of these experiments show that the Universal Table schema has the same or better performance than the Private Tables schema when retrieving or inserting data, except when inserting a large amount of data, the Universal Table schema is slower than the Private Tables schema. Such experimental results lead to conclusion that the query performance of Universal Table schema is the best performance out of the five multi-tenant schema techniques, as the Private Tables schema is only suitable for a small number of tenants. Overall, the experimental results make the Universal Table schema the optimal schema to use for a multi-tenant database when it is compared to Pivot Tables, Chunk Table, Chunk Folding, and XML Table. Nevertheless, the Universal Table can be too large introducing overhead with the number of NULL values, which the database has to handle. This suggests that the currently available multi-tenant database schemas still have remaining challenges, and represent suboptimal designs. Section 5 presents an example that clarifies how the data is populated in the seven multi-tenant database schema designs that are discussed in this section.

III. ELASTIC EXTENSION TABLES

The EET multi-tenant database schema proposes a novel way of designing and creating an elastic database that consists of three table types, the first type is CTT, the second type is ET, and the third type is VET. Fig. 1 shows the details of EET multi-tenant schema. The design of this schema enables tenants to build their own virtual database schema by creating the required number of tables and columns, rows, creating virtual database relationships, and assigning suitable data types and constraints for table columns during the runtime execution of a multi-tenant application.

A. Common Tenant Tables

The Common Tenant Tables are the tables that can be shared between tenants who are using a multi-tenant single database schema. These tables are RDBMS, and are used as a business domain database schema that is shared between multiple tenants. For example, a multi-tenant application of a sales business domain may have a database schema with sales tables, such as salesperson, customer, product, sales-fact, and any other sales tables. These tables have columns that are used by most of the tenants, and the column tenant ID is used to differentiate between the tenants’ rows. For example, the ‘sales_person’ CTT in Fig. 11 shows some common columns, such as ‘first_name’, and ‘last_name’, while the ‘tenant_id’ column is used to differentiate between the tenants’ rows.

B. Extension Tables

The Extension Tables are metadata tables that are used to create virtual tables for multiple tenants who are using a single multi-tenant database schema during the application’s runtime execution. They consists of the following eight physical tables:

1) Db_table Extension Table

The ‘db_table’ ET allows tenants to create virtual (logical) tables and give them unique names. The structure of this table has a composite primary key that consists of ‘db_table_id’ and ‘tenant_id’ columns. The ‘db_table_id’ column is a unique primary key of the table, while the ‘tenant_id’ column is a foreign key refers to the ‘tenant’ CTT and at the same time is a combined primary key with ‘db_table_id’ for this table. In addition, this table has the ‘db_table_name’ column that stores the virtual tables’ names. In using this table, each tenant can have unique table names. For example, tenant-A can create a VET name ‘sales_person’, but cannot create the same VET name again for his VETs. However, tenant-B can create the ‘sales_person’ name even if tenant-A already created this VET’s name.
2) **Table_column Extension Table**

The ‘table_column’ ET allows tenants to create virtual columns for a VET that created in the ‘db_table’ ET. The structure of this table has a composite primary key consists of ‘table_column_id’, ‘tenant_id’, and ‘db_table_id’. The ‘table_column_id’ is a unique primary key for this ET, while the other two columns ‘tenant_id’ and ‘db_table_id’ are primary keys in this table, and foreign keys that refer to primary key columns of the ‘tenant’ CTT, and the ‘db_table’ ET. Moreover, this table has other columns, including ‘table_column_name’, ‘default_value’, ‘data_type’, ‘is_indexed’, ‘is_null’, ‘is_relationship’, ‘is_primary_key_column’, and ‘is_unique_column’. The ‘table_column_name’ column has UNIQUE constraint, and VARCHAR data type. The ‘default_value’ column stores already defined value to be used once the database saves a table row, when there is no value specified to be stored in this column. The ‘data_type’ column specifies the data type of a virtual column that is stored into any of the three row ETs, which are presented in the following point. The ‘is_indexed’ column specifies whether a column has an index or not. The ‘is_null’ column specifies whether a column accepts to store NULL values or not, and if it does not, then this column is considered a mandatory column that must have a value. The ‘is_relationship’ column specifies whether a column has at least one relationship with any of the CTTs or the VETs. The ‘is_primary_key_column’ column specifies whether the column is a primary key. The ‘is_unique_column’ column specifies whether a column has a UNIQUE constraint.

3) **The Row Extension Tables**

The row ETs store virtual table rows for virtual extension columns in three separate ETs. Such ETs are separated in three tables in order to store small data values in the ‘table_row’ ET, which stores values such as NUMBER, DATE-and-TIME, BOOLEAN, VARCHAR and other data types. While large data values are stored in other two ETs, the first ET is the ‘table_row_blob’ that stores BLOB values of virtual columns that stores BLOB data type (e.g. Images, Audio, Video), and the second ET is the ‘table_row_clob’ that stores CLOB values for virtual columns that store TEXT data type (e.g. E-mails, web pages). The EET design separates these three ETs to reduce the impact of BLOB and CLOB values from slowing down virtual schema queries. These three tables have the same columns, except the table row ID column, which is called differently in the three tables. In the ‘table_row’ ET called ‘table_row_id’, in the ‘table_row_blob’ ET called ‘table_row_blob_id’, and in the ‘table_row_clob’ called ‘table_row_clob_id’. A table row ID can be given for several columns that map to one row in a VET. Fig.14 shows an example of this mapping. The corresponding columns in these three tables include, first, the ‘serial_id’ column which is a composite primary key in these tables. This column stores a serial number of a virtual column that maps to a row in the virtual table. Second, the foreign key columns, including ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’ which at the same time are composite primary keys with the Table Row ID column and the ‘serial_id’ column. Third, the ‘value’ column that stores the virtual column values, however, the data types of these columns vary in each of the three row tables according to the data types that supposed to be stored in each table. These three row ETs are capable to store data types, including traditional relational data, texts, audios, images, videos, and XML in structured, unstructured, and semi-structured format. The structured data, such as traditional relational data can be stored in CTTs and VETs as it is presented in the EET design in Section 5. The un-structured data files such as images, audios, videos can be stored in EET, by storing the Uniform Resource Identifier (URI) of a file in the ‘table_row_blob’ ET. Then the actual physical file can be stored in a folder of a file system, and then this file can be accessed using the URI that stored in the ‘table_row_blob’ ET and mapped to the physical file that stored in a folder. The semi-structured data such as XML files can be used in two ways. Firstly, using the same method as used for storing unstructured data, then accessing the XML file using the URI that stored in the ‘table_row_blob’ ET and mapped to the physical XML file that stored in a folder. Secondly, an XML file can be stored as text in the ‘table_row_clob’ ET as a CLOB file, and then accessed from the ‘table_row_clob’ ET. It is being argued that RDBMSs are not scalable, because they are limited in offering good performance and scalability properties. Nevertheless, this issue can be resolved by using any of the available distributed software products in the market that scale and optimize RDBMSs on the cloud, such as MySQL Cluster, VoltDB, Clustrix, ScaleDB, NuoDB, ScaleBase [20], and many others.

4) **Primary Key Extension Table**

The ‘table_primary_key_column’ ET allows tenants to create virtual primary keys for the virtual extension columns which are stored in the ‘table_column’ ET. The structure of this table has a composite primary key consists of ‘table_primary_key_column_id’, ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’. The ‘table_primary_key_column_id’ column is a unique primary key of the table, while the other three columns ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’ are primary keys and foreign keys. The ‘is_auto_increment’ column specifies whether a primary key can be auto-incremented or not. The ‘is_composite_key’ column is used to specify whether a virtual primary key that is stored in a table is a single primary key or a composite primary key.

5) **Relationship Extension Table**

The ‘table_relationship’ ET allows tenants to create virtual relationships between their VETs and CTTs. The table structure has a composite primary key consists of ‘table_relationship_id’, ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’. The ‘table_relationship_id’ column is a unique primary key of the table, while the other three columns ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’ are primary keys and foreign keys. The ‘table_type’ column specifies whether the relationship is with a CTT or a VET. The ‘target_table_id’ column is used to create a master-detail relationship between two VETs, by storing into it the table ID of the master VET that is stored in the ‘db_table’ ET, while the ‘targeted_table_id’ column is used to store into it the primary key ID of the master VET for the same relationship. The ‘shared_table_name’ column is used to create a master-detail relationship between a CTT and a VET, by storing into it the name of the master CTT while the name of
the ‘shared_column_name’ column is used to store the primary key column name of the CTT for the same relationship. Furthermore, this ET can create a master-detail relationship between two VETs, or a CTT and a VET, even if the master table has composite primary keys. Such a relationship can be achieved by storing multiple table rows into the ‘table_relationship’ for the relationship that is between the master table that has a composite primary key, and the details VET. Each of these table rows denotes one of the primary key columns of the composite primary key that relates to the master table. The following are the database relationships that can be created using the ‘table_relationship’ ET between two VETs, two CTTs, or one VET and one CTT, including One-to-One, One-to-Many, Many-to-One, Many-to-Many, and Self-referencing.

6) Index Extension Table

The ‘table_index’ ET is used to add indexes for virtual columns of a VET to improve and speed up the query execution time when retrieve data from this VET. The structure of this table has a composite primary key consists of ‘table_row_id’, ‘serial_id’, ‘tenant_id’, ‘db_table_id’, and ‘table_column_id’. The column ‘table_row_id’ and ‘serial_id’ are unique primary keys that are referred to values stored into ‘table_row_id’ and ‘serial_id’ columns in the ‘table_row’ ET. While the other three columns ‘tenant_id’, ‘db_table_id’ and ‘table_column_id’ are primary keys and foreign keys for this table. The ‘value’ column stores a value that is stored in the ‘table_row’ ET and this value relates to an indexed virtual column, which is specified as an index in the ‘table_column’ ET by storing the necessary value in the ‘is_indexed’ column.

C. Virtual Extension Tables

Virtual Extension Tables are the tables that tenants can create during the application’s runtime execution to extend an existing business domain database schema, or they can create their own virtual database schema from the scratch to fulfill their business needs. In Section 5, a detailed example is presented to explain how the tenants can create their VETs. In using this approach, the service provider who is offering a business domain database, can accommodate a large number of virtual tables by allowing tenants to populate these eight ETs with their data. This approach allows multi-tenant database service providers to manage their services in an efficient and cost-effective manner, and at the same time, it allows each tenant to configure its database schema according to its requirements.

IV. ELASTIC EXTENSION TABLES DATABASE MODELS

The EET multi-tenant database schema allows the service provider to offer his tenants with the choice of using any of the following three database models (Fig. 2):

A. Multi-tenant relational database

This database model allows tenants to use a standard relational database schema for a particular business domain database without the need to extend the existing database structures. This business domain database, can be shared between multiple tenants and differentiate between them by using a Tenant ID column in the CTTs (physical tables). This model can be applied to any business domain database such as Customer Relationship Management (CRM), Accounting, Human Resources (HR), or other business domains.

B. Integrated multi-tenant relational database with virtual relational database

This database model allows tenants to use a standard relational database schema for a particular business domain, extend it by adding additional virtual database tables, and combine these tables with the existing database structure by creating virtual relationships between them.

C. Multi-tenant virtual relational database

This database model allows tenants to create their virtual database schema from the scratch, by creating VETs, virtual database relationships between the VETs, and other database constraints to satisfy the tenants’ special business requirements of the tenants’ business domain applications.
For example, if a service provider offers a sales database schema to be used by multiple tenants, and with this database schema the service provider uses the EET, then this service provider can offer the three database models listed above that fulfill various business requirements. This example assumes that the service provider has three tenants.

The first user evaluated the Sales database, and found that this database suits his business requirements without any modifications. Therefore, this user will use the Sales database schema as originally provided by the service provider as illustrated in Fig. 3 (a). The second user has evaluated the Sales database schema and found that he needs to add extra tables to fulfill his business needs. Thus, this user created VET 1, VET 2, and VET 3, and then, created virtual database relationships between these VETs and the already existing physical tables (CTTs) in the sales database schema. The database model for this user is shown in Fig. 3 (b). The third user evaluated the same database schema and found that it did not suit his business requirements. Therefore, he decided not to use the Sales database schema at all, and instead created virtual relational tables from scratch and established database relationships between them as shown in Fig. 3 (c). This example illustrates the three database models of EET multi-tenant schema. These three database models allow tenants to design their databases and automatically configure their behaviors during their application’s runtime execution.

V. AN EXAMPLE TO COMPARE MULTI-TENANT DATABASE SCHEMA DESIGNS WITH ELASTIC EXTENSION TABLES

This section presents an example that clarifies the seven multi-tenant database schema designs that presented in the related work section, and clarifies the differences between these designs and the EET multi-tenant schema design. This example shows three different tenants, including Tenant-A, Tenant-B, and Tenant-C. Each of these tenants uses a multi-tenant database, and in this database, they configure their sales database structure according to their different business needs. For simplicity, this example illustrates only one sales table that stores a sales person’s information by using different multi-tenant database schema designs. Moreover, this example presents how the EET enables tenants to create their own database schema by extending an existing RDBMS database schema, including the required number of tables and columns, rows, virtual database relationships with any of the CTTs or VETs, primary keys for the columns, indexes for the columns, and assigning suitable data types for columns during multi-tenant application runtime execution. In order to show the difference between the table structures and how database is populated we use the same data across all the designs in this example.

The Private Tables in Fig. 4 show three tenants each of them with different Sales Person table that fulfill their business requirements. Tenant-A has the ‘sales_person_tenant_a’ table, which consists of six columns, including ‘sales_person_id’, ‘first_name’, ‘last_name’, ‘phone’, ‘age’, and ‘gender’. Tenant-B has the ‘sales_person_tenant_b’ table, which consists of four columns, including ‘sales_person_id’, ‘first_name’, ‘last_name’, and ‘business_id’. Tenant-C has the ‘sales_person_tenant_c’ table; the columns in this table are the same as ‘sales_person_tenant_a’ table. The same data that was used to populate the private table was used to populate the rest of the multi-tenant database schema designs and EET schema, which are presented in the example of this section.

The Extension Tables in Fig. 5 show how the columns of the Sales Person tables for the three tenants split-up between the base table ‘sales_person’ and two extension tables ‘sales_person_tenant_a’ and ‘sales_person_tenant_b’.

Fig. 4 Private Tables.

Fig. 5 Extension Tables.
of these three tables have two fixed common columns, including 'tenant_id' and 'row'. The 'tenant_id' column is used to map data rows in the base table and the extension tables with the tenant who owns these rows. The 'row' column is used to give each row in the base table a row number and map it with other rows in the extension tables. The 'sales_person' base table has five columns, including 'tenant_id', 'row', 'sales_person_id', 'first_name', and 'last_name'. All the tenants share the last three columns. The extension table 'sales_person_tenant_a_& c' has five columns, including 'tenant_id', 'row', 'phone', 'age', and 'gender'. This table is shared by two tenants Tenant-A and Tenant-C, due to the similarity in the extension columns that both tenants need. The 'sales_person_tenant_b' is used by Tenant-B, which has three columns 'tenant_id', 'row', and 'business_id'.

![Image](67x386 to 285x558)

The 'sales_person' base table has five columns, including 'tenant_id', 'row', 'sales_person_id', 'first_name', and 'last_name'. All the tenants share the last three columns. The extension table 'sales_person_tenant_a_& c' has five columns, including 'tenant_id', 'row', 'phone', 'age', and 'gender'. This table is shared by two tenants Tenant-A and Tenant-C, due to the similarity in the extension columns that both tenants need. The 'sales_person_tenant_b' is used by Tenant-B, which has three columns 'tenant_id', 'row', and 'business_id'.

![Image](47x208 to 297x261)

The Pivot Tables in Fig. 7 show how the tenants' data with a specific data type is stored in a particular pivot table. The 'int' column is used to map a data type value to a particular table. The 'str' column is used to map a data type value to a particular row in a particular table. The 'row' column is used to map a data type value to a particular row in a particular table.

![Image](313x564 to 586x673)

The Chunk Table in Fig. 8 shows how a set of data columns with a mixture of data types is structured. The 'chunk_int_str' table has six columns, including 'tenant_id', 'table', 'chunk', 'row', 'int1', and 'str1'. The 'tenant_id' column is used to map each table row in a chunk table with a tenant. The 'table' column is used to map a table row to a particular table. The 'chunk' column is used to compound data for more than one logical column for a particular table. The 'row' column is used to map a data value to a particular row in a particular table. The 'int1' column is used to store all the INTEGER data values for different columns of different tables. The 'str1' column is used to store all the STRING data values for different columns of different tables.

![Image](349x267 to 562x383)

The Chunk Folding tables in Fig. 9 show how the most commonly used tenants' columns are structured in the 'account_row' table, while the remaining columns are structured into Chunk Folding table called 'chunk_row'. The remaining columns that are used by tenants have extra business requirements, which are not applied in the common columns in the 'account_row' table. The 'tenant_id' column in both tables is used to map each table row with a tenant. The 'row' column in both tables is used to map a data value in a particular row of a particular table. The table 'account_row' consists of five columns, including 'tenant_id', 'row', 'sales_person_id', 'first_name', and 'last_name'. The last three columns in this table are the common columns that are shared by the three tenants (Tenant-A, Tenant-B, and Tenant-C). The 'chunk_row' table consists of six columns, including 'tenant_id', 'table', 'chunk', 'row', 'int1', and 'str1'. The 'table' column is used to map a row to a particular table. The 'chunk' column is used to
combine data for more than one column for a particular table. The ‘int1’ column is used to store all the INTEGER data values for different columns of different tables. The ‘str1’ column is used to store all the STRING data values for different columns of different tables.

<table>
<thead>
<tr>
<th>tenant_id</th>
<th>row</th>
<th>sales_person_id</th>
<th>first_name</th>
<th>last_name</th>
<th>int1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>100</td>
<td>Joseph</td>
<td>Richard</td>
<td>0213456789</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Sarah</td>
<td>Smith</td>
<td>123</td>
<td>123456789</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>David</td>
<td>John</td>
<td>098</td>
<td>0987654321</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Sam</td>
<td>Zion</td>
<td>321</td>
<td>3210987654</td>
</tr>
</tbody>
</table>

**Fig. 9 Chunk Folding.**

The XML Table in Fig. 10 shows how this technique combines RDBMS and XML by having fixed columns shared by all tenants, including ‘tenant_id’, ‘sales_person_id’, ‘first_name’, ‘last_name’. The ‘tenant_id’ column is used to map each table row in the ‘account_row’ table with a tenant. The rest of the columns are Sales Person columns that are shared by all tenants. The fifth column is ‘ext_xml’, this column is used to store an XML structure includes the rest of the logical columns that tenants may need to fulfill their extra business needs. For instance, as shown in the first table row in the ‘account_row’ table, there are three values stored using XML structure in the ‘ext_xml’ column, including phone, age, and gender.

<table>
<thead>
<tr>
<th>account_row</th>
<th>sales_person_id</th>
<th>first_name</th>
<th>last_name</th>
<th>ext_xml</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>Joseph</td>
<td>Richard</td>
<td>&lt;phone&gt;0213456789&lt;/phone&gt; &lt;age&gt;25&lt;/age&gt; &lt;gender&gt;male&lt;/gender&gt;</td>
</tr>
<tr>
<td>2</td>
<td>123</td>
<td>Sarah</td>
<td>Smith</td>
<td>&lt;phone&gt;0987654321&lt;/phone&gt; &lt;age&gt;45&lt;/age&gt; &lt;gender&gt;female&lt;/gender&gt;</td>
</tr>
<tr>
<td>3</td>
<td>321</td>
<td>David</td>
<td>John</td>
<td>&lt;phone&gt;7896543210&lt;/phone&gt; &lt;age&gt;30&lt;/age&gt; &lt;gender&gt;male&lt;/gender&gt;</td>
</tr>
</tbody>
</table>

**Fig. 10 XML Table**

Fig. 11 shows an example of the EET, which have three VETs that were created using the ETs. These three VETs are the tenants’ tables that presented in the Private Tables in Fig. 4. In this example, the ‘sales_person’ table is a CTT shared by all the three tenants and has predefined columns that are commonly used by these tenants. The Tenant-A has a business requirement to have a Sales Person table that includes the columns that predefined in the ‘sales_person’ CTT, in addition to three extra columns, including ‘phone’, ‘age’, and ‘gender’. This business requirement can be fulfilled by creating the ‘sales_person_tenant_a’ VET and adding to this table these extra three columns. In addition to, adding the ‘sales_person_id’ column that is a virtual foreign key, which builds the virtual relationship between ‘sales_person_tenant_a’ VET and the ‘sales_person’ CTT. The Tenant-B has a business requirement to have a Sales Person table that includes the columns that are predefined in the ‘sales_person’ CTT, in addition to the ‘business_id’ column as an extra column to the CTT. This business requirement can be fulfilled for this tenant by creating the ‘sales_person_tenant_b’ VET, in addition, adding the ‘sales_person_id’ column that is a virtual foreign key, which builds the virtual relationship between ‘sales_person_tenant_b’ VET and the ‘sales_person’ CTT. The Tenant-C has a business requirement the same as the business requirement of Tenant-A. Therefore, the ‘sales_person_tenant_c’ VET of the Tenant-C has a similar structure and relationship of the ‘sales_person_tenant_a’ VET. The shared columns of the ‘sales_person’ CTT store the three tenants’ data, while the rest of the tenants’ data is stored in VETs by using the ETs, including ‘db_table’, ‘table_column’, ‘table_row’, ‘table_relationship’, ‘table_index’, and ‘table_primary_key_column’. The details of this data are shown in Fig. 12 – 18.

**Fig. 11 Virtual Extension Tables (VET).**

**Fig. 12 The data stored in the ‘sales_person’ CTT**

**Fig. 13 The data stored in the ‘db_table’ ET**
In this section, we compare the performance of accessing data from EET and Universal Table Schema Mapping (UTSM) [2]. In EET, data is partitioned vertically, when in UTSM data is partitioned horizontally. Liao et al. [2] state that the data architecture of UTSM is similar to Salesforce data architecture, which originated from the Universal Relations [6]. In addition, a number of database query examples presented in [2], [3], and [1] used to retrieve data from this data architecture. Some of these queries are used in the experiments in this paper, in addition to other queries that are used to show the difference in accessing data from EET and UTSM. The UTSM technique had to be chosen to compare it with EET technique, because as discussed and concluded in the related work section, the Universal Table that is used in UTSM, is considered as the optimal schema design for multi-tenant applications. Moreover, this is one of the multi-tenant database schema techniques implemented commercially by Salesforce. The data architecture of UTSM is shown in Fig. 19. The ‘Data’ table is the universal table that stores all tenants’ data, and it has fixed number of data columns. The number of columns of this table should be large to accommodate the number of columns required by different tenants (e.g. Salesforce uses 500 columns for this table). These columns store data that maps to objects and fields created in the ‘Objects’ and ‘Fields’ tables. The data type of these columns is VARCHAR, which allows the storage of different data types (STRING, NUMBER, DATE, etc.). The ‘Objects’, ‘Fields’, and ‘Relationships’ tables are used to construct virtual tables and their virtual columns, and build relationships between these virtual tables. Whereas the ‘Index’ and ‘Uniquefields’ tables are used to optimize the query execution time of retrieving data from the ‘Data’ universal table [1], [2].

In this performance evaluation, the focus is on comparing the performance of accessing data from EET and UTSM directly from the database level, irrespective of the software solution built on top of these two multi-tenant database schemas for two reasons: (1) The most significant challenge in multi-tenant applications is designing multi-tenant database schema that improves multi-tenant query processing. This schema design influences the software design built on top of the schema and its performance. (2) Comparing the performance of two multi-
tenant software solutions under the same conditions, and using the same hardware resources is difficult, in particular as some software may not be available to be installed on the same application server.

For each single tenant from the multi-tenant database. These experiments are divided into four types that are sharing the details of this data set. Each query of these experiments is performed ten times, and the average execution time of these queries is shown in Fig. 21 – 28. The queries that are related to EET and UTSM are shown in Table 1. The inputs and the outputs of EET and UTSM queries are the same. However, the structures of these queries are different because the data architectures of the two schemas are different. The four experiments details are listed below:

A. Experimental Data Set and Setup

Typically, multi-tenant databases store massive data volumes across multiple servers to optimize the performance of data retrieval. However, before considering scale-up or scale-out for multi-tenant databases to optimize its performance, we believe that we should perform a comparison between EET and UTSM using a single server instance. In order to test the effectiveness of accessing data from these two multi-tenant database architecture designs without affecting their performance by using any scalability. In our experiments, we focus on benchmarking the performance of the main tables of both data architectures where most of the tenants’ data is stored, and we disregard the lookup queries. For example, in EET, we discard the queries which check whether a virtual column is indexed or not from the ‘table_column’ ET. On the other hand, we disregard the queries which check whether a column is indexed or not from the ‘fields’ table of UTSM. In this case, our focus in EET is on ‘table_row’, and ‘table_index’ ETs, and in UTSM is on ‘Data’, ‘Index’, and ‘Uniquefields’ tables. Furthermore, in order to run comparative experiments, exactly the same data was populated in the ‘table_row’, and ‘table_index’ ETs of EET in a separate database, and the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM in another database. No indexes were used other than the default indexes of each schema, which are the primary keys and the foreign keys indexes that are automatically generated in the RDBMS once the primary key and foreign key constraints are specified. The number of virtual rows that were already populated in ‘table_row’ ET is 200,000 rows and the same number of rows in the ‘Data’ universal table. These rows belong to the ‘product’ virtual table, and the structure of this table in EET and UTSM is shown in Fig. 20. There was no data populated in these two databases other than the populated 200,000 rows.

In the multi-tenant database, each tenant’s data is isolated in a table partition. Therefore, the experiments are per-formed for one tenant to evaluate the effectiveness of retrieving data for

1) Retrieving Rows Experiment (Exp.1)

The aim of this experiment is to benchmark the query execution time of retrieving rows from EET and UTSM. This experiment is divided into four experiments including:

Retrieving Rows without Using Query Columns Filters Experiment (Exp.1.1): In this experiment, Query 1 (Q1) and Query 2 (Q2) are executed. The Q1 retrieves rows from the ‘table_row’ ET of EET without specifying any query filters other than the tenant ID, and the ‘project’ table ID. Whereas the Q2 retrieves rows from the ‘Data’ universal table without specifying any query filters other than the tenant ID and the ‘project’ object ID. In this study, eight tests using these two queries are performed to retrieve 1, 10, 50, 100, 500, 1000, 1500, and 2000 rows.

Retrieving Rows Using Columns Query Filters Experiment (Exp.1.2): In this experiment, Query 3 (Q3) is executed on the ‘table_row’ ET of EET and Query 4 (Q4) is executed on the ‘Data’ universal table. Both queries are filtered by specifying particular numbers of product IDs stored in the ‘product’ virtual table. In this study, three tests using these two queries are performed to retrieve rows by specifying 1 product ID for the first test, 10 product IDs for the second test, and 50 product IDs for the third test. The structure of Q4 has presented in [3], but with different value settings.

Retrieving Rows Using Primary Key Indexes Experiment (Exp.1.3): In this experiment, Query 5 (Q5) is executed on the ‘table_row’ and ‘table_index’ ETs of EET and Query 6 (Q6) is executed on the ‘Data’ and ‘Uniquefields’ tables of UTSM. In this experiment, a primary key index is used to retrieve rows from the ‘product’ virtual table from the ‘table_row’ ET and from the ‘Data’ table. In this study, three tests using these two queries are performed to retrieve 1, 10, and 50 rows. The structure of Q6 has presented in [2], but with different value settings.

