

IJCSIS Vol. 13 No. 8, August 2015
ISSN 1947-5500

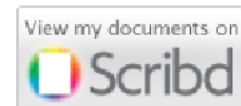
International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2015
Pennsylvania, USA



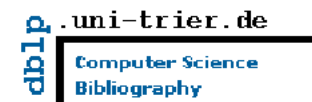
Cogprints

Google scholar



SciRate.com

CiteSeer^x beta



DOAJ DIRECTORY OF OPEN ACCESS JOURNALS



ProQuest

IJCSIS

ISSN (online): 1947-5500

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 2015 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 Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.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/>

 SCIRUS
search engine for science

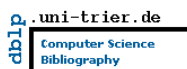
 ScientificCommons

 Scribd

 .docstoc
find and share professional documents

 BASE
Bielefeld Academic Search Engine

 CiteSeerX beta

 dblp.uni-trier.de
Computer Science
Bibliography

 DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS



 ProQuest

For more information, please visit the journal website (<https://sites.google.com/site/ijcsis/>)

Editorial Message from Managing Editor

*The **International Journal of Computer Science and Information Security (IJCSIS)** is a high impact international publication featuring emerging research findings and industry solutions involving all aspects of computing and security. The editorial board is pleased to present the August 2015 issue. The purpose of this edition seeks to expand existing experimental and theoretical research from both industry and academia in the broad areas of Computer Science, Information Security, Cloud Computing and ICT related areas. We are glad to see variety of articles focusing on the major topics of innovation and computer science; high performance computing; security; genetic algorithms; interdisciplinary applications & mobile technologies etc. This scholarly resource endeavors to provide international audiences with the highest quality research manuscripts and accounts of the constant evolution of information science and technology in whole. Researchers, academicians, practitioners and doctoral students will find this journal as a critical source of reference.*

Over the last years, we have revised and expanded the journal scope to recruit papers from emerging areas of green & sustainable computing, cloud computing security, forensics, mobile computing and big data analytics. IJCSIS archives all publications in major academic/scientific databases and is indexed by the following International agencies and institutions: Google Scholar, CiteSeerX, Cornell's University Library, Ei Compendex, Scopus, DBLP, DOAJ, ProQuest, ArXiv, ResearchGate and EBSCO.

We thank and congratulate the wonderful team of editorial staff members, associate editors, and reviewers for their dedicated services to select and publish high quality papers for publication. In particular, we would like to thank the authors for submitting their papers to IJCSIS and researchers for continued support to IJCSIS by citing papers published in IJCSIS. Without their continued 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 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. 13, No. 8, August 2015 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):





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

Professor Yong Li, PhD.

School of Electronic and Information Engineering, Beijing Jiaotong University,
P. R. China

Professor Ying Yang, PhD.

Computer Science Department, Yale University, USA

Professor Hamid Reza Naji, PhD.

Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran

Professor Elboukhari Mohamed, PhD.

Department of Computer Science, University Mohammed First, Oujda, Morocco

Professor Mokhtar Beldjehem, PhD.

Sainte-Anne University, Halifax, NS, Canada

Professor Yousef Farhaoui, PhD.

Department of Computer Science, Moulay Ismail University, Morocco

Dr. Alex Pappachen James

Queensland Micro-nanotechnology center, Griffith University, Australia

Dr. Sanjay Jasola

Professor and Dean, School of Information and Communication Technology,
Gautam Buddha University

Dr Riktesh Srivastava

Assistant Professor, Information Systems, Skyline University College, University
City of Sharjah, Sharjah, PO 1797, UAE

Dr. Siddhivinayak Kulkarni

University of Ballarat, Ballarat, Victoria, Australia

Dr. T. C. Manjunath

HKBK College of Engg., Bangalore, India

Dr. Naseer Alquraishi

University of Wasit, Iraq

Dr. Shimon K. Modi

Director of Research BSPA Labs, Purdue University, USA

Dr. Jianguo Ding

Norwegian University of Science and Technology (NTNU), Norway

Dr. Jorge A. Ruiz-Vanoye

Universidad Autónoma del Estado de Morelos, Mexico

Prof. Ning Xu

Wuhan University of Technology, China

Dr . Bilal Alatas

Department of Software Engineering, Firat University, Turkey

Dr. Ioannis V. Koskosas

University of Western Macedonia, Greece

Dr Venu Kuthadi

University of Johannesburg, Johannesburg, RSA

Dr. Kai Cong

Intel Corporation, & Computer Science Department, Portland State University, USA

Dr. Omar A. Alzubi

Prince Abdullah Bin Ghazi Faculty of Information Technology
Al-Balqa Applied University (BAU), Jordan

Dr. Zhihan Iv

Chinese Academy of Science, China

Dr. Umar Ruhi

University of Ottawa, Canada

TABLE OF CONTENTS

1. Paper 31071522: Towards Creating a Digital Privacy Framework (pp. 1-4)

Jasmin Cosic, ICT Section of Police Administration, Ministry of the Interior of Una-sana canton, Bihac, Bosnia and Herzegovina

Zoran Cosic, Statheros, d.o.o., Kaštel Stari, Split, Croatia

Miroslav Baca, Faculty of Organization and Informatics, University of Zagreb, Varazdin, Croatia

Abstract — In this paper authors will discuss about (digital) privacy. They will try to define a new approach to defining a digital privacy and propose a framework for «calculating» a percentage of privacy in a specific case. Most important factors and representation of this framework will be presented. It will be proposed a set of concepts mostly used in this framework –taxonomy diagram of potentially created ontology of digital privacy.

Keywords - *privacy, digital privacy, ontology, privacy framework, taxonomy diagram, DPF*

2. Paper 31071529: On the Data Mining Process for Classification of Fetal Death Causes (pp. 5-8)

Luis Huerta, José Huesca, Nubia Cabrera, Juan Ruiz, Luis Hernandez

Informatics Department, University of Istm, Ixtotec, México

Abstract — This paper describes a set of tests, where different kinds of algorithms in order to classify fetal death causes were applied. In our tests, the kind of lazy and tree classification algorithms presented best performance. Moreover, different kinds of algorithms for attribute selection were employed, less than 13 of 48 attributes of the database were selected without affecting considerably the classification performance. Finally, since the database classes were unbalanced, a set of classification tests were performed with re-sampled and balanced databases. The classification was correct approximately with 70% and 80 % of accuracy with a re-sampled dataset at 50% and 100% from the original size of the database, respectively.

Keywords-component: Data Mining; Fetal Death; Classification.

3. Paper 31071530: Modelling and Design E-Commerce SMI Sector Using Zachman Framework (pp. 9-14)

Yana Hendriana, Informatics Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Rusydi Umar, Informatics Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Andri Pranolo, Informatics Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Abstract — Bantul regency already has 44.778 SMI (Small And Medium Industries) group and partially of these have blog or website, which is used specifically to market SMI products, but Its has not had a special web merchants to market their products, to help SMI Organization field of domestic trade be required obtain information and for product marketing SMI merchants. Its requires the modeling and design of e-commerce systems in the hope can be used as a reference for building e-commerce systems. Data were collected by library research, interview and observation. Modeling and design stage includes data search, analysis, modeling and design-making system with methods of Zachman framework and models of linear sequential process. The research resulted in the modeling and design of e-commerce system with the goal after the system is built and the SMI Organization received the required information. The test results can be recommended to the field of trade with the test value for 100% testing analysis and for testing usability testing to the respondent buyers value the value 3.1, SMI merchants 3.3 and employees of value 3. Indicate satisfaction or user acceptance.

Keywords - *E-commerce System; Zachman Framework; SMI*

4. Paper 31071537: Microwave Imaging System's New developments for Security Applications (pp. 15-26)

*Sultan Almazroui, School of Engineering and Informatics University of Sussex Brighton, UK
Weiji Wang, School of Engineering and Informatics University of Sussex Brighton, UK
Guangfu Zhang, School of Electronic Science and Engineering, National University of Defense Technology,
Changsha, Hunan, China*

Abstract - Microwave imaging techniques are extensively researched already in the medical field but not so widely in the security field. The art of this research was how to convert from medical imaging to security imaging according to the requirement of security. The algorithm used for this technology has advanced for better results and quality imaging resolution. This paper will discuss the history of terrorist and how important security systems should be considered according to the previous incidents to support always the research of new technologies such as microwave Imaging. This microwave system has proved that microwave can be used for security applications.

Keywords; Security System, Imaging, Microwave imaging, Dielectric, Terrorist, TR-MUSIC, Security Management.

5. Paper 31071539: Overcoming Barriers to Client-Side Digital Certificate Adoption (pp. 27-34)

*Karim Sultan, Faculty of Graduate & Postdoctoral Studies, University of Ottawa, Ottawa, ON, Canada
Umar Ruhi, Telfer School of Management, University of Ottawa, Ottawa, ON, Canada*

Abstract — Public Key Infrastructure (PKI) is a critical component of any cyber security strategy, yet diffusion rates have been dismal within the greater Internet community. Multiple barriers to adoption of client-side certificates exist, including technical complexity, economical burden, legal compliance and social awareness. Entrenched industry practices dating from early Internet-era ideals have obstructed disruptive innovation in this space. Consumer adoption of client certificates is arduous, causing the current deployment model to fail at the general user level. This paper explores the client digital certificate further while identifying barriers to acceptance. A proposal is made for the issuance of “very-low assurance” digital certificates via a Web API, offering one-click simplicity.

Keywords — *Public Key Infrastructure; PKI; Digital Certificate; Personal Certificate; Client-side Certificate; Technology Adoption*

6. Paper 31071548: Using Parallel Computing to Implement Security Attack (pp. 35-38)

Sedeeq Hassn Albana Ali Al-Khazraji, Computing and Information Sciences, Rochester Institute of Technology, New York, USA

Abstract - In 2003, Philip Oechslin invented a new technology to implement the security attack called Rainbow table. Rainbow table is time memory trade off which aims to reduce the calculation happened during the cryptanalysis. Rainbow table reduce the required time for the attack, but generating of the Rainbow table required long time. In this paper we try to achieve parallel implementation for Rainbow table using Message Passing Interface (MPI) with the frame work Intel Cluster Suite. The proposed system support five hashing algorithms, yet our case study was two windows hashing algorithms lm and ntlm. We used Linux operating system in RC computing lab and made our parallel implementation using 201 processing unit to generate Rainbow table. We decrease the time to generate table from 7.1 days in sequential implementation to 46.4 minutes in parallel implementation; as a result we achieve 221.5 speedup.

Keywords- Parallel processing, Security, Privacy & login, Rainbow tables.

7. Paper 31071508: Access Model with the checking of scenarios “AMWCS” (pp. 39-45)

Samir TAHIRI, Hassan II University, ESTC,RITM Lab, Casablanca Morocco

Nadia AFIFI, Hassan II University, ESTC,RITM Lab, Casablanca Morocco
Hicham BELHADAoui, Hassan II University, ESTC,RITM Lab, Casablanca Morocco
Reda FILALI HILALI, Hassan II University, ESTC,RITM Lab, Casablanca Morocco
Mohammed Ouzzif, Hassan II University, ESTC,RITM Lab, Casablanca Morocco

Abstract — The safeguarding of the confidentiality of information and data in an information system has become a major factor nowadays. Indeed with the omnipresence of data processing, the setting on line of the applications, the challenges of security have also become considerable. The access control is a mechanism which governs the way in which data or information must be exploited. It defines and gives authorizations and prohibited accesses. To define or adapt a model of access becomes impossible to circumvent in order to guarantee an optimal security for an information system. With the growth, the diversity and the wealth of information systems, the traditional models of access control show considerable limits. These limits contributed to the birth of other models that are more adapted to our needs. In this article we propose a model of access control that we will set up for in order to deal with the progression of a flow in information system. This model is based on a cutting of the way traversed by a flow in several stages. The passage of a stage has another east governed by rules and conditions. This model makes it possible to challenge the abnormal behavior during the execution of an operation. It is based on the checking of the legitimacy of the presence of an entity in one of the stages of the system.

Keywords— *Security, Authentication, Control, Model, Scenario, Transaction.*

8. Paper 31071524: Facial Expression Recognition Using Gabor Wavelet & Neural Networks (pp. 46-52)

Amira Elsir Tayfour, King Khalid University, Abha, Saudi Arabia
Dr. Altahir Mohammed, Sudan University of Science & Technologies, Khartoum, Sudan
Dr. Moawia Yahia, King Faisal University, Saudi Arabia

Abstract — This paper presents methods for identifying facial expression. The objective of this paper is to present a combination texture oriented method with dimensional reduction for identifying facial expressions. Conventional methods have difficulty in identifying expressions due to change in the shape of the cheek. By using simple two dimensional image analysis, the accuracy of the expression detection becomes difficulty. Without considering the three dimensional analysis, by using texture extraction of the cheek, we are able to increase the accuracy of the expression detection. In order to achieve the expression detection accuracy, Gabor wavelet is used in different angles to extract possible texture of the facial expression. The texture dimension is further reduces by using Fisher's linear discriminant function for increasing the accuracy of the proposed method. Fisher's linear discriminant function from transforming higher dimensional feature vector into two-dimensional vector training and identifying expressions. Different facial expressions considered are angry, disgust, happy, sad, surprise and fear are used. These expressions can be used for security purposes.

Keywords-component; Fisher's linear discriminant function, Wavelet Gabor filter.

9. Paper 31071502: Reduce collision in assigned tree slotted aloha anti-collision protocol in the RFID anti-collision systems (pp. 53-56)

Akram Shangi ghahi, Mohammad Ali Pourmina
Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran

Abstract — Radio Frequency Identification (RFID) is a wireless technology that has replaced barcodes. The major advantages of radio frequency identification (RFID) technology over barcodes are that the RFID-tagged objects do not require to be in line-of-sight with the reader for their identification and multiple objects can be read simultaneously. But when multiple objects are read simultaneously there is always a problem of collision which reduces the efficiency of the system. But when multiple objects are read simultaneously there is always a problem of collision which reduces the efficiency of the system. In this study new algorithms called DyATSA (Dynamic Assigned Tree Slotted Aloha) and DyImATSA (Dynamic Improved Assigned Tree Slotted Aloha) have been

proposed to the third category of Hybrid-based. These two proposed algorithms have been made dynamic by adding new method to ATSA protocol to determine the F0 value prior to the identification of tags. To evaluate the proposed method, two of the most important network parameters including the number of collision slots and idle slots rate were studied in constant tags. By comparing the results of the diagrams, it can be concluded that DyImATSA protocol toward ImATSA protocol, show network performance improvement in tag identification process in simulations.

Index Terms — RFID, Anti-Collision, ATSA protocol, Radio Frequency Identification (RFID), Slotted Aloha protocol.

10. Paper 31071505: Enhanced Secure Hash based Client Puzzle approach to defend against Cyber Attacks (pp. 57-68)

M. Uma, Ph.D Research Scholar, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore -641043

Dr. G. Padmavathi, Professor and Head, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore -641043

Abstract - Game theory is a widely used technique for network security. As technology grows, the cyber worlds are more vulnerable to unknown cyber attacks. There are many cyber attack detection methods available for known attacks; however, efficient methods are essential to detect the unknown cyber attacks. In this research work, an enhanced hash based game theory approach is introduced to defend against cyber attacks. The proposed method is tested in a simulated environment and the method is evaluated using the performance metrics like Throughput, End to end delay, Packet delivery ratio, routing overhead, energy consumption and latency.

Keywords: Game theory, Client puzzle, Hash Chain, Cyber Attacks, Elliptic curve cryptography

11. Paper 31071514: fMRI Slice Registration using Hilbert-Huang Transform (pp. 69-79)

(1) P. Magesh Kumar, (2) S. Purushothaman and (3) P. Rajeswari

(1) Department of MCA, VELS University, Chennai

(2) Department of Electrical and Computer Science Engineering

(2,3) Institute of Technology, Haramaya University, DireDawa, Ethiopia

Abstract - In this paper, brain image slices are considered for registration task. The Fuzzy logic algorithm is used for registration of the brain image slices. As a convention, floating image has misalignment. The floating image has to be transformed and aligned with the target image. Two approaches can be used to create floating image. The first approach is to use the actual image obtained in scanning and it is considered as the target image. The second approach is to introduce misalignment in an existing image slice to obtain a floating image. The application area considered is, registration of image slices of human brain acquired using magnetic resonance imaging scanner. This paper presents implementation of Hilbert Huang transform for fMRI slice registration.

Keywords: medical image registration, fmri slice, Hilbert-Huang Transform (HHT)

12. Paper 31071523: Data Security Protocol for Wireless Sensor Network using Chaotic Map (pp. 80-89)

*Haider M. Al-Mashhadi, Hala B. Abdul-Wahab, Rehab F. Hassan
Computer Science Dept., University of Technology, Baghdad, Iraq*

Abstract - In last years, many cryptosystems relay on the chaotic maps have been proposed. Many significant features of chaotic systems can be exploited in cryptography like: ergodicity, instability to initial condition, and confusion feature. These features lead to a significant relationship between cryptography and chaos. Because of widely usage of WSNs in variety environments, it is important to save the transferred messages from unwanted

access. Security of these data while transferring through the network happens to be more critical. In this study, a new cryptosystem called Hybrid Chaotic Cryptosystem Tent-PWLCCM (HCCTPWLCCM) have been suggested, based on two chaotic methods to create keys and encrypt the WSN's data in a multistep manner to enhance the security of WSN's. The analysis and experimental results show that the execution time and the security achieved by the proposed method are very suitable for securing communications in a variety of WSNs applications, and real-time applications.

Keywords- Block cipher; cryptography; skew tent map; PWLCCM; Wireless Sensor Networks (WSNs).

13. Paper 31071525: Reducing the effects of interference in multi-user multi-antenna systems using pre-coder in the wireless system (pp. 90-94)

Ghodsie Ghalamkarian, Mohammad Ali Pourmina

Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran

Abstract — From the perspective of the information theory, the capacity of multi-user “multiple-input multiple-output” (MIMO) channels is attainable using the “dirty paper coding” (DPC) technique. Due to its high computational load in practical systems, using this technique can be quite complex. Therefore, linear pre-coding techniques such as “zero forcing co-channel interference” (ZF-CCI) and “block Diagonalization” (BD), which are less complex in nature, are proposed in order to remove “multi-user interference” (MUI). These two methods were initially proposed to remove the interference between users in a multi-user system and did not address the “other cell interference” (OCI) that can reduce the performance of cellular communications systems, especially for users that are located at the edge of cells. Two balancing techniques for inter-cell interference and the use of the “minimum mean-squared error” (MMSE) in receivers were proposed in order to reduce OCI without taking MUI into account. An improved version of the BD algorithm, which uses a whitening filter in the receiver, is proposed in multi-user MIMO channels with OCI. However, just like the original BD technique, this technique also faces with the restriction of limited transmitting antennas in most practical applications. Therefore, in order to solve the problem of limited transmitting antennas in the base station, OCI's elimination or control problem should be examined, using the GCI algorithm. Since this technique cannot eliminate the whole multi-user interference, unlike the BD technique, and leaves some amount of interference behind in the system, we propose an optimization problem in the present study in order to allocate energy among users of a weighted set with maximum optimization. The energy allocation problem is a convex one and, therefore, solvable by the “water filling” (WF) technique. The limitation of both these techniques is that the transmitter should be aware of the covariance matrix of the aggregate noise and interference, which may lead to user feedback.