![Fig. 19 Universal Table Schema Mapping [2].](image1)

![Fig. 20. The virtual ‘product’ table structure.](image2)
Retrieving Rows Using Custom Index Experiment (Exp.1.4): In this experiment, Query 7 (Q7) is executed on the ‘table_row’ and ‘table_index’ ETs of EET and Query 8 (Q8) is executed on the ‘Data’ and ‘Index’ tables of UTSM. In this experiment, a custom index is used, which is a selective filter in the tenant’s query. This index should be other than the primary key and foreign key indexes. This custom index retrieves rows from the ‘product’ virtual table for both ‘table_row’ and ‘Data’ tables. The ‘standard_cost’ virtual column is chosen to filter the queries by looking up for all the products, which have a standard cost greater or equal ‘$ 9000’ from the ‘product’ virtual table. In this study, four tests using these two queries are performed to retrieve 1, 10, 50, and 100 rows.

2) Inserting Rows Experiment (Exp.2)

The aim of this experiment is to benchmark the query execution time of inserting rows into EET and UTSM. Query 9 (Q9) is executed on the ‘table_row’ and ‘table_index’ ETs of EET and Query 10 (Q10) is executed on the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM. In this study, four tests using these two queries are performed to insert 1, 10, 50, and 100 rows.

3) Updating Rows Experiment (Exp.3)

The aim of this experiment is to benchmark the query execution time of updating rows into EET and UTSM. Query 11 (Q11) is executed on the ‘table_row’ and ‘table_index’ ETs of EET and Query 12 (Q12) is executed on the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM. In this study, four tests using these two queries are performed to update 1, 10, 50, and 100 rows.

4) Deleting Rows Experiment (Exp.4)

Deleting Rows Experiment (Exp.4): The aim of this experiment is to benchmark the query execution time of deleting rows from EET and UTSM. Query 13 (Q13) is executed on the ‘table_row’ and ‘table_index’ ETs of EET, and Query 14 (Q14) is executed on the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM. In this study, four tests using these two queries are performed to delete 1, 10, 50, and 100 rows.

The experiments were performed on PostgreSQL 8.4 database, using the default configuration setup. This database installed on a PC with 64-bit Windows 7 Home Premium operating system, Intel Core i5 2.40GHz CPU, 8 GB RAM memory, and 500 GB hard disk storage.

B. Experimental Result

This section gives four experimental results as follows:

1) Retrieving Rows

This experimental result was divided into four results as follows. The experimental study of Exp.1.1 shows that the execution time of Q1 that perform on the ‘table_row’ ET of EET is approximately 76% faster on average than the execution time of Q2 that perform on the ‘Data’ universal table when 1, 10, 50, 100, 500, 1000, 1500, and 2000 rows were retrieved. The details results of this experiment are shown in Fig. 21 – 22. The experimental study of Exp.1.2 shows that the execution time of Q3 that perform on the ‘table_row’ ET of EET is approximately 94% faster on average than the execution time of Q4 that perform on the ‘Data’ universal table when 1, 10, and 50 rows were retrieved. The details results of this experiment are shown in Fig. 23. The experimental study of Exp.1.3 shows

<table>
<thead>
<tr>
<th>Query No.</th>
<th>Query Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>SELECT * FROM table_row tr WHERE tr.table_row_id IN (SELECT distinct(tr2.table_row_id) FROM table_row tr2 WHERE tr2.db_table_id = 16 and tr2.tenant_id = 1000 LIMIT 1)</td>
</tr>
<tr>
<td>Q2</td>
<td>SELECT * FROM data WHERE tenantid = 1000 and objectid = 1 LIMIT 1</td>
</tr>
<tr>
<td>Q3</td>
<td>SELECT * FROM table_row tr WHERE tr.tenant_id = 1000 and tr.db_table_id = 16 and tr.table_column_id IN (50,52,54) and tr2.tenant_id = 1000 and tr2.db_table_id = 16 and (tr2.table_column_id = 47 and tr2.value = '163336' )</td>
</tr>
<tr>
<td>Q4</td>
<td>SELECT price, cost, weight FROM (SELECT value0 AS id, value4 AS price ,value2 AS cost, value6 AS weight FROM data WHERE objectid = 1 and tenantid = 1000 ) AS product WHERE product.id = '163336'</td>
</tr>
</tbody>
</table>

Q6 [2] SELECT * FROM data WHERE objectid = 1 and tenantId = 1000 and dataguid in (SELECT dataguid FROM uniquefields WHERE objectid = 1 and tenantId = 1000 and numvalue IN (163337));

Q11 INSERT INTO table_row (serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,1000, '230.50',16,50);

Q12 INSERT INTO table_index (tenant_id, value, db_table_id, table_column_id) values (50000061,8,1000, '300',16,54);

Q13 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,4,1000, '222.50',16,50);

Q14 INSERT INTO table_index (tenant_id, value, db_table_id, table_column_id) values (50000061,7,1000, '40',16,53);

Q15 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,3,1000, '50000',16,49);

Q16 INSERT INTO table_index (tenant_id, value, db_table_id, table_column_id) values (50000061,6,1000, '242.50',16,52);

Q17 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,2,1000, '1000',16,48);

Q18 INSERT INTO table_index (tenant_id, value, db_table_id, table_column_id) values (50000061,1,1000, '000',16,47);

Q19 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,1000, '05000000',16,47);

Q20 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,6,1000, '300',16,54);

Q21 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,7,1000, '40',16,53);

Q22 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,8,1000, '300',16,54);

Q23 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,1,1000, '000',16,47);

Q24 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,9,1000, '500',16,52);

Q25 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,1000, '05000000',16,47);

Q26 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,6,1000, '242.50',16,52);

Q27 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,2,1000, '1000',16,48);

Q28 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,1,1000, '000',16,47);

Q29 INSERT INTO table_row (table_row_id, serial_id, tenant_id, value, db_table_id, table_column_id) values (50000061,1000, '05000000',16,47);

Q30 INSERT INTO table_index (tenant_id, value, table_row_id, serial_id, db_table_id, table_column_id) values (50000061,6,1000, '300',16,54);
that the execution time of Q5 that perform on the ‘table_row’ and ‘table_index’ ETs of EET is approximately 88% faster on average than the execution time of Q6 that perform on the ‘Data’ and ‘Uniquefields’ tables of UTSM when 1, 10, and 50 rows were retrieved. The details results of this experiment are shown in Fig. 24. The experimental study of Exp.1.4 shows that the execution time of Q7 that perform on the ‘table_row’ and ‘table_index’ ETs of EET is approximately 60% faster on average than the execution time of Q8 that perform on the ‘Data’ and ‘Index’ tables of UTSM when 1, 10, 50, and 100 rows were retrieved. The details results of this experiment are shown in Fig. 25.

2) Inserting Rows
The experimental study of Exp.2 shows that the execution time of Q9 that perform on the ‘table_row’ and ‘table_index’ ETs of EET is approximately 19% slower on average than the execution time of Q10 that perform on the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM when 1, 10, 50, and 100 rows were inserted. The details results of this experiment are shown in Fig. 26.

3) Updating Rows
The experimental study of Exp.3 shows that the execution time of Q11 that perform on the ‘table_row’ and ‘table_index’ ETs of EET is approximately 51% faster on average than the execution time of Q12 that perform on the ‘Data’, and ‘Index’ tables of UTSM when 1, 10, 50, and 100 rows were updated. The details results of this experiment are shown in Fig. 27.

4) Deleting Rows
The experimental study of Exp.4 shows that the execution time of Q13 that perform on the ‘table_row’ and ‘table_index’ ETs of EET is approximately 32% faster on average than the execution time of Q14 that perform on the ‘Data’, ‘Index’, and ‘Uniquefields’ tables of UTSM when 1, 10, 50, and 100 rows were deleted. The details results of this experiment are shown in Fig. 28.
I. CONCLUSION AND FUTURE WORK

In this paper, we propose a novel multi-tenant database schema design called EET, which consists of CTT, ET, and VET. EET allows tenants to create their own virtual database schema, including the required number of tables, columns, rows, virtual database relationships with CTTs or VETs, and assigns suitable data types and constraints for columns during the runtime of multi-tenant applications. EET is a single multi-tenant database schema that has a flexible way of creating database schemas for multiple tenants, by extending a business domain database based on RDBMS, or creating tenants business domain database from the scratch. EET design improves the multi-tenant database performance by avoiding NULL values, assigning primary keys to unique columns, providing indexes to table columns, and storing BLOB and CLOB data types in separate designated tables. In addition, EET design allows the storage of different data types, including structured, semi-structured, and unstructured data. In this paper, we only use structured data for the empirical evaluation, for two reasons. First, storing and retrieving data in XML files (semi-structured data) has the highest response time among the reviewed multi-tenant database schema designs. Thus, while semi-structured data can be stored in EET, it is not recommended as storage for multiple tenants. Second, there are many techniques for storing and retrieving different data types, and comparing all of these techniques with EET within the scope of a single paper is difficult due to the paper length limitations.

EET approach allows the creation of virtual relationships between the tenants’ shared physical tables (CTT) and the tenants’ virtual tables (VET), and allows tenants to choose from three database models: (1) Multi-tenant Relational Database, (2) Integrated Multi-tenant Relational Database with Virtual Relational Database, and (3) Virtual Relational Database. According to our knowledge, this capability is not included in any other multi-tenant database schema design.

We have compared and evaluated the performance of EET and UTSM. The design of EET partitions data vertically to avoid storing rows with NULL values. In contrast, the design of the Universal Table in UTSM partitions data horizontally, which can be associated with significant overheads as a result of the large number of NULL values. The experimental study reported in this paper shows an improvement when retrieving, updating and deleting data from EET over the UTSM. In particular, the experiments of retrieving data from EET indicate better performance when compared to UTSM. The execution time for inserting rows into EET is slightly longer than for inserting rows into UTSM. Overall, this experimental study makes the EET schema a good candidate for implementing multi-tenant databases and multi-tenant SaaS applications. As discussed in the related work section, the Universal Table used in UTSM is widely accepted as an optimal schema design for multi-tenant applications. Therefore, this study measured the feasibility and effectiveness of EET by comparing it with UTSM. Comparing EET with other existing multi-tenant database schema designs that are based on RDBMS and other data storage models will be considered in our future research. Furthermore, in our future research, we will evaluate the performance of EET using multiple tenants and focusing on the scalability of the EET approach.

REFERENCES

Haitham Yaish is an assistant professor at American University of the Middle East, and a member of Centre for Quantum Computation & Intelligent Systems at University of Technology, Sydney. Haitham received his PhD in information technology from University of Technology, Sydney in 2014. He has 16 years industrial experience in the information technology field. His research interest is in Cloud Computing, Software as a Service, Big Data, and multi-tenancy.

Madhu Goyal is working as a Lecturer in the School of Software, University of Technology Sydney. She has done PhD in Computer Science (2002) from University of New South Wales, Australia. Her research is well recognized in the areas of agent-based computing, data mining and cloud computing. She has developed applications for the real-world systems or for domains such as Firefighting world, ecommerce, bioinformatics and intelligent tutoring systems. Her research in Cloud Computing is focused on how Software as Service providers can provide highly secured, optimized, configurable environment for same software and computing environment for multiple tenants.

George Feuerlicht is a senior lecturer at the University of Technology Sydney, and an Associate Professor at the Prague University of Economics, and Unicorn College. George is the author of over 100 publications across a range of topics in information systems and computer science, including recent publications on enterprise architectures, SOA, and Cloud Computing models. George is a member of ACM and a number of conference organizing and program committees. He holds a PhD from the Imperial College, London University, U.K.
Triangle Area Based MCA Technique and Anomaly Based Detection Technique for Detecting DOS Attacks

Varsharani Dudhande
ME Computer (Second Year)
Modern Education Society’s College of Engg., Savitribai Phule Pune University, India.

Sharmila Wagh
Department of Computer Engineering
Modern Education Society’s College of Engg.
Savitribai Phule Pune University, India.

Abstract—The availability of network services are being menaced by the increasing number of Denial-of-Service (DoS) attacks. The availability of such interconnected systems is severely degraded by increasing number of DOS attacks. Denial-of-Service (DoS) attacks cause serious impact on these computing systems such as router, host or entire network. DoS attack detected using Multivariate Correlation Analysis (MCA) technique. Multivariate correlation analysis employs for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. The proposed system uses the Multivariate Correlation Analysis (MCA) technique for accurate characterization also uses the anomaly based detection technique in attack recognition. Anomaly based detection makes system capable of detecting seen and unseen attacks. Moreover, a triangle area based technique is planned to reinforce and increases performance of MCA. The impact of each non-normalized information and normalized information on the performance of the proposed detection system is tested.

Keywords — Denial- of- Service attack, network traffic characterization, multivariate correlations, triangle area.

1. Introduction

Most of the existing commercial IDS products are signature-based but not adaptive or self learning. A common methodology employed in DENIAL-OF-SERVICE (DoS) attacks is to deluge the system with a flood of useless packets that leading to online system crashes.

DoS attacks have emerged as a sort of network intrusive behaviors and have exhibit serious threats to the infrastructures of computer networks and numerous network-based services. DoS attacks severely decrease the provision of a sufferer, which might be a host, a router, or a whole network. The sufferer can be forced it to prevent providing services to alternative parties of network from a couple of minutes to many days. So, effective mechanism for Denial-Of-Service (DOS) attack detection are extremely demanded to safeguard services running on the sufferer. The till principally focus on network primarily based attack detection. The system supported this mechanism monitor traffic passing on the protected network. This mechanism deterrent the servers from monitoring attack and make sure that the servers facilitate with quality services in minimum delay while responding. Moreover network-based detection systems are classified in 2 main approaches. Misuse based detection system employs to spot far famed intrusions with the help of signature of antecedently define rules. Misuse-based detection system having low false positive rate and provides accuracy in detecting work far-famed attacks. This is often not applicable just in case of unknown attacks.
As signature rules are generated manually, it becomes difficult to keep updating and to safeguard network security. To overcome the drawbacks of misuse based detection system in addition to archive novelty tolerant detection system and to develop a new advance idea like anomaly based detection system. Anomaly-based system detects known as well as unknown attacks by monitoring network behavior. Furthermore paper focus on feature correlation analysis. In this approach entire incoming group of traffic observed as legitimate or illegitimate but not individual from group of traffic. To deal with this, paper employs approach supported triangle area to get an improved normalized feature. However approach is depending on information of malicious behavior. Denial of Service (DOS) attacks are unlimited menace to internet websites and among the troublesome security hassle in these days web. The problem of Denial of service attacks has become well known, but it’s been troublesome to look the Denial of Service on the net. During this MCA based detection system to safeguard online servers against Dos attack that is based on previous work in [16]. In this paper Denial-of service (Dos) attack detection system employs the triangle area based detection technique and anomaly based detection technique. Such system provides correct characterization of traffic and detection of known and unknown intrusions.

II. RELATED WORKS

Sharmila Wagh, V. Pachghare, S. Kolhe [1] proposed the idea of applying machine learning techniques for intrusion detection is to automatically build the model based on the training data set. This data set contains a collection of data instances each of which can be described using a set of attributes (features) and the associated labels. The attributes can be of different types such as categorical or continuous. Machine Learning Intrusion Detection system has been giving high accuracy and good detection of novel attacks. V. Paxson [17] describes that increasing Internet connectivity is good opportunities for attackers to get entry in computers over the network. The detecting such attacks are termed network intrusion detection, enormously new area of security research. From a security tracking perspective, drops can completely defeat the monitoring, since the missing packets may contain precisely the thrilling site visitors that identify a network intruder. Given our first layout requirement excessive-speed tracking then averting packet clear out drops will become another robust requirement. Aruna Jamdagni, Zhiyuan Tan, Priyadarshani Nanda, Ping Hill [14] proposed the principle component analysis technique that employs data preprocessing, mahalanobis map for extracting features from incoming packets. It also propose iterative feature selection engine for characteristic choice cause. This gadget detects payload based assaults in real time. Z.Tan, A. Jamdagni, X. He, P. Nanda and R.P.Liu [15] illustrate that the detection of dos attack is essential for safety of the online offerings services. The DOS assault detection mainly specializes in the development of the network primarily based detection mechanism [3]. The detection structures have two strategies specifically misuse detection and anomaly detection. Misuse detection is used to identify the known attacks, using the signatures of predefined rules [2]. The relied on profile generation is constructing and handed over to the assault detection module, which compares the tested profile with the normal profile.

Z. Tan, A. Jamdagni, X. He, P. Nanda [14] describes Dos attack temporarily
prevent services from connecting to the internet. The detection, which monitors any network activity presenting any significant deviation from their normal profiles as a suspicious intrusion. It also proposed the analysis method that employs information preprocessing, mahalanobis map for extracting functions from incoming packets. It also propose iterative feature selection engine for characteristic choice cause. This gadget detects payload based assaults in real time. It has 3 key capabilities. First, for anomaly detection operates on aggregate visitors, without glide separation or deep-packet inspection. Both of those traits are vital for a realistic and deployable anomaly detection technique. At the same time as it’s far real that the source and destination IP addresses of each packet are usually available on the routers, port numbers aren’t available without glide separation. A few previous works makes use of features associated with the supply and destination port numbers and so will not be capable of hit upon anomalies in aggregate or VPN tunneled visitors. Notice that working on combination visitors is sufficient to detect anomalies. Shuyuan Jin, denial so young, xizhao wang [11] illustrate that covariance matrices employs multiple network attack detection. Network based detection system categorized in two different approaches misuse based detection and anomaly based detection. Misuse based detection have low false positive rate as well as accurate detection of known attacks. This is not applicable in case of unknown attack. It uses signature of predefined rule. Anomaly system detects known as well as unknown attacks by monitoring network behavior presenting significant deviation from legitimate traffic as suspicious object. The paper proposes the covariance matrices to find out the impact of coherent relations and feature depending on multiple attacks. The effectiveness of intrusion detection system by evaluating percentage of known and unknown attack. A covariance matrix keep two types of information: first is information in group of samples and second is correlation information among the observed features. Furthermore, the covariance based detection employs performance improvement by using group of samples in the detection and efficiency differentiate different classes where mean based detection approaches fails.

P. Garcia-Teodoro, J. Diaz-Verdejo and E. Vazquez [2] puts the adaptive security related approaches:anomaly based intrusion system protect online or protected system against malicious behavior. Intrusion detection system architectures is based four functional modules:
1. Analysis boxes: processing modules for analyzing and detecting potentials behavior.
2. Database boxes: This element uses to store information from E blocks.
3. Response boxes: the intention of this type of block is the execution.
The intrusion detection system may be either host based or network based. Host mainly analyzes event related to OS information such as system calls. Intrusion detection system is categorized as either signature or anomaly based detection system. Signature based defined pattern within analyzed pattern, within analyzed data. Anomaly system detects known as well as unknown attacks by monitoring network activities presenting deviation from legitimate traffic as suspicious object. Chih-fong tsai, chai-ying lin [13] described a learning model based on triangle area based nearest neighbors (TANN) in order to detect attack with accuracy. This method illustrate that the technique of triangle area based nearest neighbors (TANN) by combining unsupervised and supervised learning technique to detect attacks. The classification technique is used as component and then clustering technique.
Like supervised it is not able to distinguish data with accuracy. Hence, initially classifier is trained and then it provides output. Then this output is given as a input to cluster for the purpose of improving clustering performance. The proposed TANN is composed of 3 steps: 1) clusters center extraction, 2) new data formation by triangle area and KNN training, 3) training and testing based on new data. The centroids from given dataset having capabilities of distinguish between similar and dissimilar data or classes. Therefore triangle area represents the new features for evaluating similar attack. Then KNN classifier used features of triangle area to detect attack.

III. MULTIVARIATE CORRELATION ANALYSES IN DETAIL

Incoming network attack traffic treats diversely from normal network traffic and those are reflected by statistical properties. To describe such properties MCA technique is used. The network attack traffic causes changes to the correlation of features. So that such changes can be used for identify malicious behavior.

The MCA employs triangle area for extracting the geometrical correlation between features of incoming network traffic. All triangle areas are arranged on the map. The values of the diagonal elements are set to zero because only considering correlation between each pair of distinct features of incoming traffic. Then comparing two TAMs along with their main diagonal. To make immediate comparison between two TAMs choose either upper or lower triangle of TAM.

The advantages provided by the MCA technique are as follows:
1. It does not require the knowledge about historical traffic to perform analysis.
2. It provides the characterization for individual network traffic record.

Given an arbitrary dataset $x^T = [x_1, x_2, x_3, ..., x_n]$
Where $x^T = [f_1, f_2, f_3, ..., f_m]$ represents ith m-dimensional record. Where $f_i$ is the value of the lth feature in the ith traffic record. To achieve the triangle build by using two features. For analysis purpose all possible permutations of any two distinct features in the vector X are extracted. With the help of those features triangle areas are formed.

IV. PROPOSED SYSTEM

A. Architecture

For accurate network traffic characterization our system uses Multivariate Correlation Analysis (MCA). In decision making system incoming requests are compared with the normal profile. In this system there are three types of actors, such as user, expert user and admin. So, when user wants service of system, he sends a request. The expert user accepts the request and then provides services to the user. The admin having the capabilities that he is able to know this all interaction between user and expert user. When user trying to send the request containing malicious data then system recognize the attacks in it. Admin able to block the respective user. In this system every single request is detected by comparing with normal profiles.
B. Modules

1) Network Traffic

Capturing the packets from incoming network traffic. Instead of monitoring malicious traffic, concentrate on related inbound traffic.

2) MCA

Multivariate Correlation Analysis contains Triangle Area Map Generation module. The triangle area is used to calculate the relation between incoming packets. The feature normalization module is used to normalize traffic record. The malicious requests change the correlation. Hence, changes can be identifying as intrusive activity.

3) Decision Manager

The anomaly based detection method is employs in Decision Making and responsible to filter the malicious data and traffic data. It detects DOS attacks without having relevant knowledge.

4) Normal Profile

In the Training Phase the normal profiles build for various types of legitimate requests, and the generated normal profiles are stored in a database.

5) Detection Phase

In the test phase The Tested Profile builds for the purpose of observing the individual requests coming from MCA module. Such observed requests are then sent for attack detection. The Attack Detection module compares tested profiles with the respective stored normal profiles. If the dissimilarity is more than the expected threshold, then particular request is recognized as malicious request and that user is blocked by the system. Else recognize as a normal and provide the requested service.

C. Normal Profile Generation Algorithm

1: Input network traffic of n element.
2: Extract original features from individual records.
3: Apply the technique of triangle area to extract the geometrical correlation between the extracted features in the vector x.
4: Normal profile generation.
   i. Generate triangle area map of each record.
   ii. Generate covariance matrix.
   iii. Calculate MD between legitimate records TAM and input records TAM.
iv. Calculate mean.

v. Calculate standard deviation.

vi. Return pro.

5: Attack Detection.

i. Input: observed traffic, normal profile and alpha.

ii. Calculate MD between normal profile and incoming traffic.

iii. If MD ≤ threshold
   Detect Normal
   Else
   Detect attack.

D. Mathematical Model

Input: Incoming network traffic record.

System S = {NP, MD, TD, T}

Where,
S be the system
NP = Normal Profile
MD = Mahalanobis Distance
TD = Traffic Detection
T = Threshold

Output: Traffic Detection

TD = {AT, NT}

Where,
AT = Abnormal Traffic
NT = Normal Traffic.

E. Features of proposed System

The DoS attack detection system presented in this paper employs the principles of MCA and anomaly-based detection. They equip our detection system with capabilities of

1. Detect of known and unknown attacks respectively.
2. To speed up the process of MCA.

3. Eliminate bias from raw data by using normalization technique.

F. Detection rate and false positive rate of normalized data

<table>
<thead>
<tr>
<th>Threshold</th>
<th>1σ</th>
<th>1.5σ</th>
<th>2σ</th>
<th>2.5σ</th>
<th>3σ</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR</td>
<td>1.93%</td>
<td>1.19%</td>
<td>0.63%</td>
<td>0.60%</td>
<td>0.58%</td>
</tr>
<tr>
<td>DR</td>
<td>100.00%</td>
<td>99.83%</td>
<td>99.68%</td>
<td>99.68%</td>
<td>93.35%</td>
</tr>
<tr>
<td>Accuracy</td>
<td>99.95%</td>
<td>99.81%</td>
<td>99.67%</td>
<td>99.67%</td>
<td>93.50%</td>
</tr>
</tbody>
</table>

As shown in above table, the threshold controls the degree of the dissimilarity, which is accepted by the system, between a test object and the respective learnt normal profile. If the dissimilarity is beyond the determined threshold, the test object is classified as an attack. On one hand, it can be seen clearly from Table that a better FPR is achieved when a greater threshold is accepted. On the other hand, greater thresholds produce lower DRs.

G. Experimental Details

In this system there are 3 actors such as user, expert user and admin. The admin handles the overall server providing services. The user sends request to access the services from the system. The expert users, then accept the request and then reply with the expected service. Suppose if the user trying to send the malicious request, then system detect as an attack else normal. The admin has the ability that he can block that particular user.

Figure 2 and 3 describes about user registration and successful login
respectively. Figure 4 shows user able to send requests to the system. As shown in figure 5 traffic is captured from the network. Figure 6 shows an administrators dash board which contained detailed information about normal user’s requests and expert user’s details. Attack detected by the system when incoming traffic deviates from normal profiles as shown in figure 7.

Fig. 2. User Registration

Fig. 3. User Login

Fig. 4. User Profile
V. Conclusion

This MCA-based DoS attack detection system is powered by a triangle-area based MCA technique and an anomaly-based detection technique. This technique extracts geometrical correlations hidden in individual pairs of two distinct features within the each network traffic record, and offers more accurate characterization for network traffic behaviors. The normalized data provides more accuracy in detection. This system is able to distinguish between known and unknown DoS attacks from proper network traffic.

REFERENCES


Proposed Hybrid model to detect and prevent SQL Injection.

Abstract- SQL Injection vulnerability takes advantages of the poorly coded web application and exploits the sensitive and critical information stored in an application’s database by compromising the authentication logic of the database server. In Most of the web applications user inputs in the dynamic web pages are the vulnerable points for SQL injection attack. A Single detection tool cannot handle the sophisticated injection attacks by the intelligent hackers. The proposed hybrid model with SQLI-Rejuvenator on an Application Program Interface is tested and proved as an efficient technique to detect and prevent SQL injection. In this architecture, the malicious queries are blocked and an alert message is generated if the injection is detected. Only the benign query is allowed to access the data from the backend database server. The Unique identity created by the template creator application, the Rejuvenator module and evaluation engine are significant features of the proposed model to prevent the Injection attack and can facilitate better availability of the application.

Keywords – Authentication; Injection; Vulnerability; Hackers; Detection; Rejuvenation;

1. INTRODUCTION

Most of the SQL injection vulnerabilities occur when the on line application does not validate the input entries accepted through web forms, cookies and other input parameters. These type of attacks by-pass the authentication logic, breaks the confidentiality of the database. Vulnerability scanners, Similarity measures and many other automated tools for verifying SQLIA statically in source code and dynamic validation during execution are also available within the web applications. A single tool or procedure cannot effectively handle the upcoming sophisticated attacks. SQL Injection has been an issue for many years, and there are enough researches carried out to tackle this situation yet the risk rate of SQL injection is increasing exponentially in proportional to the behavior and size of online business applications[1]. Most of the commercial applications are offering closer interactions to its users or visitors than earlier in order to be competent, these features should be implemented with appropriate security measures. As there are fully automated injection tools available with the intelligent hackers they are discovering better methods and services that are susceptible to SQL Injection attack, which can execute the malicious injection even in the old application. Most of the available validation tools required source code modification which is a tedious task and will affect the performance of the underlying web application and the storage requirement is also high[2].