Index Terms — MIMO, BD algorithm, precoding, GCI algorithm.

14. Paper 31071527: An Improved Multiple-level Association Rule Mining Algorithm with Boolean Transposed Database (pp. 95-104)

Ruchika Yadav, Department of Computer Science and Application, Kurukshetra University, Kurukshetra, Haryana, India

Dr. Kanwal Garg, Department of Computer Science and Application, Kurukshetra University, Kurukshetra, Haryana, India

Abstract - Mining of multiple level association rules is a process of data mining, in which significant implication relationship of useful items can be extracted in the form of knowledge at different levels of abstraction. It determines interesting relations between data items through various levels. Association rules with multiple levels of abstraction are more practical and superior as compare to single level association rules. Numerous algorithms had been proposed by the researchers for finding multilevel association rules. The majority of the presented algorithms in this direction relied upon Apriori, and FP-growth, which are based on tire-out explore methods and face problems with large databases. To facilitate multilevel association rules searching, from large databases, a novel algorithm named as “MLTransTrie” is proposed in this paper which is based on bottom-up approach. This newly developed algorithm

helps in reducing number of iterations of database as well as it takes less space in computer memory due to transposed representation of database.

Keywords- Frequent Itemsets; Minimum Support; Multiple Level Association Rule; Transposed Database; Trie.

15. Paper 31071528: A Review on Development of GIS and m-Health Based Patient Registration System to Enhance Support for Epidemiological Analysis: A Case Study of Tanzania Hospitals (pp. 105-113)

*Judith Leo, Kisangiri Michael, Khamisi Kalegele
School of Computational and Communication Science and Engineering, Nelson Mandela African Institution of Science and technology, P. O. Box 447, Arusha, Tanzania*

Abstract- Over the past decades, there has been great advances in ICTs, which has led to the evolution and deployment of mobile phone application technology and GIS in the health sector. Despite of the expanded use of advanced ICT in the health sector, there is still ineffective data collection and presentation of patient and general health data in Tanzanian HIS. This paper shows different proposed and used GIS and mobile applications in perfecting HIS systems. It further proposes the best way on how these technologies can be used to provide effective data collection and presentation. Based on the discussions, a module is proposed to be integrated into the HIS. The ultimate goal of this paper is to improve collection and presentation of health/patient data, in order to enable enhancement of epidemiological analysis.

16. Paper 31071536: Radio Frequency Identification based Drug Management and Monitoring System, Case of Public Hospitals in Tanzania (pp. 114-119)

*Prisila Ishabakaki, Shubi Kaijage
Department of Communication Science and Engineering, Nelson Mandela AIST, Arusha, Tanzani*

Abstract — RFID is an automatic identification technology that enables tracking of people and objects. Recently, the RFID technology has been deployed in hospitals for patient and equipment tracking, surgical equipment monitoring, medication monitoring, and improving health record access in emergency cases. The pharmacy department in public hospitals faces challenges due to manual record keeping and inventory management, which result in theft and diversion of the drugs by unfaithful workers. This work identifies the potentials behind use of the RFID technology in addressing these challenges. The paper focuses on reviewing the current situation at the hospitals to identify loopholes causing these problems and later suggests the solution based on RFID to counteract the challenges. The case study methodology is used where 5 public hospitals in Tanzania were visited to obtain data based on real situation. It was discovered that the drug management and monitoring process is done manually, involves paper based record keeping, manual counting of stock during each staff shifting time, which is hard to track in case of any loss. Therefore, there is need to develop a technological solution to manage the process and secure the drugs.

Keywords: RFID, UHF Radio Frequency, Drug management and monitoring, public hospital

17. Paper 31071535: Cloud-Aware Web Service Security: Information Hiding in Cloud Computing (pp. 120-124)

Okal Christopher Otieno, Department of Information Technology, Mount Kenya University, Nairobi, Kenya

Abstract - This study concerns the security challenges that the people face in the usage and implementation of cloud computing. Despite its growth in the past few decades, this platform has experienced different challenges. They all arise from the concern of data safety that the nature of sharing in the cloud presents. This paper looks to identify the benefits of using a cloud computing platform and the issue of information security. The paper also reviews the concept of information hiding and its relevance to the cloud. This technique has two ways about it that impact how people use cloud computing in their organizations and even for personal implementations. First it presents the

potential to circulate harmful information and files that can adversely affect the data those users upload on those platforms. It is also the basis of the strategies such as steganalysis and cryptographic storage architecture that are essential for data security.

18. Paper 31071538: Managing & Analyzing Large Volumes of Dynamic & Diverse Data (pp. 125-130)

Okal Christopher Otieno, Department of Information Technology, Mount Kenya University, Nairobi, Kenya

Abstract - This study reviews the topic of big data management in the 21st-century. There are various developments that have facilitated the extensive use of that form of data in different organizations. The most prominent beneficiaries are internet businesses and big companies that used vast volumes of data even before the computational era. The research looks at the definitions of big data and the factors that influence its access and use for different persons around the globe. Most people consider the internet as the most significant source of this data and more specifically on cloud computing and social networking platforms. It requires sufficient and adequate management procedures to achieve the efficient use of the big data. The study revisits some of the conventional methods that companies use to attain this. There are different challenges such as cost and security that limit the use of big data. Despite these problems, there are various benefits that everyone can exploit by implementing it, and they are the focus for most enterprises.

Towards Creating a Digital Privacy Framework

Jasmin Cosic

ICT Section of Police Administration
Ministry of the Interior of Una-sana canton
Bihac, Bosnia and Herzegovina

Miroslav Baca

Faculty of Organization and Informatics
University of Zagreb
Varazdin, Croatia

Zoran Cosic

Statheros, d.o.o.
Kaštel Stari, Split, Croatia

Abstract— in this paper authors will discuss about (digital) privacy. They will try to define a new approach to defining a digital privacy and propose a framework for «calculating» a percentage of privacy in a specific case. Most important factors and representation of this framework will be presented. It will be proposed a set of concepts mostly used in this framework – taxonomy diagram of potentially created ontology of digital privacy.

Keywords-privacy, digital privacy, ontology, privacy framework, taxonomy diagram, DPF

I. INTRODUCTION

It seems that everyone is talking about privacy but is not clear what actually they are talking about.[1] Today there is no specific definition of privacy, there is a few dimension and there is a risk that, in defining process, some dimension will be omitted. [2]

There is a few aspects from which scientific trying to understand a privacy. To better understanding a digital privacy, let's to try understand a privacy, a term that is thousand year old. A term privacy is superset of term digital privacy.

A rudiments (beginning) of privacy concept binds to Aristotle and 350 y. B.C.S. Aristotle was separate a public space and political activities (“polis”) of private and family life (“iokos”). [3]

The Romans uses a forum, and Greeks uses parliament (agora) for political life, separate from family life.

Some authors today define privacy like «the way to protect autonomy and the desired level of intimacy of individual». Autonomy means in relation with other individuals, and

intimate means in relation with other individuals. [2] Privacy concerns is a desire to do not allow access to personal data to any others individual.[4]

Authors Smith and Shao [5] observed the historical development of privacy through four phases:

- The infancy of privacy,
- The legal age of privacy,
- Privacy in the technological age and
- Privacy in information age.

Previous studies concerning privacy identified a several factors that are considered to cover various privacy issues. These factors show on multidimensional term of privacy. Authors Ashworth and Free note that previous studies does not answer the question why these factors should be important to users. [6]

After this short review of term privacy, now we can analyze what «online» or «digital» privacy is?

II. DIGITAL PRIVACY

It will be used term on-line or digital privacy in same mining. This kind of privacy can be defined like concerns of Internet users related to control the collection and use of data that are generated about him during his online activities or are collected on the Internet.[7]

The key thing is not what a privacy is, than how to manage with privacy in digital age and *on-line* activities. According [8] there are a three key component for managing a user privacy:

- User must be informed with potential risk according privacy when using a *on-line* services
- User must have a possibility to limit their exposure to others according disclosure of personal data, and finally
- Third component is a user possibilities to have control over their personal data after they disclose to third parties

Author [9] highlights that online privacy can be defined like control over transaction between user and others.¹

In this paper authors deals with a few most important factors which determine a digital privacy. Those factors are identified like a:

- Vulnerability of Services that Users Use (Technology Vulnerability),
- Formal or/and Informal Education of Internet Users (User Education),
- Amount of Personal Data processed or provide to Services (Amount of Personal Data), and finally
- Legislation that regulates Policy of Privacy (Legal or Law),

III. DESCRIPTION OF A FACTORS

In the following section, each of these factors will be described as following:

A. Technology Vulnerability (TV)

Vulnerability of used services or technology vulnerability is most important factor affecting the level of privacy. What is really meaning this term? In digital age, every user uses some web or internet services to facilitate his live. Internet users every day uses some G2C services (e-Insurance, e-Pension system, e-ID card, e-Banking etc...). There is a great possibilities that some (or all) of those services are vulnerable. [10] [11] That mean that using this services on vulnerable platform can effect on user digital privacy. The higher level of service vulnerability means the lower degree of privacy (inverse proportionality).

B. User Education (UE)

Level of User Education has an important role in proposed Framework for calculating a digital privacy. This education can be a formal or informal. Users "must know" what they are doing using some web/internet services, and must be aware of threat on the internet. Some authors in his papers deals with users perception of online privacy and assessment of quality of e-service.[3] User education and technology knowledge will determine a level of digital privacy. The higher level of user education and technology means higher degree of privacy (direct proportionality).

C. Amount of Personal Data (AoPD)

The amount of Personal Data directly affects the level of privacy. Usually, when users using some Internet resources, they provide certain personal information. Sometimes among of these data are "sensitive" data, and very easily can identify the person or user of these resources. Either way, the amount of personal information given, at the example registering to a web service or an Internet resource, it is inversely proportional to the level of privacy. For example, if a Web service requires from users only an email address, it is not the same as when requiring name, surname, address or ID number!

D. Law or Legal (L)

In most European and World economically developed country, privacy is regulated by the law, regulated even and Constitution. User's privacy will be guaranteed if the regulations in Privacy domain is at a higher level, at level rules, procedures and policies. This factor is directly proportional to level of digital privacy, increasing this factor will increases the level of privacy!

IV. INTERDEPENDENCE OF THE FACTORS

Now, let's try to present interdependence of the factors, respectively put in dependence all of those factors that determine the privacy:

DEFINITION: We can say that digital privacy (DP) is a function depends of following parameters Law, User Education, Technology Vulnerability and Amount of Personal Data:

$$DP = f \{ L, \quad // \text{Law} \\ UE, \quad // \text{User Education} \\ TV, \quad // \text{Technology Vulnerability} \\ AoPD // \text{Amount of Personal Data} \\ \}$$
 (1)

When these parameters are placed in dependence, formula will look like (2), which means that the level of the digital policy is directly proportional to the Law or Legal and Users

¹ «Others» means web pages or web sites

Education, and inversely proportional Technology Vulnerabilities and the Amount of Personal Data processed.

This hierarchical structure is top-down based.

$$DP = \frac{L * UE}{TV * AoPD} \quad (2)$$

V. DIGITAL PRIVACY TAXONOMY

Now we will propose digital privacy taxonomy and use an ontological approach to describe a framework.

This is necessary, because the target domain are very often misunderstood, and ontology and taxonomy diagram are very good methods for better understanding and clear defining a problem. Another reason for this is a share common understanding of the structure, enable reuse of domain knowledge, make domain assumptions explicit and separate domain knowledge from the operational. [12][13]

CONCLUSION AND FURTHER RESEARCH

In this paper is discussed about privacy and digital privacy concept. The authors have identified the factors that determine the level of privacy and recommended a framework for digital privacy and taxonomy diagram for this domain.

Next problem that authors deals in the future is how to make a metrics and how to measure values of these factors? Very good method is a Saaty's scale.[14] Another very interesting problem is a digital privacy ontology and intelligent system in which can be "calculated" percentage of privacy before users start using some internet resources.

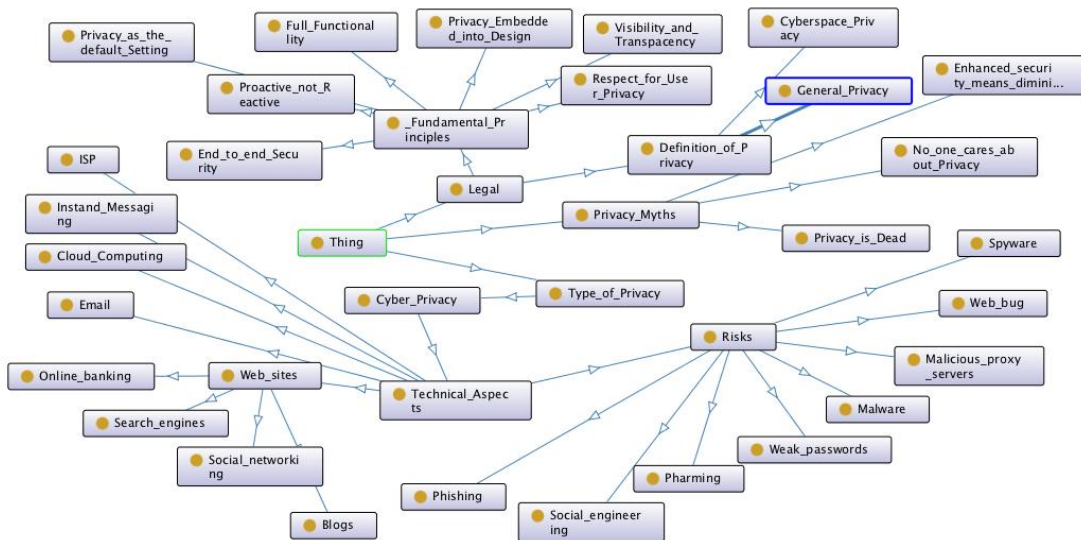


Figure 1. Taxonomy diagram of (digital) privacy concept

Figure 1 present an ontology graph – taxonomy diagram of (digital) privacy concepts. We use this classification schemes to make things easier to find and to add value to a group of objects. By adding value we mean that a classification (describing a group) may provide more information about the members of that group that is obvious from an analysis of a member. The ontology graph displays a domain ontology that matches concepts to help users determine their current problem. The ontology graph depicts hierarchical relations as arrows. [13] The proposed taxonomy diagram consists of few layers.

REFERENCES

- [1] D. Solove, *Understanding privacy*. The George Washington University Law School, 2008.
- [2] J. L. Goldie, "Virtual Communities and the Social Dimension of Privacy," pp. 133–167, 2006.
- [3] R. Mekovec, "Factors of user perception of online privacy and their relations with assessment of the quality of e-service)," University of Zagreb, 2010.

- [4] D. O Neil, "Analysis of Internet Users Level of Online Privacy Concerns," *Soc. Sci. Comput. Rev.*, 2001.
- [5] R. Smith and J. Shao, "Privacy and e-commerce: a consumer-centric perspective," *Electron. Commer. Res.*, vol. 7, no. 2, 2007.
- [6] L. Ashworth and C. Free, "Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns," *J. Bus. Ethics*, vol. 67, pp. 107–123, 2006.
- [7] J. A. Castaneda and F. J. Montoro, "The effect of Internet general privacy concern on customer behavior," *Electron. Commer. Res.*, vol. 7, no. 2, pp. 117–141, 2007.
- [8] R. Mekovec, "Online privacy: overview and preliminary research," *J. Inf. Organ. Sci.*, vol. 34, no. 2, pp. 195–209, 2010.
- [9] M. Lallmahamood, "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model," *J. Internet Bank. Commer.*, vol. 12, no. 3, 2007.
- [10] S. Saha, D. Bhattacharyya, T. Kim, and S. K. Bandyopadhyay, "Model Based Threat and Vulnerability Analysis of E-Governance Systems," *Int. J. u- e- Serv. Sci. Technol.*, vol. 3, no. 2, pp. 7–22, 2010.
- [11] J. Cosic, "Web 2.0 services (vulnerability , threats and protection measures)," *Proc. 20th Cent. Eur. Conf. Inf. Intell. Syst.*, 2009.
- [12] A. Rector, N. Noy, H. Knublauch, S. Guus, and M. Mark, "Ontology Design Patterns and Problems: Practical Ontology Engineering using Protege-OWL," *J. Univ. Manchester*, 2005.
- [13] J. Cosic, Z. Cosic, and M. Baca, "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence," *J. Inf. Organ. Sci.*, vol. 35, no. 1, pp. 1–13, 2011.
- [14] T. L. Saaty, *The Analytic Hierarchy Process*, New York: . Pittsburgh: RWS Publications., 1980.

AUTHORS PROFILE

Doc.dr.sc. Jasmin Ćosić has received his Doctoral degree in Information Science, from University of Zagreb (Croatia) in 2014. He is working in Ministry of the Interior of Una-sana canton in B&H in ICT Section. He is a Assistant professor (docent) in Pedagogical Faculty of Bihac University (B&H). He is also a ICT Expert Witness, and a member of of various professional societies His areas of interests are Digital Forensic, Computer Crime, Information Security, Information Society and DBM Systems.

He is author or co-author more than 35 scientific and more than 30 professional papers and one book.

Prof.dr.sc. Miroslav Bača is currently an Full professor, University of Zagreb, Faculty of Organization and Informatics. He is a member of various professional societies and program committee members, and he is reviewer of several international journals and conferences. He is also the Head of the Biometrics centre in Varaždin, Croatia. He is author or co-author more than 100 scientific and professional papers and two books. His main research fields are Computer Forensics, Biometrics and Privacy.

Dr.sci. Zoran Ćosić, CEO at Statheros ltd, and business consultant in business process standardization field. He received his Doctoral degree in Information Science, from University of Zagreb (Croatia) in 2015. He is a member of various professional societies and program committee members. He is author or co-author more than 35 scientific and professional papers. His main fields of interest are: Informational security, Biometrics and Privacy, Business Process Reengineering.

On The Data Mining Process for Classification of Fetal Death Causes

Luis Huerta, José Huesca, Nubia Cabrera, Juan Ruiz, Luis Hernandez

Informatics Department
University of Istmio
Ixtepec, México

Abstract— This paper describes a set of tests, where different kinds of algorithms in order to classify fetal death causes were applied. In our tests, the kind of lazy and tree classification algorithms presented best performance. Moreover, different kinds of algorithms for attribute selection were employed, less than 13 of 48 attributes of the database were selected without affecting considerably the classification performance. Finally, since the database classes were unbalanced, a set of classification tests were performed with re-sampled and balanced databases. The classification was correct approximately with 70% and 80 % of accuracy with a re-sampled dataset at 50% and 100% from the original size of the database, respectively.