II. MOTIVATION

Web application features like logon pages, contact forms, search function, feedback fields and the functions used for delivery of dynamic contents are all susceptible to SQL injection attacks even after the implementation of
model checking, Vulnerability scanners and firewalls. There should be an effective mechanism to handle this situation[3]. As the popularity of web applications demand better user interactions for the routine services, the sophistication of attacks is also growing proportionally and there is a requirement for a stronger method to prevent any kind of exploits on the sensitive information through the vulnerable points. Most of the existing SQLIA prevention approaches target only a subset of SQLIA attack types, a single service can handle only a portion of the attack spectrum and only a few approaches are developed to handle first and second order injections in parallel[4]. There is high demand for an effective approach which can work under a lighter storage specification, without false positives and reduced time space complexity[5].

III. SQL INJECTION

SQL injection vulnerability is a weakness in the web application source code, commonly occur when there is an improper validations on the values received from web form, cookie and other input parameters. SQL-Injection attack is one of the top listed vulnerability by OWASP that can be classified under immediate or persistent attack and mostly referred as first order and second order attack respectively[18] . If a malicious user can control the input send to an SQL query, where the data is interpreted as code, he may be getting a malicious entry to the backend server for manipulating the confidential data that can compromise all sensitive and critical information stored in backend database.

A. SQL-Injection Categories

Some of the sample Intended/legal queries , Input queries and detection field identified with the proposed template creator application by the users are tested in the proposed model and the detection field in the template creator application is listed as:

1) Intended Query: SELECT username,password FROM users WHERE lastname=$lastname AND firstname=$firstname;  
Injected Query: SELECT username,password FROM users WHERE lastname=$lastname AND firstname=$firstname AND $status IN (SELECT statuses from STATUS WHERE pid=$pid OR pname=$pname);  
Detection Fields: identified with template creator application: Operator, Query Type, Fields, Tables.

2) Intended Query: UPDATE users SET password='Nicky' WHERE id=2 and username='Olivia';  
Injected Query: UPDATE users SET password='Nicky' WHERE id=2 and username='Olivia';  
SHUTDOWN;  
Detection Fields: Number of independent Queries

3) Intended Query: SELECT ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE ProductName LIKE 'G%';  
Injected Query: SELECT ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE ProductName LIKE 'G% ' UNION SELECT name, type, id FROM sysobjects;--  
Detection Fields: Operator, Fields, Comment

4) Intended Query: UPDATE users SET password='Nicky' WHERE id=2 and username='Olivia';  
Injected Query: UPDATE users SET password='Nicky' WHERE id='2' AND username='hai' or ' '=';  
Detection Fields: Operator.

5) Intended Query: INSERT INTO users (username,password) VALUES('jack',''');  
Injected Query: INSERT INTO users (username,password) VALUES('jack','123', (Exec(char(0x73687574646f776e)));--);  
Detection Fields Comment.

Most of the SQL-Injection can be categorized under first order and second order attacks, more specifically under the category of Tautology, Union Queries, and Piggy backed queries, logically incorrect queries, stored procedure, inferences and alternate encoding[6].
IV. RELATED WORK

There are number of code checkers and detection tools available to mitigate the SQL injection vulnerabilities in both static and dynamic run time queries generated through the user input by a web application before accessing it to the database server[7]. There are hybrid models available to detect and prevent the SQL injection in some of the models are having limited functionality and scope. AMNESIA is a model based approach which makes use of dynamic and static analysis to build the query model. Identifying the hot spot, Building query model, Implement the application and Run time monitoring are the important stages in this model[8]. It is a completely automated model where the queries breaching the model are considered as injection and will be blocked before execution at the database server. Primary limitation of this model is that this technique is depending on the accuracy of its static analysis phase. SQL- Prob is a proxy server based approach; it dynamically recognizes and removes malicious user input [9]. It can detect the listed, all the major categories of SQL Injection attacks with a very minimum resource utilization. Since it is a complete black box approach, it does not require any application modification or any other types of complex input validations. SQL-IDS are a specification based technique to detect the exploitation of SQL injection vulnerabilities [10]. In this model the major focus is on query specific detection and has negligible computation overhead. There is no occurrence of false positive and false negative. SQL_DOM works on an API with type checking facilities and uses call Level Interfaces. The encapsulation techniques are taking care of authentication access to the database server [11]. Even though there is appropriate filtering and input checking, the model still requires further research support against the upcoming sophisticated queries demanded by the clients of an application. The available tools and techniques identified are having its own limitations and weaknesses and cannot give complete assurance against the injection attack [12].

V. THE PROPOSED HYBRID MODEL

The proposed Hybrid Model embedded on an application Program Interface is an effective mechanism to detect SQL Injection before it is executed by the Data base server. It is a novel template based approach for detection and prevention of various categories of SQL-Injection. The architecture of the proposed hybrid model is as shown in “Fig. 1”.

A. Standard Query Template creator and Template Store

In most of the web applications each page can generate multiple database requests and so there will more than one legitimate query pattern corresponding to those queries. Template files can be created by parsing the query based on template specification format designed [13]. Template specification format is shown in “Fig. 2”. All the generated queries with unique identity will be stored at the Template repository.
B. SQL-Template Mapper

The proposed approach has the specific parsing and mapping procedure to match between the template fields corresponding both standard query and Injected query later direct the alert message/result to the query evaluation engine. Both the files are stored in JSON format. The template mapper retrieves template contents from the JSON file. Sample query format with a unique identity is shown in “Fig 3”. Since it is stored in a JSON format accessing will be faster, which is an added advantage.

C. Query Evaluation Engine

The query evaluation engine compares the unique Identity created for the standard query template and the input query template [14]. If the Injection is not detected in the first level it will refer to the second level detection. In any level a contrast is found, then the malicious query message is reported and only the benign query directed to the database server[15]. The SQLI-Shield, a Jar file, embedded in API allows matching regular expressions against columns which are related to the user input components in the corresponding web application. In such cases, the system procures this input from the input query and performs validation against the regular expression. The SQLI-Shield format can be initiated by giving the appropriate template Identity of a intended query as shown in “Fig. 4”.

D. Query extractor class

The Query extractor class used in Java based application developed for the hybrid model has identified the major categories of specifications as shown in “Table 1”.

<table>
<thead>
<tr>
<th>Sno</th>
<th>Specification type/string extracted</th>
<th>Sno</th>
<th>Specification type/string extracted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Query type</td>
<td>7</td>
<td>Global variables</td>
</tr>
<tr>
<td>2</td>
<td>Joints</td>
<td>8</td>
<td>System Variable</td>
</tr>
<tr>
<td>3</td>
<td>Aggregate functions</td>
<td>9</td>
<td>Quoted String</td>
</tr>
<tr>
<td>4</td>
<td>comments</td>
<td>10</td>
<td>Input string</td>
</tr>
</tbody>
</table>
E. SQLI Detection Engine

In this module the SQL Detection Engine evaluates the incoming queries with the specification template by checking possibility of injection and gives the alert messages. Malicious queries are blocked, only the benign queries are allowed to access the database server [16]. The Query Reconstruction module in the proposed hybrid model will reconstruct the queries by eliminating injections and also rebuilding missing portions, if any, and removing injected part of the user query [17].

F. The Query Reconstructor

The proposed strategy is to verify the query and reconstruct it, if it is possible using the Application Program Interface, before actual execution in the database server. The important features in the proposed approach is automatic creation of standard query template with training dataset, validation of user input against regular expression patterns and reconstruction of injected queries[14]. The core of this system is a class named “SQLI-Shield” which can be instantiated with a parameterized constructor with parameter values as standard query template path and an output folder path [17]. The status report of rejuvenation process is as shown in “Fig. 5”.

VI. THE SQLI_REJUVENATOR.JAR, PACKAGE FILE

In order to get better system availability rather than rejecting the query without much validation, the proposed hybrid model has a special package file, SQLRejuvanre.jar. The constructors and functions used in this package file are shown in Table 2.

<table>
<thead>
<tr>
<th>Constructor/Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLRejuvenate(String standardSqlString)</td>
<td>A constructor to initializes the standard SQL string</td>
</tr>
<tr>
<td>SQLRejuvenate(String standardSqlString, String[] regularExpression)</td>
<td>A constructor to initializes the standard SQL string and array of regular expressions for inputs</td>
</tr>
<tr>
<td>SQLRejuvenate(File trainingDataSetfile, String[] regularExpression)</td>
<td>A constructor to initializes the standard SQL string that created from training data and array of regular expressions for inputs.</td>
</tr>
<tr>
<td>detectSQLIA(String inputSqlString)</td>
<td>A function , detects the SQL injection and returns true if found</td>
</tr>
<tr>
<td>validateNoOfIndependentOrSubQueries(String inputSqlString)</td>
<td>A function checks the number of independent or sub-queries. Returns true if no injection found.</td>
</tr>
<tr>
<td>validateQuerytype(String inputSqlString)</td>
<td>A function, checks query type in the order they appear. Returns true if no injection found.</td>
</tr>
<tr>
<td>validateUsedTables(String inputSqlString)</td>
<td>A function, checks used tables in the order they appear. Returns true if no injection found.</td>
</tr>
<tr>
<td>validateColumns(String inputSqlString)</td>
<td>A function, checks columns in the order they appear. Returns true if no injection found.</td>
</tr>
</tbody>
</table>
validateSystemVariables(String inputSqlString)  A function, checks system variables in the order they appear. Returns true if no injection found

validateGlobalVariables(String inputSqlString)  A function, checks global variable in the order they appear. Returns true if no injection found

validateFunctions(String inputSqlString)  A function, checks aggregate or built-in SQL functions in the order they appear. Returns true if no injection found

validateJoins(String inputSqlString)  A function, checks joins in the order they appear. Returns true if no injection found

validateSpecialSymbols(String inputSqlString)  A function, checks special symbols the order they appear. Returns true if no injection found

validateOperators(String inputSqlString)  A function, checks operators used in the order they appear. Returns true if no injection found

validateCommentSymbols(String inputSqlString)  A function, checks comment symbols in the order they appear. Returns true if no injection found

validateKeywords(String inputSqlString)  A function, checks keywords in the order they appear. Returns true if no injection found

setInputFields(String[] regularExpression)  A function sets regular expression for each input field in the order they appear.

validateAllInput(String inputSqlString)  A function, checks input field values with regular expressions. Returns true if all inputs are valid.

detectSQLIAWithReconstruction(String inputSqlString)  A function, detects SQL injection and returns reconstructed query with valid input values if any injection found.

VII. RECONSTRUCTION ALGORITHM

Reconstruction of query is possible by comparing it with Regular expression and by implementing this strategy the application system availability can be increased. The Reconstruction algorithm is shown in “Table 3”.

**TABLE :3 RECONSTRUCTION ALGORITHM**

<table>
<thead>
<tr>
<th>Algorithm Reconstruction</th>
<th>(InputQuery, ValidQuery)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1. RegularExpression[] =</td>
<td></td>
</tr>
<tr>
<td>2. getRegularExpression(ValidQuery);</td>
<td></td>
</tr>
<tr>
<td>3. SplitList1[] =</td>
<td></td>
</tr>
<tr>
<td>4. getQuerySplitter(InputQuery);</td>
<td></td>
</tr>
<tr>
<td>5. For i = 0 to length(InputList)-1</td>
<td></td>
</tr>
<tr>
<td>SplitList2[].remove(InputList[i]);</td>
<td></td>
</tr>
<tr>
<td>//First Case: When extra queries are inserted and removed.</td>
<td></td>
</tr>
<tr>
<td>6. For i = 0 to length(ValidQuery)-1</td>
<td></td>
</tr>
<tr>
<td>If(SplitList1[i].isEqualTo(SplitList2[i]))</td>
<td></td>
</tr>
<tr>
<td>intermediateQuery = SplitList2[i];</td>
<td></td>
</tr>
<tr>
<td>Else</td>
<td></td>
</tr>
<tr>
<td>If(i&lt;length(ValidQuery)-1) Then</td>
<td></td>
</tr>
<tr>
<td>intermediateQuery+=ValidQuery[i];</td>
<td></td>
</tr>
<tr>
<td>Next</td>
<td></td>
</tr>
<tr>
<td>For j = i to length(ValidQuery)-1</td>
<td></td>
</tr>
<tr>
<td>intermediateQuery;</td>
<td></td>
</tr>
<tr>
<td>End If</td>
<td></td>
</tr>
<tr>
<td>Return</td>
<td></td>
</tr>
<tr>
<td>//Second Case: When injection in Input field.</td>
<td></td>
</tr>
<tr>
<td>7. For i = 1 to length(InputList)</td>
<td></td>
</tr>
<tr>
<td>If(validateInputWithRegularExpression(InputList[i],RegularExpression[i]))</td>
<td></td>
</tr>
<tr>
<td>ValidInput[i] = InputList[i];</td>
<td></td>
</tr>
<tr>
<td>Else</td>
<td></td>
</tr>
<tr>
<td>ValidInput[i] = NULL;</td>
<td></td>
</tr>
<tr>
<td>End If</td>
<td></td>
</tr>
<tr>
<td>Next</td>
<td></td>
</tr>
<tr>
<td>8. Temp=0;</td>
<td></td>
</tr>
<tr>
<td>For i = 1 to length(InputList)</td>
<td></td>
</tr>
<tr>
<td>Index=ValidQuery.indexOf(InputList[i]);</td>
<td></td>
</tr>
<tr>
<td>RejuvenateQuery+=intermediate.substring(Temp,Index)+InputList[i];</td>
<td></td>
</tr>
<tr>
<td>Temp=Index+1;</td>
<td></td>
</tr>
<tr>
<td>Next</td>
<td></td>
</tr>
</tbody>
</table>
VIII. PERFORMANCE EVALUATION

The proposed architecture is complimentary to many of the available model due to faster detection and low overhead on storage. Using the sample cheat sheet of test data for malicious input query on the web applications are tested on the Template creator application test result as shown in "Table 4". All major vulnerable categories of malicious queries were identified and tested for SQL Injection and proved that there is 100% detection is possible with the proposed model, which shows that the proposed system is very efficient as there are no false positives reported.

<table>
<thead>
<tr>
<th>Sno</th>
<th>Type of Queries</th>
<th>False Positives</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tautology</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>2</td>
<td>Union Queries</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>Piggy Backed Queries</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>Logically Incorrect Queries</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>5</td>
<td>Stored procedure</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>6</td>
<td>Inference</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>7</td>
<td>Alternate Code</td>
<td>0</td>
<td>100%</td>
</tr>
</tbody>
</table>

Performance evaluation of the research work also carried by executing the Injected queries shared within the applications mentioned in the URL and Cheat sheet given in the table using the Template creator application of the proposed model. The test result shown in “Table. 5”. TABLE 5. TEST RESULTS OF VULNERABILITIES FOUND IN CHEAT SHEETS.

<table>
<thead>
<tr>
<th>Program</th>
<th>Mode</th>
<th>Proposed Template based hybrid SQLI detection model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schoolmate</td>
<td>SQLI</td>
<td>6</td>
</tr>
<tr>
<td>Webchess</td>
<td>SQLI</td>
<td>12</td>
</tr>
<tr>
<td>Faqforge</td>
<td>SQLI</td>
<td>1</td>
</tr>
<tr>
<td>EVE</td>
<td>SQLI</td>
<td>2</td>
</tr>
<tr>
<td>Geccbbite</td>
<td>SQLI</td>
<td>2</td>
</tr>
<tr>
<td><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku#LineCommentAttacks">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku#LineCommentAttacks</a></td>
<td>SQLI</td>
<td>5</td>
</tr>
<tr>
<td><a href="http://www.sqlinjection.net/union/">http://www.sqlinjection.net/union/</a></td>
<td>SQLI</td>
<td>14</td>
</tr>
</tbody>
</table>

VIII. CONCLUSION AND FUTURE WORK

The test result shown in “Table. 4” and “Table. 5” proves that Proposed Architecture of the Hybrid model on an Application program Interface is an efficient and effective approach towards the detection of SQL Injection and prevents SQL Injection attack. The parsing techniques, storage format JSON and Jar files used in the used in the template creator application of the model will increase the efficiency of the detection technique and provides faster processing time. 100% detection is possible with this approach, If the user input is evaluated by assigning and matching it with an appropriate template Identity during the implementation of the web application with the proposed hybrid architecture. There are no false positives reported with the current test data and cheat sheet used for evaluation. Due to the
expanding trend of attack spectrum, 100% security cannot be assured. According to the WASP security report still there are security holes through which exploiting of confidential information is possible, which requires further research, development with sophisticated detection techniques.

REFERENCES:


****
HAND GESTURE RECOGNITION SYSTEM

ABBES Zeineb, CHIBANI Chaala
Dept of industrial computing. Higher Institute of Computer and Multimedia
Gabes, Tunisia

Tarek Frikha, Abir Hadriche
CES Lab, REGIM Lab
Sfax, Tunisia

Abstract: in this article, we will propose a real-time human hand gesture recognition system which will perform translations from the sign language to the common French language. The processes is composed by three basic steps:

➢ The detection and extraction of the hand pattern characteristics during the image stream acquisition, which is obtained from an integrated camera.
➢ The analysis process, in which the obtained characteristics are classified as either a recognized sign language gesture or an unclassified hand movement. Preset characteristics of each effective hand gesture are stored locally.
➢ The message-assembling phase: at the end of cycle of each iteration of the two previous steps, the obtained result is either neglected or concatenated with the assembled message so far. The message is then displayed.

Keywords: human-machine communication, gestural interaction, French sign language, linked gesture recognition.

1. INTRODUCTION

Recently, many human machine interfaces have been implemented to ease the user experience (such as keyboard, mouse, joystick or touch-sensing devices) and open possibilities for further technology exploitation (3D mouse, virtual reality based systems) and push ahead ergonomic specifications to facilitate operating these systems for specific user categories.

Several experiences in operational state are proved their incompleteness for specific cases, which occur rather frequently, especially when used by people with special needs.

Therefore, researches were oriented to satisfying more natural, specific and richer interactions, which is the case for gestural HMIs.

Gestures researched were mainly head gestures, pupil gestures and commonly hand gestures. Therefore, gestural servitude was founded.

Hand gesture is the one best and most expressive processing friendly human movement with its distinguished organ shape and wide range of posture possibilities. Thus, a gesture has an exact and rich expression.

The hand Sign Language is the most expressive evidence; it indicates the robustness of the hand gesture expression and its importance in communication, which competes with speech interactions in fulfilling the purpose of the communication.

This type of communication, easy to be comprehended by humans, however it have many difficulties to be implemented by the process technologies, needs an acquisition and processing tool to make it.
This tool should provide real time sensing via an external sensor (such as cameras, biometric sensors or digital censoring gloves).

In addition, deaf people would not always dare to insist on describing their needs, expose the best practices to follow to ensure better and easier communication and especially will not insist on re-expressing their thoughts due to possible psychological issues.

From there, we issued our idea to implement our hand gesture recognition system to help support communication for those who find obstacles within it.

II. RELATED WORK

Several applications/libraries have been developed to perfect the hand gesture recognition for the common purpose of recognizing the hand “object”, thus, we find a wide range of utilization in this objective.

Some of the developed HMI [1] benefits of the electrical gloves equipped with inflection sensors to ensure recognizing the hand posture allowing freedom of positioning relatively to the system in the same time, offering also more flexibility of the hand orientation and the movement direction and solves radically the problem of left handed / right handed person situation.

Others [2] propose an alternative which facilitate hand shape detection: the use of specially colored gloves to standardize the anticipated color of the hand rather than processing the skin color which is very variant and subject to many different conditions (therefore, especially solving the problem of race difference)

In addition, there was developed the “hand to machine interface device [3] that provides real-time gesture, position and orientation information. The key element is a glove and the device as a whole incorporates a collection of technologies. Analog flex sensors on the glove measure finger bending. Hand position and orientation are measured either by ultrasonic, providing five degrees of freedom, or magnetic flux sensors, which provide six degrees of freedom.”

Finally, there were many applications developed to improve and make the challenge to recognize the bare hand directly just by relying on multi-level complex algorithms, which was the hardest but most effective solution, just because it offers the most amount of ergonomics to the user, which again, is the main purpose of implementing these systems generally, and our system specifically.

III. THEPROPOSEDSOLUTION

The solution provided by this system is composed of three main steps, which are divided to sub sequences and composites.

The first step is the acquisition phase, a real time image stream transfer is provided from an integrated live camera, which is supposed to engulf the gesture material (the user hand).

The second step is the analysis and classification phase and it is mainly composed by two sub-tasks:

The analysis: each frame of the image stream received was segmented then we start the extraction of specified characteristics.

The classification: when having the characteristics on hand, the system could tell whether the scene is containing an impression of an effective (significant) human hand signal or not based on the specified present characteristics stored on the integrated memory.

In the favorable case, the system stores the equivalent significance and reiterates until given the order to pass to other message or halt (detected automatically in another level of the algorithms)

The last step consist of assembling, correction and outputting the message accumulated by iterations of phase two.
A. the database

An image database containing the effective messages which the comparison process will use while recognizing the received messages. Same example of picture the database:

Fig. 2. (a) the alphabet A, (b) the alphabet I, (c) the alphabet B, (d) the alphabet L, (e) the alphabet V, (f) the alphabet U
After making the segmentation of these images and saves in a memory.

![The segmented images](image1)

**B. hand shape detection**

For the hand detection, we are using the background subtraction method provided by the OpenCV Image Processing Library.

Given the situation, the system will operate on the hand detection phase’s main purpose is to identify whether or not the image is containing a human hand, and if it ‘is the case, what gesture is it performing.

To do this, we need an algorithm that gives the segmentation, the shape recognition and the similarity detection of shapes contained in the scene to decide if it contains a hand or doesn’t.

![hand detection](image2)

**CONCLUSION**

Till the present moment, we have succeeded to implementing the image characteristic database and the hand detection module, yet the comparison process is still under development and we are finding difficulties in calibrating the results of the comparison. Most of the occurrences of the process does not recognized, the good characteristics and classifies the input as an ineffective message.

In the present time, we are still developing the system and we are trying alternative algorithms to surpass this issue.
REFERENCES

[1] Thomas Baudel, Annelies Braffort: GESTURE RECOGNITION OF HAND IN REAL ENVIRONMENT.
[10] Simena86.github.io
An Optimization Technique for Brain Tumour Recognition

Dr. D. Rajya Lakshmi 1, Shaik Salma Begum 2

Vice-Principal, Professor of CSE, UCEN, JNTUK Narsaraopet1, Research Scholar, CSE Dept, JNTUK, Kakinada2

Abstract
In this paper, we have proposed a robust technique to detect and classify the tumour part from medical brain images. In recent times, a number of image segmentation and detections techniques have been proposed in the literature. But, the detection of brain tumour through the help of classification technique has received significant interest among the research community. By considering the above issue, here, we combine three different techniques such as, cuckoo search, neural network and fuzzy classifier to detect the tumour part effectively. Our proposed approach consists of four phases, such as, pre-processing, region segmentation, feature extraction and classification. In the pre-processing phase, the anisotropic filter is used for reducing the noise and in the segmentation process; K-means clustering technique is applied. For the feature extraction, the parameters such as contrast, energy and gain are extracted. In classification, a modified technique called Cuckoo-Neuro Fuzzy (CNF) algorithm is developed and applied to detection of tumour region. In the modified algorithm, cuckoo search algorithm is employed for training the neural network and the fuzzy rules are generated according to the weights of the training sets. Then, classification is done based on the fuzzy rules generated. Experimental results shows that the proposed technique achieved the accuracy of 79.49% but existing technique achieved only 76.92%.

Keywords: CNF, contrast, energy, entropy, K-Means, anisotropic filter, sensitivity, specificity, accuracy

1. Introduction

Image segmentation theory, as digital image processing has become an important part of people active research. It is pertinent to note here that Image segmentation is a sine-qua-non of medical image processing and finds itself extensively applied in manifold and varied tasks [1] [14]. In addition, medical image segmentation casts an amazing part in the treatment planning, identifying tumours, tumour volume, patient follow up and computer guided surgery. There is a flood of varied methods for performing the function of medical image segmentation [3]. In addition the underlying objective of segmentation is to segregate an image into diverse components possessing robust correlation with domains of concern in the image. As far as medical image processing is concerned, segmentation of MR brain image is a noteworthy feature as MRI is predominantly proper for brain investigations as it bristles with brilliance in view of its superb distinction of soft issues, non invasive characteristic and the added advantage of a high spatial resolution. As a result, segmentation of tissues and structures from medical images is treated as the foremost action in several image assessment techniques launched for medical diagnosis [4]. It is simply imprudent to contrast the Manual segmentation of the abnormal tissues with the hi-tech swift computing systems throwing open the facility to visually monitor the volume and locality of unwanted tissues [8].

Consequently, pre-processing is done to improve quality of image; image pre-processing involves different techniques to improve image quality before actual segmentation process. It removes irrelevant information like noise and enhances contrast to improve image quality. The diverse pre-processing functions employed include Histogram Equalization, Binarization, and Morphological Operations. Afterwards, the feature extraction procedure assumes significance involving crucial stages, where traits tend to be the characteristics of the objects forming part of an image. Feature extraction is the task of mining definite features from the pre-processed image. Nowadays, many diverse methods are employed for estimating texture like co-occurrence matrix, Fractals, Gabor filters, wavelet transform. Gray Level Co-occurrence Matrix (GLCM) features are extensively utilized to break-up regular and irregular brain tumours. GLCM is the abridged form of gray-level co-occurrence matrix (GLCM), otherwise termed as the gray-level spatial dependence matrix) [3] [9].

K-means clustering is an appropriate method for biomedical image segmentation as the quantity of clusters is generally identified for images of particular regions of the human anatomy. A number of experimenters have launched associated investigations into K-means clustering segmentation. Though a significant and noteworthy advancement has been made in this regard, still there is greater computational intricacy and the need for superfluous software functionality [6]. Clustering programs, like k-means and ISODATA, function in an unsupervised mode and have been performed on an extensive domain of categorization dilemmas [7]. For categorizing the tumour segments, physical classification tends to lead to manual flaws, in addition to relying heavily on person to person, protracted and elongated runtime along with non-reproducible outcomes. Therefore, an automatic or semi-automatic classification technique is the need of the hour as it tends to scale down the burden on the individual spectator, and also because accuracy does not become the casualty on account of exhaustion and mammoth quantity of images [3]. In respect of tumour detection, several schemes such as, K-NN, bayes classifier, neural network, fuzzy classifier are performed for automatic detection. When comparing with these methods, Neuro-Fuzzy is found to be better and this technique has been used in a lot of research areas.

2. Motivation of the Proposed Approach

Segmentation is a significant technique used in image processing to detect objects in an image. As same as, MRI Image segmentation plays a critical role in many medical imaging applications. In accordance with brain tumour segmentation and detection, numerous significant algorithms and methods are published in this area. Some of the recent related works regarding the segmentation are reviewed and its
limitation and application are tabulated in the table-1. They developed a framework for multi-object segmentation of deep brain structures in medical brain images. Deep brain segmentation is difficult and challenging because the structures were small size and have significant shape variations. To tackle these problems, they proposed a template-based framework and Markov dependence tree methods [13], which were used to segment the deep brain structure. However, like most segmentation problems, tumour detection and quantification of brain tumour was very difficult. Also, A.K. Qin [14] and Tao Wang et al. [15] have developed a vector flow method to overcome the gradient vector flow, boundary vector flow, and magneto static active contour, but it has the limited range only.

<table>
<thead>
<tr>
<th>Author</th>
<th>Description</th>
<th>Application</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jue Wu, Albert C.S.Chung</td>
<td>Template based Frame Work and Markov dependence tree</td>
<td>Segmentation of deep brain structures</td>
<td>Large Training set is available, Difficult to do.</td>
</tr>
<tr>
<td>Tao Wang et al. [15]</td>
<td>Fluid vector flow</td>
<td>Brain tumor segmentation</td>
<td>Limited capture range, poor convergence</td>
</tr>
<tr>
<td>Zafer Iscan et al. [16]</td>
<td>2D Continuous wavelet Transform</td>
<td>Segmented magnetic resonance brain images</td>
<td>It have noise</td>
</tr>
<tr>
<td>Minakshi Sharma, Dr. Sourabh Mukharjee [3]</td>
<td>Adaptive Neuro-Fuzzy Inference System (ANFIS)</td>
<td>Brain Tumor Segmentation</td>
<td>Does not measure thickness and volume of tumor</td>
</tr>
<tr>
<td>Jayashri Joshi, Mrs. A.C. Phadke [12]</td>
<td>Statistical structure analysis Based tumor segmentation</td>
<td>Semi-Automated MRI brain tumor segmentation</td>
<td>It is difficult to do</td>
</tr>
<tr>
<td>M. Rakesh, T. Ravi [6]</td>
<td>color based segmentation method and FCM algorithm</td>
<td>Detection of Tumor Objects in MRI Brain Images</td>
<td>It have average speed</td>
</tr>
<tr>
<td>Reza Farjam et al. [17]</td>
<td>An approach for computer-aided detection</td>
<td>Brain metastases in post-Gd T1-weighted MRI</td>
<td>Its only designed to localize small brain metastatic lesions</td>
</tr>
<tr>
<td>Our method</td>
<td>Cuckoo-Based Neuro-Fuzzy Classifier</td>
<td>Brain tumour segmentation and detection</td>
<td>N/A</td>
</tr>
</tbody>
</table>

On other hand, for segmenting the brain tumors in magnetic resonance images, a technique has been proposed by Zafer Iscan et al. [16]. There, tumour identification was done by 2D Continuous wavelet transform. But, during tumour identification process noise occurred, which is the main limitation of their proposed method. Moreover they visually demonstrated brain metastases in post Gd-T1-Weighted MRI using CAD. Reza Farjam et al. [17] developed an approach it designed to localize small brain metastatic lesions. Key problem in medical imaging was automatically segmenting an image into constituent heterogeneous process. Jayashri Joshi and Mrs. A.C. Phadke [12] have performed Semi-Automated MRI brain tumor segmentation. However, no completely automatic segmentation has yet been adopted. To solve these challenging problems, also, various methods proposed in the literature have met with only limited success due to complexity of feature extraction and classification. M. Rakesh and T. Ravi [6] have developed segmentation technique for brain temporising fuzzy C-means algorithm. The segmentation performed only average speed in their method. Minakshi Sharma and Dr. Sourabh Mukharjee [3] developed an approach for segmenting the brain tumor using Adaptive Neuro-Fuzzy Inference System (ANFIS) to overcome the fuzzy C-means algorithm. But, in their method is difficult to find the volume of the tumour.

By considering the above challenges and to improve the tumour segmentation and classification limitations, an efficient approach is urgently needed. In this paper we present a new method for brain tumour segmentation and detection using cuckoo-based neuro-fuzzy classifier. The results of this approach are used to four efficient algorithms for automatic tumour detection and classification. To prove this point, totally four different phases are developed. Then, performance of the procedure is tested on different brain MRI images. The rest of the paper is organized as follows: Introduction of proposed technique is presented in 1. Motivation of the paper is described in section 2. Contribution is discussed in section 3. The proposed tumour detection and classification system is described in section 4. The experimental results and performance evaluation discussion is provided in Section 5. Finally, the conclusions are summed up in Section 6.
3. Contribution of Proposed Technique

- The novelty and contribution of the proposed method is that we introduce a Cuckoo-Neuro fuzzy (CNF) classifier to detection of tumour region. In CNF classifier, cuckoo search algorithm is employed for training the neural network and the fuzzy rules are generated according to the weights of the training sets. Then, classification is done based on the fuzzy rules generated.

4. Proposed Brain Tumour Segmentation and Detection Technique Using FCM and CNF Classifier

Segmentation of brain tumours from MR images is a difficult task that involves a range of disciplines covering pathology, MRI physics, radiologist’s perception, and image analysis based on the intensity, shape and size. It is unfortunate that various critical hassles and tribulations habitually haunt and put roadblocks against the appropriate segmentation of brain tumours. As per the recent data released by the World Health Organization (WHO), it is estimated that a whopping number of over 400,000 people per annum invariably resort to intensive medical care for the purpose of treating the catastrophic and cruel brain tumours. These tumours, in fact, exhibit a unique tendency to appear in diverse ways such as in shape, size and location, and they have an uncanny way of gate-crashing into diverse places with dissimilar intensities. This has thrown open unfathomable challenges before the medico-community in their intensive efforts to locate the accurate tumour which has adversely affected the cells in the brain. It is high time we recognize the supreme significance of the precise segmentation of brain tumours and initiate instant and effective steps for the purpose. In essence, Brain tumours fall in to two different groups which may be classified as initial benevolent tumours that have not broadened their domain of destruction to other localities and the advanced or malignant brain tumours that have already cast a havoc by gradual swelling and found a way from other parts of the physique ultimately winning to reach the brain. Patients supposed to suffer severely from tumours go through various rigorous steps including diagnostic CT scans and MRI in super-speciality hospitals. Although, the radiologist performs these diagnoses, it is very difficult to identify a tumour in the brain due to the involvement of various abnormalities, noise and intensities. Various methods proposed in the literature have met with only limited success due to complexity of classification. Considering the above issues, in this paper, we have proposed a technique to detect and classify the tumour region from the brain MRI dataset.

As depicted in figure 1, four main phases of the proposed tumour segmentation algorithm are described in the following section:

- **Phase 1: Pre-processing**
  A pre-processing phase in image segmentation works is used to remove unwanted noise from the brain images. Here, anisotropic filter is utilized to remove noise from the MRI images.

- **Phase 2: Segmentation of Region**
  The second phase detects the region of brain images using K-means clustering algorithm.

- **Phase 3: Feature extraction**
  In this phase, feature parameters such as contrast, energy and gain are extracted using segmented regions.

- **Phase 4: Classification**
  Finally, in this phase, a Cuckoo-Neuro Fuzzy algorithm is developed and used to detection of tumour region.

In the following subsections, we describe our proposed tumour segmentation system by first introducing the pre-processing steps and then detailing the tumour detection and classification approach.

4.1 Pre-Processing

Pre-processing is the standard procedure in general brain image segmentation, aiming to reduce image noise. Here, an anisotropic filter is used to smoothen the MRI image and reduce the noise. Each input MRI images is performed to the noise removal process and given to the region segmentation process.

4.2 Segmentation Using K-Means Algorithm

In this stage, region is segmented from the pre-processed MRI brain image by means K-means clustering algorithm. After we have achieved success in extracting the region, the recognition is carried out by means of feature extraction and classification technique to categorize it as either normal or tumour. K-means clustering segments the concerned MR image into two specific regions. The former region comprises the normal brain cells where as the second region is composed of the timorous brain cells. K-means clustering segments the brain MR image in accordance with intensity pixels constituting the image. K-means is considered as one of the significant unsupervised learning algorithms in respect of clusters. Clustering the image is grouping the pixels according to the some characteristics. It is nothing but just to cluster the items into \( k \) number of clusters according to certain features. The main target of K-mean clustering is to categorize the data by minimizing the sum of squares of distances between data and the corresponding centroid of the cluster [18] [19]. In this case, K-means clustering is employed to group the pixels into two distinct clusters \( (k = 2) \). The detailed step-by-steps of K-means clustering algorithm is described as follows:

1. Give the number of cluster value as \( k \). Here, we have chosen \( k = 2 \).
2. Randomly choose the \( k \) cluster centers.
3. Calculate mean or center of the cluster
   \[
   M = \frac{\sum_{i=1}^{N_{k}} x_{i}}{N_{k}}, \quad k = 1, 2, ..., K
   \]
4) Next to that, the pixels of the image are assigned to the closest cluster which satisfies the minimum Euclidean distance from the pixels values to the center of each cluster.

\[ D(i) = \arg \max \| x_i - M_k \| ^2, i = 1, ..., K \] (2)

5) If the distance is near to the center then move to that cluster.

6) Otherwise move to next cluster.

7) Re-estimate the center.

8) Repeat the process until the center doesn't move.

### 4.3 Feature Extraction

Feature extraction is an important stage of image segmentation process and which is used to compute a characteristic of a digital image able to numerically describe its texture properties. After region segmentation, we are considering varying features for the tumour image classification.

\[ FV = \{ F_1, F_2, F_3 \} \] (3)

These features are calculated for two segmented regions in each MR image such as tumour and non-tumour and the feature vector which we have formulated is

\[ FV = \{ F_{1T}, F_{1NT}, F_{2T}, F_{2NT}, F_{3T}, F_{3NT} \} \] (4)

Where,

- \( F_{1T} \rightarrow \) Contrast feature set of tumour region
- \( F_{1NT} \rightarrow \) Contrast feature set of Non-tumour region
- \( F_{2T} \rightarrow \) Energy feature set of tumour region
- \( F_{2NT} \rightarrow \) Energy feature set of Non-tumour region
- \( F_{3T} \rightarrow \) Entropy feature set of tumour region
- \( F_{3NT} \rightarrow \) Entropy feature set of Non-tumour region

The feature vector \( FV \) is calculated by following features:

**Contrast:**

The contrast (C) feature is defined as the divergence moment of the P matrix and constitutes a significant measure of the contrast or alternatively the amount of local variations present in an image. The formula for the estimation of the contrast is given below:

\[ F_1 = C = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} (i-j)^2 p(i, j) \] (5)

**Energy:**

Energy (E) is generally employed to express a measure of information in an image. The formula for determination of the energy is furnished as follows:

\[ F_2 = E = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} [p(i, j)]^2 \] (6)

**Entropy:**

An entropy (H) measure is described as a significant statistical measure of randomness which is employed to distinguish the texture inherent in the candidate region. Moreover, entropy is capable of enabling us to judge the vicinity of the pixel appropriately leading to further precision in the categorization of the texture

\[ F_3 = H = -\sum_{i=0}^{G-1} \sum_{j=0}^{G-1} p(i, j) \log_2 [p(i, j)] \] (7)

The extracted features in 3.12 and the features are given to a cuckoo based neuro-fuzzy classifier to accomplish the classification process.

### 4.4 Tumor Detection Using CNF Classifier

In this section, the extracted feature set \( FV = \{ F_{1T}, F_{1NT}, F_{2T}, F_{2NT}, F_{3T}, F_{3NT} \} \) is given to the CNF classifier. In the CNF classifier, cuckoo search algorithm is employed for training the neural network and the fuzzy rules are generated according to the weights of the training sets. Then, classification is done based on the fuzzy rules generated.

Section 4.4.1 describes best rule generation process using cuckoo search algorithm. Section 4.4.2 describes classification using neuro-fuzzy classifier.

#### 4.4.1 Best rule generation using Cuckoo search

Our aim of this section is to generate best rules and these rules are provided to fuzzy logic system. Here, cuckoo search algorithm [20] [21] is utilized to generate best rule and these best rule is given to the further process. Cuckoo search algorithm is an optimization algorithm and developed by Yang and Deb in 2009 and has undergone a substantial development. This method is very different from other meta-heuristic optimization algorithm. The detailed process of the generating the best rules using cuckoo search algorithm is explained using the following section,

**Discretization:**

Before the cuckoo search process, initially, the training dataset \( DS_{TR} \), which consists of \( "N" \) number of attributes, is provided to the discretization function to relocate the input records into a discretized one. The generalization form of the training dataset is expressed by:

\[ DS_{TR} = \{ ds_{ij} | 0 \leq k \leq m \text{ and } 0 \leq l \leq n \} \] (8)

Discretization is a vital step in data processing to transform the data or records into specific interval. In this case, we have utilized an innovative discretization method following the conservative manner. The utmost and least values of each and every attribute are located and the \( T \) interval is traced by consideration the relation between the deviated value and \( T^{th} \) value.

For each and every \( l \), deviated value is estimated as follows:

\[ Dev_l = \frac{Max(ds_l) - min(ds_l)}{4} \] (9)

\[ DS_{VL} = min(ds_l) \leq (min(ds_l) + Dev_l) \] (10)

\[ DS_{HL} = (min(ds_l) + 2*Dev_l) \leq (min(ds_l) + 2*Dev_l) \] (11)

\[ DS_{VM} = (min(ds_l) + 3*Dev_l) \leq (min(ds_l) + 3*Dev_l) \] (12)

\[ DS_{HM} = (min(ds_l) + 3*Dev_l) \leq (min(ds_l) + 3*Dev_l) \] (13)
Where, \( VL \rightarrow \) Very Low, \( H \rightarrow \) High, \( M \rightarrow \) Medium, \( L \rightarrow \) Low

Then, every value that comes under within the range is replaced with the interval value so that the input data is transformed to the discretized data \( DS_{TR} \). After discretization function, the training dataset \( DS_{TR} \) is converted into discretized format \( DDS \). Where, the entire data element \( DS_D(k,l) \) contain only the VL, L, M or H if \( T = 4 \).

**Generating initial set of nests:**

At the outset, \( \langle n \rangle \) number of nests are engendered and each and every nest is endowed with the ensuing rules which can be broadly detailed as Very High (\( VL \)), High (\( H \)), Medium (\( M \)), Low (\( L \)) and one class (\( C \)). Here \( C \) corresponds to class (whether tumour or non-tumour). The population of nest \( \langle n \rangle \) is supplied to the client along with the dimension (attributes) of the each and every nest \( R_i(f_j,c) \) forming part of the image feature dataset. In other words, \( \langle n \rangle \) solutions are furnished in a preliminary group of host nests, and each and every nest stands for the corresponding features. Where, \( f_j \) is the number of features, in which 1 represents Very High (\( VL \)), 2 represents High (\( H \)), 3 represents Medium (\( M \)), 4 represents Low (\( L \)) and \( C \rightarrow \) class. The initial solution and solution encoding process is depicted in figure 2.

**Fitness calculation:**

We compare the outcome result with the training and testing dataset and we calculate the accuracy through the following equation (14) as fitness function for each nest.

\[
\text{Fitness} = \text{sum of rule } R_i \text{ in the discretized dataset } DS_D
\]  

Where,
\( DS_D \rightarrow \) discretized format data
\( R_i \rightarrow \) Rules

**Nest updation:**

At this point, an arbitrary number (\( j \)) is created by using levy flight and the comparative remedy is chosen. Subsequently, the fitness of nest located in the initial group of nest corresponding to the arbitrary number is replaced by means of a new finest nest. When the estimation of the fitness of the initial remedies is over, newest remedy is found out in accordance with the cuckoo operator. Based on the modifiable Levy flight, the cuckoo operator generates new remedies. A new remedy \( x^{(t+1)} \) for cuckoo \( i \) is produced by employing a Levy flight along with the following equation:

\[
x^{(t+1)} = x^{(t)} + \alpha \text{Levy}( \lambda )
\]

Where, \( \alpha (\alpha > 0) \) symbolizes a step scaling size. This parameter must be connected to the scales of issue the algorithm is trying to locate a key to. In almost all the cases \( \alpha \) can be fixed to the value of 1 or a specific dissimilar constant.

**Best rule generation:** From cuckoo search algorithm, logical rules, represented as \( R = \{ R_j; 1 \leq j \leq m \} \) are derived by performing several iterations. Here, the rules should have two different decisions such as, 1 and 2. From the cuckoo search algorithm, best rules \( R_{best} \) are generated and given as figure 3:

**Classification using Neuro-Fuzzy:**

**Generation of fuzzy score using fuzzy system:** The NFC is a multi-layer feed forward network which comprises the ensuing levels. The fuzzy interference system performs three dynamic functions as detailed below:

- Fuzzification
- Rule Evaluation
- Defuzzification

Fuzzy inference is the unique procedure of generating a mapping from a prearranged input to the resultant output by the employment of a fuzzy logic. Thereafter, the mapping heralds a foundation and from this foundation appropriate decisions can be taken, and the patterns can be distinguished. The key task of fuzzy inference involves Membership Functions, Logical Operations, and If-Then Rules. The schematic graph of the fuzzy inference system (FIS) is vividly illustrated in Fig. 4.
The extracted features are \(F_1^T\), \(F_1^{NT}\), \(F_2^T\), \(F_2^{NT}\), \(F_3^T\) and \(F_3^{NT}\), for each feature we perform fuzzification process. For the fuzzification process, we collect all the \(F_1^T\), \(F_1^{NT}\), \(F_2^T\), \(F_2^{NT}\), \(F_3^T\) and \(F_3^{NT}\) features of the training images and compute each feature minimum (min) and maximum (max) values. The fuzzification process is performed following equations.

\[
[F_{1i}^T]_{\text{Min Limit}} = \min\left(\frac{\text{max} - \text{min}}{3}\right)
\]

\[
[F_{1i}^T]_{\text{Max Limit}} = \max\left(\frac{\text{max} - \text{min}}{3}\right)
\]

In above equations \(\lfloor F_{1i}^T \rfloor_{\text{Min Limit}}\) and \(\lfloor F_{1i}^T \rfloor_{\text{Max Limit}}\) are the minimum and maximum limit values of the feature \(F_1^T\). The same equations are used for the features \(F_1^T\), \(F_1^{NT}\), \(F_2^T\), \(F_2^{NT}\), \(F_3^T\) and \(F_3^{NT}\) to compute the minimum and maximum limit values.

**Fuzzy Membership function:**

The membership function of each and every input is recognized in this stage. The membership function is planned by selecting the appropriate membership function. One of the prominent challenges in all fuzzy sets involves the appropriate decision of fuzzy membership functions,

1. The membership function discharges its task efficiently by performing the complete demarcation of the fuzzy set.
2. A membership function furnishes an assessment tool for estimating the level of resemblance of an element to a fuzzy set.
3. Membership functions may assume any shape; however, there occur certain general patterns which tend to emerge in bona fide applications.

**Rule Evaluation**

Using cuckoo search algorithm, we already generated the fuzzy rule set \(R_{best} = \{R_{j}^{i}_{best}: 1 \leq j \leq m - T_{1}\}\) that are given in the fuzzy rule base. The rule base contains a set of fuzzy rule in the form of Figure 3.

**Neural network process:** After the fuzzy interference process, the fuzzy score is generated and assigned to the neural network output parameter. Totally, we have assigned two output classes (parameter), (i) fuzzy score (ii) original feature set. The neural network is well trained with these extracted features and different number of unknown brain MRI images is tested. The important steps involved in neural network are as follows,

**Step 1:** Put the input weights to every neuron except the neurons in the input layer. Here, \(F_1^T\), \(F_1^{NT}\), \(F_2^T\), \(F_2^{NT}\), \(F_3^T\), and \(F_3^{NT}\) are the input features such as contrast, energy, entropy for the tumour and non-tumour segmented region i.e. input of the network and \((C_k)\text{output}\) is the decision result from the FIS and original feature set, i.e. output of the network. The neural

**Step 2:** The neural network is designed with six input layers, \(H_1\) hidden layer, and two output layer. The weights and then added to the neural network and it is biased.

**Step 3:** To the output layer the output of the activation function \(f(\ln(H_1))\) is then broadcast all of the neurons:

\[
(C_k)\text{output} = \eta_i + \sum_{n=1}^{N} W_{2ml}C_i(n)
\]

Where \(\eta_i\) and \(\eta_k\) are the biases in the hidden layer and the output layer.

**Step 4:** Compute the error between the desired output \((C_k)\text{target}\) and the output \((C_k)\text{output}\) produced by the feed-forward neural network, this is given by

\[
E_v = (C_k)\text{target} - (C_k)\text{output}
\]

In equation (19) \((C_k)\text{target}\) -is the target output and \((C_k)\text{output}\) -is the network output.

**Figure 5:** Proposed neural network structure

In testing phase, the input testing feature \([F_1, F_2, F_3]_{\text{test}}\) is given to fuzzy interference system and corresponding fuzzy score is generated. This fuzzy score is given to the neural network. The resultant value of neural network’s output class is represented as \(A_1\) and \(A_2\), and this value is compared with threshold value \(T_1\).

\[
\text{Result} = \begin{cases} 
\text{Abnormal}; A_1 \geq T_1 \\
\text{Normal}; A_2 < T_1 
\end{cases}
\]

In this way the brain MRI images are classified into normal and abnormal.

5. **Simulation Results and Discussion**

This section presents the results obtained from the experimentation and its detailed discussion about the results. The proposed tumour detection and classification technique is experimented with the brain MRI image dataset and the result is evaluated with the sensitivity, specificity and accuracy.

5.1 **Dataset Description**

The dataset contains the MR images acquired from the internet. The proposed method was tested with different MR images with different shapes, sizes and intensities. A dataset of 60 images (40 normal and 20 abnormal) has been developed to the test performance. This image dataset contains 60 brain MRI images which includes tumour and without tumour brain images as shown in figs 6. The brain image dataset are divided into two sets such as, (1) Training dataset (2) Testing dataset. To segment the brain tumour images the training dataset is used and to analyze the performance of the proposed technique the testing dataset is used. In this novel technique, training and testing images are altered in various ratios like 60/40, 70/30, 80/20 and 90/10 for the purpose of testing. The
Figure 6 shows some of the sample MRI images with tumour images and non-tumour images.

<table>
<thead>
<tr>
<th>Non-tumour images</th>
<th>Tumour images</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Non-tumour images" /></td>
<td><img src="image2.png" alt="Tumour images" /></td>
</tr>
</tbody>
</table>

**Figure 6: Non-tumour and Tumour images**

### 5.2 Experimental Setup and Evaluation Matrices

The proposed technique is performed in a windows machine having configurations Intel (R) Core i5 processor, 3.20 GHz, 4 GB RAM, and the operation system platform is Microsoft Window7 Professional. We have used mat lab latest version (7.12) for this proposed brain tumour detection and classification technique.

The evaluation of proposed technique in different brain MRI images are carried out using the following metrics as suggested by below equations,

\[
\text{Sensitivity} = \frac{number\ of\ true\ positives}{number\ of\ true\ positives + number\ of\ false\ negatives} \\
\text{Specificity} = \frac{number\ of\ true\ negatives}{number\ of\ true\ negatives + number\ of\ false\ positives}
\]

\[
\text{Accuracy} = \frac{number\ of\ true\ positives + number\ of\ true\ negatives}{number\ of\ true\ positives + number\ of\ false\ negatives + number\ of\ true\ negatives + number\ of\ false\ positives}
\]

### 5.3 Experimental Results

Nowadays, manual segmentation of brain tumour from MR images has emerged not only as a thorny issue but also as a time consuming function. The proposed tumour detection technique is endowed with the faculty of efficiently segmenting a tumour once the parameters are laid down free of fault. The underlying objective of the proposed technique is targeted at facilitating the tumour detection in brain images irrespective of whether they are affected by tumour or not. The test outcomes yielded by the novel method are furnished in table 1. The table 1 demonstrates the original image and corresponding filtered and segmented images for tumour and non-tumour images. Table 2 depicts the three features results.

<table>
<thead>
<tr>
<th>Input image</th>
<th>Filtered Image</th>
<th>Segmented Image</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Input image" /></td>
<td><img src="image4.png" alt="Filtered Image" /></td>
<td><img src="image5.png" alt="Segmented Image" /></td>
</tr>
</tbody>
</table>

**Table 2: Segmented results of proposed technique**
Feature Extraction Results:

Table 3: Feature extracted results of proposed technique

<table>
<thead>
<tr>
<th>Input Images</th>
<th>Contrast</th>
<th>Energy</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.8014</td>
<td>651173</td>
<td>1.2102</td>
</tr>
<tr>
<td></td>
<td>0.6946</td>
<td>934521</td>
<td>1.4533</td>
</tr>
<tr>
<td></td>
<td>0.7031</td>
<td>783346</td>
<td>1.1985</td>
</tr>
<tr>
<td></td>
<td>0.7956</td>
<td>712774</td>
<td>1.3016</td>
</tr>
<tr>
<td></td>
<td>0.6978</td>
<td>806406</td>
<td>1.2333</td>
</tr>
<tr>
<td></td>
<td>0.7767</td>
<td>711766</td>
<td>1.2853</td>
</tr>
<tr>
<td></td>
<td>0.7935</td>
<td>695191</td>
<td>1.2769</td>
</tr>
<tr>
<td></td>
<td>0.7318</td>
<td>712434</td>
<td>1.1348</td>
</tr>
<tr>
<td></td>
<td>0.6726</td>
<td>826969</td>
<td>1.1489</td>
</tr>
<tr>
<td></td>
<td>0.7702</td>
<td>703274</td>
<td>1.2571</td>
</tr>
<tr>
<td></td>
<td>0.8153</td>
<td>593832</td>
<td>1.1076</td>
</tr>
</tbody>
</table>
5.4 Comparative Analysis

In this section, we will indicate sensitivity, specificity and accuracy achieved by the proposed brain tumour detection technique while segmenting and classifying the brain MRI images and we use three evaluation matrices for comparing the performance of our method CNF classifier. Also, we have compared against K-means with neuro-fuzzy classifier and proved our proposed tumor detection system is better performance with help of sensitivity, specificity, accuracy. The evaluation results of the proposed against existing technique graphs are figure 7 to 9. In figure 7, the proposed approach achieved the sensitivity of about 96.2% where existing approach achieved only 8% in training-testing ratio (70-30). In figure 8, the proposed technique achieved the specificity of 79.49% where existing approach achieved only 73.53% in training-testing ratio (80-20). In figure 9, the proposed approach achieved the accuracy of about 79.49% where existing approach achieved only 76.92% in training-testing ratio (90-10). Totally, the proposed tumour detection technique is achieved better performance when compared existing technique.

![Sensitivity graph](image1)

**Figure 7:** Sensitivity graph of proposed against existing technique

![Specificity graph](image2)

**Figure 8:** Specificity graph of proposed against existing technique

![Accuracy graph](image3)

**Figure 9:** Accuracy graph of proposed against existing technique

5.5 Severity Analysis

In severity analysis, we have taken seven images, which are tumour images as shown in table 4. Here, we have used pixel based similarity matching for proposed approach tumour image and manual segmented tumour image. Here, we have used Jaccard coefficient for similarity matching which is following by equation (21),

\[
J(A, B) = \frac{|A \cap B|}{|A \cup B|}
\]  

(21)

Where, A is the pixels of proposed approach tumour image and B is the pixels of manual segmented image.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Tumor MRI images</th>
<th>Jaccard coefficient value (pixel count)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image1" alt="Image 1" /></td>
<td>0.9828</td>
</tr>
<tr>
<td>2</td>
<td><img src="image2" alt="Image 2" /></td>
<td>0.8766</td>
</tr>
<tr>
<td>3</td>
<td><img src="image3" alt="Image 3" /></td>
<td>0.9912</td>
</tr>
<tr>
<td>4</td>
<td><img src="image4" alt="Image 4" /></td>
<td>0.9622</td>
</tr>
<tr>
<td>5</td>
<td><img src="image5" alt="Image 5" /></td>
<td>0.9821</td>
</tr>
<tr>
<td>6</td>
<td><img src="image6" alt="Image 6" /></td>
<td>0.9607</td>
</tr>
</tbody>
</table>

Table 4: Severity analysis for different MR images
6. Conclusion

This paper proposes a method for segmenting and classifying brain tumour images from MRI images. The overall steps of proposed tumour detection and classification technique includes four phases namely, pre-processing, segmentation, feature extraction and classification. In the pre-processing step, the anisotropic filter is utilised for reducing the noise and in the segmentation process, K-means clustering technique is applied. For the feature extraction, the parameters such as contrast, energy and gain are extracted. In classification, a modified technique called Cuckoo-Neuro Fuzzy (CNF) algorithm is developed and applied to detection of tumour region. In the modified algorithm, cuckoo search algorithm is employed for training the neural network and the fuzzy rules are generated accordingly to the weights of the training sets. Then, classification is done based on the fuzzy rules generated. The proposed technique was tested on the magnetic resonance images of the brain for tumour segmentation and its performance was evaluated visually and quantitatively.