Keywords-component: Data Mining; Fetal Death; Classification.

I. INTRODUCTION

Many families have experienced fetal death, a phenomenon that has long existed, in spite of this, pertinent data are often disregarded or are not properly addressed. [1]. Many people are unaware of what causes this fatal disorder. Even medical personnel and expecting mothers remain unaware of prenatal-care measures that they need to consider to prevent perinatal deaths. Important statistics indicate that fetal death is responsible for over 50% of the perinatal deaths in developed countries [1]. Race, advanced age, low socioeconomic status, diabetes mellitus, arterial hypertension, obesity, infections, renal failure and multiple pregnancy are all related to an increased risk of fetal death, is cited in [2].

In México, the National Institute of Geography, Statistics and Informatics (INEGI, abbreviation in Spanish) has been registering fetal death in databases since 1985 [3]. In our research, we performed data mining techniques on the INEGI databases in order to extract causal factors related to fetal death and we used them to classify causes of fetal death.

Furthering our basic and medical understanding of the patterns present in fetal death events could be helpful in preventing future fetal fatalities.

II. EXPERIMENTAL DATABASE

Data for our research, as described in [4], were gathered from the Civil Records Office, the Secretary of Health, the

Office of Judicial Affairs and from legislative studies in the Federal District, Mexico.

The experimental database has 49 attributes with information on gender, fetal weight, age and occupation of the mother, type of abortion, perinatal care, attending health institution and the locality where the event occurred, to name a few. All of these are numerical type, except the cause of fetal death which is nominal type. There are 196 causes of fetal death in the database, labeled according to The International Classification of Disease.

In this paper causes of fetal death were classified by using basic medical information: type of abortion, fetal weight, number of pregnancies, number of live and dead births, number of medical consultations, health institution where the pregnant was attended, extraction or expulsion of the fetus, gestational age, perinatal attention, skin health status and type of health care personnel present at the fetal-death event. The remaining data are related to geographical location and the background of the mother. In section VI, we will cite precisely the data used to classify the fetal death causes.

In the experimental database, there were 66 classes of fetal death containing only one instance; 28 with only two instances and 14 with three. In general, 162 classes had less than 50 instances. In order to have enough instances in the learning of the algorithms, our research considered those causes that had at least 50 instances of fetal death, resulting in 34 classes finally.

III. ATTRIBUTE SELECTION PROCESS

Attribute selection is one of the activities carried out during the pre-process phase of Data Mining, its goal is to identify and use only the relevant attributes and discard attributes which would not provide information during the algorithmic process. Attribute selection reduces the time and memory required for the Data Mining algorithms, thus facilitating the easy visualization of information as well as noise reduction [5].

Table 1 shows the attributes selected, one of the best in the tests, based on the accuracy provided by them in the

classification. The evaluation was performed with *CfSubsetEval* from the WEKA data-mining tool, the search method employed was *Genetic Search*. A set of genetic-search parameters: population values, cross probability-percentages and number of generations were tested.

Although they propose relevant attributes, they can also discard important attributes which provide accuracy in the classification. Initially, all 48 attributes from the database were tested, lastly, the seven attributes displayed in the last two rows of the Table 1 and five more, were used in the classification tests.

TABLE 1. ATTRIBUTES SELECTED BY THE CFSUBSETEVAL FILTER WITH GENETIC SEARCH.

Population	Generation	Cross	Attributes Selected
1000	200	0.6	Mun_regis, Ent_ocurr, Mun_ocurr, Eda_prod, Pes_prod, Atn_pren, Anio_ocurr, Sitio_ocur, Certific, Atencion, Tip_abor, Pro_expu, Esc_madr, Cond_madr, Dia_cert, Violencia, Par_agre, Dis_re_oax
1000	200	0.8	Ent_regis, Eda_prod, Pes_prod, Emba_fue, Ocu_part, Sitio_ocur, Pro_expu
2000	500	0.8	Ent_regis, Eda_prod, Pes_prod, Emba_fue, Ocu_part, Sitio_ocur, Pro_expu

The attribute *Ent_regis* refers a country state (federative entity) where the fetal death occurred; *Eda_prod* refers to the age of the fetus at the time of death and extraction; *Pes_prod* is the fetus weight; *Emba_fue* refers to whether or not the pregnancy was normal or complicated; *Ocu_part* refers to whether or not the death occurred before or during the pregnancy; *Sitio_ocur* refers to the physical space or health institution where the fetal death occurred; finally, *Pro_expu* refers to the means of fetal extraction. The description of the remaining variables is detailed in [4].

IV. DATABASE RESAMPLE

The unbalanced classes do not have the same number of instances, this is true for the experimental database, see Fig. 1. These kinds of databases are more representative of real world machine learning applications [6]. On the other hand, the natural distribution frequently is not good for the learning of classifiers [8].

In Fig. 1, the biggest bar represents a class with 8217 instances, the smallest bar represents a class with only 60 instances, in general, the number of instances in each class is different. When the distribution of instances is not uniform, the resampling of the experimental database is necessary.

A. The Resampling Filter

In the tests, the WEKA resampling filter on the database was applied, this filter obtains a random subsample. In order to achieve balanced classes, WEKA can use a resampling with replacement which replicates some instances within classes,

whenever the classes have just a few instances. Otherwise, modality without replacement can be used, which does not replicate instances. Also, supervised and unsupervised resamples can be used. The supervised resample requires a nominal class attribute, whereas the unsupervised resample requires a numerical class. In the experimental database, the class attribute called *Causa_def* is nominal, where an identifier for the cause of fetal death is stored using a format in the range {P000,...,Q999}.

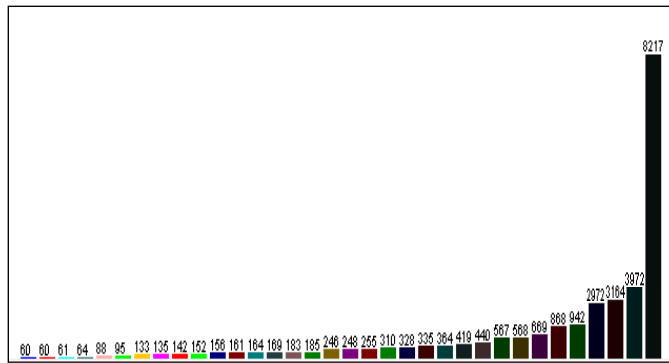


FIG. 1. UNBALANCED CLASSES OF THE FETAL DEATH DATABASE, LABELED WITH THE NUMBER OF INSTANCES.

The *Resampling* filter either maintains the sample distribution or adjusts the class distribution toward a uniform distribution [9]. The parameter of this filter is *biasToUniformClass*, which accepts values in the 0-1 range, where 0 indicates maintain the original distribution of classes, and the value 1 indicates that the filter is set to obtain a new dataset with a uniform distribution among the classes. The *SampleSizePercent* parameter indicates the subsample size as a percentage of the original size, and the *randomSeed* parameter is set at a random value in order to begin the subsampling process.

B. Subsampling the Experimental Database

Two subsamples of the experimental database were obtained. In the

TABLE 2, the parameter values used to obtain each subsample are shown:

TABLE 2. SUBSAMPLING PARAMETERS TYPE I AND TYPE II.

Subsampling	bias	randomSeed	sampleSizePercent
Type I	1	7	50%
Type II	1	7	100%

In both sub-samples, the goal was to obtain a dataset with uniform distribution from the database. The Type-I subsample was set at 50% of the original database size, and the Type-II subsample was set at the original database size (100%). In Fig. 2, the distribution for the Type-I subsample is shown.

Fig. 1 shows the class size represented by the cause “other specified conditions originating in the perinatal period”, it is graphed on the right side bar, and this class is identified with P968 label in the database, which has the greatest number of instances, 8217.

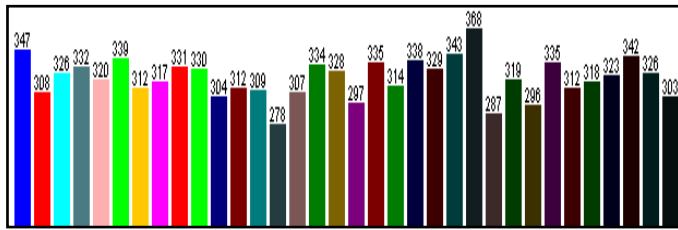


FIG. 2. DISTRIBUTION OF SUBSAMPLE SET AT 50% OF THE ORIGINAL DATABASE SIZE.

In Fig. 2, the P968 class in this subsample has only 303 instances; the subsample has a total of 10919 instances for all classes. Some classes, like the P968, were subsampled, in other words, many instances were ignored in order to approach a uniform distribution. On the other hand, many occurrences were oversampled, like the P031 class, represented in the first bar on the left side of Fig. 2, which contains 347 instances, but had only 60 originally. In this situation, the occurrences are replicated in order to approximate to uniform distribution.

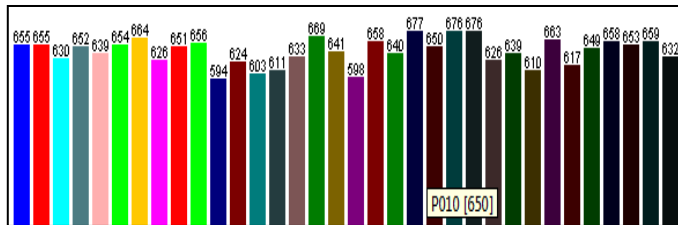


FIG. 3. DISTRIBUTION OF RE-SAMPLING AT 100% SIZE.

In Type-II resampling, the original database size with 28838 instances was sought, uniform distribution approximately was obtained, as can be seen in Fig. 3. In the classification algorithms, both resamples were used. Classifier performance results are shown in section VI.

V. CLASSIFICATION ALGORITHMS

The goal of classification is to establish a class-attribute model as a value function based on the other attributes, the target is: unknown samples must be assigned to a class in the most precise manner possible.

Different kinds of classification algorithms were applied on the experimental database. The *k-NN* and the *Random Forest* classifiers had a better accuracy in the classification of fetal death causes.

A. *kNN*, the *k Nearest Neighbors*

The Nearest Neighbor algorithm, well known as *kNN*, is often preferred in classification tasks because of its simplicity. The *k-NN* bases were proposed by Fix and Hodges in [10].

The *kNN* algorithm needs basically three things in order to classify the unknown sample: a stored dataset, a distance metric and the *k* number of the nearest-neighbor. In order to classify the unknown sample, the distance to each sample in the stored dataset is computed, the *k* nearest neighbors to the unknown sample are identified and the predominant class in them will be used to label the unknown sample.

B. *Random Forest*

The *Random Forest* is an algorithm that uses *decision trees* to perform classification. Decision trees are considered good classifiers because of their quick execution. However, they cannot fully adapt the data complexity while maintaining accuracy in the test data. Tim Kam Ho from Bell laboratories proposed a method called *Random Forest* [11] based in decision trees. The *Random Forest* method is based on tree classifiers with an expandible capacity for training and test data. *Random Forest* builds a tree set by using a subset of features randomly selected for each node. The trees with different subsets of features can generalize the classification in a complementary way, and this combined classification, leading to general improvement.

VI. EXPERIMENTAL TESTS

In this section, the experimental tests using Type I and Type II resampling were performed, see the

TABLE 2. The algorithms with the best performance in the classification task were the *kNN* and *Random Forest*. A set of algorithms were tested like *J48*, *Random Tree*, *MLP*, *SM*, to name a few, underperforming in respect to the two best; we have taken only the *BayesNet* to show its performance. In the tests, the ten-fold cross validation was applied.

TABLE 3. CLASSIFICATION USING 48 ATTRIBUTES.

Resample	Algorithm	Time to build the model (seconds)	% Correct Classification
Tipo I	<i>kNN</i>	0.01	67.47
	<i>Random Forest</i>	12.07	69.26
	<i>BayesNet</i>	0.53	18.60
Tipo II	<i>kNN</i>	0.01	81.25
	<i>Random Forest</i>	5.32	81.84
	<i>BayesNet</i>	0.85	24.25

The Table 3 shows that when resampling type I is done, better classification is obtained by the *Random forest*

(69.26%), however time to build the model in WEKA is bigger than *kNN* (67.47%). On the other hand, *BayesNet* shows poor performance. *Random Forest* and *kNN* show similar performance, however *kNN* is the easy one to work. Algorithms using Type II resample, showed a better performance in 10%, this is because the resample was done at 100% in respect to the original size, and this means many classes were over-sampled with repeated data, making the data more predictable.

Results for 12 attributes tested are showed in *Table 4*. Here are included seven attributes from *Table 1* (second row) and five more: *Edo_piel*, *Tipo_Abor*, *Violencia*, *Eda_madr* y *Ocu_madr*. These latter attributes were added because were suggested by *Ranker* selector algorithm and they contain data directly related with the patient and fetus.

TABLE 4. CLASSIFICATION USING 12 ATTRIBUTES.

Resample	Algorithm	Time to build the model (seconds)	% Correct Classification
Tipo I	<i>kNN</i>	0.02	68.84
	<i>Random Forest</i>	1.44	68.54
	<i>BayesNet</i>	0.22	16.62
Tipo II	<i>kNN</i>	0.01	81.50
	<i>Random Forest</i>	3.27	81.38
	<i>BayesNet</i>	0.18	21.40

Test using the seven attributes showed in *Table 1* were done, the results are showed in *Table 5*. Algorithm *kNN* and *Random Forest* show similar behavior using seven attributes, however, *kNN* is slightly better. The algorithms performance is acceptable, taking in consideration 34 classes. It needed to have in mind that with larger classes or attributes, complexity is increased [12].

TABLE 5. CLASSIFICATION USING SEVEN ATTRIBUTES

Remuestreo	Algorithm	Time to build the model (seconds)	% Correct Classification
Tipo I	<i>kNN</i>	0.01	64.48
	<i>Random Forest</i>	1.59	63.62
	<i>BayesNet</i>	0.07	16.38
Tipo II	<i>kNN</i>	0.01	75.04
	<i>Random Forest</i>	2.62	74.08
	<i>BayesNet</i>	0.17	20.92

The accuracy of classification was near to 70% with resample type I, and close to 80% with type II using 12 attributes. No difference was found with results from *Table 3* where 48 attributes were used. The use of the five attributes proposed by the *Ranker* selector algorithm, improve the accuracy in the classification above 4%.

VII. CONCLUSIONS

In this work a set of tests that employed different kind of algorithms in order to classify fetal-death events were applied. Based on experiments is possible to determinate, with the

accuracy reported here, the cause of fetal death taking in consideration fetus weight, fetus age, type of pregnancy, skin status of the mother, mother occupation, familiar violence, relationship aggressive, mother age, abort type, state of the country (entity) and the physical space where the fatal event occurred.

In classification task, algorithms *Random Forest* and *kNN* showed good performance with resample type II, being the *kNN* slightly better. With 12 attributes and using resample type I were obtained accuracy close to 70% and type II close to 80%.

In future research we will mix attributes proposed by selectors additional to the *Genetic Search* and *Ranker*. We will search reduce the dependency of geographical data like *Entity* (*Ent_ocur*) and *Places* (*Sitio_ocur*), in order to use exclusively biometrical data during the classification.

- [1] Secretaría de Salud, «Diagnóstico y Tratamiento de Muerte Fetal con Feto Único.» CENETEC, México, 2010.
- [2] Molina S., «Muerte fetal anteparto: ¿es una condición prevenible?», *Universitas Médica.*, vol. 51, n° 1, pp. 59-73, 2010.
- [3] Instituto Nacional de Estadística Geografía e Informática (INEGI)., «Instituto Nacional de Estadística Geografía e Informática (INEGI).» 08 06 2015. [En línea]. Available: <http://www.inegi.org.mx/>. [Último acceso: 04 08 2014].
- [4] Instiuto de Estadística Geografía e Informática, «INEGI. Estadística de Defunciones Fetales. Descripción de la Base de Datos.» México D.F., 2012.
- [5] Witten, I. et al. «Data Mining, Practical Learning Tools and Techniques». Morgan Kauffman Publishers. (2011).
- [6] Tan P., *Introduction to Data Mining*, Addison Wesley, 2005.
- [7] Chawla N., *Data Mining and Knowledge Discovery Handbook.*, Springer US., 2005.
- [8] Chawla, N. «Proceedings of the ICML'2003 Workshop on Learning from Imbalanced Data Sets II». (2003).
- [9] Hall M. e. al., *The WEKA Data Mining software: An update.*, vol. 11, SIGKDD Explorations, 2009.
- [10] Hodges J., Fix E., «Discriminatory analysis, nonparametric discrimination: Consistency properties.» Technical Report 4, USAF School of Aviation Medicine, Randolph Field, Texas, 1951.
- [11] Ho T., «Random Decision Forest» *Proceedings of the 3rd International Conference on Document Analysis and Recognition*, pp. 278-282, 1995.
- [12] Zongxing X. et al. «ASIC: Supervised Multi-class Classification using Adaptive Selection of Information Components». *International Conference on Semantic Computing*, 2007. ICSC 2007. pp. 527-534. (2007)

Modelling And Design E-Commerce SMI Sector Using Zachman Framework

Yana Hendriana
Informatics Department
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Rusydi Umar
Informatics Department
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Andri Pranolo
Informatics Department
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Abstract—Bantul regency already has 44.778 SMI (Small And Medium Industries) group and partially of these have blog or website, which is used specifically to market SMI products, but its has not had a special web merchants to market their products, to help SMI Organization field of domestic trade be required obtain information and for product marketing SMI merchants. Its requires the modeling and design of e-commerce systems in the hope can be used as a reference for building e-commerce systems. Data were collected by library research, interview and observation. Modeling and design stage includes data search, analysis, modeling and design-making system with methods of Zachman framework and models of linear sequential process. The research resulted in the modeling and design of e-commerce system with the goal after the system is built and the SMI Organization received the required information. The test results can be recommended to the field of trade with the test value for 100% testing analysis and for testing usability testing to the respondent buyers value the value 3.1, SMI merchants 3.3 and employees of value 3. Indicate satisfaction or user acceptance.

Keywords—*E-commerce System; Zachman Framework; SMI*

I. INTRODUCTION

The development of information and communication technology today has boomed. With advances in technology and information, company or organization doing business to improve the quality and competitiveness are supported by information and communication technologies.

E-commerce is the buying, selling and marketing goods and services through electronic systems. Many convenience gained from *e-commerce* one does not need to hold merchandise traders in the market due to the use of *e-commerce* merchants simply upload wares. Goods are uploaded can be viewed by potential buyers from different regions. Prospective buyers do not need to come to the place of the trader as examples of goods already on the web [1].

The Framework for Enterprise Architecture (the “Zachman Framework”) is a normalized schema, one (meta) fact in one place. That is what makes it a good analytical tool. Don’t add or change the Rows or Columns or you will denormalize it and it will cease to be a good analytical tool. The Framework is a semantic structure. It implies nothing about implementation

processes (methodologies) or tools whether they are top-down, bottom-up, left-to-right, right-to-left, or where to start [2].