References

Permission Based Android Malware Detection System using Machine Learning Approach

Mayuri Magdum
Computer Engineering
Modern Education Society’s College of Engineering,
Pune, India

Prof. Sharmila.K.Wagh
Computer Engineering
Modern Education Society’s College of Engineering,
Pune, India

Abstract— Mobile computing has grown and developed in recent years with huge popularity. Gadgets like Smart phones, Tablets, etc have become trendy by the ease of use. Android is more famous platform and turned out to be the most important target of Malware developers in precedent years. The malware hazard for cellular telephones is evaluated to increment security and usefulness of smartphones. Hackers and malware program developers are benefitted by the limited capabilities and lack of standard security mechanism of Android. Nowadays smart phones are omnipresent, i.e. they fill numerous needs such as data storage, personal mobile communication, multimedia and entertainment etc. therefore, implementing secure mobile connections is challenging. As a result, it becomes essential to have some valuable and probabilistic detection along with preventive mechanisms. Many preventive tools are available in market but current trend for malware security is before installing the app user should be able to identify possible threats. Hence we propose permission based mobile malware detection system. It has 3 components in it 1) Client 2) Server 3) Signature Database. In the whole analysis process, Server plays important role and user is warned at the end of analysis process whether the requested app contains malware or not.

Keywords- Mobile, Android, Malware, Security, Machine Learning, Static Analysis.

I. INTRODUCTION

Mobile malware is a malicious software program with the main intention to damage mobile phones. It includes things such as virus, worms, Trojan horses, etc. Intent of this malicious software could be to steal confidential data, or to obtain root privileges. It is an overall scourge.. Study shows that effect of malware is deteriorating step by step exceptionally in banking and financial section. Thus it is important to study different types of malware, their impact and their detection techniques. Peer-to-peer networks are used widely and are helpless against malware. This potential weakness in P2P networks could permit malware to infect, so we should ensure a strong protection against malware attack using different malware detection techniques.

Mobile computing has developed so rapidly and fast in last 5 years. Smartphones are used for people for online shopping, e-banking, online reservations. A mobile malware is capable to call premium numbers from contact list, steal confidential data and flush all the memory as well as contact list. Android has turned out to be the most important target of Malware developers in precedent years. The malware risk for mobile phones is estimated to increase along with the functionality of phones. Android’s main protector mechanism against malicious apps is a permission based access control mechanism. As a result, it becomes essential to have some valuable and probabilistic detection along with preventive mechanisms.

There are many malware detection and preventive tools proposed in market but our main focus is on android malware detection as its been constantly sharing highest market share and famous compared to other platforms. We will categorize them based on features used to analyze the app as

1) Static analysis
2) Dynamic analysis
3) Hybrid approach
4) Application Metadata.

Latest trend in anti-malware tool shows that these features are when combined with machine learning algorithm gives better results. Thus we propose a novel approach for permission based android malware detection system which is depends upon static investigation. It alerts user if the app is malicious or benign based on which user can proceed whether to continue with it or not. In this system, the app will detect the label or category of the application and accordingly classify them.

In this paper, Section 1 presents Introduction and motivation of mobile security. Section 2 describes the Literature Review and Related Work on mobile malware detection. Section 3 lists some Malware Detection Strategies in smartphone. Section 4 gives overview of Mathematical Model and section 5 presents overview of Proposed Work. Section 6 Experimental Results are given. In Section 7 Conclusion and Future scope is given.

II. RELATED WORK

The malware research has been begun from the year 2005[1]. An broad exploration has been done in this field and to fix the issue of mobile malware Jacques Klein et al. proposed a strategy called '10 fold cross validation'[2]. Younghshe Park et al. Mark Stamp presented a common and typical behavior of malware. They used graph clustering to capture such behaviors and then their proposed method produces graph in which they have used clustering technique [3].

Many features like the permission based features (static) and the API call based features are considered in order to train
the system and classification decision is made using probability theory is given by V. Natarajan et al. [4]. Talha et al. presented a strategy based on permissions used in an application. It uses static investigation and combined with machine learning algorithms such as logistic regression to detect mobile malware [5].

Huy Kang Kim, et al. proposed a system based on similarity matching of malware-driven and malware inventor driven information which is able to detect and classify malware in similar subgroups [6]. DONG Hang et al. invented a system to recognize malware in Android gadgets and to capture a malware they used streamlines Dalvik directions. This technique depends on simplification of instruction [7].

Doaa Hassana et al. found the similarity based way to detect the malware. In their strategy, similarity between methods is computed by using the normalized compression distance (NCD). Later with the help of either zlib or bzip2 compressors similarity measure is computed. System is trained using the computed similarity score and then afterward’s results are predicted whether the app is malicious or benign [8].

Another approach to discover noxious applications is discovered by Yajin Zhou et al. They proposed a strategy in which they utilized permission based behavioral footprinting method to detect malware. Afterword’s they used a heuristics-based filtering scheme to recognize behavior of new and unknown malware [9].

Seung-Hyun Seo, et. Al invented a method to detect mobile malware threats to homeland security. In their proposed method they defined various characteristics in mobile malware and show mobile attack patterns which are feasible. They inferred a static investigation tool, DroidAnalyzer, which predicts possible attacks from android app [10]. B. Shapira, et al. found a system to discover mobile malware which is based on semi supervised machine learning regardless of general static and dynamic based analysis [11].

Ping Wang, Yu-Shih Wang invented a method based on footprinting (signature) based analysis and they used SVM to detect malware. They additionally utilized a cross validation scheme for improving accuracy of malware detection [12].

Karim O. Elish et al. described a method which is based on classification strategy which is further used to detect malicious android app. Results demonstrated that the strategy proposed is highly accurate [13].

Jehyun Lee et al. invented a technique for malware screening which incorporates method to extract a set of family representative binary patterns from already analyzed family members as a signature. In evaluation phase it classifies each set of variants into a malware family with prior calculation of similarity to the signatures. This likeness they utilized recognizes malware as a part of their proposed strategy [14]. Wanqing You et al. invented a hybrid approach for mobile malware detection. In their proposed approach they inspected the program execution. The primary advantage of their strategy is that they utilized a hybrid approach for analysis [15].

### III. Malware Detection Strategies in Smartphone

#### A. Android Malware

1. **Adware:** At this age we don’t know how exactly adware malware exists and main intention to access critical information by phone.

2. **Infostealers:** As the name suggests primary focus is on stealing the information such as contact list and critical stage is stealing the passwords.

3. **Spy phone:** These apps are very commonly found. Typically this app is used to spy on owners phone.

4. **SMS Trojans:** Main intention of this malware is to send the SMS and user is charged for the message.

5. **Banking Trojans:** These type of malwares are making remarkable move to the banking industry. Typically they are involved in banking frauds.

6. **Ransomware:** This form of mobile malware consists of encryptors and fake security software.

#### B. Behavioral Classification

Behavior based classification is also refereed as anomaly detection. In such detection strategies normal behavior of the malware is as mapped against established dataset of normal behavior. If mismatch occurs between both then it is considered as malware. Advantage of such system is, many new detections are captured which were not found earlier. Major disadvantage of such system is major false positives are confirmed. Following fig. 1 shows the classification of malware based on behavior.

<table>
<thead>
<tr>
<th>Malware</th>
<th>Behavior</th>
<th>Description</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexiSPY</td>
<td>Stealing user credentials</td>
<td>Track user information such as emails, photos, browser history and then send it to server.</td>
<td>Symbian, Windows Mobile and BlackBerry</td>
</tr>
<tr>
<td>Face app</td>
<td>Content delivery manipulation</td>
<td>Runs in background when clicking on media player application. Send SMS Messages to premium rated numbers.</td>
<td>Android OS</td>
</tr>
<tr>
<td>Zite (Zast In The Mobile)</td>
<td>Stealing user credentials</td>
<td>Forwards incoming SMS messages from mobile phones to remote server for access of bank accounts.</td>
<td>Android OS</td>
</tr>
<tr>
<td>Skitter</td>
<td>Content delivery manipulation</td>
<td>S. overwrites system files without user’s knowledge as a result smart-phones would stop working and had been unlocked off.</td>
<td>Symbian OS</td>
</tr>
<tr>
<td>Gemini</td>
<td>SMS Spam</td>
<td>It sends multiple spam messages containing phishing links</td>
<td>Android OS</td>
</tr>
<tr>
<td>Hong Tou Tou</td>
<td>Search engine optimization</td>
<td>Improves website ranking in search engines.</td>
<td>Android OS</td>
</tr>
</tbody>
</table>

**Figure 1. Malware Behavioral classification**
C. Frequently Used Features in Mobile Malware Detection

There are three broad categories of features such as

1) Static Feature
2) Dynamic Feature
3) Hybrid Feature

All the features can be summarized diagrammatically as below

---

IV. MATHEMATICAL MODEL

Set representations:

Let ‘$S$’ be the system which predicts whether an application contains malware or not using machine learning technique

$S = \{X, I, Y, D, P\}$

Where,

$X$ = Input to the system
$I$ = Intermediate phase of the system
$Y$ = Output to the system

$x \in \{D\}$

$D$ = Set of datasets
$D = \{Da, Db\}$

$Da$ = Malicious dataset
$Db$ = Benign dataset

$Da = \{d_1, d_2, d_3, \ldots, d_m\}$

$Db = \{d_1, d_2, d_3, \ldots, d_n\}$

$m \neq n$

$I = \{TD, TVC, MSC\}$

$TD$ = Training the dataset
$TVC$ = Threshold value calculation
$MSC$ = Malware score calculation

---

Building permission database

$P = \{Set \ of \ permissions\}$

Such as

$\{android.permission.CALL_PHONE,$
$android.permission.SEND_SMS,$
$android.permission.READ_CONTACTS,$
$android.permission.CHANGE_CONFIGURATION,$
$android.permission.INTERNET, \ldots N\}$

---

$D (one) \rightarrow P (many)$

$P \in D$

Training dataset

$\alpha = \frac{e^a + bx}{1 + e^a + bx}$

(1)

Calculating Malware score

$AMS = \sum PMS$

Where,

$AMS = \frac{\text{Number of malware that uses that permission}}{\text{Number of all malware}}$ (2)

If $AMS \geq \text{threshold } \alpha$, then the requested application can be malicious.
Else if $AMS \leq \text{threshold } \alpha$ then the requested application can be benign.

$O = \{M, B\}$

$M$ = Malicious
$B$ = Benign

---

Finally, calculating the accuracy of the application

$\text{Accuracy} = \frac{TN + TP}{TP + FP + FN + TN}$ (3)

The complexity of above proposed strategy is $O(n \log n)$.

We are classifying malware using a machine learning technique. Calculating threshold plays an important role here. We compute it from the proposed model above it takes less than 100 iterations. So the time complexity of the above proposed model is $O(n \log n)$.

V. PROPOSED WORK

To overcome the problems caused by mobile malware, we are proposing a system which is based on feature selection as its first phase. Second phase consists of classification based on Logistic regression and Decision Tree algorithm and finally we are evaluating the performance of the system by computing its accuracy. All the procedure is described in below image.

---

A. Features

There are total 144 permissions for Android Kit Kat (4.4)[5]. At first we need to retrieve some features (permissions) from APK files. These required features are fetched from androidmanifest.xml file. These extracted permissions we are storing in SQL file. We are considering the permission count...
for detecting the malware. Figure 4 shows the how we are extracting and storing the permissions. We will discuss some sample features

- **android.permission.CAMERA:** This permission is requested when device needs to access camera.
- **android.permission.ACCESS_FINE_LOCATION:** This permission typically grants access to precise location.
- **android.permission.ACCESS_WIFI_STATE:** This permission allows to access information about WIFI state.
- **android.permission.BATTERY_STATS:** This permission allows device to collect battery statistics.
- **android.permission.READ_CONTACTS:** The application can read users contacts.
- **android.permission.INTERNET:** With this permission applications can open Network Socket.

**Figure 4.** An example of permission extracted from malware.

### B. Feature Extraction

This subsection explains the broad steps which we followed to obtain required data from apk files.

1. Download and collect the malicious and benign applications.
2. Decompress the applications and extract the content.
3. Extract the permissions from the files.
4. Build the dataset.

### C. High Level Architecture and Proposed System

The figure 5 shows the APK Auditor is a permission-based malware assessment system. APK Auditor consists of 3 main components:

1. APK Auditor Client,
2. A signature Database,
3. A Central Server that communicates with client and also with the signature info and handles the analysis method.

The Fig. 5 [5] presents a summary of APK Auditor’s computer code design.

#### APK Auditor Client

APK Auditor client merely offers associate degree analysis request, showing whether or not the application is trustworthy or not. This client application lets users associate degree analysis to each native application on an server device and remote applications on Play Store. This analysis is kept specifically on server as limited computing power of mobile compared to PC.

#### APK Auditor Signature Database

Application's area unit keeps within the APK Auditor signature information along with the results of the analysis. APK Auditor server classifies applications through these permissions, supported their existence in malwares. Service and receiver info is neglected as a result of their application specific definitions and also keeps analysis results for every application area unit displayed.

#### APK Auditor central server

The APK Auditors central server governs and monitors analysis method and works as a mediator between signature info and client whereas analyzing requested applications. The central server will download high rated applications from Play Store and analyzes them. This official market needs authentication associate degree a tool symbol so as to transfer an application. It will set the threshold using logistic regression function. Afterword’s in evaluation phase it will predict the whether the app is malicious or benign.

**Proposed algorithm is using ID3 decision tree**

Steps are mentioned as bellows.

1) Calculate the entropy of each and every attribute from the data set S. Dataset S contains the malicious as well as benign apks. Attributes considered from the dataset are malware score, permission count for malicious dataset, permission count for benign dataset Threshold value.

For that we have to use the formulas below [16].

\[
H(S) = - \sum_{x \in X} p(x) \log_2 p(x)
\]  

Where,

- **S** – Data set
- **X** - Set of classes in S
- **p(x)** - The proportion of the number of elements in class x to the number of elements in set S.

Then Information gain is calculated [16].

\[
IG(A,S) = H(S) - \sum_{t \in T} p(t)H(t)
\]

Where,

- **H(S)** - Entropy of S
- **T** – Subsets created from splitting set S by attribute A such that S=∪ t.

2) Classify a subset of attributes for which information Gain maximum.(or ultimately entropy is minimum).

3) Form a decision tree node which contains that attribute.

4) Recursively performs the same for remaining subsets of attributes.
D. Dataset

We have collected a malware dataset from malware repository called Contagio and malware.lu [18][19]. From Contagio we have collected 30 malware apks and from malware.lu we have collected 80 malicious apks. To collect benign apks we have used Google Play store. We have collected 75 clean apks. In first dataset we have successfully analyzed 80 permissions. In the second dataset we have successfully analyzed 140 permissions.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>No of APK samples used</th>
<th>Permissions Analysed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dataset 1</td>
<td>40</td>
<td>80</td>
</tr>
<tr>
<td>Dataset 2</td>
<td>126</td>
<td>140</td>
</tr>
</tbody>
</table>

E. Evaluation Setup

We have implemented proposed model explained in section IV using .net 2010 on windows 7. In training phase it will analyze the apk file and gives permission statistics. In Evaluation phase it will predict the about the app whether it is malicious or benign. Figure 6 shows the app evaluation process.

VI. EXPERIMENTAL RESULTS

Our aim is to enhance the security of the smartphones as well as to enhance the accuracy. In first dataset of 40 apps we have used 18 benign apps and 22 malicious apps. In Second dataset We have used 75 benign apps and 51 malicious apps. Table 2 shows the results, when we evaluate over the dataset as mentioned in Table 1. Final results are shown in the form of Accuracy percentage and False positive ratio.

As mentioned in table II when we evaluate our system over 40 dataset using Logistic Regression accuracy of the classification is 90% and false positive ration is 9%.

A. Performance Evaluation Criteria

We are using machine learning technique to classify the malicious behavior of app. So performance Evaluation is based on confusion matrix. Following 4 items define the members of confusion matrix.

- **True Positive**: Number of correctly classified benign application.
- **False Positive**: Number of incorrectly classified malware applications.
- **True Negative**: Number of correctly classified malicious applications.
- **False Negative**: Number of incorrectly classified benign application.

\[ \text{Accuracy} = \frac{TN + TP}{TP + FP + FN + TN} \]  

- **False Positive Ratio**: Percentage of wrongly classified malware applications.

In the next phase when we increase our dataset and train the system using 140 permissions then we found accuracy is increased, and classification percentage comes out to be 96% resulting in decreasing FPR.

Again when we evaluate the system using decision tree then accuracy noted here is 95% and false positive ratio is 4%.
FPR = \frac{FP}{FP + TN} \quad (7)

VII. CONCLUSION AND FUTURE SCOPE

The mobile security has gained wide attention in past few years. There are many more techniques available to tackle the mobile security issue. Proper literature review and deep study will explore many more methods to capture the malware. Different methods have different accuracy impact on malware detection.

In some tools we will find increased classification accuracy and in some tools we will find although classification accuracy is good FPR ratio is high. It is possible to have other methods than the proposed methodology in the paper.

The primary goal of our system is to enhance security and to improve accuracy of the malware detection. The accuracy of malware detection is much more dependent on the malicious and benign dataset. Dataset plays important role in setting threshold value of computation. Many preventive tools are available in market but main drawback observed is False positive ratio is high in such tools. As we are dealing with permissions of apps while analyzing, privacy should be maintained and should not reveal the confidential information to each other.

The immediate next future direction of our system is, it is based on static analysis so capturing 0 day malware and runtime behavior of the features should be further studied, which in turn will predict correct label. It is possible to detect mobile malware using other machine learning technique such as SVM, Naive Bays Theorem etc. Our existing system is scalable with such techniques and should be further studied with the same.

REFERENCES


[18] http://contagiodump.blogspot.in/

[19] https://malware.hu/
Analysis of Decision Making factors for Automated Intrusion Response System (AIRS): A Review

Dileep Kumar Singh and Praveen Kaushik
Dept of CSE, MANIT Bhopal, India

Abstract—Increasing amount of dependability on computer networks and internet services are also increasing intrusions. Intrusion Detection System (IDS) tools detect the intrusions and produce alerts. An automated Intrusion Response System (AIRS) is required to analyze the alert and trigger appropriate response to mitigate the intrusion without delay. In this paper, cost evaluation methods and response decision making capabilities of various AIRS models are analyzed. Various decision making factors that are involved in the response selection process are also identified and then categorized in response, attack and system level factors.

Index Terms—Intrusion Response System, AIRS, Response selection, Response factors, Response cost.

I. INTRODUCTION

Network attacks or intrusions incidents are becoming more complex and increasing with the rapid expansion of the networks and services over the networks. According to PWC Global State of Information Security Survey-2016 [1], the intrusion incidents are increased by 38% compared to the previous year. The constant increasing incidents required a powerful defense mechanism in order to overcome the organization loss.

There are the tools available for monitoring the intrusion on the system called Intrusion Detection Systems (IDS) that generates the alerts to the network administrator in case any intrusion is detected. For the network administrator, it becomes very complex and tedious to respond the each alert without any delay, exclusively when the generated alerts are in hundreds, thousands or even more in numbers. So an Automated Intrusion Response System (AIRS) is required to handle the large amount of alerts and respond appropriately without much delay [2], [3].

The goal of an AIRS is to select automatically the correct response for the alerts to mitigate the attack with less penalty cost [4]. An effective AIRS should be designed so that it should have adaptive and cost sensitive characteristics with achieving the balance between the response cost and the damage cost [3].

Various frameworks and models are proposed for the AIRS, which considered various factors and cost evaluation techniques for the selection of the response. In this paper, the comparative study and analysis of the various available AIRS models for cost evaluation and response selection are presented. The comprehensive list of factors that has been used for the decision making for response selection is also identified and categorized.

This paper is organized as follows. Section II describes the various available models and framework for the intrusion response system, Section III presents the analysis of the various AIRS models. Section IV presents the discussion and section V is the conclusion.

II. AIRS RESPONSE SELECTION MODELS

Sven Ossenbuhl et al. [5], proposed REASSESS (Response Effectiveness Assessment) response selection model containing five phases named – input & configuration, alert processing, response selection, response execution and documentation. REASSESS model compares the available responses and for a given alert provides a most suitable response (having highest effectiveness). The comparison is modeled with the response effectiveness which is evaluated on the basis of positive and negative effects of a response. The negative impact is evaluated with the help of the importance of the service and the capability reduction that depends on the performance of system/services either due to a
deployment of a response measure or in the event of an attack. Positive effects are based on the response success rate which is further dependent on the ratio of the number of deployments of response that successfully mitigated the attack and the total number of deployments of response.

The evaluation of model is done based on the following characteristics – Automatic deployment, Scalability, Adaptability, System independency, Calculation efficiency, Usability Security mechanisms and found the model comparatively better performing than the ADEPTS, CS-IRS and IE-IRS.

They used the amount of alerts to measure the performance of the proposed model. According to the authors, there are various challenges that need to be focused on like determining the set of eligible responses for a system and the impact of an attack on the given system. Aderonke Justina et al. [6], have presented the COSIRS (Cost Sensitive Intrusion Response System) response cost assessment model by considering the three factors – damage cost caused by the intrusion, response cost and the operational cost. COSIRS contains two major components – Intrusion Detection System (IDS) and the Response Engine (RE). Further, the RE is divided into various sub-components – alert filter & correlation, response manager (RM), database (contain information about intrusion specification, profile and response actions), adaptability module, cost sensitivity evaluation module (CSEM) and response deployment module.

The Intrusion Cost (the cost of damage caused by an intrusion $i_n$) is evaluated using the intrusion impact on the system and operational cost (cost of daily maintenance of various aspect of the detection system). Intrusion impact on the system is derived with the help of the set of resources provided by the system, a number of resources which are being affected by the intrusion, the severity level of the attack, security policy (confidentiality, integrity & availability) and the weight of each security policy.

Response cost is derived using Response impact on the system and Operational Cost. Response impact on the system derived based on the number of available response ranks, a number of resources affected, resources affected by the deployed response and weight of each security policy.

Natalia Stakhanova et al. [7], proposed the cost sensitive automated IRS model with pre-emptive and adaptive characteristics. The proposed model relies on the pattern based IDS which can represent the normal and the anomalous pattern of the system behavior in state-transition graph. The model manually associated response action with each known intrusive pattern in the abnormal graph. The preemptive response is deployed only if the prefix pattern (of known attack sequence) matched with monitored sequence with greater than the pre-defined probability threshold. The probability of occurrence of the sequence is referred as a confidence level.

Confidence level = (number of Sequence-Occurrence / total number of sequences with this prefix)

From the set of candidate response, the selection of the appropriate response is determined based on damage cost (DC) and response cost (RC). They have associated the damage cost using prior information to each attack pattern. The response is selected for which the condition $DC*confidence level$ > $RC$ holds.

The success factor (SF) and risk factors (RF) are considered for the selection of the optimal response action which provides maximum benefit with the lowest risk. Used utility theory and defined expected value (EV) of response $r_S$ to a sequence $S$ as: $EV(r_S) = (Pr_{succ}(S)*SF) + (Pr_{risk}(S)*(-RF))$, where $Pr_{succ}(S)$ is the probability that sequence $S$ will occur and $Pr_{risk}(S) = 1 – Pr_{succ}(S)$. Based on the highest EV the optimal response is selected. The model achieves adaptability by adjusting the $SF$ by increasing or decreasing by one for every success or failure respectively.

Chris Strasburg et al. [8], presented a host based framework for cost sensitive assessment for intrusion response selection with the goal of selecting a set of responses so that, given a possible intrusion set minimizes the potential system damage. The factors associated with the response action evaluation are broadly defined into two groups called factors associated with intrusion damage and factors describing response cost.

The intrusion damage $D$ further categorized as: deployment of response due to false alarms ($D_{FalseAlarm}$), deployment of no response when an intrusion occurs (false negative alarms) ($D_{FalseNegative}$), deployment of sub-optimal response due to a miss-labeled alarm ($D_{MisslabeledAlarm}$) and deployment of response for true attack ($D_{true}$).

The system damage caused by the true attack is defined using three components: System resources affected by intrusions – such as services provided by the system (FTP, HTTP, etc.), the resource importance for system confidentiality, integrity & availability and the weight of these factors on the security policy of the system. The damage cost is evaluated with the intrusion impact on system resources and operational cost.

The response cost estimation is composed of three components – Operational cost (OC), response goodness (RG) and response impact on the system (RSI). So
Response Cost $RC$ for applying a response $r$ for intrusion

$I$: $RC(r, I) = OC + RSI - RG$

Yu Sun et al. [9], proposed an Aggregation and Cost Based Automatic Intrusion Response System (ACAIRS) model containing the components: IDSs, Interface, Alert Aggregation, Response Process Unit (RPU), Response Actions, Response Cost, Response Policy and Response Log. They mainly focused on the aggregation of the alerts, for which the alerts are categorized mainly in four categories: U2R, DOS, R2L, and PROBE, which is further partitioned according to the attack type, destination IP address and interval. The aggregation is defined based on the similar degree of each intrusion incident $S = A + D + I$, where $A$, $D$ and $I$ are the similar degree of attack type name, destination IP address and interval respectively. Further $A$, $D$ and $I$ are described as:

$A = \{1 \text{ and } 0\}$ for {names are identical and names are not identical}, $D = \{1, 0.5 \text{ and } 0\}$ for {IP addresses are identical, IP are not identical but on the same subnet and IP addresses are not on the same subnet} and $I = \{1, (30-T)/20 \text{ and } 0\}$ for $T \leq 10 \text{ min}, 10 \text{ min}<T \leq 30 \text{ min}$ and $T>30 \text{ min}$. There will be defined a threshold for each of the four categories. Each incident alert $N$ will be compared with the N-1 alerts, so $SN = \{S1, S2, ..., SN-1\}$ and the $SM = MAX\{SN\}$ is calculated and compared with the threshold, if found less than considered a new alert else treated as the repeated alert. After aggregation process complete they have mentioned the response selection process by writing the generic rules with the condition of $Dcost \leq Rcost$, where Dcost and Rcost are damage and response cost respectively.

Bingrui Foo et al. [10], presented automated intrusion response mechanism called ADEPTS, based on the intrusion graph called $I$-GRAPH, with a feedback mechanism for evaluating the deployed response. $I$-GRAPH models the knowledge about intrusion where each intrusion goal is represented by one node in the graph with dependency relationships and edges are categorized as OR, AND, and Quorum edges.

For generating the $I$-GRAPH, used a semi-automated method called $I$-GRAPH Generation (PIG), which takes two inputs: vulnerability descriptions and system services description (SNet). SNet is directed graph (created manually); where individual services are represented by nodes and the edges between nodes A & B represent the intrusion centric channel, means if A is compromised then the intrusion can spread to B through the channel. They defined five kinds of channels: DOS channel, Network channel, Shared file channel, Shared memory channel and Super channel (the combination of the other channels). The second input to PIG, vulnerability descriptions, can be obtained from any common vulnerability databases, such as CERT, Bugtraq, CERIAS-VDB etc.

To determine the response location they have proposed the response set computation based on the alert confidence (provided by the detector or set to one) and compromised confidence index (CCI) computation. CCI of a node represents the likelihood that the node has been achieved.

To compute response set the $I$-GRAPH is traversed in reverse order of CCI computation until all reachable nodes are traversed at most once and during traversal, each node is labeled as: Strong Candidate (SC), Weak Candidate (WC), Very Weak Candidate (VWC) and Non-Candidate (NC). So, SC label on a node is a strong indicator that the node has been achieved, while the WC or VWC label indicates smaller likelihoods. After this in the case of conservative policy, all SC nodes that have at least one immediate NC parent node are chosen and placed in the response set, whereas in moderate policy all SC and WC nodes and in aggressive policy all SC, WC & VWC nodes are placed in the response set. Finally, the deployment of the response is achieved with the help of Response Repository, Response Control Center and distributed Response Execution Agents. Response with highest Response Index ($RI – calculated using Effectiveness Index and Disruptiveness Index$) is chosen to deploy by the control center.

Zheng Wu et al. [11], presented the response decision model based on Analytic Hierarchy Process (AHP), which uses the pair-wise comparison to represent the relative importance of one criterion over another, avoiding the drawback of accurate measurement for influence factors in order to select the proper response mechanism. They described the general IRS in four components: Response Policy Library (RPL), Response Decision Module (RDM), Response Implementation Module (RIM) and Response Tools Library (RTL).

They have considered the common four influence factors for response selection that are: Attack Restraint (AR), Service Maintenance (SM), Time Spending (TS) and Resource Consumption (RC). Developed the AHP model with three layers, where the root layer representing the response selected and the middle layer representing the criterion representing the various factors as mentioned above & the bottom layer represent the response alternatives options and created the relative matrix of “response selected”. They categorized the intrusion as: Information Gathering (IG), Right Escalating (RE), File Operation (FO) & Resource Depletion (RD) and presented the relation of intrusion and the common response in the form of the table.
Chengpo Mu et al. [12], presented the various response factors that are applicable in the response decision making models. They identified 15 different factors and classified as: Attack-related factors – Alert confidence, Attack type, Attack severity, Attack amount, Attacker type & Attack time; Response-related factors – Response goal, Response intensity, Response negative impact & Response effectiveness and Target-related factors – The importance of resources, Exposed extent of vulnerability, Service capability of system & Policy constraint.

Further, they have categorized the factors in Objective factors – which can be directly get from IDS alerts, vulnerability scan tools & network configuration and Subjective factors – which can be determined by administrators and experience.

They have analyzed the response factors and concluded with what factors are important for the response time decision making and what for the response measure decision making.

Chengpo Mu et al. [13], have presented Intrusion Detection Alert Management and Intrusion Response System (IDAM&IRS), which is an intrusion response decision-making model based on hierarchical task network (HTN) planning having response measure decision-making as well as response time decision-making capability with the features of self-adaptive and balancing of response effectiveness & response negative impact. HTN is a planning system that searches for a sequence of actions to achieve the desired goal, referred as intrusion response plan.

They represented the hierarchical structure of IDAM&IRS response planning based on an intrusion scenario that is being detected and responded, response goal set by an administrator (such as analyze the attack, catch the attack, mask the attack, maximize confidentiality, maximize data integrity, minimize cost etc), response strategy corresponding to the response goal and response key points. Different subtasks and their orders in KP can produce different strategies in the response process. They have mentioned 13 response key points (KP) such as general alarm subtask P1, reinforced alarm subtask P2, general evidence record subtask P3, and weak attack block subtask P7 etc. Further, they have refined the response goal into various subtasks.

The response time decision making methods are described for different subtasks such as, for alarm subtasks, evidence record subtasks and backup subtasks (executed at the host level) the time decision-making model expressed as:

### Decision-making Model

\[
IF \quad RI_{pi} \geq RIH_{pi} \quad THEN \quad P_i \begin{cases} \text{BEGIN} \quad \text{AND} \quad T_{pi} = t_i \\
\end{cases}
\]

Here, \( RI_{pi} \) is the risk threshold in the host level and the above equation represent that when the risk \( RI_{pi} \) caused by an intrusion scenario \( k \) in a host is greater than or equal to the threshold \( RIH_{pi} \), then begin subtask \( P_i \) and take the time \( t_i \) as the beginning time of subtask \( P_i \).

The response scheme decision making methods also defined for various subtasks such as the response measure decision making process for alarm subtasks, evidence record subtasks, backup subtasks, block subtasks and counterattack.

Chengpo Mu et al. [13], have presented Intrusion Detection Alert Management and Intrusion Response System (IDAM&IRS), which is an intrusion response decision-making model based on hierarchical task network (HTN) planning having response measure decision-making as well as response time decision-making capability with the features of self-adaptive and balancing of response effectiveness & response negative impact. HTN is a planning system that searches for a sequence of actions to achieve the desired goal, referred as intrusion response plan.

They represented the hierarchical structure of IDAM&IRS response planning based on an intrusion scenario that is being detected and responded, response goal set by an administrator (such as analyze the attack, catch the attack, mask the attack, maximize confidentiality, maximize data integrity, minimize cost etc), response strategy corresponding to the response goal and response key points. Different subtasks and their orders in KP can produce different strategies in the response process. They have mentioned 13 response key points (KP) such as general alarm subtask P1, reinforced alarm subtask P2, general evidence record subtask P3, and weak attack block subtask P7 etc. Further, they have refined the response goal into various subtasks.

The response time decision making methods are described for different subtasks such as, for alarm subtasks, evidence record subtasks and backup subtasks (executed at the host level) the time decision-making model expressed as:
### Table-1: Analysis of various AIRS models

<table>
<thead>
<tr>
<th>S No</th>
<th>Model</th>
<th>Damage Cost (DC) and Response Cost (RC) evaluation techniques</th>
<th>Response selection Process or Techniques</th>
<th>Factors Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sven Ossenbu hl, (REASS ESS)</td>
<td>$A_0 = (F_{s}(e) + S(e))/2 \in [0..1]$&lt;br&gt;$A_r = rsr E_i SI i D j$&lt;br&gt;Here, $A_0$ and $A_r$ are positive and negative effects $S(e)$ and $F_{s}(e)$ are importance of service e and the capability reduction $F_{s}(e)$ performance of an entity e and $rsr E_i SI i D j$ is the response success rate for a given response r, and alert a, $dps_i (a_j) = n_i dp_i ort_i = a_j/0..1]$</td>
<td>Based on highest response effectiveness&lt;br&gt;Cost sensitive&lt;br&gt;Having the Learning ability&lt;br&gt;Cost sensitive&lt;br&gt;Having the Learning ability&lt;br&gt;DPS</td>
<td>AF&lt;br&gt;RF&lt;br&gt;Nil&lt;br&gt;Negative effect&lt;br&gt;Service importance</td>
</tr>
</tbody>
</table>
| 2    | Aderonk e Justina, (COSIR S) | Damage cost (damage caused by an intrusion in) $DC_n = IS + OC_i$

$$IS_j = \sum_{Sr \in SR} E_i (sr, \omega_j)$$

Response cost RC = $IS + OC_i$

$$IS_r = \sum_{Sr \in SR} \frac{1 - \frac{r}{m} |Sr, \omega_j|}{k * m}$$

Where, $IS_i$ and $OC_i$ represents the intrusion impact on the system and operational cost $sr$ = resources provided by the system. m = number of resources which are being affected $E_i = severity level of the attack j = security policy (CIA)$ $\omega_j = weight of each security policy k = a normalization value$ | Not clearly mentioned the process of selecting the responses, instead given the method of evaluating the damage and response cost. Cost sensitive<br>Although Adaptability module is mentioned but no method is clearly described for the calculation of the effectiveness of the previous response and further learning through feedback<br>Cost sensitive | AF<br>RF<br>SF<br>Negative effect<br>Security policy |
| 3    | Natalia Stakhanova et al., 2007 | Confidence level = number of Sequence-Occurrence / total number of sequences with this prefix<br>select response actions while $DC^{\text{confidence level}} > RC$ $Expected Value (EV)$ of response $r_i$ to a sequence $S$: $EV(r_i) = (Pr_{true}(S)^{SF}) + (Pr_{true}(S)^{(-RF)})$, where $Pr_{true}(S)$ is the probability that sequence $S$ will occur and $Pr_{true}(s) = 1 – Pr_{true}(S)$. | Based on the highest $EV$ the optimal response is selected<br>Cost sensitive<br>Adaptability is achieved by adjusting the SF by increasing or decreasing by one for every success or failure respectively<br>Using State Transition Graph to model the system behavior<br>Associating response action with each known pattern of anomaly – done manually<br>Methods to evaluate Damage and Response cost are not explicitly mentioned | AF<br>RF<br>Nil<br>SF<br>Negative effect<br>Security policy |
| 4    | Chris Strasburg et al., 2009 | Damage Cost by true attack $DC_{true} (i_k) = SL(i_k) + OC(i_k)$

Where, intrusion system impact:

$$SL(i_k) = \sum_{n_j \in SR} E(i_k, sr_j) \times W_{n_j}$$

OC(i_k) $\in [0..1]$ | Selecting a single response based on the response effectiveness value $RV(r, I_s)$ Cost sensitive<br>Host based | AF<br>RF<br>SF<br>Negative effect<br>Previous response success percentage |
<table>
<thead>
<tr>
<th>Page</th>
<th>Authors</th>
<th>Methodology</th>
<th>Result</th>
<th>Factors</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 5    | Yu Sun et al., 2008 (ACAIR S) | Compromised Confidence Index of a node –  
\[ CCI = \begin{cases} 
\max(CCI_i) \text{, OR edge} \\
\min(CCI_i) \text{, AND edge} \\
\end{cases} \begin{cases} 
\text{alert confidence} \text{ no children} \\
\text{no detectors} \\
\end{cases} 
\]  
\[ f' = \begin{cases} 
\text{mean}(CCI_i), \text{ if } CCI_i > \tau, \text{ Quorum met} \\
0, \text{ quorum not met} \\
\end{cases} \]  

Here, function f represents the statistical mean, and CCI, representing the CCI of the ith child and \( \tau \) is a per node threshold. | Responses are categorized in passive and active responses  
Response Selection is based on generic rules with the condition of DC>RC  
Methods to evaluate Damage and Response cost are not explicitly mentioned | AF  
RF  
SF  
• Alert Confidence  
• Response Cost  
• Operating System in use  
• System Vulnerabilities  
• System services |
| 6    | Bingrui Foo et al., 2005 (ADEPT S) | Based on Relative matrix –  
\[ A = (a_{ij}) (i, j = 1, 2, 3, \ldots) \]  
\[ a_{ij} \text{ is the comparison value of alternatives in contribution to one criterion as} - \]  
\[ \text{if } a_{ij} = a_j, \text{then } a_{ij} = 1, \text{a}_i = 0 \]  
\[ \text{if } C_i \text{ is the same importance as } C_j, \text{then } a_{ij} = 1, \text{a}_j = 1 \]  
The priority of each alternative is calculated by eigenvector of the relative matrix. | Adaptive by using response feedback to adjust the EI  
Response selection is based on response index RI  
Choose the response with the highest RI  
Handling unknown alerts by reporting and applying general responses | AF  
RF  
SF  
• Alert Confidence  
• Response Effectiveness  
• System vulnerabilities  
• System services |
| 7    | Zheng Wu et al., 2008 | Created Intrusion Response Plan as –  
\[ \Xi = \{k, \Psi, \zeta, KP\} \]  

\[ \text{time decision-making model} - \]  
\[ R_{i}^c \geq R_{HI}^c \text{THEN BEGIN AND} \\]  
\[ \text{if } i \in \{1, 2, 3, 4, 5, 6\} \]  

Based on hierarchical  
Task network planning (HTN)  
Uses effective index (EI) and Disruptive impact index (DI)  
Using response time and response measure decisions  
Selects the response measures with the highest EI / DI ratio | AHP is used to select the Optimal response  
Not dependent on the accurate measurement of the decision making factors | AF  
RF  
SF  
• Attack Restraint  
• Time Spending  
• Resource Consumption  
• Service Maintenance |
| 8    | Cheng o Mu et al., 2010a and 2010b (IDAM &IRS) | Alarm Matrix  
\[ A = (a_{ij}) \]  
\[ a_{ij} \text{ represent the number the attack type i alarmed to j by IDS} \]  

Not clearly mentioned the methodology of response selection, but work on the evaluation of the various factors | AF  
• Alarm confidence Level  
• Attack frequency  
• Response cost  
• Risk assessment |
It can be noticed from the above analysis that most of the models are missing attack factors in order to the selection of the appropriate response. Many models not explicitly mentioned the computation of the response selection process. Most of those only considered true positives (i.e., the number of correct responses) for checking the effectiveness of their approach. False positive must also be taken into account.

It is important to know how responses for AIRS have been wrongly identified. The online risk assessment component is not tightly integrated and attuned with the response systems. There are no correlations between the responses in almost all the above mentioned models. These require the further depth research in order to make a complete AIRS.

IV. DISCUSSION

Automated Intrusion Response Systems (AIRS) are very much essential in today scenario where many services and businesses depend on the networks and there is a rapid increase in the intrusions on the networks. In order to design the AIRS effective and efficient, it is required to identify and choose various decision making factors for selection of optimal response precisely.

Based on the above study, various factors that can be considered for developing more effective AIRS is divided broadly into three categories as mentioned in table-2.

Table-2: Decision making factors

<table>
<thead>
<tr>
<th>S No</th>
<th>Category</th>
<th>Factors</th>
</tr>
</thead>
</table>
| 1    | RF       | 1. Response Cost/Negative effect  
        • Factors related to Response measured and/or assigned by the network administrator or the experts  
        2. Response time  
        3. Response effectiveness  
        4. Response success rate/ Response goodness  
        5. Previous response success percentage  
        6. Response Time |
| 2    | AF       | 1. Alarm confidence Level(probability of occurrence of intrusion)  
        • Factors related to intrusions/Attack and can be obtained from the IDS systems  
        2. Attack frequency  
        3. Attack severity level |
| 3    | SF       | 1. Service/Resource/System importance  
        • Factors related to the System  
        2. Service/Resource/System performance  
        3. System Resources affected by intrusion  
        4. Intrusion impacts on system resource  
        5. Operating System in use  
        6. Damage cost  
        7. Security Policy (CIA – Confidentiality, Integrity, Authentication) |

All the models not showing the uniformity on the factors that should be involved on decision makings. In general, it is found that the Alert confidence, damage cost, response cost, response effectiveness and the importance of resources are commonly used in all kinds of decision-making models mentioned above.

The methodology that the mentioned AIRS models used for response selection process can be categorized as cost-sensitive based, graph based, analytic hierarchy process (AHP) based and hierarchical task network (HTN) planning based models. Although most of the models consider the response effectiveness as key factors for response selection, but all the factors mentioned in table-2 in response category should also be required to be considered in order to design the most effective AIRS.

V. CONCLUSIONS

In this paper, we analyzed various AIRS models. The decision making factors considered in models are identified and categorized based on the response, intrusion and system level factors. It is found that mostly all the models are not synchronized in terms of decision making factors that they have considered. Therefore, a performance comparison of the models with each other might produce the ambiguous result. There are total 16 factors altogether that are identified based on the study that can be considered for an effective design of the AIRS. But one of the biggest challenges is the accurate measurement of these decision making factors.

Further depth researches are required on creating the general and widely acceptable measurement of the response decision making factors. Further, it requires more research on the methodologies that are less dependent on accurate measurement of the decision making factors such as analytic hierarchy process (AHP).

REFERENCES


SQL Injection Prevention using Query Dictionary Based Mechanism

Adwan F. Yasin¹
Department of Computer Science, Arab American University
Jenin, Palestine.

Nael Zidan²
Department of Computer Science
Arab American University
Jenin, Palestine.

Abstract — SQL Injection Attack (SQLIA) is a technique of code injection, used to attack data driven applications especially front end web applications, in which heinous SQL statements are inserted (injected) into an entry field, web URL, or web request for execution. "Query Dictionary Based Mechanism" which help detection of malicious SQL statements by storing a small pattern of each application query in an application on a unique document, file, or table with a small size, secure manner, and high performance. This mechanism plays an effective manner for detecting and preventing of SQL Injection Attack (SQLIA), without impact of application functions and performance on executing and retrieving data. In this paper we proposed a solution for detecting and preventing SQLIAs by using Query Dictionary Based Mechanism.

Index Terms — SQL Injection Attack, SQL Injection Attack Detection, SQL Injection Attack Prevention, Query Dictionary.

1 INTRODUCTION

Structured Query Language (SQL) [1, 2] is a standard, comprehensive language, based on the relational model, SQL includes capabilities of many functions. DDL statements for creating schemes and specifying data types and constraints. DML statements for specifying data retrieves, and data modifications. SQL Language is a textual language that used on all relational database management systems (RDBMS), the most known and used are Oracle, Microsoft SQL Server, MySQL, PostgreSQL, DB2 and SQLite.

SQL Injection Attack (SQLIA) [3] is a code injection technique, used to attack data driven applications especially front end web applications, in which heinous SQL statements are inserted (injected) into an entry field, web URL, or web request for execution, used to gain unauthorized data, or to retrieve information from SQL relational database. SQLIA used most often to attack databases for retrieving and extracting secret information such as credit card information, private information, user information’s, and financial records. The highest risk application for attack is web applications, since web applications accessed through internet and available for all internet users and devices, also mobile applications now are at highest risk for SQLIA. An application is vulnerable for SQLIA since the injection is legal for SQL standards, and DB engine execute it. The vulnerability exists at user inputs, in which they bypass validation or no validation at all and passed to dynamic SQL statement without validation and checking. If we are validating the user input, then with another way we are forbidden them to entering single and double quotes, multiple dashes, and SQL Language keywords in the input. Hackers have ability to input directly malicious queries via a web form or by directly insert it to the end of the URL or to URL variables or through HTTP headers. For example, if the query accepts username and passwords like this:

```
"SELECT User_Name, User_FullName FROM TABLE_USERS WHERE User_Name=' AhmAd' AND User_Password='";
```

The above query will select "Username" from the table "TBL_USERS" by filtering using query search condition "User_Name" and "User_Password". Now we can manipulate it by various SQL code snippets by just input them in User_Name and User_Password fields at web form or URL variables like Ahmad' or '1 = '1'. When web form front end processes web form and generates SQL statement to send it to DBMS, generated SQL query with above inputs will be:

```
SELECT User_Name, User_FullName FROM TBL_USERS WHERE User_Name='Ahmad' AND User_Password='or 1 = 1';
```

Because of malicious input the query search condition is always true condition as the query is asking to retrieve User_Name and User_FullName with condition that User_Name is Ahmad and USER_PASSWORD equal to " or 1 = 1. We can also use SQL comments operator "--", so SQL engine ignore the portion after comment operator, if User_Name field input is Ahmad--, this will manipulate query search to just check condition on User_Name only, UNION can also lead to a successful SQL injection attack.

Open Web Application Security Project [4] published that SQL Injection Attack (SQLIA) is the top one and most vulnerable among the top ten web application vulnerabilities.

SQL Injection attack not limited for web applications, it could be on desktop applications, mobile applications. According to OWASP [5], according to reports on 2008 for SQL injection vulnerabilities, 25% of all vulnerabilities reported for web applications.

In this paper we are proposing a solution for detection and prevention of SQL Injection Attack (SQLIA) using
Query Dictionary Based Mechanism, in which we will store all queries search portion patterns, then we compare query generated from web forms back end and compare with stored one, the result will show if form query is injected, based on result action taken. In section 2 we are talking about Web Application and SQL Injection attacks, Section 3 about Types of SQL Injection Attacks. Section 4 about SQL Injection Attack Detection. Section 5 is a summary of related work on SQL Injection detection and Prevention. Section 6 we are talking about our Proposed solution. In last section the conclusion.

2 WEB APP AND SQL INJECTION ATTACKS

Web application is a computer application that located on a server and users request it using web browsers through World Wide Web abbreviated (WWW). Web applications requested using HTTP or HTTPS protocols. In early web application started to be static, with web technology development most of web applications now dynamic content, this means its contents from a database. Client using browser by entering web application URL request a web application document by using HTTP methods “Get, Post, Put, Delete”. Web application N-tier architecture consists of Presentation, Business/Logic, and Data tiers. The most architectures used is 3-tier in which each layer can potentially run on a different machine and the three layers are disconnected as shown on Fig.1.

![Fig. 1. 3-teir Web Application Architecture](image)

This architecture in which presentation layer exists on client machine which is displayed using browsers like Google Chrome, Mozilla Firefox, Microsoft Internet Explorer. In addition, the ability of user for changing URL variables also input fields and weakness of client validation and easy of validation bypassing allow hackers to use vulnerabilities of dynamic SQL queries generated at web application backend programming code. SQL Injections [6] are attacks by which an attacker makes changes on the structure of the original SQL query by inserting (injecting) additional SQL code in the input fields of the web form or desktop app form or on URL in order to acquire unauthorized access to the database. Despite that vulnerabilities that drive to SQLIAs are well known and understood, they persist and continued to be available because of lack of effective solutions and techniques for detecting and preventing them. SQLIA is a hacking technique in which attacker makes modifications on SQL statements through web form or application form inputs or web form URL variables or hidden fields to access unauthorized resources. Weakness of input field and URL variables validation help hacker to success. Web application vulnerabilities is the main cause of SQL injection, the most of these vulnerabilities are:

A. **Weakness in input validation:** this the common vulnerability in which no input validation for web form input fields or URL variables, so this allow hacker to add SQL code easily.

B. **Generous privileges:** when web application access a database need a user with specific privileges, for example privileges for reading data, modification of data includes insertion, updating and deleting, privileges for DDL like creating tables, dropping tables. So the weakness here to use a general user that have all privileges, so any SQL statement this DB user can execute. So here if attacker bypass authentication he gains access to all DB user privileges, for example he can drop any table.

C. **Uncontrolled variable size:** variable sizes that uncontrolled and generic specially the biggest domain of them like String, lead to an easy way for attacker to alter SQL query with many characters the variable contains.

D. **Error message:** the generated error messages by backend server code may return to client, these messages may contain database name, tables name and attributes, etc., this information help hacker to know the structure of database. So error messages should not be shown to client and should the web application send it to webmaster by email or audit it in a log file.

E. **Dynamic SQL:** SQL queries that dynamically generated on backend code, these queries generated by concatenating SQL where condition attributes with variable values from input field or hidden fields or URL variables. In dynamic SQL the most research focus since no way to prevent using it, and it should not infect with SQLIAs.

F. **Client-side only control:** if web application web forms validation depends on client side only, this is vulnerable, since hacker can bypass validation and validation scripts at client can be altered by using cross-site scripting.

G. **Stored procedures (SP):** SP is an assigned name for a set of SQL statements and logic of procedures that compiled, verified and stored in database server, and it controlled through database server security. SP is more secure than web form dynamic generated query. The vulnerability to use dynamic generated SQL statements and use database function like EXEC to execute generated query, in this case it is vulnerable same with web form dynamic generated query.

H. **Input Output file support:** if database user has privilege to execute input form file or output file, then it will allow hacker to execute any statement that output to text file or excel file, for example MariaDB and MySQL “SELECT INTO OUTFILE…”.

I. **Multiple statements:** database user privilege for executing multiple statements allow hacker to use UNION and retrieve additional information, or he can add additional insert statement or delete statement or drop table statement.

J. **Sub-selects:** supporting of sub-selects or sub-queries lead to vulnerability, so additional SQL query can be
added inside WHERE condition. There are code practices [7] should be followed to reduce SQL IA, the most important of these practices are:

A. **Manual Coding Practices Defense:** here developer learn SQL IA techniques and how to prevent them on coding stage, these practices divides to four categories. **Using Parameterized Queries or Stored Procedures,** this will reduce vulnerabilities on dynamic query generation by concatenating, and replace values with placeholders (parameters) with values. Also stored procedures can check of parameters data types and hide query structure from attacker. And developers should avoid using dynamic generation of queries in Stored procedures. The second category is **Escaping,** which is a technique for elimination SQL keywords. Each Programming language or script language has suitable connector to DBMS and it has its own escaping functions embedded in their libraries, as an example MySQL connector for PHP has mysql_real_escape_string() function. Third category **Data Type Validation,** here developer should use suitable data types and he should check and validate inputs with data types. Last group is **White List Filtering,** [8], by filtering allowed and legitimate key words, then check for list to accept and execute.

B. **SQL DOM:** [9] the solution is an executable “sql-domgen”, which executed with connection to database and generate a compiled Dynamic Link Library (DLL) file. This file used by developer to execute against database. DLL file contains classes refer to them with SQL Domain Object Model (SQL DOM).

C. **Parameterized Query Insertion:** by using this technique, SQL queries vulnerabilities is detected inside source code and replaced with secure parameterized Structured Query Language (SQL) queries.

### 3 Types of SQL Injection Attacks

There are different methods performed together or sequentially depending on attacker goals. For an effective and sccceeded SQLIA, attacker should add a command with right syntax to the original SQL query. SQLIAs [6, 10] classified to:

A. **Tautology.**

B. **Illegal/Logically Incorrect Queries.**

C. **End of Line Comment.**

D. **Timing Attack.**

E. **Union Queries.**

F. **Blind SQL Injection Attacks.**

G. **Piggy-Backed Queries.**

For clarifying these types of SQLIAs I will use an example of a web form that contains two input fields Username & Password and a login button as shown in Fig. 2. In this example we use below URL HTTP://www.anydomain.com?page=login to request login page. We use Username “Ahmad” and Password “P@ssw0rd”, after Ahmad click on Login button, at backend web form code that connects to database to verify that Ahmad account is available and correct. If SQL query return “True’ Ahmad will be redirected to his account main page, if “False” a message will appear from him telling him a wrong username or password. For a more reading of code read it from [10]. Now we will discuss the seven types “methods” of SQLIAs and show how an attacker access Ahmad account main page without knowing the correct full Account information, in our example, the username and password of “Ahmad” account.

#### A. Tautology

This SQLIA attack injects to SQL query so query evaluated to “True” always.

Injected Query:

```
SELECT User_Name, User_FullName FROM TABLE_USERS WHERE User_Name='Ahmad' AND User_Password='12345';
```

#### B. Illegal/Logically Incorrect Queries

This type of SQLIA collect database information from making page return error messages from backend code. Attacker inject junk input to URL or input fields or SQL query tokens to produce syntax or logical errors. In our example attacker inject to URL variables a single quote.

**HTTP://www.anydomain.com?page=login**

Injected Query:

```
SELECT PAGE_LOC FROM TBL_PAGES WHERE Page_ID=’login’
```

This injection will fire a syntax error when generating dynamic query that return location of login page form database and the error will show: Error: Invalid Query “SELECT PAGE_LOC FROM TBL_PAGES WHERE Page_ID=’login’”

#### C. End of Line Comment

In this type of SQLIA attacker use SQL comment operator “--” to ignore part from SQL query search.

In our example attacker insert for Username input field “Ahmad’--” and Password “12345”

Injected Query:

```
SELECT User_Name, User_FullName FROM TABLE_USERS WHERE User_Name=’Ahmad’-- AND User_Password=’12345’;
```

#### D. Timing Attack

An inference attack. In this type attacker make timing between web page responses. This technique used “IF-Then” conditional statement for queries injection and “WAITFOR” to make database delay query response by a specific time.

---

**Fig. 2. Login Page**
E. Union Queries
This type attacker appends a new query to original one using SQL UNION keyword, so he can access to unauthorized data. In our example attacker can inject a union query to URL: HTTP://www.anydomian.com?page=login’ union all select UserName from TBL_USERS’. Injected Query:
SELECT PAGE_LOC FROM TBL_PAGES WHERE Page_ID='login' UNION ALL SELECT USERNAME FROM TBL_USERS
This injected query will return all user names stored in table TBL_USERS which is not authorized to page navigator to access to this information.

F. Blind SQL Injection Attacks
An inference attack, as we talked one of best code practices to hide error messages from shown to client. So in this case attacker does not have any error messages since developer make error to a generic web page error. It difficult for attacker now to make SQLIA but it does not impossible. Attacker can request True/False requests from SQL queries and he could success and steal information.

G. Piggy-Backed Queries
In this SQLIA type, attacker use SQL statements delimiter “;”. Attacker append additional statement so he can execute more that query. In our example attacker could add another query to URL: HTTP://www.anydomian.com?page=login’;DROPTABLE TABLE_USERS’
Injected Query:
SELECT PAGE_LOC FROM TBL_PAGES WHERE Page_ID='login' UNION ALL SELECT TABLE_USERS’
So here in this case first SQL query is legal, but the second is illegal and will fire database to drop table TABLE_USERS.