Based Bantul Perindagkop Strategic Plan 2012-2017 and the SMI of Bantul Regency merchant number of SMI in the Regency / City recorded in 2013 as many as 44.778 SMIs. Increasing the number of SMIs that become obstacles for Bantul Disperindagkop in service. Promotion and marketing processes in SMIs in Bantul has been facilitated through the website and blog. But on the web is still a mixture of different types of goods. In the promotional display is not distinguishable types of products. In the SMI merchants themselves have not provided specific web for promotion and sales.

Use of information systems and technology can support existing business processes. But it is not easy to apply. Therefore, the government bureaucracy needs to make the *e-commerce* system in order to obtain data Agency is *up-todate* and the overall number of traders which include SMIs in Bantul, the list of SMI merchants, types of products sold by traders SMIs.

II. LITERATURE REVIEW

A. Accomplished Research Study

Applications *E-commerce* Sales Perfumes Online “*E-commerce* can connect sellers and buyers of different places and not be an obstacle in the transaction. Prospective buyers can find out more info about the product such as price, type, brand and so on ” [4]. Implementation of *E-commerce* Sales Book Publisher Waves Based on *Framework* “The use of *e-commerce* technology provides a very broad market opportunity given the technology of the Internet has spread widely throughout the corners of the world. *E-commerce* provides many advantages and conveniences, one of which reduces operating costs and for consumers to shop faster time and a lot of information about products available ” [5].

B. Software process models

Resolve the problem, software engineering or the team engineer should incorporate development strategies that encompass coating processes, methods and aids as well as

Identify applicable sponsor/s here. (*sponsors*)

generic phases. There are several models of software processes, namely: linear sequential model, prototype, RAD, spiral, assemblies, concurrent development and formal. The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations [3].

C. Understanding Electronic Commerce (E-commerce)

One of the most commonly used data mining techniques for E-commerce is finding association rules between a set of co-purchased products, dynamic set, technology, applications, and business processes that connect corporate, consumer, and certain communities through electronic transactions and trade in goods, services, and information that will be conducted electronically [6].

Recommender systems are used by E-commerce sites to suggest products to their customers. The products can be recommended based on the top overall sellers on a site, based on the demographics of the customer, or based on an analysis of the past buying behavior of the customer as a prediction for future buying behavior. Broadly, these techniques are part of personalization on a site, because they help the site adapt itself to each customer. Recommender systems automate personalization on the Web, enabling individual personalization for each customer. Personalization to this extent is one way to realize Pine's ideas on the Web. Thus, Pine would probably agree with Jeff Bezos, CEO of Amazon.com™, when he said "If I have 2 million customers on the Web, I should have 2 million stores on the Web" [8].

D. Zachman Framework

The Zachman Framework was first published by John Zachman in 1987. This framework in the form of a matrix size of 6x6. ZF is used for developing and documenting enterprise architecture or practically. The vertical axis provides a variety of perspectives / perpekstif of the overall architecture, while the horizontal axis is an abstraction classification of architectural artifacts. The six components of the Zachman framework are: data, functions, network, personnel, time, and motivation. Each component is described and seen by six perspectives: the perspective of the planner, owner, designer, builder, sub-contractors and users [7].

The Framework can be used to help to think about (analyze) any thing or any Enterprise or portion thereof. The broader defined the analytical target, the better leverage going to get on integration, reusability, interoperability, etc., etc but the more complex the analysis. Conversely, the narrower drew the boundary of the analytical target, the simpler the analysis but the less leverage going to get on integration, reusability, interoperability, etc., etc. If you draw the boundary beyond your jurisdictional control, you can no longer declare the models, you will have to negotiate the models. If you draw

the boundary more narrowly than your jurisdictional control, you will disintegrate your Enterprise, that is, you will build a "legacy" [2].

III. METHODOLOGY

A. Research stages

- 1) Search Data
Contains data retrieval methods used in the research. The method used to adjust the method of the Zachman framework.
- 2) Analysis
 - a) Analysis of Current Conditions
Business process areas of domestic trade, traders and buyers SMIs. General business processes between the field of domestic trade, SMI Traders and buyers are trading field to market products SMI merchants, shoppers buy products SMI trader. SMI traders also sold with the cast, meeting business and trade missions.
 - b) Analysis Conditions Expected
This stage is the stage of determining the conditions expected by Disperindagkop field of domestic trade.
 - c) SWOT Analysis
Useful to analyze the factors in Disperindagkop field of trade in business evaluation methods to find strategies that will be done. SWOT analysis only describes the situation that occurs is not solving the problem.

B. Making the modeling and design of e-commerce

Making of this thesis using the Zachman framework combined with a linear sequential process model. In the sequential model of the liner only to the design phase. As created, namely Column Data: ERD, the business data model of entities and attributes, data architecture. Function column: DFD, application architecture and system design. Network column: logistics network, information architecture, technology architecture. Column One: organizational structure, interface architecture and user interface.

C. Prototype testing

- 1) Testing Analysis is a test of the analysis has been made on whether it can be recommended for Disperindagkop field of domestic trade.
- 2) Usability Testing
 - a) Acceptance testing (usability testing) is testing by providing a number of tasks that have been prepared in advance. The task given to two employees, 15 traders SMIs and 30 buyers. This task is used as a 'means of interaction' in the measurement of usability.
 - b) Analysis of usability testing is a recap of the results of a questionnaire that has been deployed.

IV. RESULT AND DISCUSSION

After searching the data, analysis of current conditions, expected conditions analysis and SWOT analysis, the next step

is the manufacture of modeling and design of e-commerce systems. The steps are as follows:

A. Business process

Business process proposed to the field of domestic trade. The business process is a business process merchant account registration SMI, buyer registration, login, promotion, sales, registration of the exhibition, following the registration of the trade mission, following the registration of business meetings, coaching training, coaching (Exhibitions, Trade Missions and Business Meeting), coaching (social assistance), Monitoring Data Merchants SMI, sales monitoring, supervision fairs, Trade Missions and Business Meeting.

B. Analysis of system requirements

Determining and disclose the needs of e-commerce system that includes: the buyer needs is a menu for the buyer account, details of the agenda of the Office menu, menu selection announcement details exhibition, menu by purchase, login display, the display forgotten the password, display successful login, view and purchase process , confirmation of purchase display, menu about, help menu, my account menu, menu poduk category. Trader needs of SMIs: SMI merchants login menu, the menu lists the SMI merchants, SMI traders forgotten password menu, menu promotions, sales menu, menu proposals, menu information, see the list of activities of the Department, purchase information menu, menu reply Agency proposals, invitations menu Office. Needs Service employee: employee login menu, the main menu of employees in trade, menu display the list of candidates to follow the activities of the Office of SMI merchants, menu development training, coaching menu exhibition, input provision activities list Office, Office of the input stage of registration activities, business meetings coaching menu, menu fostering trade mission, the menu guidance of social assistance, counter proposals menu, the menu of data monitoring SMI merchants, sales monitoring menu (menu supervision of annual sales, monthly sales supervision menu), menu supervision exhibitions, business meetings supervision menu, menu control trade missions, inputan on the menu, input help menu, change password menu.

C. Entity Relationship Diagram (ERD)

A description of the data needs of the entity as shown in fig.1.

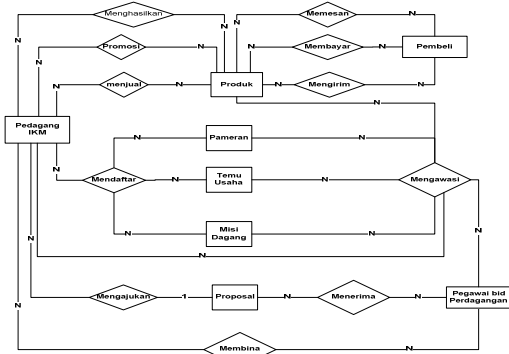


Fig. 1. Entity Relationship Diagram

D. Logistics Network

Enterprise model by exposing the enterprise network model in the form of the location and interconnection proposal to Disperindagkop. At this logistk network also includes SMIs account registration module, which is taken from the SCM system as shown in Fig.2.

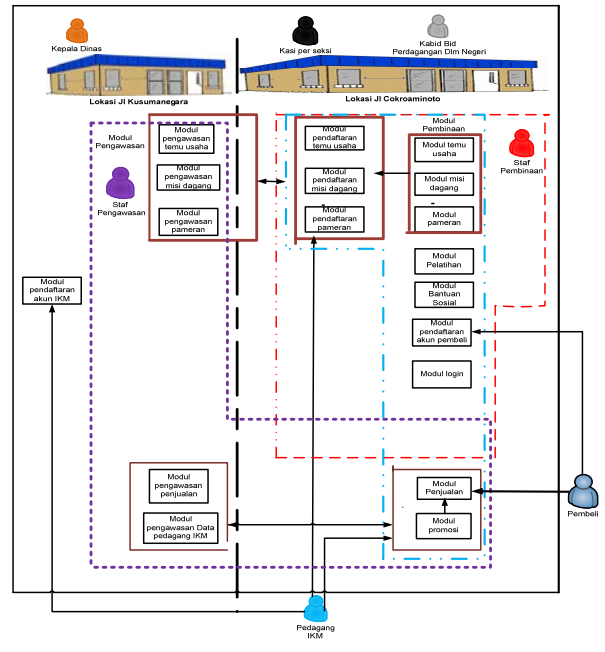


Fig.2. Logistics Network

E. Context Diagram

Diagram illustrating the general of an information system. In the context of the diagram there is only one main process that processes input data to produce output data from all entities connected as shown in Fig. 3.

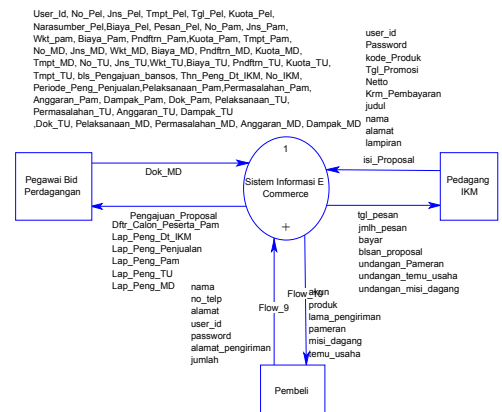


Fig. 3. Context Diagram

F. Application Architecture

Application that contains modules aim to define the modules needed to manage the data and support the business functions in Disperindagkop. Step manufacture: the candidate list of modules and module definitions, impact analysis, matrix

module vs functions and matrix module vs organization as shown in Table 1.

Table 1. Matrix module vs organization

Modul	Organisasi				
	Kepala Dinas	Kabid bid Perdagangan Dim Negeri	Kasi per seksi	Staf Pembinaan	Staf Pengawasan
Modul Pendaftaran akun IKM	3	3	1	3	3
Modul Pendaftaran akun Pembeli	3	3	1		
Modul Login	3	3	1	3	3
Modul Promosi	3	3	1	3	1
Modul Penjualan	3	3	1	3	1
Modul Pendaftaran Pameran	3	3	3	3	1
Modul Pendaftaran Misi dagang	3	3	3	3	1
Modul Pendaftaran Temu Usaha	3	3	3	3	1
Modul Pelatihan	3	3	1	1	
Modul Pameran	3	3	1	1	
Modul Misi Dagang	3	3	1	1	
Modul Temu Usaha	3	3	1	1	
Modul Bantuan Sosial	3	3	3	3	
Modul Pengawasan Data Pedagang IKM	3	3	2		1
Modul Pengawasan Penjualan	3	3	2		1
Modul Pengawasan Pameran	3	3	2		1
Modul Pengawasan Misi Dagang	3	3	2		1
Modul Pengawasan Temu Usaha	3	3	2		1

Table 1 shows Specification: 1 : Creating, repairing, and using, 2 : Renew and Using, 3 : Only Use

G. The design of the system to the modules

The design of the system to the modules is a technical definition of the design process by describing the system needs to perform and support the process. The design of the system to be created on the system in the form of modules that can be accessed by the user. The modules are tailored to the business processes that have been made.

H. Data Architecture

The construction data architecture, the main data types that support business functions that have been defined on the business architecture must be identified and defined. In the candidate business entity data entities added merchant account registration SMI of SCM system. Step manufacturing: making all candidate data entities, making the definition of entities and attributes and matrix process vs data entities as shown in Table 2.

Table 2 : Matrix process vs data entities

KELAS DATA	Proses	Pedagang IKM																	
		Pembeli	Menghasilkan	Promosi	Meretas	Menjual	Membayar	Mengirim	Mendatir	Pameran	Misi_Dagang	Temu_Usaha	Pegawai_Bid_Perdagangan	Membina	Meretas	Proposal	Produk	Mengawasi	
Proses	Pendaftaran akun IKM	R																	
	Pendaftaran akun Pembeli	R																	
	Login	R																	
	Promosi	R																	
	Penjualan	R																	
	Pendaftaran Pameran	R																	
	Pendaftaran Misi dagang	R																	
	Pendaftaran Temu Usaha	R																	
	Pelatihan	R																	
	Pameran	R																	
	Misi Dagang	R																	
	Temu Usaha	R																	
	Proses	Bantuan Sosial	R																
Pengawasan Data Pedagang IKM		R																	
Pengawasan Penjualan		R																	
Pengawasan Pameran		R																	
Pengawasan Misi Dagang		R																	
Pengawasan Temu Usaha		R																	
Pendaftaran akun		R																	
Pendaftaran akun Pembeli		R																	
Login		R																	
Promosi		R																	
Penjualan		R																	
Pendaftaran Pameran		R																	
Pendaftaran Misi dagang		R																	
Pendaftaran Temu Usaha	R																		
Pelatihan	R																		
Pameran	R																		
Misi Dagang	R																		
Temu Usaha	R																		
Bantuan Sosial	R																		
Pengawasan Data Pedagang IKM	R																		
Pengawasan Penjualan	R																		
Pengawasan Pameran	R																		
Pengawasan Misi Dagang	R																		
Pengawasan Temu Usaha	R																		

I. Architecture Technology

An infrastructure needs to be provided to support the data path and modules used by the organization. In making technology architecture modules listed SMEs account registration, and web jogiaplaza SCM system interconnected with the e-commerce system. Step manufacture: the principle of technology platforms, the list of platforms used, the platform needs and specifications, the relationship of technology and manufacture modules and network topology as shown in Fig. 4.

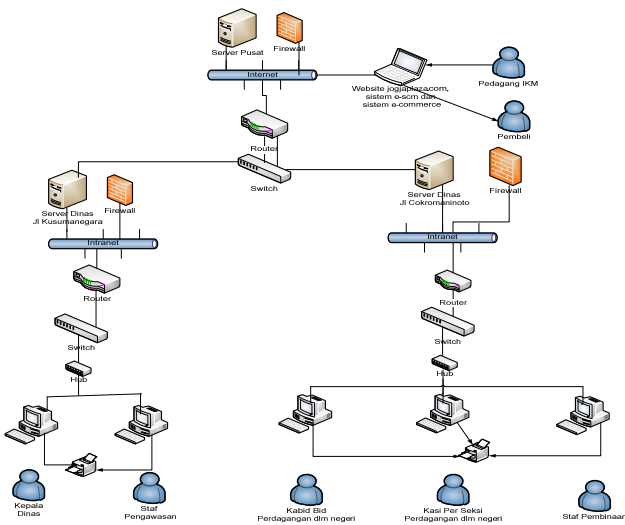


Fig. 4. Network Topology

J. User Interface

1) System Behavior

The system can only be accessed when the user that the buyer and the merchant SMIs have registered or registered by the admin for employees of the Department.

2) Security Design

Buyer Security Plan and traders SMIs are given the opportunity three times if you forget the password and employees can call if you forget your admin password.

K. Interface Architecture

Interface architecture is based on the analysis of the needs of the system and modules.

1) The initial view of the e-commerce system

The options provided to the user if one link will show the expected as shown in Fig. 5.



Fig. 5 The initial view of the e-commerce

2) The promotion menu SMI Traders

Data entry facility to incorporate the products to be displayed at the website as shown in Fig. 6.



Fig. 6. The promotion menu SMI Traders

3) The main menu trade sector employees

Data entry facility for monitoring and coaching SMI trade sector employees as shown in fig.7.



Fig.7. The main menu trade sector employees

L. Feasibility Test

1) Testing analysis

Analytical testing is done by providing a document along with an explanation prior to the respondent namely Service employee. Testing is done by way of explaining the proposed new business processes, entity relationship diagram, information architecture, data architecture, data flow diagrams, application architecture, system design, logistics network, organizational structure, and interface design. From the results of questionnaires given that the proposed analysis can be recommended for Perindagkop and SME areas of domestic trade with the presentation of 100%.

2) Usability testing

The feasibility test carried out to buyers, traders SMI, and staff at the Department. Testing is done by giving Task-Task

Usability Testing and questionnaires have been prepared. With the results of value for buyers respondent 3.3, SMI merchants 3.1 and employees of the Department 3. From the test who gained concluded that usability testing can be received by each user.

V. CONCLUSION

Generate analysis in the form of new business processes, ERD, information architecture, data architecture, data flow diagrams, application architecture, system design, logistics network, technology architecture, organizational structure, interface architecture and user interface.

Modeling and design system generated e-commerce can be recommended to the SMI Bantul Regency Disperindagkop and domestic trade field. It is evident from analysis testing to employees Perindagkop with percentage 100% and prototype testing with the results of each respondent buyers merchant value 3.3 Merchant SMI value of 3.1 and Service employee value 3. The test results explained that the analysis and design of the interface can be recommended for pembuatan modeling and system design e-commerce field of domestic trade.

REFERENCES

- [1] Wong, Jony. *Internet marketing for beginners*. Elex Media Komputindo, 2010.
- [2] Zachman, John. *The zachman framework for enterprise architecture*. Zachman Framework Associates, 2006.
- [3] Pressman, Roger S. *Rekayasa Perangkat Lunak*. Yogyakarta: Andi, 2002
- [4] Fansyuri, Ahmad. 2012. *Aplikasi E-Commerce Penjualan Parfum Secara Online*. Skripsi. Yogyakarta: Program Studi Teknik Informatika Universitas Ahmad Dahlan.
- [5] Yanti, Nur Fitri. 2011. *Implementasi E-Commerce Penjualan Buku pada Penerbit Ombak Berbasis Framework*. Skripsi. Yogyakarta: Program Studi Teknik Informatika Universitas Ahmad Dahlan.
- [6] Sarwar, Badrul, et al. "Analysis of recommendation algorithms for e-commerce." *Proceedings of the 2nd ACM conference on Electronic commerce*. ACM, 2000.
- [7] Surendro, Kridanto. *Pengembangan Rencana Induk Sistem Informasi*. Bandung: Informatika Bandung, 2009.
- [8] Schafer, J. Ben, Joseph Konstan, and John Riedl. "Recommender systems in e-commerce." *Proceedings of the 1st ACM conference on Electronic commerce*. ACM, 1999.