4 SQL INJECTION ATTACK DETECTION
There are many techniques used for SQLIA detection [2, 7], we will present them:

A. SQLUnitGen
Abbreviation for “SQL Injection Testing Using Static and Dynamic Analysis. This technique proposed by Shin and fellow workers. It uses static analysis to track flow of user inputs for testing attacks. Most tools and techniques utilize “JCrasher” which is a tool used to obtain test cases upon generated attack inputs.

B. MUSIC
Abbreviation for “Mutation-based SQL Injection vulnerabilities checking”. This technique proposed by Zulkemine. He used mutation method based on error checking and catching by injecting syntax errors to check if any mishapen occurred. Then by comparing output it can conclude if a query contains mishapen and vulnerabilities.

C. SUSHI
It is an abbreviation which stands for “string constraint solver”. It proposed by Fu and Li. It is a recursive algorithm that found it very help in finding complex SQLIAs. It Solves SLSE (Simple Linear String Equation) constraint in an effective approach.

D. Ardilla
A technique and a tool for creating SQLIA. It proposed by Kiezu and fellow workers. This tool generates attacks as inputs and run the application for each attack input. So it can check and detect the SQLIA from generated attack inputs.

E. String Analyzer
Wassermann and Su proposed this technique. Their solution depends on a based grammar algorithm, it strategizes string values as context free grammar (CFGs) and operations based on transducers of language following minimization. This technique then labels user input strings and summarize them and find contexts. Then by regular languages and context free languages usage, it checks the security of each labeled string in aspect of syntax.

F. PHP Miner
It is a solution rather than a tool, it proposed by Khin Shar and Kuan Tan. This solution statically looks for attributes in source code, then produces models and flowcharts of vulnerabilities prediction.

G. Vulnerability and Attack Injection
A method proposed by Fonseca and fellow workers, the solution upon attack application by pragmatic SQL injection vulnerabilities. For getting more pragmatic results the solution used predefined collected data from actual attacks. The technique composed of two parts that work together, a tool for injection attack and another for injection of vulnerability.

5 RELATED WORK
Deevi Radha Rani, B.Siva Kumar, L.Taraka Rama Rao, V.T.Sai Jagadish, M.Pradeep [3]. They proposed a technique that handles all SQLIAs types. The technique upon encryption of user information and using of stored procedures. They apply that on users’ authentication information (Username, Password). They encrypt user data with AES algorithm using 40-bit secret key. On user registration, his info encrypted and stored as a chipper text in database. On user authentication, on back end code at login form called stored procedure with parameters “Username, Password, Secret Key”. Stored procedure encrypt Username & Password using secret key, after that it compares the generated encrypted username and password with encrypted username & password saved at users table. This technique is not suitable for dynamic queries from various tables since encryption of big data will consume time and size. But it is very valuable for injection attacks on user authentication.

and data contents of SQL queries implemented in web application forms, which will be stored in parallel. She generates a formula which it is a combination of DDL & DML Mapping along with Vectorization of SQL Queries. The Vectorization of SQL queries stored in a new created tables in mirror database, for including different syntax. She resolves the parse tree of different generated queries. She monitors the detection of anomalies among the queries within production database from the result of the output of the different generated queries. For SQLIA detection she used two methods. Static method which is known as pre-generating approach. In static method developers follow some guidelines and validation checking. The second method is Dynamic approach which is known as post-generated approach, a technique used in run time. It analysis dynamic or runtime generated SQL query from web form after user inputs or web form request.

Inyong Lee a, Soonki Jeong b, Sangsoo Yeoc, Jongsub Moond [12]. They proposed a simple, easy and effective technique for detecting SQLIAs based on static and dynamic analysis and by taking of attribute values at runtime (Dynamic Analysis) and compare it with original one in which also removed attribute values (Static Analysis). The technique used for numeric attributes and string attributes. They create an algorithm for attribute values removal from query. Also they create a generalized SQLIA detection algorithm to check if the query at web forms is normal or abnormal in advance.

Debabrata Kar, Suvasini Panigrahi [13] proposed a technique for SQLIA detection using query transformation and hashing. Their technique to transform the original query parameter values “where condition parameter” with question mark symbol “?” and SQL keyword to uppercase keywords, system objects like table names and column names with keywords they proposed. So with this transformation they reduce number of different queries structure, also this will reflect on performance of search. They used hashing function for generating unique hash key, so the search will be efficient during runtime. The advantages of using hashing is the size of hash key will be smaller than the transformed query, so size needed in storage reduced. Also the same hash will be primary index, as they are unique, to facilitate fast and efficient searching at runtime.

R. Latha, Dr.E. Ramaraj [14] proposed a technique for detection of SQLIA by replacement query search condition attributes string of original query used in web form with symbols they proposing like “PQ, GQ, STR, NUM, etc.”. At runtime they are making a replacement of query search condition attributes for both the original query and dynamic generated query from web form after user inputs. So they have now a two generated restructured queries. They compare the two restructured queries for SQLIA detection by measuring the distance between the two restructured queries using levenshtein method. This technique satisfies both static and dynamic analysis.

Swapanil Kharchel1, Jagdish patil, Kanchan Gohad, Bharti Ambekar [15]. They proposed an efficient technique and algorithm for detection and prevention of SQLIAs using Aho–Corasick pattern matching algorithm. Their proposed technique has two phases, static phase and dynamic phase. In static phase they create a list of known anomaly pattern, and SQL queries that checked by enforcing static pattern matching algorithm by comparing of known anomaly pattern list created. During runtime and using dynamic phase if new anomaly is occurring, then new anomaly will be generated and added to static anomaly pattern list. On new anomaly generation score calculated for the query, if the score greater than a determined threshold then the query passed to an administrator to analyses the query manually, if the query infected a new anomaly generated and added to static anomaly list.

6 PROPOSED SOLUTION

We propose an effective solution for SQL Injection detection and prevention without any impact on application functions and performance. This solution based on a Query Dictionary Mechanism. Our solution general view focus on:

A. SQL query statements numbers.
B. SQL query has UNION
C. SQL Query where suffix pattern.

To save this information about each query, many approaches can be used. It could be generating a memory allocation at application start, so this information can be collected for all queries exists on the application start one time, or it could be collected on first query calling and appended to memory allocation. For memory allocation we propose to create application variable that contains a list of objects to save query information on, the allocation created below using C# language and ASP. NET web application.

```csharp
class SQLIA_DP
{
    public int Id { get; set; }
    public string Query_Caption { get; set; }
    public byte Query_Statemnts_Count { get; set; }
    public string Query_Caption { get; set; }
    public int Id { get; set; }
    public string Query_Caption { get; set; }

    List<SQLIA_DP> ls = new List<SQLIA_DP>;
}
```

At Global class, in Application_Start method we create an application variable that holds the ls instance of query information, the statement for creating is:

```csharp
Application["SQLIA_DET_PREV"] = ls;
```

Another approach to save query information is in a JSON file or in NoSQL Database for example MongoDB, the format as following:

```json
["Id":1,
 "Query_Caption":"loginfrm",
 "Query_Statements_Count":1,
 "Query_Has_Union":"FALSE",
 "Query_Pattern":
 "WHEREUser_Name=ANDUser_Password=
"
]
```

Another approach to save query information on any relational database table, it could be on same application database or in a different database, table structure will be:
CREATE TABLE [dbo].[TBL_SQLIA_DET_PREV](
    [Id] [BIGINT] IDENTITY(1,1) PRIMARY KEY,
    [Query_Caption] [VARCHAR](15) NOT NULL,
    [Query_Statements_Count] [TINYINT] NOT NULL,
    [Query_Has_Union] [BIT] NOT NULL,
    [Query_Pattern] [VARCHAR](1000) NOT NULL );

Another approach to save query information on XML file as shown in Fig. 3.

For Query Pattern extraction, it could be generated and inserted manually by developers or database designers, or developers can use below proposed algorithm that automatically extract query pattern and insert it to SQLIA_DET_PREV list, or developers could use this algorithm at runtime. The algorithm for Query Pattern extraction as following and as shown on Fig. 4:

STEP 1: Take Dynamic generated SQL Query without values from source code.

STEP 2: Check if UNION key word exists and

STEP 3: Count semicolon times which represents number of SQL statements in Query.

STEP 4: Split SQL Query by “WHERE” key word.

STEP 5: If Splitted SQL Query Output Array has more than one item then next steps for second items in Array, if it has one item then next steps for First Item (One Item means Query does not have where statement)

STEP 6: Remove single quote and values between from chosen array item.

STEP 7: Remove each value after SQL Equal Operator “=" and before first Space.

STEP 8: Remove all Spaces.

STEP 9: Save Needed information on SQLIA_DET_PREV list, if Semicolon times is zero then save it one.

So our example query “SELECT User_Name, User_FullName FROM TABLE_USERS WHERE User_Name='Ahmad' AND User_Password='12345'” does not has UNION, zero semicolon, after splitting and execute steps from 5 to 9, Query Pattern will be “WHERE User_Name=ANDUser_Password=" values saved as shown in Fig. 3, since semicolon times is zero, this mean the query consist of one statement. For “Query_Caption”, this field can be used for query retrieve to increase search performance, so developer can use it the same for example “loginfrm” for queries in login form as shown in Fig. 3 so I linked it with web form class which can extracted dynamically.

Above extraction algorithm could be used static or dynamic, depends on application and developer needs. On application run and after user enter the inputs send his request and we assume here user is an attacker and he injected SQL query. Query after its dynamic generation and before sending to database engine for execution should send to SQLIA_CHECK algorithm which described as following:

STEP 1: Use Query Pattern Extraction Algorithm above to extract new dynamic generated query with parameter values.

STEP 2: Create SQLIA_DP object (SQLIA_DP_CURRENT).

STEP 3: Get Query Pattern object saved at SQLIA_DET_PREV List, if not available it should be generating using Query Pattern Extraction Algorithm and save it to (SQLIA_DP_ORIGIN).

STEP 4: Compare Query_Statements_Count on SQLIA_DP_CURRENT and SQLIA_DP_ORIGIN, if result is equal GO TO STEP 4, if not Return 1 and Exit.

STEP 5: Compare Query_Has_Union on SQLIA_DP_CURRENT and SQLIA_DP_ORIGIN, if equal GO TO STEP 5, if not Return 1 and Exit.

STEP 6: Compare Query_Pattern on SQLIA_DP_CURRENT and SQLIA_DP_ORIGIN, if equal Return 0 and Exit, if not Return 1 and Exit.

Above Algorithm return value 1 means there is an SQLIA, so query execution should be canceled. If return value 0 then query is clean and it should be send to database engine for execution.

In our example if attacker inject a query “SELECT User_Name, User_FullName FROM TABLE_USERS WHERE User_Name='Ahmad' AND User_Password='" or '1'='1';”

The generated query will be send to SQLIA_CHECK ALGORITHM, the result explanation will be as following:

STEP 1: Query Pattern will be “WHEREUser_Name=ANDUser_Password=or=" and no UNION key word and 1 statement, this info saved to (SQLIA_DP_CURRENT) object.

STEP 3: Get Saved Query Pattern from List, this will return 1 statement, no UNION, “WHEREUser_Name=ANDUser_Password=" and saved to (SQLIA_DP_ORIGIN) object.

STEP 4: Compare result is equal Go to Step 5

STEP 5: Compare result is equal Go to Step 6

STEP 6: Compare Query Pattern is not Equal, Algorithm return 1 so there is an SQLA and Query does not forward to database engine.

7 CONCLUSION

In this paper we have presented an effective SQL Injection Attack detection and prevention without any impact in application functions and performance. Our proposed solution used static and dynamic approaches. Easy to implement by developers and database designers or developers. Our solution detects all types of SQLIAs. Upon application needs or and developer experience or and application sensitive degree it could be implemented for part of queries or for all queries, it could be implemented static or dynamic. Query information extracted could be stored in encrypted manner to make the solution more secure. As a future work we could implement our solu-
tion and calculate performance issues and compare it with other solutions.

**Fig. 4 Query Pattern Extraction Algorithm**

**REFERENCES**


Adwan Yasin is an associate Professor, Former dean of Faculty of Engineering and Information Technology of the Arab American University of Jenin, Palestine. Previously he worked at Philadelphia and Zarka Private University, Jordan. He received his PhD degree from the National Technical University of Ukraine in 1996. His research interests include Computer Networks, Computer Architecture, Cryptography and Networks Security.

Nae'l A. Zidan received the B.S. in Computer Information Technology in 2005 from Arab American University Jenin (AAUJ), Palestine. He is a Master candidate of Computer Science at AAUJ, Palestine. He has 10+ years’ experience of programming and development, networking, data-bases, and virtualization. His research interests include Computer Networks and Information Security.
An optimized approach toward intrusion detection using cluster-like behavior of attacks

Aliakbar Tajari Siahmarzkooh
Faculty of Mathematical Sciences
Department of Computer Science
Iran, Tabriz, University of Tabriz

Jaber. Karimpour
Faculty of Mathematical Sciences
Department of Computer Science
Iran, Tabriz, University of Tabriz

Shahriar Lotfi
Faculty of Mathematical Sciences
Department of Computer Science
Iran, Tabriz, University of Tabriz

Abstract— Most of intrusion detection researches suffer from the following drawbacks: Dependencies between network nodes and cluster-like behavior of anomalies. Hence, this paper proposes a cluster-based approach in which the anomalies are detected using a new criterion related to the behavior of attacks. In addition, we provide a cluster-based data set which uses the flow-based data and graph properties to model the network traffic over time. The data set is built over the DARPA. Moreover, the anomalies are revealed by means of a criterion which is computed from internal and external weight of clusters. Finally, the proposed approach is evaluated and compared to other approaches. The evaluation results show the preference of our approach relative to other ones.

Keywords- Anomaly; DARPA data set; flow; graph clustering; intrusion detection

I. INTRODUCTION

In more specific, one of the approaches for solving the scalability problem in packet-based IDSs is packet header extraction approach. Mahoney et al. [4] proposed an approach by means of the packet header extracting such that the anomaly is detected using the normal values learning for each packet header. In addition, Manandhar et al. [5] proposed an approach that used the traffic data. They checked the information of packet header for anomaly detection. Also, Karimpour et al. [6] proposed a flow-based clustering algorithm to detect attacks in DARPA data set. They used some proper time intervals and threshold points to reveal the attacks in high accuracy.

As comparing of these two methods, the flow-based IDS is more suitable than packet-based one in high speed networks. Moreover, in these approaches, flow data are analyzed instead of the contents of packets. In 2010, Sperotto et al. [7] devised an approach based on the flows in the network and used the time series to reveal the attacks. In this study, the performance of flow-based IDS in comparison with the packet-based one in the network is proved and a data set is proposed to evaluate the flow-based IDSs.

Further, Hellemons et al. [8] proposed another method that is based on the flow concept in 2012. This research includes two parts. In first part, a high performance algorithm is designed for intrusion detection. In second part, a prototype of the IDS has been implemented. In fact, the authors proposed an algorithm to detect dictionary attack. The algorithm splits the attacks into 2 or more phases. The criteria that are used in the algorithm are packet per flow criterion and minimum number of flows which are calculated in 1 minute time intervals. Based on this algorithm, threshold points are considered in each phase of the attack. They assumed that the dictionary attack has 3 phases: scan, brute-force and die-off phase. They detected the attack in high accuracy mode by applying threshold points to those three phases.

Also, Graph-based intrusion detection systems are the type of security approaches using the properties of the network, not the content of packets. These systems detect the intrusion by analyzing the network graphs that can detect the high scalability attacks such as the worms. In this study, Zhou et al. [9] proposed an approach to use the graph concept for implementing the multi variable time series and their relation in each time, Iliofotou et al. [10] in 2007 proposed an approach to monitor and analyze the network traffic using traffic dispersion graph (TDG). They defined the traffic dispersion graph as the graphic presentation of interactions among the groups of nodes. The advantage of using the traffic dispersion graph is its power to presenting the structural relations of the attacks. Another approach is proposed by Le et al. [11] in 2011 based on the graph theory fundamentals such as degree of nodes, maximum degree of graph and similarity distance of graph.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500
One of the important fields in the graph-based intrusion detection is graph clustering method. In this field, Muniyandi et al. [12] used decision tree to optimize k-means algorithm for intrusion detection systems. Mingjiang et al. [13] in 2012 and Yin et al. [14] in 2014 also used the graph clustering to detect the attacks. Mingjiang et al. assumed three sets for normal, pending and anomaly clusters and placed the data in N clusters and the clusters are placed in 3 types of defined clusters based on the rate of the normal and anomaly data that are already specified. The existing clusters in the set of pending clusters are placed in one of the normal or anomaly groups using local deviation coefficient. Yin et al. has optimized this approach and used local deviation coefficient instead of the local deviation coefficient.

These approaches consider the dependencies between nodes, but they don't consider the cluster-based behavior of attacks in the network traffic graph and don't define an appropriate criterion to detect the attacks. This paper proposed a new criterion based on the graph clustering and considered the cluster-like behavior of attacks. The best results of detecting attacks are concluded by applying the appropriate time intervals and threshold points to the proposed cluster criterion in time series.

II. PROPOSED APPROACH

This paper proposes an approach to increase the detection rate, decrease the false alarms rate and eliminate the restrictions in detection of all types of attacks. Hence, an anomaly-based intrusion detection approach along with the flow and graph concepts are utilized. To prepare the data for the proposed method, it is necessary to perform some preprocessing on the initial traffic which is described in the next subsections. Then, our proposed approach is explained in details. Finally, the approach and its strength and weak points are discussed.

A. Preliminaries

In the preliminary stage, the flows are extracted from the packet-based traffic. Then, these flows are clustered using the graph clustering algorithm in several time series that is based on genetic algorithm. These steps are described in sections 2.1.1 and 2.1.2.

A.1. Flow simulation

In this step, the packets with common properties are placed in the same flow and also the number of packets for each of the created flow is calculated. Now, we have some flows with 1 second time intervals such that we can use them in different time series. A 7-tuple is used to indicate the simulated flow [15]:

(IP-Src, IP-Dst, Pcks, Time, Port-Src, Port-Dst, Prot)

The items of the 7-tuple represent source and destination IP addresses, number of packets related to the flow, the sending time of the flow in the network, source and destination port numbers and protocol type, respectively.

A.2. Graph clustering of the flows

A genetic-based graph clustering algorithm [16] is used in the suggested approach in which the flows are considered as the inputs (graph edges) to the algorithm. The following steps are included in this step:

1. In first step, an initial population is created. The encoding phase of the algorithm is based on random numbers generation such that the length of a chromosome is equal to the number of graph nodes that are encoded by the random numbers from 1 to the number of nodes which indicate the cluster's number.

2. In second step, the fitness function is computed that it consists of 2 parts:

2.a. Internal communication in the clusters: The internal communications in each cluster is obtained as follows:

\[ A_i = \frac{\mu_i}{N_i} \]

In the equation 1, \( \mu_i \) and \( N_i \) represent the normalized weight of edges and the number of nodes in i-th cluster, respectively. So \( 2N_i \) represents the total number of edges with maximum weight in i-th cluster.

2.b. External communication in the cluster: The external communications between the clusters are calculated using the equation 2:

\[ E_{ij} = \begin{cases} 0 & \text{if } i = j \\ \frac{s_{ij}}{2N_iN_j} & \text{if } i \neq j \end{cases} \]

The equation 2 represents the number of communications between i-th and j-th cluster. In this equation, \( s_{ij} \) represents the normalized weight of edges between i-th and j-th cluster and \( N_iN_j \) expresses the maximum weight of edges between 2 clusters.

Therefore, the fitness function is obtained from equation 3:

\[ M_i = \frac{\sum_{k=1}^{N_i} A_k}{\sum_{k=1}^{N_i} E_{ik}} \quad \forall k > 1 \]

3. Selection phase of genetic algorithm is performed using the selection function and roulette wheel.

4. 2-point crossover and swap mutation are performed.

5. New population and new generation are produced using the replacement operation.

After graph clustering, some properties such as sending time, number of clusters and nodes, number of internal and external packets, number of internal and external flows are calculated in the time series to create a new criterion. Thus, the cluster-based data set [17, 18] with mentioned properties are obtained. As an example, some time series of created data is presented in Fig. 1 that is related to DARPA data set and the network traffic in 4th week, Tuesday [18].
B. Proposed criterion

The appropriate criterion will be described using the explained concepts and the properties that are related to the graph clustering data set. Thus, the best criterion is needed to achieve a system with high accuracy, high true alarms rate and low false alarms rate.

In more specific, the number of internal flows is defined to represent the number of connections among the IPs (nodes). To achieve an appropriate internal criterion in the time series, and according to the behavior of some attacks such as IP scan, it is expected that the average weight of internal flows represents an increasing value. We define this criterion in equation 4.

\[
C_i = \frac{\sum_{t=0}^{T} IntPckt_i}{\sum_{t=0}^{T} Intflow_i} \tag{4}
\]

In this equation, IntPckt\(_i\) and Intflow\(_i\) represent the number of internal packets and internal flows in i-th time bin, respectively.

In addition, the cluster with minimum number of external communications shows the nodes that are connected to less number of other clusters. In this situation, the nodes of mentioned cluster will be considered as an attacker and the other nodes that are connected to these nodes will be assumed as victims. To achieve this criterion, the following step is performed in the time series: the number of external flows of each cluster is calculated and the cluster which has the minimum number of external weight is selected. We represent this as E\(_i\) in each time interval (equation 5). In this equation, ExtPckt\(_i\), Extflow\(_i\) and Nodes represent the number of external packets, external flows and nodes in i-th time interval, respectively.

\[
E_i = \frac{\sum_{t=0}^{T} ExtPckt_i}{\sum_{t=0}^{T} Extflow_i \cdot \text{Nodes}} \tag{5}
\]

By analyzing the behavior of some other attacks such as DoS [19], it is expected that in these types of attacks, there exist external flows among the most of clusters and the sum of external weights of other clusters are more than the most value.

The final criterion is achieved by dividing the C\(_i\) into E\(_i\). According to the mentioned cases, if the value of this criterion is rather than a threshold point, an anomaly has been occurred. This criterion is calculated based on the equation 6:

\[
C_{\text{final}} = \frac{C_i}{E_i} \tag{6}
\]

III. THRESHOLD POINTS AND TIME INTERVALS

In this paper, a static way is used to identify the best threshold point based on comparison between the normal and anomaly points. Therefore, 4th week data of DARPA is analyzed for some time intervals and threshold points.

To access the highest detection rate and also, minimum false alarms rate, the data is tested in several time intervals and threshold points. Four time bins are considered: 45, 60, 75 and 90 seconds. For these 4 time intervals, a threshold point is identified for the introduced criterion. Also, the evaluation rates of intrusion detection methods are calculated.

In 45 seconds time interval, at first, the traffic is split to the equal time intervals (45 seconds) and the time series are created in 45 seconds time bins (t\(_1\), t\(_2\), …, t\(_n\)) such that t\(_i\) indicates the first 45 seconds, the second 45 seconds and the n-th 45 seconds. Then, each of these intervals is tested in the final model.

Tables 1-4 represent the results of the time windows such that four appropriate threshold points are obtained for intended criterion and the evaluation rates are identified due to it. The observations represent that the threshold points at 55, 50, 75 and 75 have the maximum detection rate in the time intervals, respectively.

After applying the final model on four different time windows, the evaluation rates are obtained according to the appropriate threshold points and the best threshold points are selected for each of time windows. Then, to investigate that which of the time bins have the maximum detection rate and minimum false alarm rate, the results of selected threshold points are compared. As we see in table 5, 75 seconds time interval has the best results in comparison with the other ones. Also, other time windows have high detection rates, however, 75 seconds has the highest accuracy relative to others. Therefore, if the results checked based on the detection rate, it is clear that the detection rate decreases with the increase in the time window, but if the results checked based on the false alarm rate and the detection rate, it is not concluded that the smaller time window always obtains the best result.

<table>
<thead>
<tr>
<th>TABLE I. EVALUATION RATE IN 45 SECONDS TIME WINDOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold point</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>&gt; 35</td>
</tr>
<tr>
<td>&gt; 45</td>
</tr>
<tr>
<td>&gt; 55</td>
</tr>
<tr>
<td>&gt; 65</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II. EVALUATION RATE IN 60 SECONDS TIME WINDOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold point</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>&gt; 30</td>
</tr>
<tr>
<td>&gt; 50</td>
</tr>
<tr>
<td>&gt; 70</td>
</tr>
<tr>
<td>&gt; 90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE III. EVALUATION RATE IN 75 SECONDS TIME WINDOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold point</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>&gt; 45</td>
</tr>
<tr>
<td>&gt; 60</td>
</tr>
<tr>
<td>&gt; 75</td>
</tr>
<tr>
<td>&gt; 90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE IV. EVALUATION RATE IN 90 SECONDS TIME WINDOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold point</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>&gt; 45</td>
</tr>
<tr>
<td>&gt; 60</td>
</tr>
<tr>
<td>&gt; 75</td>
</tr>
</tbody>
</table>
According to the explained cases, we select 75 seconds time interval and use it to evaluate and compare the proposed approach to other methods.

In table 6, the detection rates for each attack are shown; the maximum detection rates are related to the scan and the DoS attacks.

The results of the best case for the proposed approach in comparison of the packet-based methods are shown in table 7 based on the appropriate time window and threshold point. The results of the table show the performance of using the flow concept in our procedure such that in the detection rate of packet-based method is less than the flow-based one.

In this part, the results of the methods before and after the clustering are compared. Hence, the detection rate, true positive and false positive rate are calculated before and after the clustering using the time window and appropriate threshold point. The best threshold point is 75 before the clustering and is 60 after the clustering. The results of this comparison are shown in table 8.

The results show the performance of clustering approaches. According to the fixed false detection rate, the cluster-based detection rate has 25% increasing value that is significant and the detection rate increases 15% that is related to using the clustering approach in our methods.

In this section, the results of proposed approach are compared with the other new methods on DARPA data set [18]. Also, false positive rate (false alarm), true positive (detection), detection rate are used for capability in detecting the types of attacks. The rate of capability to detect the types of attacks represents that the proposed approach is offered to detect which one of the attacks.

Table 9 represents the comparison of the final results of our proposed method to the Manandhar’s approach which is used the packet header analyzing and just detect the TCP-based attacks. In the Manandhar’s approach, 2 results are obtained that one of them is based on the low false alarm rate and the other one is based on the high true detection rate.

The results of table 8 show the performance of our approach in the detection rate and the false positive rate. The detection accuracy of our proposed approach has 20% increasing for the results with the high detection rate and 5% increasing for the results with the low false alarms. Also, in the proposed approach, the false positive rate has been decreased 5% to 10% in the comparison to the other methods and the other approach has been increased 1% to 5% in the positive phase. The other approach can detect 85% of attacks, while our approach can detect 95% of them and it can be the reason of decreasing in the true positive rate in our approach towards the Manandhar’s approach.

### IV. Conclusion

In this paper, a new cluster-based data set was provided. It was built over the DARPA data set. We also proposed a new flow-based approach to detect anomalies. It uses a new criterion which is computed from internal and external weights of clusters of the network graph. The comparison results show that high detection accuracy is achieved through the proposed approach. As future work, we aim to consider new cluster-based criteria to achieve higher detection rates.

### REFERENCES


AUTHORS PROFILE

Aliakbar. Tajari Siahmarzkooh received the B.Sc. in Software Engineering from the Ferdowsi University of Mashhad, Iran, the M.Sc. degree in Computer Science from the University of Tabriz, Iran. He is Ph.D student at the University of Tabriz. His research interests include network security, cryptography and intrusion detection systems.

Jaber. Karimpour received the B.Sc. Degree in Computer Science and Applied Mathematics from University of Tabriz (Iran) in 1998, the M.Sc. Degree specializing in the computer systems are of Applied Mathematics from University of Tabriz in 2000, and the Ph.D. degree in Computer Systems form University of Tabriz. He is currently an Assistant Professor in the Department of Computer Sciences at University of Tabriz and has been manager of Information Technology of the university since 2011. His current research interests include cryptography, network security, formal specification, and verification.

Shahriar. Lotfi received the B.Sc. in Software Engineering from the University of Isfahan, Iran, the M.Sc. degree in Software Engineering from the University of Isfahan, Iran, and the Ph.D. degree in Software Engineering from Iran University of Science and Technology in Iran. He is Assistant Professor of Computer Science at the University of Tabriz. His research interests include compilers, super- compilers, parallel processing, evolutionary computing and algorithms.
A Comparative Study of Smoothing a Vehicle’s Trajectory which is calculated by an Evolutionary Algorithm

Bayram Ali BURAN¹, Suleyman Hikmet CAGLAR² and O zgur Koray SAHINGOZ³

Abstract—Determining a vehicle’s trajectory is a complex and hard to solve type problem in the literature and it is identified as a NP-Hard optimization problem which is studied in different engineering disciplines such as computer, electrical and industrial engineering. It has been observed that such complex problems can be solved by using various approaches and lots of them are focused on the usage of Evolutionary Algorithms especially in case of a large number of controls points which are needed to be visited. Although these algorithms provide near optimal solutions, in the real world, vehicles are not able to follow this determined path (trajectory) without any deviation. Because vehicles are moving objects and each one moves with a certain speed. Therefore it is impossible for a vehicle to make a sharp turn after visiting control points. These vehicles need to make smoothed turns over these points. Therefore there will be a certain difference between the calculated path and the real path. It is needed to determine the real path by using necessary mathematical solutions for smoothing these paths. To ensure the motion continuity of vehicles, they need to follow paths determined according to a certain criterion. In this study, the most common smoothing methods which are used to ensure these continuities (Bezier, B-Spline and Dubins) have been compared and it is aimed to show the different approaches in an application area of path planning problems as a comparative study.

Keywords—Unmanned Aerial Vehicle, Path Planning Evolutionary Algorithm, Bezier Curves; B-Spline Curves, Dubins Path.

I. INTRODUCTION

Trajectory Planning Problem can be defined as a computation of a trajectory of a single vehicle (or a group of vehicles) to reach the desired goal state by avoiding obstacles and collisions. Trajectory planning can also be described with different meanings in the literature such as path planning, motion planning, trajectory optimization, etc. The vehicle in trajectory planning can be used either as a car/robot or in a more complex way it can be used as an Unmanned Aerial Vehicle (UAV).

Usage of various vehicle types results in different challenges in the optimization of trajectory due to their specific characteristics. For instance, a robot, a car or a quad-copter have

1 B.A. Buran is with the Department of Basic Sciences, Turkish Air Force Academy, Istanbul, Turkey, 34149 e-mail: bburan@hho.edu.tr.
2 S.H. Caglar is with the Department of Mathematics and Computer Science, Istanbul Kultur University, Istanbul, Turkey, 34149 e-mail: s.caglar@hho.edu.tr.
3 O.K. Sahingo z is with the Department of Computer Engineering, Turkish Air Force Academy, Istanbul, Turkey, 34149 e-mail: sahingo z@hho.edu.tr. Manuscript June 2016

the ability to return sharply from the corners and to stop and go backwards, however, a fixed-wing UAV has to fly with a minimum velocity not to fall to the ground.

In this study, it is aimed to implement a trajectory planning methodology for various autonomous vehicle types. However, it is especially focused on applications and scenarios for UAVs as depicted in Figure 1. The trajectory can be constructed with different evolutionary approaches [1], [2] which will be detailed in the next section. However, these produced routes have sharp returns, and this cannot be done with most of the vehicle types such as UAVs or fast cars. Therefore, for a realistic planning, there is a need to determine a smoothed path according to physical constraints of the vehicle. In this study, it is aimed to construct a smoothed path by using mostly used smoothing methods such as Bezier, B-Spline, and Dubins. We try to make a comparative study of these methods and lead the researchers on this topic.

Fig. 1. 3d Trajectory Planning for multiple UAVs

In the literature mainly two types of trajectory plannings are studied: as two dimensional and three dimensional. In trajectory planning, environmental conditions (mountains, buildings, trees, etc.) and properties of used vehicle are also our constraints which we might be encountered, and this increases the complexity of the problem also.

A path planning on which vehicles could pass over the pre-determined points on the basis of performing the tasks autonomously is required. The number of control points can change according to the planned task, and that number sometimes finds thousands. With an increasing the number of control points, the priority of visiting points is turning into an optimization problem in terms of time and total distance. In the literature review, we found that Evolutionary Algorithm is widely used and accepted method in many research studies to solve this problem [3], [4].
After the determination of priority of the visiting the control points, by combining the points there occurs a path that is out of mobility of the vehicle. By smoothing that path, the path seems more realistic as in the real world. The smoothing effect of the vehicle’s path is seen in the Figure 2. In our literature review about this issue, we found that smoothing methods were acquired by Bezier Curves, B-Spline Curves, and Dubins Path [5]–[11].

![Regular Path Planning vs Smoothed Path Planning](image)

**Fig. 2. Vehicle Paths**

The outline of the paper is organized as follows. Section 2 first presents some background knowledge about trajectory planning such as evolutionary algorithms and additional artificial intelligence search techniques. The smoothed algorithms of the path are described in Section 3 by giving the details of the Bezier Curve, B-spline Curves, and Dubins curves. Section 4 concludes the paper by presenting some discussions and future works.

II. Trajectory Planning Algorithms

Even though in Travelling Salesman Problem (TSP) type optimizations the primary part of path planning a kind of optimization problem it is a type of NP-Hard (Non-Polynomial Hard) problem which cannot be solved by traditional mathematical methods. In this type problems, there can be many number of the control point, which each vehicle need to visit them. However, if the number of control points increases, it cannot be solved with standard mathematical models. Therefore, in the literature, some additional approaches are used.

Some researchers tried to use Voronoi diagrams to determine the trajectory of the vehicle by getting into account the distance of each point. Mainly in this type problems, points are defined as the center of the threat area. Therefore the vehicle tries to go as far as from these points. However, this type of solution is not acceptable for controlling some specific point in the mission theatre [12].

Therefore, evolutionary algorithms and swarm based optimization algorithms are used for solving the problem. Genetic algorithms are used especially for simply producing some solution and try to improve their quality with creating new generations [13]. With the usage of a specific operator such as crossover and mutation, the solution can be improved in each iteration. However, this is not sufficient for reaching the global best solution. This algorithm produces a near-optimal solution in its domain.

Ant Colony optimization algorithm is preferred in some research, and in this approach inspired by the foraging behavior of real ant colonies. In this approach, each ant leaves a deposit pheromone on the ground (as an indirect communication) to mark the route for him and also for other ants of the colony [14]. This approach, and also the genetic algorithm, can be easily implemented in a parallel structure. Therefore, can be executed quickly. Also, some additional approaches like RRT and Bee Colony Optimization are preferred for solving the problem. These methods are not mathematical methods but heuristic methods. These methods are similar to iteration method which is used in mathematics.

III. Smoothing Strategies

Construction of a path can be solved by using some different type of algorithms. However in the real world, these predetermined paths cannot be followed by the vehicles due to their physical constraints such as velocity. Therefore, there is a need to smooth these calculated paths in a more feasible way. Robots and quad-copter type vehicles can follow their determined path because they can make sharp turns in their motion. However, in trajectory planning of UAVs or cars, velocity factor must be taken into consideration with additional physical factors such as turning angle, etc. In mathematics, there exist some smoothing strategies as Bezier, B-Spline, and Dubins. In the following section, these approaches are detailed.

A. Bezier Curves

Bezier Curves were developed by Pierre Bezier who is an engineer in order to design vehicle bodies. Using a specific number of points the curve segment can be approximated. These curves dont pass over the points except first point and last point. A Bezier Curve in N-th order is generated by N+1 control point. Bezier Curves are generated by the construction called convex combinations because they are contained in the convex hull composed of control points [5].

The Bezier Curve is mathematically formulated based on Bernstein Polynomials. According to this basis function of n-th order is shown in Equation 1 by using i parameter for control points [6].

$$B_{i,n}(t) = \binom{n}{i} t^i (1-t)^{n-i}$$

(1)

Curve, $P_i$ i-th control point and basis function related to $B_i(i, n)$, is algebraic formulated in Equation 2.

$$C(t) = \sum_{i=0}^{n} P_i B_{i,n}(t)$$

(2)

By using an adequate-order Bezier Curve, various figures can be produced. However, while the degree of the algorithm increases, the complexity also increases and the calculation process will take longer than expected. Because of the increasing complexity high degree curves are affected more due to the rounding errors. As a result of this, the relation between control points and curve decreases.

Because of these adverse effects, it is common to form complex pathing figures by multiple Bezier Curves. Especially, hybrid use of second and third order Bezier Curves, according to the number of the control points, is more common.
Formulations of the Bezier Curves are presented in the ongoing part; Linear Bezier Curve is shown in Equation-3, Quadratic Bezier Curve is shown in Equation-4 and Cubic Bezier Curve shown in Equation-5.

\[
B_{1,1}(t) = (1 - t) P_0 + t P_1 \quad (3)
\]

\[
B_{2,2}(t) = (1 - t)^2 P_0 + 2t (1 - t) P_1 + t^2 P_2 \quad (4)
\]

\[
B_{3,3}(t) = (1 - t)^3 P_0 + 3t (1 - t)^2 P_1 + 3t^2 (1 - t) P_2 + t^3 P_3 \quad (5)
\]

In the equation of Cubic Bezier Curve coefficients of \( P_i, i = 0, 1, 2, 3 \) are terms of binomial expansion of \( (1 - t + t)^3 \). This property is applicable for all Bezier Curves given by \( N+1 \) control points. \( N+1 \) control points \( P_i, i = 0, 1, N \), coefficients of these points are terms obtained from binomial expansion of \( ((1 - t) + t)^N \). This can be easily seen when analyzed Equation 2.

In Figure 3, there are the figures of a) Quadratic Bezier Curve and b) Cubic Bezier Curve samples in \( t \in [0, 1] \) interval and given with the tangent at \( t = 0, 5 \). See that given with curves lie within the convex hull generated by given control points.

![a) Quadratic Bezier Sample](image1)

![b) Cubic Bezier Sample](image2)

Fig. 3. Quadratic and Cubic Bezier Samples

When analyzed Figure 4 generated by combination of two figures in Figure 3, Figure 4 doesn’t comply with maneuverability constraint the vehicles. For the continuous curve, when we combine two curves, ending point of the first curve and starting point of the second curve must be same.

![Fig. 4. Combination of two Bezier Curve](image3)

But continuity is not sufficient for an effective path planning. Bezier Curve that is planned to have same tangent on the combination points, and they have \( C^1 \) continuity and more smooth combination. Because of the low probability of the getting curves with \( C^3 \) continuity spontaneously by inserting imaginary points the Bezier Curves with \( C^1 \) continuity are obtained as is seen in Figure 5.

![Fig. 5. Smooth Combination of two Bezier Curve](image4)

According to problem type, there can be a need for the addition and insertion of some points to the curves. When analyzing the Quadratic and Cubic Bezier Curves in Figure 4, the tangents which are at the end points are created by using control points which are the ending point of the previous curve. \( C^1 \) continuity (in other words continuity of the first derivatives) can be accomplished if and only if the tangents at the point of junction must be same straight line. This condition can be made by inserting an imaginary point after the starting point of the second curve.

The control points forming the first curve are:

\[ P_i; i = 0, 1, i \]

The control points forming the second curve are:

\[ P_j; j = i, i + 1, k \]

Let show the imaginary point that we want to insert the second curve with \( P_{i+k} \). Meanwhile because of inserting a new point, the order of the second curve will increase.

\[ P_{i-1}, P_i \] and \( P_{i+k} \) will be on the same straight line and as we know the priority of points, distance between
the imaginary points. The effect of inserting imaginary points is shown with Berlin 52 TSP sample in Figure 6. Mainly this is to work on minimizing the effects of imaginary point on curve length and trajectory by choosing k parameter positive but very small. The effect of inserting imaginary points is shown in Figure 6.a this path cannot be converted to a continuous curve by using a Quadratic Bezier Curve. Due to the new control points, it will be the same tangent in point of junction so C^1 continuity is provided. We get the Equation 6.

\[
P_i - P_{i-1} = k (P_{i*} - P_i) \quad \text{and} \quad P_{i*} = \frac{kP_i + P_{i-1}}{k} \quad (6)
\]

By using the Equation 6, for each curve segment, a imaginary point is inserted just after the merging point with previous curve. Due to the new control points, it will be the same tangent in point of junction so C^1 continuity is provided. We are going to work on minimizing the effects of imaginary point on curve length and trajectory by choosing k parameter positive but very small. The effect of inserting imaginary points is shown in Figure 6.a this path cannot be used by a vehicles such as UAV's. Therefore the planned path must be in a continuous format. As can be seen in Figure 6.b this path can be converted to a continuous curve by using some imaginary points.

B. B-Spline Curves

The first important studies on B-Splines basis functions were carried out about 70 years ago by Schoenberg after this fundamental algorithm was developed by Cox and de Boor. Many pioneer researchers in the field, Riesenfeld, Boehm, Schummer and more, proved that B-Splines were in the scope of CAGD-Computer Aided Geometric Design were available and attractive presentation method and they were feasible [7–9].

Also B-Spline Curves, like Bezier Curves, do not pass over all of the control points. They can be used in various orders. When Bezier Curves were generated by control points, like data points, it is necessary to make sure that derivatives are continuous. Also, if the place at a control point changes the curves will be affected in Bezier Curves by this change. B-Spline functions have basis functions which have partial effect in order to these disadvantages of Bezier Curves. These basis functions are zero out of their domain. Hence, the curve takes form according to a few control points that are close to it. The order of B-Spline Curves and number of the control points are unrelated [10].

Defined by k-order and n+1 control points \( P_0, P_1, ..., P_n \) B-Spline Curve \( C(u) = \sum_{i=0}^{n} N_{i,k}(u)P_i \) mathematical formula is shown in Equation 7.

\[
C(u) = \sum_{i=0}^{n} N_{i,k}(u)P_i \quad (7)
\]

Here \( u \) is defined at \( 0 \leq u \leq n-k+2 \). n-k+2 explains how many segments the curve has, as well.

A B-Spline Curve with k-order generated by k-1 degree polynomial segments with \( C^k \) continuity at break points. Through, \( t_0 \leq t_1, ..., \leq t_{n+k} \), a set of non-decreasing break points a knot vector determining parametrization of basis functions is defined. See the Equation 8 and 9.

\[
T = (t_0, t_1, ..., t_{n+k}) \quad (8)
\]

\[
0 \leq i \leq n + k \quad \text{and} \quad t_i \quad \text{knots are defined as in Equation 9;}
\]

\[
t_i = \begin{cases} 
0 & \text{if } i < k \\
 i - k + 1 & \text{if } k \leq i \leq n \\
n - k + 2 & \text{if } i > n
\end{cases} \quad (9)
\]

According to a given knot vector \( T \), for \( k = 1 \), \( N_{i,k}(u) \) is combined B-Spline basis functions are defined as in the Equation 10.

\[
N_{i,1}(u) = \begin{cases}
0 & \text{if } t_i \leq u \leq t_{i+1} \\
1 & \text{if not}
\end{cases} \quad (10)
\]

For \( k > 1 \) and \( i = 0, 1, 2, ..., n \) is defined as in the Equation 11.

\[
N_{i,k}(u) = \frac{u-t_i}{t_{i+k-1}-t_i}N_{i,k-1}(u) + \frac{t_{i+k}-u}{t_{i+k}-t_{i+1}}N_{i+1,k-1}(u) \quad (11)
\]

Let's accept \( \delta = 0 \) for Equation 11 not to be undefined.
Control points generating B-Spline Curves are called as Boor points. Basis function \( N_{i,k}(u) \) and its knot vector, \( T = (t_{0}, t_{1}, \ldots, t_{k-1}, t_{k}, t_{k+1}, \ldots, t_{n-1}, t_{n}, t_{n+1}, \ldots, t_{n+k}) \), were defined by \( n + k + 1 \) element in other words sum of number of control points, \( n+1 \) and order of curve \( k \), the Equation 5 and 8. Each knot interval \( t_i < u < t_{i+1} \) was grafted on a polynomial curve between two serial correlations \( C(t_i) \) and \( C(t_{i+1}) \). Normalizing the knot vector, to cover \([0,1]\) interval, increases numerical sensitivity of at changing points because of high density of number in this interval.

When generating \( C(u) \) B-Spline Curve for \( n+1 \) control points, and \( k = 3 \) by using given Boor Algorithm with Equation 6 and 7, we can deduct Equation 12.

\[
C(u) = \frac{1}{2} (u + 1 - u)^2 P_1 + \frac{1}{2} [(u - i + 1) (i - u)] P_{i+1} + \frac{1}{2} (u - i)^2 P_{i+2}
\]

\( 1 \leq i \leq n - k + 2 \) and \( i \leq u \leq 1 \) are accepted.

If we change of variable to \( u' = u - i \) in Equation 12, then the “\( 0 \leq u' \leq 1 \)” becomes a constraint for Equation 13 is obtained.

\[
C(u') = \frac{1}{2} [(1 - u')^2 P_1 + (-2u'2 + 2u'1) P_{i+1} + u'^2 P_{i+2}]
\]

Now all curve segments are obtained from the change of \( u \) in \([0,1]\) interval. Again change of variable to \( u \) instead of \( u' \) is done and when the Equation 13 is transform into matrix form, it can be deducted the Equation 14.

\[
C(u) = \frac{1}{2} \begin{bmatrix} u^2 & u & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 & 1 \\ -2 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} P_{i-1} \\ P_i \\ P_{i+1} \end{bmatrix}
\]

For \( i \in [1, n - 1] \), each curve segment is obtained by changing \( u \) variable in \([0,1]\) interval. Because of \( k=3 \) 2-nd degree equation is obtained and dimensions of matrices are seen to be related to number 3. Consequently, \( C(u) \) B-Spline Curve in relation with \( k \) parameter can be shown in Equation 15.

\[
C(u) = U_k M_k P_k
\]

So by choosing \( k=4 \) the Formula of Cubic B-Spline Curves can be represented as in Equation 16.

\[
C(u) = \begin{bmatrix} u^3 & u^2 & u \end{bmatrix} \begin{bmatrix} -1 & 3 & -3 & 1 \\ 3 & 6 & 3 & 0 \\ -3 & 0 & 3 & 0 \\ 1 & 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} P_{i-1} \\ P_i \\ P_{i+1} \\ P_{i+2} \end{bmatrix}
\]

Although smoothness of the path created by B-spline Curves is one of the advantage of the algorithm. However the distance between the curve and the internal points is seen a main disadvantage. In this study, it is aimed to minimize the distance between the curve and internal points with some specific constraints.

**C. Dubins Path**

The shortest path between two points under curvature constraint in the plane is expressed as the Dubins Path. This method was developed by Lester Eli Dubins in 1957 by using Analytic and Differential Geometry method. By using Pontryagin’s maximum principle the researchers proved that this method meant the shortest path. This method is a special type of Euler-Lagrange equation. The shortest path in this method is generated by adding maximum curvature and straight lines to circular arcs. Using the Dubins Path in Nonholonomic vehicles, wheeled robots, air crafts, underwater vehicles is common. To calculate the length of parametric curves Equation 17 integral is used. [11]

\[
\int_a^b \sqrt{\left(\frac{dy}{d\theta}\right)^2 + \left(\frac{dx}{d\theta}\right)^2} d\theta
\]

There are minimum turning radius \( \rho \), rotation \( \theta \) and initial point \((x_s, y_s) \in R^2\) by coordinate in plane, equation of tracing is shown in Equation 18.

\[
\begin{align*}
\dot{x} &= v_0 \cos \theta \\
\dot{y} &= v_0 \sin \theta \\
\dot{\theta} &= \frac{2\pi}{\rho} u, \quad u \in [0,1]
\end{align*}
\]

Where \( v_0 \) is constant velocity and \( u \) is normalization parameter. [15]. The shortest path that corresponds to maximum curvature particularly for an air plane, can be either CLC or CCC (C:Circle, L:Line) paths or a subset of these. C refer to circular arc and L refers to straight line which is tangent to C. See Figure 6.

![Fig. 7. CLC and CCC Types of Dubins Path](https://sites.google.com/site/ijcsis/)

A Dubins Path requires the use of the following parameters as depicted in (Figure 7)

- **Initial Point** : \( P_i (x_s, y_s, \theta_s) \)
- **Final Point** : \( P_f (x_f, y_f, \theta_f) \)
- **Initial Curve** :
- **Final Curve** :

Consequently, it will be enough to enter the coordinates of initial and final points of Dubins Path.

Dubins Path finds fastest and shortest path, but the method also has disadvantages like the direction of the path, which is forward, and the increase of sub problems related the number of vehicles. The method mentioned here are open for improvement. In literature reviews, there is no research show in which method is the most advantages with constraints, though.
Consequently, it will be enough to enter the coordinates of initial and final points of Dublin’s Path. Dubins Path finds fastest and shortest path, but the method also has disadvantages like the direction of the path, which is forward, and the increase of subproblems related the number of vehicles. The method mentioned here are open for improvement. In literature reviews, there is no research show in which method is the most advantages with constraints, though.

IV. DISCUSSION AND CONCLUSION
In this paper, it is aimed to plan a path of a vehicle, such as a UAV, by using some evolutionary algorithms. However, after executing these algorithms, the produced path cannot be traceable by the vehicles. Therefore, it is needed to smooth the produced by using some mathematical approaches. In this paper four different methods were investigated and the comparison of them are presented in Table 1 to give a prior opinion for the researchers.

TABLE I. COMPARISON OF STUDIED METHODS

<table>
<thead>
<tr>
<th>Methods</th>
<th>C^0 Continuity</th>
<th>C^1 Continuity</th>
<th>Degree</th>
<th>Density of Points and Curve</th>
<th>Function Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bezier C.</td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
<td>Distail</td>
<td>Polynomial</td>
</tr>
<tr>
<td>Hybrid Bezier C.</td>
<td>Yes</td>
<td>No</td>
<td>Low</td>
<td>Close</td>
<td>Polynomial</td>
</tr>
<tr>
<td>B-Spline C.</td>
<td>Yes</td>
<td>Yes</td>
<td>Low</td>
<td>Close</td>
<td>Polynomial</td>
</tr>
<tr>
<td>Dubins Path</td>
<td>Yes</td>
<td>Yes</td>
<td>Intermediate</td>
<td>Close</td>
<td>Trigonometric</td>
</tr>
</tbody>
</table>

As can be seen from this table, researchers must be careful about their aims in selecting the smoothing algorithm. The depicted table shows the advantages and disadvantages of them. For realistic path planning, especially with autonomous vehicles with high speed, like Unmanned Aerial Vehicles (UAVs), these detailed curves with their mathematical background must be used. In this paper, three types of curve models were examined, and their advantages and disadvantages were shown. Also, necessary mathematical formulas were presented as a source for researchers studying on this subject.

For further studies, it is aimed to implement all these methods in a real world scenario such as UAV path planning which has a relatively high speed than autonomous robot cars. Firstly, a path will be constructed by using an evolutionary algorithm, such as genetic algorithm, and then this produced curve will be smoothed by using all of these compared algorithms. Finally, the total real costs will be calculated and compared.

REFERENCES

IJCSIS REVIEWERS’ LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Dr. Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnaana Dhas, Anna University, India
Dr Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Dr. Wongys Keardsri, Chulalongkorn University, Bangkok, Thailand
Dr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G./) Dimat Raipur, India
Dr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Dr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Dr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Dr. P. Vasant, University Technology Petronas, Malaysia
Dr. Wong Kok Seng, Soonsil University, Seoul, South Korea
Dr. Praveen Ranjan Srivastava, BITS PILANI, India
Dr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Dr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarme, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Dr. Tirthankar Gayen, IIT Kharagpur, India
Dr. Huei-Ru Tseng, National Chiao Tung University, Taiwan
Prof. Ning Xu, Wuhan University of Technology, China
Dr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Dr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan
Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India
Mr. Khaldi Amine, Badji Mokhtar University, Algeria
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany
Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India
Dr. Nadir Bouchama, CERIST Research Center, Algeria
Dr. R. Satishkumar, Sri Venkateswara College of Engineering, India
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco
Dr. S. Malathi, Panimalar Engineering College, Chennai, India
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India
Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India
Dr. Hamza Aldabbas, Al-Balqa’a Applied University, Jordan
Dr. G. Rasitha Banu, Vel's University, Chennai
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India
Ms. U. Sindhija, PSG college of arts &science, India
Dr. Ehsan Saradar Torshizi, Urmia University, Iran
Dr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim
Dr. Khaled Eskaf, Arab Academy for Science, Technology & Maritime Transportation, Egypt
Dr. Nishant Gupta, University of Jammu, India
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India
Assistant Prof. Tribikram Pradhan, Manipal Institute of Technology, India
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India
Dr. Rahul Malik, Cisco Systems, USA
Dr. S. C. Lingareddy, ALPHA College of Engineering, India
Assistant Prof. Mohammed Shuaib, Interal University, Lucknow, India
Dr. Sachin Yele, Sanghvi Institute of Management & Science, India
Dr. T. Thambidurai, Sun Univercell, Singapore
Prof. Anandkumar Telang, BKIT, India
Assistant Prof. R. Poorvadevi, SCSVMV University, India
Dr Uttam Mande, Gitam University, India
Dr. Poomima Girish Naik, Shah Institute of Business Education and Research (SIBER), India
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India
Dr. Mohammed Zuber, AISECT University, India
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia
Dr. K. R. Ananth, Velalar College of Engineering and Technology, India
Dr. Hasan Ashrafi-rizi, Isfahan University of Medical Sciences, Isfahan, Iran
Dr. Mazhar Malik, Institute of Southern Punjab, Pakistan
Dr. Yajie Miao, Carnegie Mellon University, USA
Dr. Kamran Shaukat, University of the Punjab, Pakistan
Dr. Sasikaladevi N., SASTRA University, India
Dr. Ali Asghar Rahmani Hosseinabadi, Islamic Azad University Ayatollah Amoli Branch, Amol, Iran
Dr. Velin Kralev, South-West University "Neofit Rilski", Blagoevgrad, Bulgaria
Dr. Marius Iulian Mihailescui, LUMINA - The University of South-East Europe
Dr. Sriramula Nagaprasad, S.R.R.Govt.Arts & Science College, Karimnagar, India
Prof (Dr.) Namrata Dhanda, Dr. APJ Abdul Kalam Technical University, Lucknow, India
Dr. Javed Ahmed Mahar, Shah Abdul Latif University, Khairpur Mir's, Pakistan
Dr. B. Narendra Kumar Rao, Sree Vidyanikethan Engineering College, India
Dr. Shahzad Anwar, University of Engineering & Technology Peshawar, Pakistan
Dr. Basit Shahzad, King Saud University, Riyadh - Saudi Arabia
Dr. Nilamadhab Mishra, Chang Gung University
Dr. sachin Kumar, Indian Institute of Technology Roorkee
Dr. Santosh Nanda, Biju-Pattnaik University of Technology
Dr. Sherzod Turaev, International Islamic University Malaysia
Dr. Yilun Shang, Tongji University, Department of Mathematics, Shanghai, China
Dr. Nuzhat Shaikh, Modern Education society's College of Engineering, Pune, India
Dr. Parul Verma, Amity University, Lucknow campus, India
Dr. Rachid Alaoui, Agadir Ibn Zohr University, Agadir, Morocco
Dr. Dharmendra Patel, Charotar University of Science and Technology, India
Dr. Dong Zhang, University of Central Florida, USA
Dr. Kennedy Chinedu Okafor, Federal University of Technology Owerri, Nigeria
CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2016
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2016 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Localization schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, ** Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

**Track B: Computer Science**

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embedded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC’s, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration: Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid
Authors are invited to submit papers through e-mail ijcisiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCISIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcisis/authors-notes.