AUTHORS PROFILE



Yana Hendriana, Received his bachelor degree (S.T.) in Informatics department from Universitas Ahmad Dahlan Yogyakarta Indonesia, and (M.Eng.) degrees from the department of Electrical Engineering concentration on Master Information Technology, Gadjah Mada University

Yogyakarta Indonesia.. His research interests include on Software Engineering, Multimedia, Human Computer Interaction, IT for Education. He has been serving as a Lecturer in Informatics Department, Faculty of Industrial Technology Universitas Ahmad Dahlan Yogyakarta Indonesia since 2009.



Rusydi Umar, Received his bachelor degree (S.T.) from the department of Electrical Engineering Gadjah Mada University Yogyakarta Indonesia, and (M.T.) degrees from the department of Informatics Institute Technology Bandung ITB Bandung Indonesia and (Ph.D) degrees from Computer Science University of Hyderabad India, His research interests include on Software Engineering, Grid Computing, Cloud Computing, Digital System. He has been serving as a Lecturer in Informatics Department, Faculty of Industrial Technology Universitas Ahmad Dahlan Yogyakarta Indonesia since 1998.



Andri Pranolo, Received his bachelor degree in Informatics Engineering (S.Kom) from University of Technology Yogyakarta in 2006 and Master Computer Science (M.Cs) from Gadjah Mada University in 2013. He work in laboratory of forest health and protection Faculty of Forestry Gadjah Mada University as Information and Communication Technology staff between 1995 to 2012. Now he work as researcher and lecturer at Informatics Engineering University of Ahmad Dahlan Yogyakarta – Indonesia. His current research including intelligent agen and data mining, expert systems, database systems, and mobil programming. He authored in severale conference including national and international conference. His research are commonly in forestry area which collaboration with Prof. SM Widyastuti – Faculty of Forestry- University of Gadjah Mada Indonesia, other research collaboration with Prof. Sti Mariyam Shamsuddin – Soft Computing Research Group - Universiti Teknologi Malaysia.

Microwave Imaging System's New developments for Security Applications

Sultan Almazroui
School of Engineering and Informatics
University of Sussex
Brighton, UK

Weiji Wang
School of Engineering and Informatics
University of Sussex
Brighton, UK

Guangfu Zhang
School of Electronic Science and Engineering, National
University of Defense Technology
Changsha, Hunan, China, 410073

Abstract --- Microwave imaging techniques are extensively researched already in the medical field but not so widely in the security field. The art of this research was how to convert from medical imaging to security imaging according to the requirement of security. The algorithm used for this technology has advanced for better results and quality imaging resolution. This paper will discuss the history of terrorist and how important security systems should be considered according to the previous incidents to support always the research of new technologies such as microwave Imaging. This microwave system has proved that microwave can be used for security applications

Keywords; Security system, Imaging, Microwave imaging, Dielectric, terrorist, TR-MUSIC, security management.

I. HISTORY

Terrorist acts have been carried out over a long period. For example, two well-known groups are the Irish Republican Army (IRA) who carried out attacks on the British police and army in the 1970s, 80s and 90s, and Germany's Red Army Faction (RAF): both organized a series of bombings and assassinations. In 1988 there was the Lockerbie bombing disaster when flight Pan Am 103 exploded shortly after take-off from Heathrow airport. The 9/11 attack on the World Trade Centre in New York and the Pentagon in Washington D.C. in 2001. In 2004 a bomb was placed on a train in Madrid and killed more than 190 people [1]. In 2005 more than 200 people were killed and injured on the underground and buses in the London bombings. The head of the Federal Service for Supervision of Transport in Russia announced recently that terrorist attacks on the Russia transport system have doubled between 2009 and 2010 [2]. In addition, on 25 December 2009, Umar Abdulmutallab managed to go through all security body scanners, including a millimetre wave scanner, with a hidden plastic explosive in his underwear to detonate a bomb on flight 253 from Amsterdam to Detroit



Figure 1: 'Underwear Bomber': Umar Farouk Abdulmutallab is arrested. Photo by Jasper Shuringa/New York Post [3]

In 2011, there was a bomb explosion at Moscow's busiest airport Domodedovo [4]. In August 2009 Abdullah Hassan Tali Al-Asiri, an Al-Qaeda suicide bomber, inserted half a kilo of explosive inside himself and detonated it at a meeting with Prince Nayef bin Abdulaziz Al Saud, killing himself and causing minor injuries to the prince [5]. There have also been recent attacks on Peshawar airport in Pakistan in 2012, and Kabul international airport in 2013 [6], [7]. The most recent attack on the Westgate mall in Kenya left 72 dead [8]. In addition, by looking at the open source Internet Worldwide Incident tracking system, attacks on the aviation and transport industry have increased despite the increase in security control after 9/11 [9]. Terrorism is not a tactical war that comes back every day and you respond to it: terrorism is planned for a long time and hits countries at unknown times. Therefore plans for such terrorism have to be robustly planned to manage it when it occurs, or detect it before it happens. Therefore, securing airports, train stations and shopping malls and ports is vital to save human lives and sustain the economy.

II. INTRODUCTION

Any terrorist act on the aviation or transport industry will result in the loss of hundreds of lives and loss of infrastructure and equipment worth of millions of pounds; such acts will therefore have a significant impact on the economy and the travel industry. Security of airports, or any other sensitive places, starts at key locations, such as the entrance or check-in points where a terrorist could take advantage to start his terrorist act. The question has always been asked about how to secure the supply chain such as airports, ports, canals and shopping malls from man-made threats such as terrorism or piracy. What is the best way to guarantee security using advanced technology? Ninety per cent of global trade flows through 39 bottleneck regions[9]. Security management is to manage the attack incidents before any crisis happens. Body scanners, such as microwave scanners for explosive detection in the human body, are useful, but they will be useless if security personnel are not very well trained in how to use them. Passengers in modern airports would like to see modern advanced technology to serve them well and secure their journey. Terrorist attacks in a country can damage its economy as a direct cost, and damage the tourism industry. They can target logistic hubs and gateways. For instance more than 14.5% of world airfreight traffic travels through Hong Kong-Shenzhen, and any attack there could have a huge impact on the global economy. Security in general costs a lot of money to make sure that people are safe. Also there is a concern that, for example, if more security has been implemented in airports, then this will mean longer queueing times for passengers and therefore higher transport costs, which will slow the movement in airports. Although this paper discusses implementing advanced technology in body scanners, concerns about cyber-attacks should be taken into account when integrating this new body scanner with other security checks at airports. As discussed later, existing technologies are the solution at the moment, but every technology has limitations, although microwave technology showed a promising imaging technology for security applications. The decision to invest in more body scanner technologies should be taken into account when planning any security investment strategy. Maybe implementing these higher end technology body scanners in international airports only, or where airports that could be a target for terrorist attacks. The transport security companies and logistics should take the lead in developing high end security technologies, i.e., body scanners, and the government should only set security regulations. At the end of the day, both the security companies and the government should collaborate together to be more effective and efficient. This paper will discuss the developing simulation results which were produced by microwave security system research in the University of Sussex [11].

III. MICROWAVE SECURITY SYSTEM SIMULATION SET UP

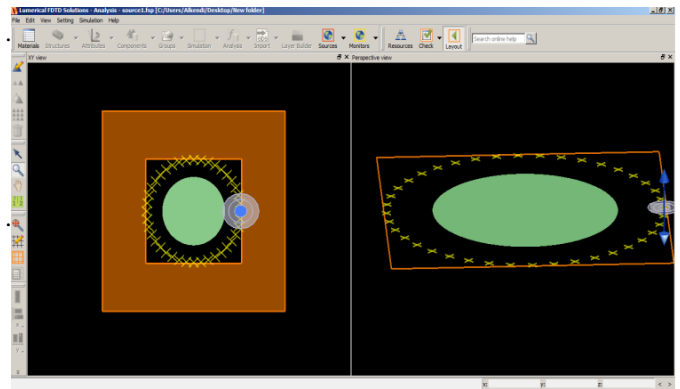


Figure 2 Shows Experiment set up in Lumerical FDTD Solution

The system contains an object which is surrounded by a circular array number of antennas. All the antennas act as transducers sending and receiving microwave to obtain the image of the objects. The configuration was set up in Lumerical FDTD solution. The FDTD solution is used to collect scattered data on each transducer. These data are then processed in Matlab with a TR MUSIC algorithm to reconstruct the image. Figure 2 shows how such a system was configured in Lumerical FDTD solution. The shown target in Figure 2 could be changed at any time to any shape required.

IV. SIMULATION RESULTS FOR DIFFERENT FREQUENCIES WITH DIFFERENT MODELS.

A. Square model using 2GHz frequency

To give the reader an idea of how we construct different type of models to be imaged using microwave the Lumerical FDTD software tool shown in Figure 2 shows how the square model has been placed to be imaged.

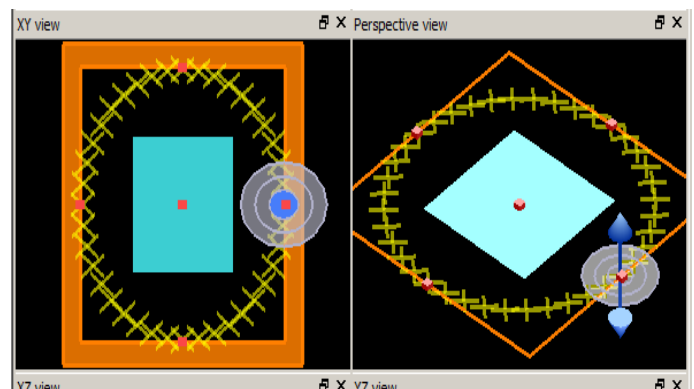


Figure 3 Square Shape Model in Lumerical FDTD software

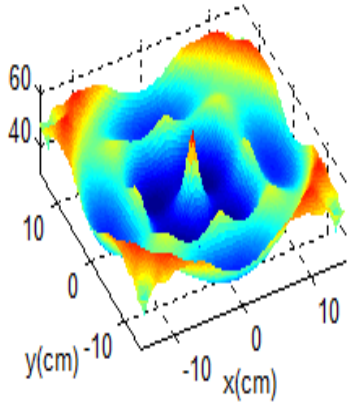
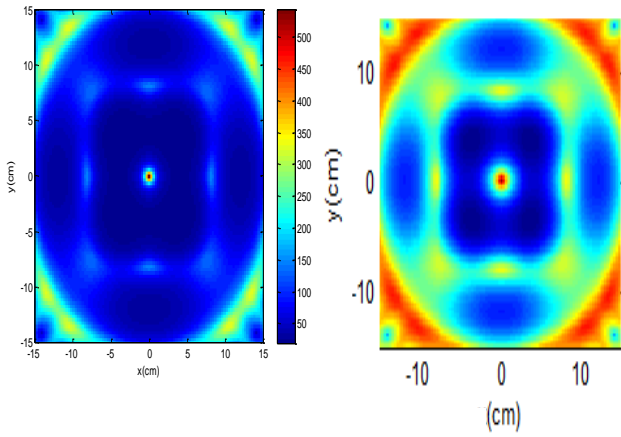


Figure 4: Lower Dielectric Square Shape Model Using 2GHz Objection

Figure 3 above illustrates the shape of a 15cm x 15cm square being imaged using 2GHz. The square has a relative dielectric of 1.4. All the other shapes and models will be constructed in different sizes and different materials: this will show us the value of utilizing this fascinating imaging technology. The common models will be squares, polygons, triangles, rectangles, spheres and embedded objects. Every model will be constructed with different frequencies objection, and then the data will be collected and imported in Matlab to run the TR-MUSIC mathematical model. This will reconstruct the image caused by this microwave antenna seen around the square, or around any other object later in this discussion.

B. Polygon model 2GHz frequency

The following figures shows a polygon shape, if all the peak points were connected, which has been generated by a TR-MUSIC algorithm. The above figure shows peaks or spotlights that exist both on the boundary of the polygon object and inside it. The polygon model points are (X,Y); (0,9), (7,-5), (7,5), (0,9), (-7,5) and (-7,-5). The simulation results shows a polygon shape, if all the peak points were connected, which has been generated by a TR-MUSIC algorithm. Figure 5 shows peaks or spotlights that exist both on the boundary of the polygon object and inside it.

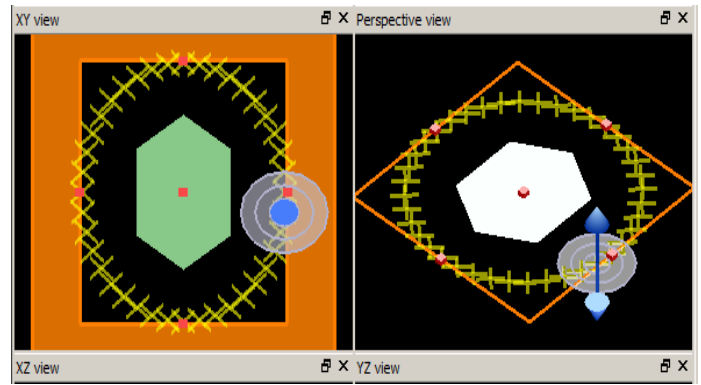


Figure 5: Polygon Shape Model in Lumerical FDTD Software

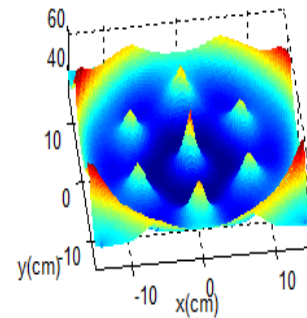
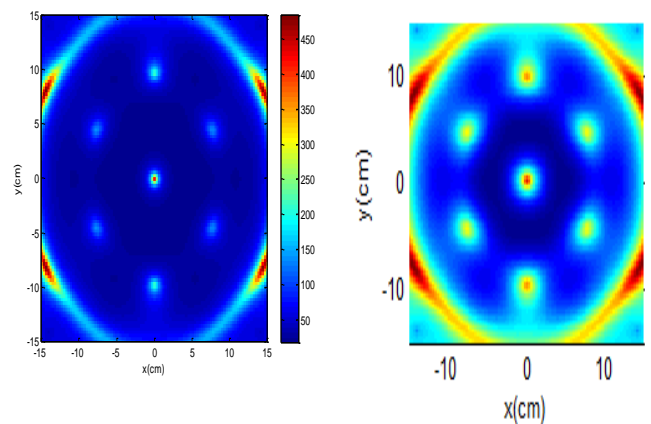


Figure 6: Lower Dielectric Polygon Shape Model Using 2GHz Objection

C. Cylinder model using 3GHz frequency

Figure 6 illustration shows a cylinder of 5cm radius with defined dielectric of 2.4. It shows the very clear shape of such a cylinder because of its extended size related to the 3GHz wavelength and the imaging region 30x30. The above scenario could be any metal or material hidden underneath passengers' clothes. Figure 7 shows a cylinder target that has a radius of 3cm and defined relative dielectric of 5. It shows part of the cylinder shape because it is not fully extended, or it could be shown clearly if we change the number of the M value. The M value is the number of the boundary between the signal subspace and noise subspace. Also this could be very small contraband materials hidden within the human body. This result makes the possibility of small targets being shown clearly very promising.

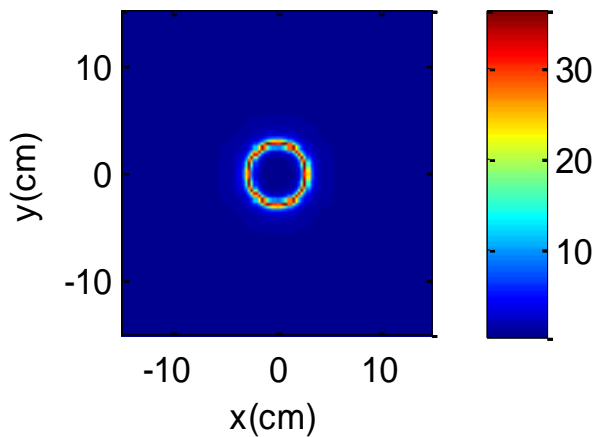


Figure 7: Cylinder of 5cm Radius Using 3 GHz Objections

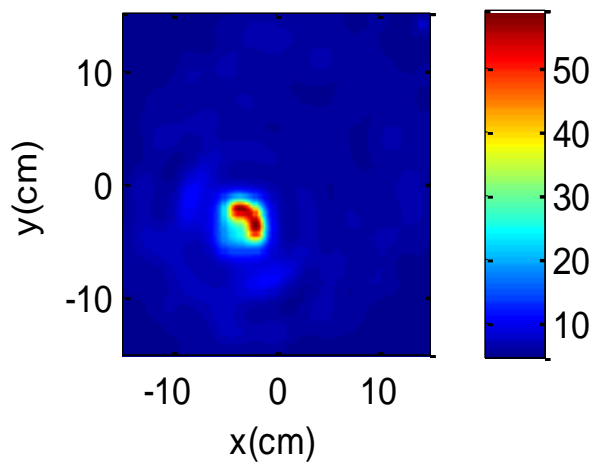


Figure 8: Cylinder of 3cm Radius Using 3 GHz Objections

Figure 8 shows a human body cross-section of 10cm radius with a defined dielectric of 5. A small size of contraband material of 2cm radius is embedded within this human body cross-section and defined dielectric of 6.5. The above figure shows both a human body and the small contraband material embedded within this human body; which could alert the operator of the possibility of illegal items being hidden within this passenger.

D. Triangle model using 4GHz frequency

The Lumerical FDTD software tool has shown in Figure 9 how a triangle has been placed to be imaged. The transceivers' data around the triangle are then collected and implemented in Matlab code to show the imaging results. Figure 9 is a triangle shape with relative dielectric of 1.4; the dimensions are (-10,5), (10,5) and (0,-10). As can be seen from this figure 10, the shape has been shown clearly: there is intensity or more details in the middle of the shape that has been shown. The image of the triangle has been detected clearly. A concentrated spot light is shown in the middle of the triangle.

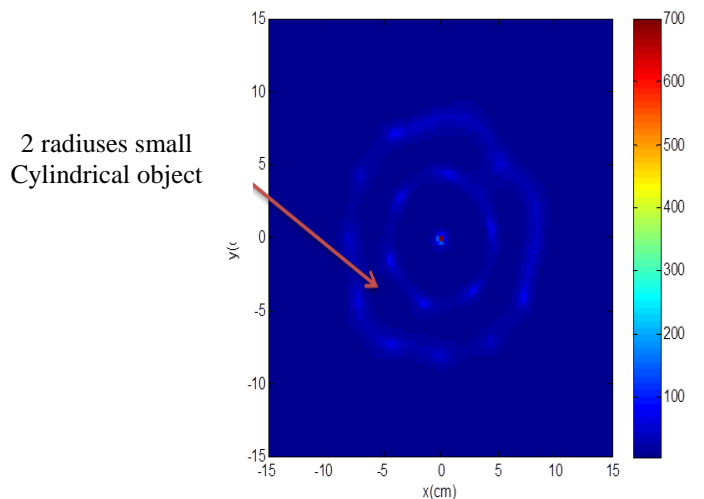


Figure 9: 10cm Human Body Cross Section with 2cm Object Hidden Inside

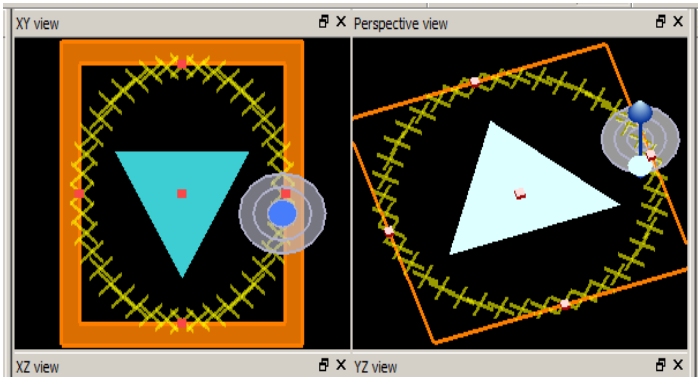


Figure 10: Triangle Shape Model in Lumerical FDTD Software

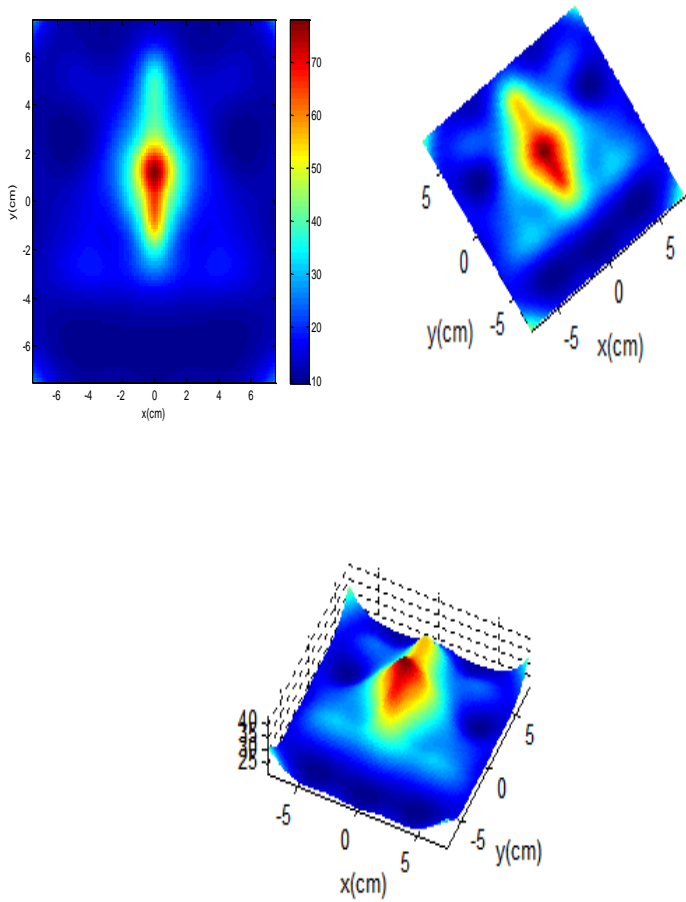


Figure 11: Lower Dielectric Triangle Shape Model Using 4GHz Objection

E. Polygon model using 4GHz frequency

Figure 11 shows how to model a polygon shape with a relative dielectric of 1.4, using 4GHz frequency. The dimensions are (X, Y), (0,-5, 49), (4.75448,-2.745), (4.75448, 2.745), (6.723e-16, 5.49), (-4.75448, 2.745), (-4.75448,-2.745). Figure 12 shows a clear image of Polygon even the dielectric of its material is low. If the material of the polygon has been changed from lower dielectric properties to metal, a perfect electric conductor, then this will cause the simulation results shown in Figure 13. According to the figure 13, a 4GHz frequency objection on the metal polygon shows the boundary of the metallic polygon very clear.

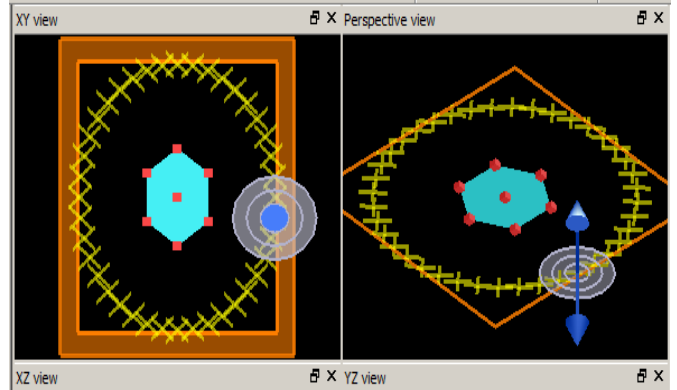


Figure 12: Polygon Shape Model in Lumerical FDTD Software

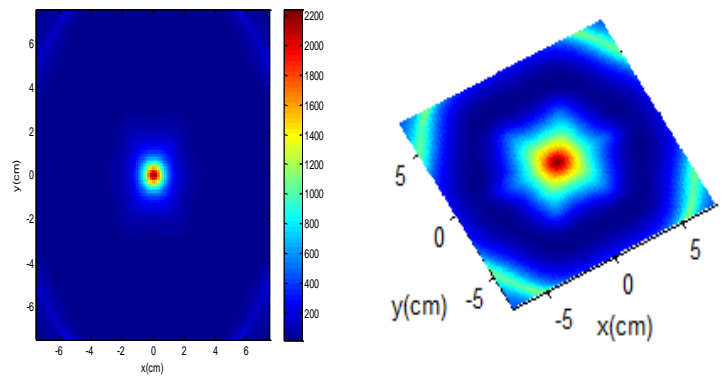


Figure 13: Lower dielectric polygon shape model using 4GHz objection

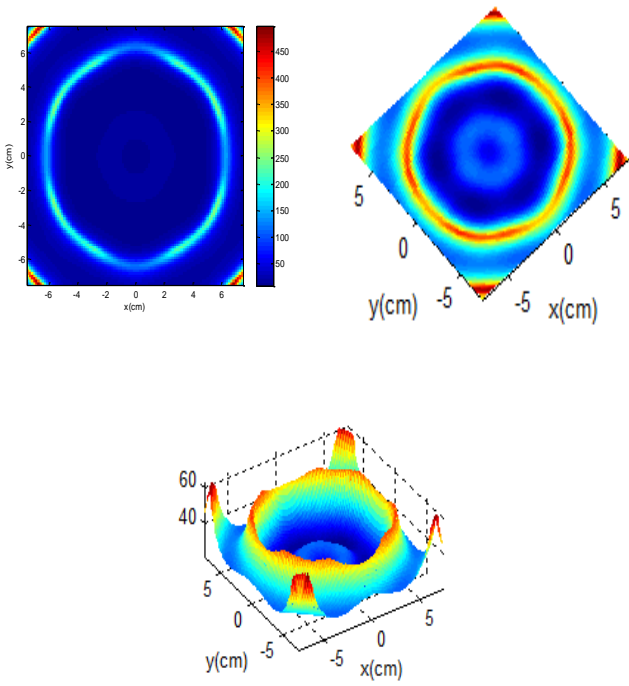


Figure 14: Metalic Polygon Shape Model and Different Angle of View Using 4GHz Objection

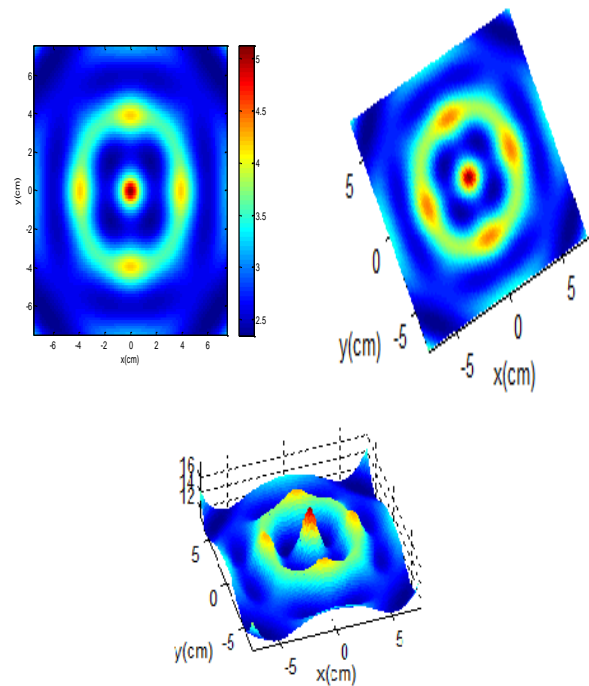


Figure 16: Lower Dielectric Square Shape Model and Different Angle of View

F. Square model using 4GHz frequency

Figure 14 shows the construction of the square model in FDTD containing relative dielectric of 1.4. The dimensions of the square are 15cm x 15cm. The results of the Matlab simulations are shown in figure 15 below. Figure 16 shows a very clear square shape boundary, with the middle of the square showing peak spotlights. When changing the dielectric properties of the square with dimensions of 15cm x 15cm to metal (PEC), the following results in figure 17 will appear. As we can see from the models below, the details inside the models has been shown; these have directed the viewer to similar shapes projected earlier using 40 antennas.

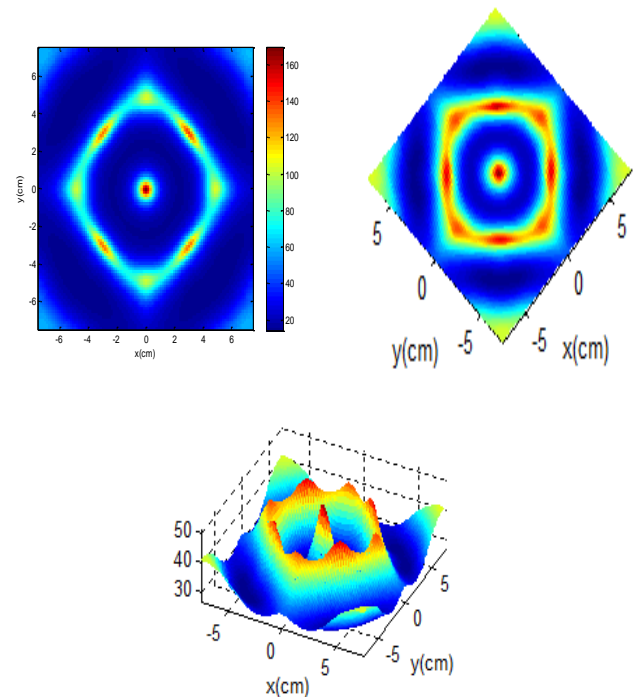


Figure 17: Metalic Square Shape Model and Different Angle of View

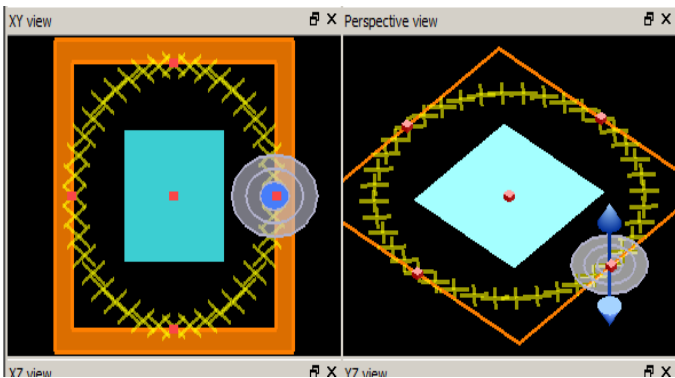


Figure 15: Square Shape Model in Lumerical FDTD Software

G. Cylinder model using 4GHz frequency

Figure 17 below shows a cylinder with a radius of 5cm and defined relative dielectric of 1.4 constructed in Lumerical FDTD. It shows in figure 18 a very clear image of this type of the cylinder, even though the dielectric value of this material is low. Figure 19 shows an extended target of a cylinder with a radius of 10cm and the index is a perfect electric conductor; this is considered to be metal in the simulation. There is a very nice shape as this cylinder has been achieved by 4GHz microwave objection. Figure 20 shows how a 4GHz pulse can image contraband material of 2cm radius, with a relative dielectric value of 1.4 imbedded inside a box of 15cm x 15cm dimension and dielectric value of 3. The box is assumed to be the human body medium.

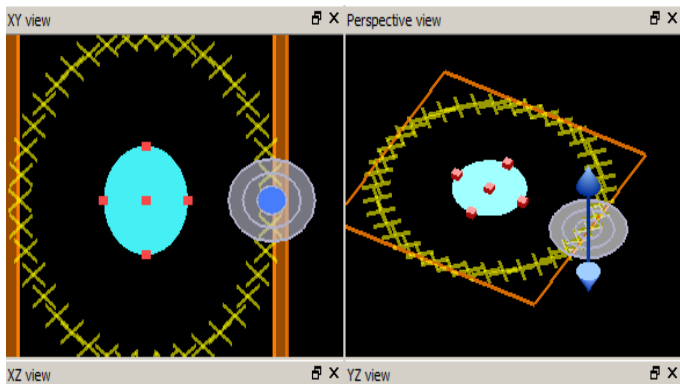


Figure 18: Cylinder Model with 5cm Radius

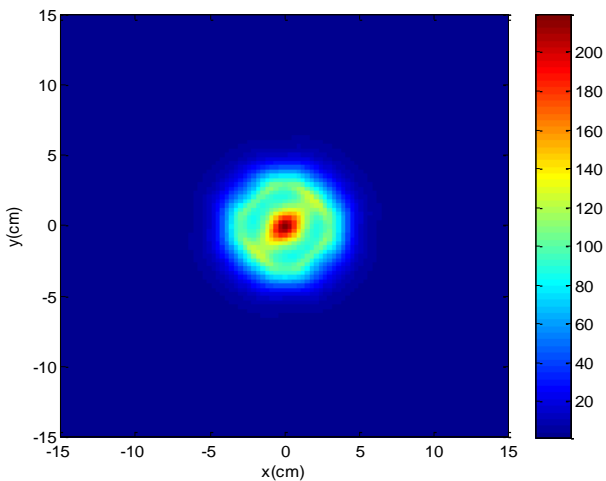


Figure 19: 5cm Cylinder Using 4 GHz Objections

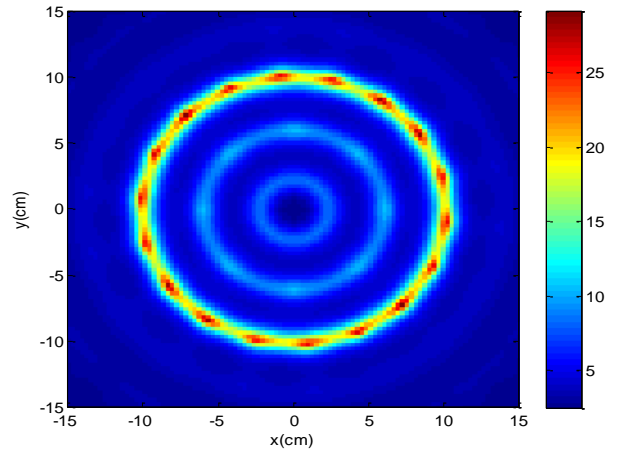


Figure 20: Cylinder of 10cm Using 4GHz

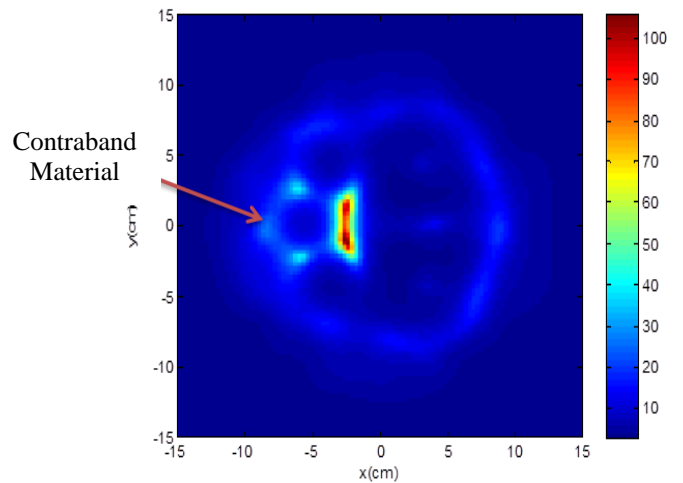


Figure 21: 2cm Hidden Target

H. Square model using 4GHz frequency

A square shape model has been constructed similar to Figure 14 above, and the results of the image reconstruction are shown in the figure 21 below. Figure 21 shows that the shape of square has been detected when applying 5GHz. The relative dielectric of the square was 1.4, and the dimensions of the square model are 15cm x 15cm. Now, if the material of the square changes to metal, then the results would show the following image in figure 22. Figure 22 shows that clear boundary lines of the square have been detected after image reconstruction.

I. Square model using 7 GHz frequency

A 7GHz projection on a square shape shows the shape of a square very clearly, as shown in Figure 23 below. The square has a relative dielectric of a perfect electric conductor or metal. The dimensions are 15cm x 15cm. Now, if we change the material of the square to a lower dielectric property such as 1.4, the result would be as follows in figure 24. The below figure 24 shows a similar but slightly different shape to the previous figure. The four boundary edges of the square show a high peak of spotlight.

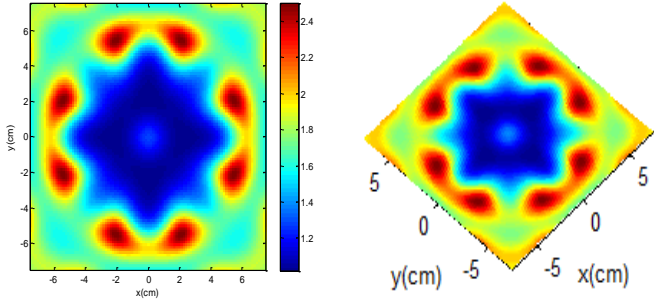


Figure 22: Lower Dielectric Square Shape Model, Dimension 15cm x 15cm and Different Angle of View Using 5GHz Objection

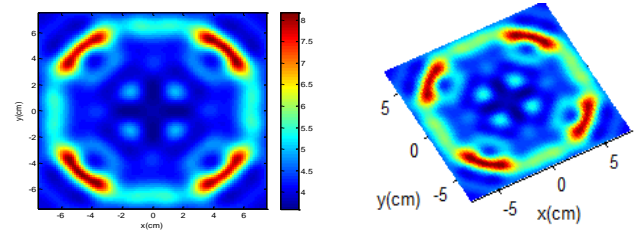


Figure 24: Metallic Square Shape Model Using 7GHz Objection

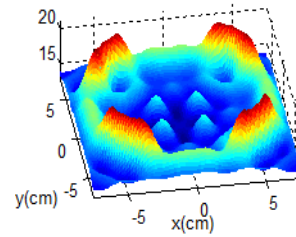


Figure 25: Lower Dielectric Square Shape Model Using 7GHz Objection

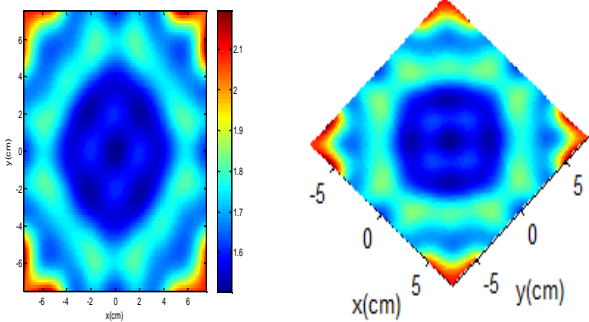
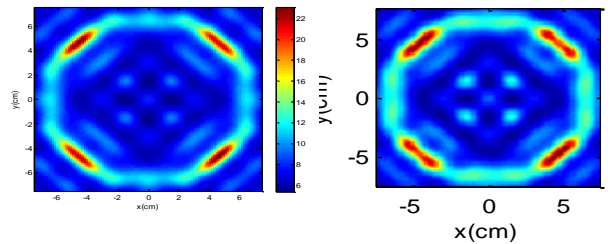


Figure 23: Metallic Square Shape Model Using 5GHz



J. Polygon model using 7 GHz frequency

A polygon model shape relative dielectric of 1.4, constructed the same as Figure 11 above in Lumerical FDTD, showed very clear peak points of all six edges of the polygon after image reconstruction in Matlab. This is shown in Figures 25 below. Now if we change the material of the polygon to metal (PEC) then the results would be as shown in Figure 26. As seen from figure 26, clear polygon boundary lines have been detected after image reconstruction on Matlab.

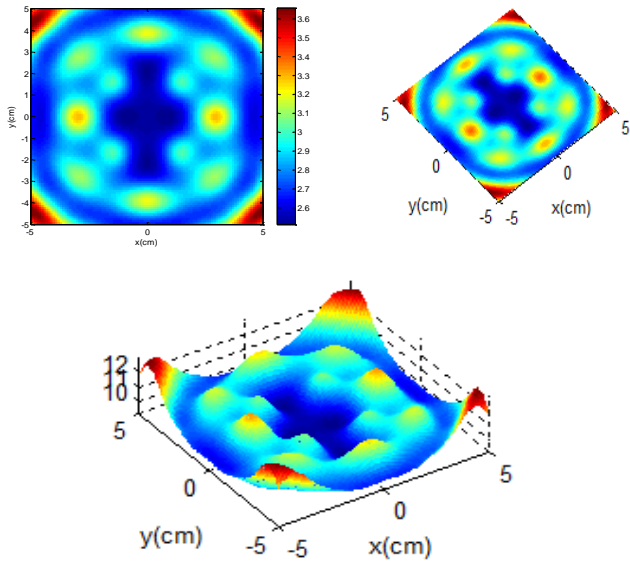


Figure 26: Lower Dielectric Polygon Shape Model Using 7GHz Objection

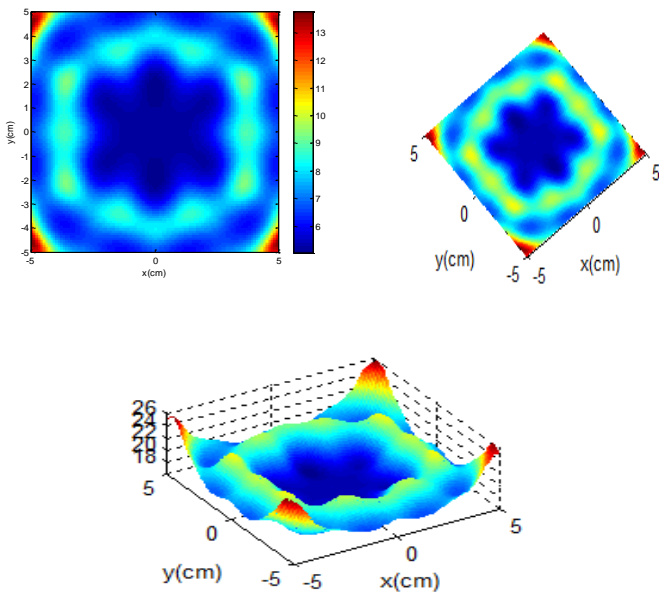


Figure 27: Metallic Polygon Shape Model Using 7GHz Objection

K. Spher model using 7 GHz frequency

Figure 27 shows the construction of a sphere model with a radius of 8cm. Figures 28 below show a sphere shape with a radius of 8cm and relative dielectric of 1.4. After simulation in MatLab, very clear boundary lines of the sphere shape can be seen.

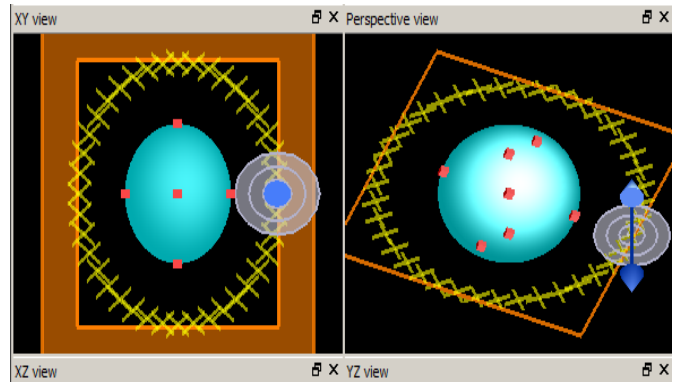


Figure 28: Sphere Shape Model in Lumerical FDTD Software

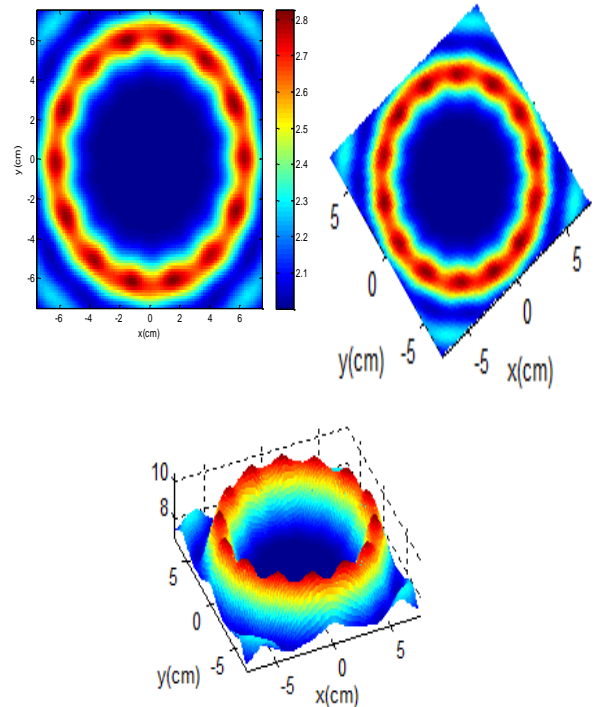


Figure 29: Sphere Shape Model Using 7GHz Objection

Now, metal in the shape of a polygon has been embedded inside the sphere to test the imaging results. This shows if it is possible to differentiate between two materials or if hidden material can be shown. Figure 29 shows how to construct this in FDTD. The idea of the illustration shown below in Figure 29 comes from the possibility of a metallic gun being hidden underneath human clothing. Normally the guns and knives used for terrorist acts are metallic. Figure 30 shows details of a polygon inside a sphere, and shows the sphere also. The polygon is PEC and the sphere is 1.4 dielectric. Now if the material of both models is shown the other way round, i.e., metal for the sphere and 1.4 for the polygon, then the results will be as shown in Figure 31 below. A lower dielectric polygon that could be hidden in any metallic object; this might be how terrorists or smugglers smuggle their illegal materials in metallic objects. Figure 31 below clearly shows how easy it is to detect materials imbedded in other material. This is an example such as when a terrorist implants objects in their baggage. It shows the boundary of the polygon and, inside it, also the boundary of the sphere. As you can see from the below figures, the models have been shown clearly with low or higher dielectric properties. It can be seen from all the above results that 7GHz can show very clear images.

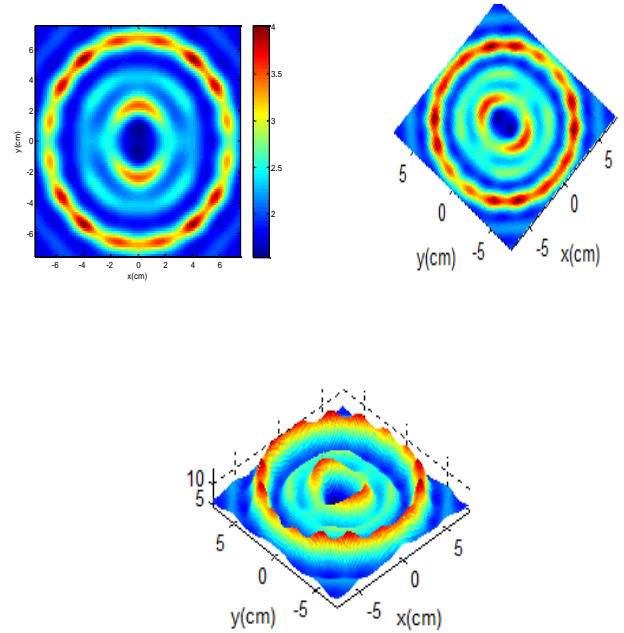


Figure 32: Lower Dielectric Polygon Model inside Metallic Sphere

L. Cylinder or human torso cross section using 7 GHz frequency.

The below figure 32 shows how to construct a 10cm radius of a cross-section shape model, assuming it could be a human torso. As you can see from the below figure 33, a 10cm radius circle that could be related to the human body cross-section is shown very clearly. The dielectric of the torso was 6 in this simulation. There is a good peak of spotlights around the cross-section that helps the viewer to visualise this model without any confusion.

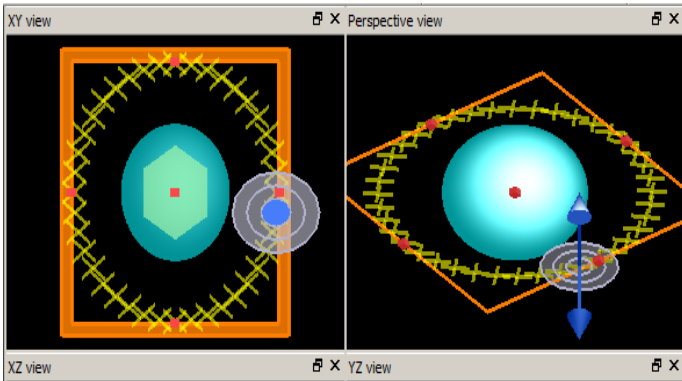


Figure 30: Metallic Polygon inside Sphere Model

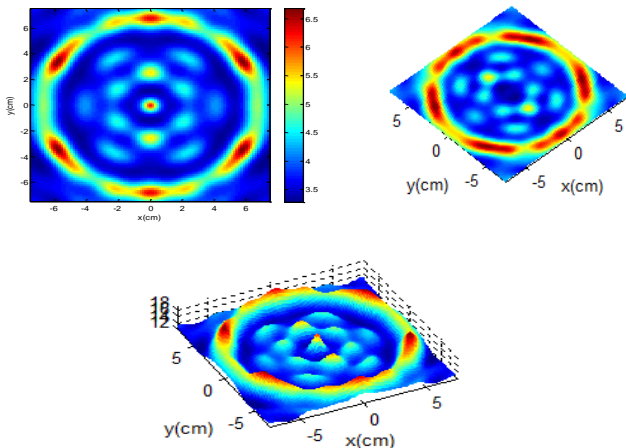


Figure 31: Metallic polygon hidden inside sphere

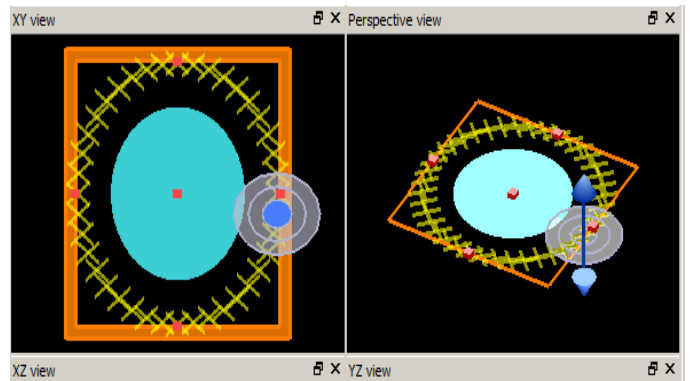


Figure 33: Circle Model, Assumed to be Human Torso

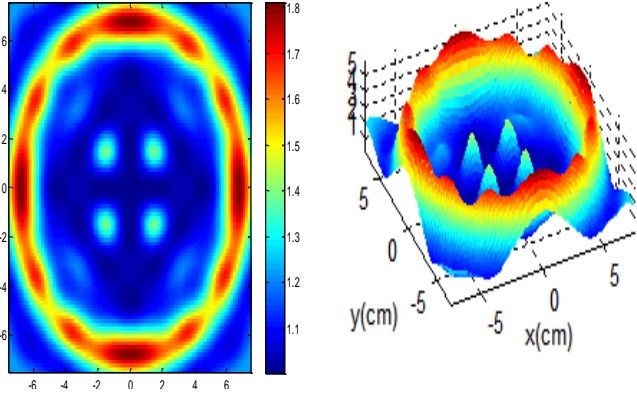


Figure 34: 10cm Radius Object, Assumed to be Human Torso using 7GHz Objection

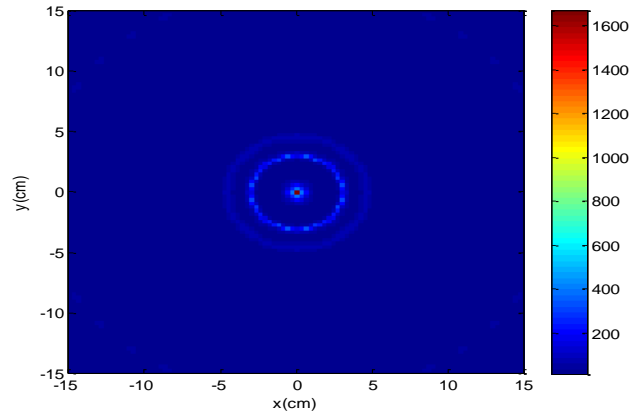


Figure 36: 10cm Radius Object

M. Square model using 10 GHz frequency

The figure 34 below shows shape details that could lead the viewer to a square shape. More detail is shown at 10GHz, which means the higher the frequency the better the image. On the other hand the smaller the wave length the higher the resolution that this robust TR-MUSIC algorithm could generate. Figure 35 shows the result from omitting a 10GHz microwave and shows a circle of 10cm radius that can be seen perfectly clearly; the inner shape of the material is also shown very clearly. This concludes that the higher the frequency the clearer the image.

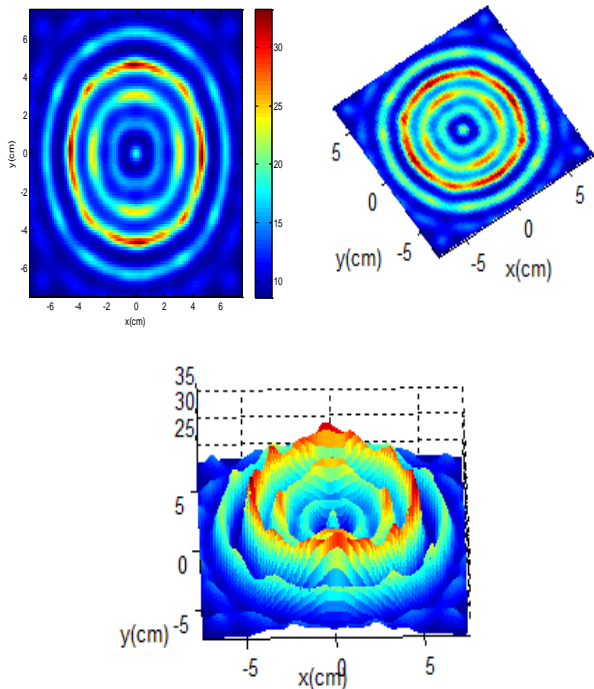


Figure 35: Metallic square Shape Model Using 10GHz Objection

V. CONCLUSIONS

This paper has concluded and proved that microwaves can be used in imaging for security systems, as shown from the simulation results. It has also proved that TR-MUSIC is a perfect algorithm to process data collected from circular arrays of antennae to give robust imaging results. It has also been proven that the higher the frequency the clearer the image and that different materials dielectric embedded in other material can be shown clearly. The future development to this project is to build a prototype of such security system using TR-MUSIC algorithm.

VI. ACKNOWLEDGMENT

The authors wish to acknowledge the financial support of the United Arab Emirates Government and its Embassy in London, also wish to acknowledge the financial support of UAE Government in Abu Dhabi in the form of sponsoring doctorate at the University of Sussex.

REFERENCES

- [1] "Madrid Train Station Blasts Kill 190," *FoxNews.com*, 11-Mar-2004. [Online]. Available: <http://www.foxnews.com/story/2004/03/11/madrid-train-station-blasts-kill-10>. [Accessed: 28-Oct-2013].
- [2] "Terror attacks at Russian transport double in 2010: official." [Online]. Available: http://news.xinhuanet.com/english2010/world/2011-03/02/c_13756267.htm. [Accessed: 01-Aug-2013].
- [3] "British airports on alert over fears that terrorists are plotting attack using 'human bombs' - Irish Mirror Online." [Online]. Available: <http://www.irishmirror.ie/news/world-news/british-airports-alert-over-fears-3806303>. [Accessed: 01-Aug-2014].
- [4] "Domodedovo International Airport bombing," *Wikipedia, the free encyclopedia*. 20-Jul-2013.
- [5] "Attempted assassination of Saudi Deputy Interior Minister fails," *Al-Shorfa*. [Online]. Available: http://al-shorfa.com/en_GB/articles/meii/features/2009/09/02/feature-02. [Accessed: 05-Aug-2014].
- [6] "2012 Peshawar airport attack," *Wikipedia, the free encyclopedia*. 27-Jul-2013.

- [7] "Taliban launch large attack on Kabul international airport | Reuters." [Online]. Available: <http://www.reuters.com/article/2013/06/10/us-afghanistan-attack-airport-idUSBRE95900P20130610>. [Accessed: 02-Aug-2013].
 - [8] "Westgate shopping mall attack," *Wikipedia, the free encyclopedia*. 25-Jul-2014.
 - [9] "Articles on Ideology | TRAC." [Online]. Available: <http://www.trackingterrorism.org/ideology>. [Accessed: 01-Aug-2013].
 - [10] "Global Agenda Council on Logistics & Supply Chain Systems 2013," *Global Agenda Council on Logistics & Supply Chain Systems 2013 / World Economic Forum*. [Online]. Available: <http://www.weforum.org/content/global-agenda-council-logistics-supply-chain-systems-2013>. [Accessed: 28-Oct-2013].
 - [11] S. Almazroui, W. Wang, and G. Zhang, "Microwave imaging using sub-space based TR-MUSIC method for security applications," 2012.
-

Sultan Almazroui is a researcher in the field of Security Management at the University of Sussex. He received his bachelor degree of electromechanical engineering and Master of Science in Embedded Digital Systems from the University of Sussex, Brighton City, in 2003 and 2005, his research interest is in the area of microwave imaging in the field of security applications. He is a member of IEEE and sponsored by the government of United Arab Emirates.

OVERCOMING BARRIERS TO CLIENT-SIDE DIGITAL CERTIFICATE ADOPTION

Karim Sultan

Faculty of Graduate & Postdoctoral Studies
University of Ottawa
Ottawa, ON, Canada

Umar Ruhi

Telfer School of Management
University of Ottawa
Ottawa, ON, Canada

Abstract— Public Key Infrastructure (PKI) is a critical component of any cybersecurity strategy, yet diffusion rates have been dismal within the greater Internet community. Multiple barriers to adoption of client-side certificates exist, including technical complexity, economical burden, legal compliance and social awareness. Entrenched industry practices dating from early Internet-era ideals have obstructed disruptive innovation in this space. Consumer adoption of client certificates is arduous, causing the current deployment model to fail at the general user level. This paper explores the client digital certificate further while identifying barriers to acceptance. A proposal is made for the issuance of “very-low assurance” digital certificates via a Web API, offering one-click simplicity.

Keywords—Public Key Infrastructure; PKI; Digital Certificate; Personal Certificate; Client-side Certificate; Technology Adoption

I. INTRODUCTION

The origins of Public Key Infrastructure (PKI) date back several decades [1, 2], yet its diffusion within the realm of end-user security applications has been slow, with limited uptake [3, 4]. An essential component of PKI is the digital certificate, a record which binds a public key to an entity via a trusted third party (TTP). The digital certificate can be proliferated safely to other parties for transactions requiring encryption, or can serve as the basis of sealing binary information with a digital signature.

PKI uses digital certificates to provide functionality for confidentiality, integrity, non-repudiation, authentication and authorization [1, 2]. Digital certificates are available for server-side use as an underlying mechanism for various authentication, encryption, and security communication protocols (e.g. VPN, IKE, SSL), as well as for client-side use to enable applications such as encrypted messaging via secure email (S/MIME), data encryption, and digital signatures. Various terms have been used in the extant academic and industry literature to refer to downstream client-side digital certificates, including personal certificates, end-user certificates, and client certificates [5]. In this paper these terms are used interchangeably.

Despite their simple definition and role, digital certificates are complex. Acceptance of the technology on the client side has been practically non-existent. Barriers to technology adoption include technical, economical, legal and social. Digital certificates are not simple for the general user to obtain,

deploy and manage. The industry as a whole has maintained a “black hat” mystique of PKI resulting in a failure to disseminate practical knowledge to drive greater adoption. Many users are unfamiliar with the concept of digital certificates despite recognizing a need for greater cybersecurity.

Digital Certificates offer a methodology for enabling PKI on an individual level, yet usage remains server-side oriented. Whereas it is common for a web site to have a digital certificate in order to offer HTTPS, it is rare for the average Internet user to possess one. Internet security is a major concern of consumers and digital certificates are essential for establishing trust. Digital certificates achieve online authentication allowing parties to perform transactions confidentially. The core technology for e-commerce is SSL, which supports the use of client-side digital certificates, yet nearly all transactions involve only server-side certificates. Client-side certificates were introduced as part of SSL version 3 around two decades ago [6, 7] to enable end-users or their devices to request authenticated access to a specific service. This authentication method provides additional level of security for client identity verification. Despite a compelling argument for personal PKI, barriers to client-side adoption have caused technology diffusion to lag and stall.

The dominant format for digital certificates is X.509v3. The X.509 PKI standard defines a digital certificate as a data structure that binds a public key to a person, computer, or organization, and verifies the identity of public key’s owner [2]. The structure has changed little over its lifespan, using a somewhat archaic format (ASN.1) in the era of XML and text-based representations. Standards are beneficial yet the convoluted nature of PKI’s entrenched practices has become a barrier to disruptive innovation. This inherent complexity remains an obstacle. The typical process in setting up PKI digital certificates includes various steps such as registration, verification, installation, publication, and renewal [8, 9], and these can be cumbersome to adopt for the end-user.

The advent of cloud services drives both a greater need for client-side certificates as well as a potential model for their management. With the emergence of computational grids, the Internet of things, and virtual organizations enabled through a cloud computing infrastructure, end-users as well as the resources and services they need access to on a regular basis span many different geographical and organizational contexts.

Consequently, there is a greater need to use mechanisms such as personal PKI certificates for identify verification and authentication of end-users requesting access to online resources and services in such distributed online environments [10]. Furthermore, with the advent of IT consumerization and Bring Your Own Devices (BYOD) initiatives in organizations, efficient mechanisms for digital certificate enrollment and provisioning are becoming a necessity for these organizations [11]. Wider acceptance of PKI end-user certificates would translate into the potential for PKI to be utilized not just within the realm of closed and controlled environments like online banking and e-commerce, but over an expansive context of different applications and services across a number of different trust domains.

Our proposed solution would enable the adoption and use of white identity certificates, i.e. certificates that are not issued for specific applications, but act as a flexible credential that could be easily re-used across different applications and trust domains [12].

Alternatives such as Pretty Good Privacy (PGP) [13, 14] and Identity-based Encryption (IBE) [15, 16] have been previously been recommended as potential solutions to alleviate the acquisition and maintenance barriers associated with public key and certificate management for end-users. However, these alternatives are not flawless and have their own specific problems – such as subjective trust assignments in PGP [17], and cumbersome revocation mechanisms in IBE [18, 19]. By trading some security assurances for ease of access, a balance can be struck which provides seamless, behind the scenes client-side certificate management to end users via cloud services.

II. DIGITAL CERTIFICATES

The classic X.509 digital certificate (also known as a public-key certificate) originates from the ITU-T; later, the IETF spearheaded Internet related proposals. The IETF defines a digital certificate as “a certificate document in the form of a digital data object... to which is appended a computed digital signature value that depends on the data object.” [20] Oppliger expands with “a certificate attests to the legitimate ownership of a public key and attributes a public key to a principal, such as a person, a hardware device, or any other entity” [21]. Vacca identifies digital certificates as the foundation of PKI; it allows the exchange of public keys between parties while assuring, to varying levels of risk, that the parties are who they claim to be. Without digital certificates, no acceptable level of trust could be established, rendering PKI ineffective [22].

The use of digital certificates solves the key distribution problem. It ensures that a public key belongs to an entity, and asserts trust on their behalf via authentication. Authentication is the process of ensuring each party is who they claim to be. Furthermore, authentication implies that a third party cannot masquerade as a legitimate party for a transaction.

PKI relies on the concept of X.509 Digital Certificates to assure authenticity of a party. Digital Certificates contain identity information of a party, as well as the party’s public

key. Certificates can be queried from a directory maintained by an authority, but in practice they are often presented by the parties. The onus is on each party to independently validate the other’s certificate.

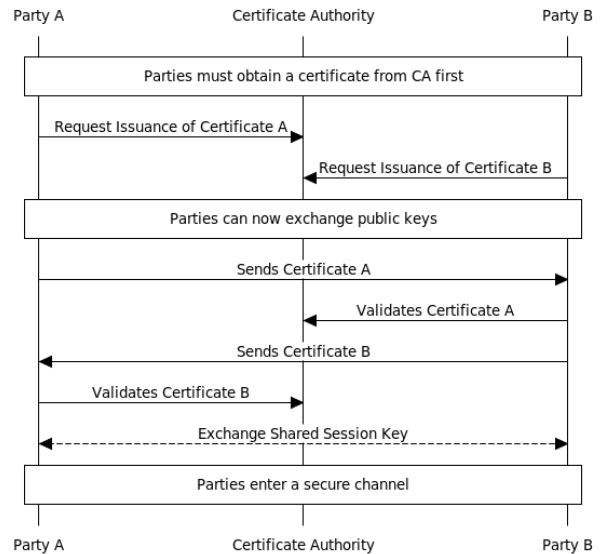


Fig. 1. Public Key Certificate Exchange

The X.509 standard relies on a complex and convoluted binary syntax known as Abstract Syntax Notation 1 (ASN.1). The intricacy of implementing a validating ASN.1 parser, the elevated licensing costs of third party solutions, and its regulated name-space have made certificates unapproachable to the general development community and soundly in the hands of specialist (such as Verisign) who charge premium prices for their services [22, 23]¹.

Digital certificates are based on trust. A trusted authority forms the root of a hierarchy and vouches for the trustworthiness of every certificate underneath it [24]. It does this via a signing process, after due diligence criteria have been fulfilled. The path through the hierarchy is called a certificate chain, with each child node being validated by the parent node.

The root authority, also called a certificate authority, is not vouched for. Instead, it must demonstrate its integrity by adhering to strict policies, both as industry best practices (such as hardware key storage) and de facto standards (such as those put forth by the CA/Browser Forum) [25, 26].

Certificates provide the necessary bridge between parties by asserting the identity is valid, and providing the corresponding public key(s) and algorithms. They allow parties to assign a level of trust to each other, and determine whether to proceed with a transaction [27].

There are many issues surrounding digital certificates, such as certificate expiration, renewal practices, wrongful issue of

¹ Attempts to introduce XML notation have been made by major players (such as Microsoft) but remain largely non-adopted.

certificates, CA malpractice and a lack of a formal standard. A compromised certificate renders all future transactions invalid, until the encryption keys are regenerated [28]. Regardless the value certificate authorities bring is such that a PKI infrastructure wouldn't be possible without them.

III. PUBLIC KEY INFRASTRUCTURE

PKI relies on digital certificates to bind public keys to entities. This allows the public key to be validated and distributed. The IETF defines PKI as “a system of Certificate Authorities [and their delegates] that perform some set of certificate management [...] functions for a community of users in an application of asymmetric cryptography” [20]. At a broader level, Davis defines PKI as “the set of hardware, software, personnel, policies, and procedures required to create, manage, store, distribute and revoke public keys” [29]. Davis views PKI as a holistic solution with comprehensively interconnected parts. In contrast, Vacca defines PKI as including “services and protocols for managing public keys [through digital certificates]” [22].

Essentially PKI must provide three services: register entities and issue digital certificates; manage certificate lifespan; and provide an archive to ensure certificate validation at a later date [20].

A. Key Distribution Challenge

If digital certificates are the cornerstone of PKI, then the Key Distribution Challenge is its raison d'être. The challenge is to distribute the secret key to all involved parties. A shared key must be distributed in advance of communicating – but how does one distribute this key securely? A chicken-or-the-egg scenario arises. Public / private keys revolutionized the cryptographic realm by allowing the publishing of a public key for encryption while secreting a private key for decryption.

Ciphers can generally be classified as symmetrical or asymmetrical. In a symmetric-key cipher (also known as Secret or Shared Key Cryptography) parties share the same key for both encryption and decryption. The key must be exchanged out of bounds and known to each party. The IETF defines symmetric cryptography as “a branch of cryptography involving algorithms that use the same key for two different steps of the algorithm... such as encryption and decryption” [20].

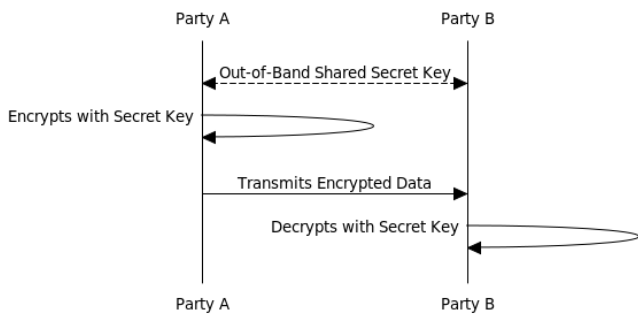


Fig. 2. Symmetric Cryptography: The challenge remains distributing the key

Symmetric encryption algorithms are usually faster than their asymmetric counterpart, having efficiency benefits in processing and memory; yet their greatest challenge is the secure distribution of the key.

Asymmetric Cryptography (also known as Public Key Cryptography) is defined as “a modern branch of cryptography... in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm” [20].

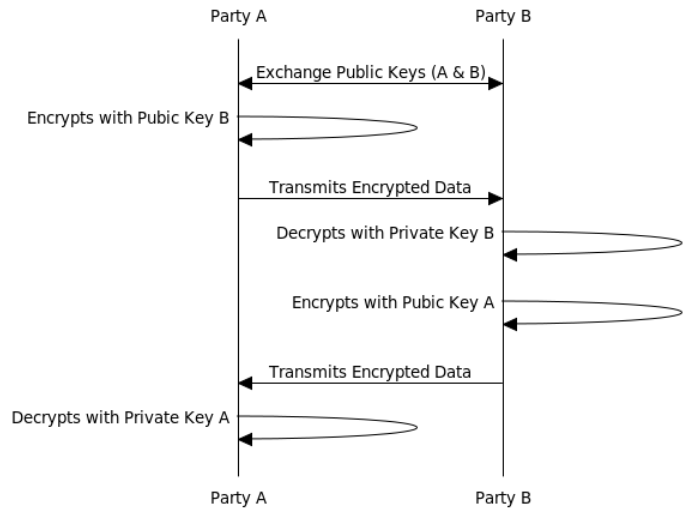


Fig. 3. Asymmetric Cryptography

This approach uses two different keys which are mathematically related. One is public and distributed while another is private and kept secret. The two keys are selected such that it is computationally infeasible to determine one from the other. One key is used for encryption (traditionally the public key, but there are special cases which use the private key) and only the other key can decrypt the data. Asymmetrical algorithms are computationally intensive, thereby incurring a sometimes severe performance penalty. Public Key Cryptography relies on digital certificates for the distribution of public keys and on Public Key Cryptography Standards (PKCS) for the secure storage of private keys [22].

Hybrid encryption is defined as “an application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption” [20]. Hybrid algorithms often use asymmetric-keys to transfer a session key, which is then used for encryption purposes via a symmetric-key algorithm. This approach has the benefit of public key security for key exchange, while gaining the performance advantages of shared key algorithms. Asymmetric algorithms generally require more computational resources than the equivalent strength symmetric ones, and therefore are not usually used for confidentiality except in distributing symmetric keys [20]. The SSL protocol uses hybrid cryptography.

B. Trust Management

All of PKI hinges on the establishment of trust between a user agent and an end entity. A user of PKI must be able to assess a certificate for trustworthiness in order to decide whether to proceed with a transaction or not. At the human interface level, this involves a judgement call based on the credibility of the notarizing party or parties and their ability to vouch for the certified entity. At the machine level, this requires a valid, unrevoked certificate digitally signed by a CA, for which the relying party has pre-approved and registered in a trusted root authority list.

Trust management is the shiny side of risk management: *“Trust management is surely exciting, but like most exciting ideas, it is unimportant. What is important is risk management, the sister, the dual of trust management. And because risk management makes money, it drives the security world from here on out”* [21]

Assessing whether one can trust is party is akin to determining the acceptable level of risk and potential loss. Therefore, to properly manage trust, one must validate both the trust model and the risk analysis.

C. Certification Authorities

A Certification Authority (alternatively, Certificate Authority or CA) is *“an entity that issues digital certificates... and vouches for the binding between data items in a certificate”* [20] CAs are a trusted third party that relying parties can assign trust to. If a CA is trusted, then all certificates issued by the CA are trusted. This does not necessarily mean that the certificate holder can be trusted, however. The CA model is designed to promote accountability over protection, and therefore is a reactive system (if party is wronged, there is a path to recourse) instead of a proactive system (party can't be wronged). Despite this hurdle, the CA model has flourished with approximately 700 active CAs in 2015. Not all CAs are created equal; each has similar responsibilities but the manner in which these responsibilities are discharged vary widely. An entity's digital certificate can be obtained either directly from the party, or through the associated CA. A CA not only vouches for the certificate holder, but they must also provide a suite of certificate management functions to both the certificate owner and the Internet community.

D. Validation Classes

The CA is responsible for verifying an applicant's identity prior to issuing a digital certificate. There are several classes of validation that have been standardized in the industry [5, 9]:

- Class 1: Basic Validation – involves minimal validation for the client, often based on confirmation of domain or email ownership. It rarely involves manual validation. This is the least trustworthy approach and is sometimes called a “low assurance certificate.”
- Class 2: Organization Validation – Considered the standard class for most SSL e-commerce servers. This class requires various corporate identity documents,

including Articles of Incorporation, tax filings, shareholder data, and CEO authorization. Note that an Identity Validation variant exists for personal digital certificate issuance.

- Class 3: Extended Validation – An EV certificate is a “high assurance certificate”. It involves a rigorous audit of the applicant, and requires the highest level of corporate identity declaration: in addition to Class 2 requirements, an organization will need to show proof of bank accounts, registered trademarks, credit cards, and a certified legal letter of acknowledgement. Class 3 EV certificates receive special treatment in browsers, with color highlighting and visible assurances to the user.

IV. CLIENT SIDE CERTIFICATES

Client-side digital certificates are applied to the user instead of the server. Whereas a server-side digital certificate likely applies to an enterprise entity, a client-side digital certificate is targeted to an individual. Two common applications of client-side digital certificates are secure email (S/MIME) and virtual private networks (VPNs). In these applications, the individual is likely to be in a corporate realm, and part of a larger PKI initiative including enterprise sponsored training and provided storage solutions. For the general population, client side digital certificates still have many applications, ranging across the security model: confidentiality (i.e., email, encryption), integrity (i.e., code signing), non-repudiation (i.e., digitally signing documents), and authentication (i.e., single sign-on, VPN).

A. Issuance

Through the use of a helper application, an individual generates a public / private key pair, and creates a certificate signing request (similar to how server side digital certificates are generated, explained earlier). The CSR is submitted to a CA who then performs validation. Validation options vary for individuals and are not as intensive as for enterprises. Currently, individuals may only apply for Class 1 and Class 2 certificates (as follows). Class 2 personal certificates involve manual verification of an individual's identity through examination of passport, driver's license and federally issued photo ID. Although it provides more assurance than a Class 1 certificate, it is still open to identity fraud as there is no face-to-face validation of the photo ID. Note that individuals are not permitted to apply for Class 3 Extended Validation certificates.

There is usually a cost component for validation, although some reputable CAs will provide Class 1 Basic Validation certificates for free after validation (usually with usage restrictions). Cost of digital certificates remains a barrier to adoption; one study showed that even when the initial digital certificates are provided free of charge, 93% of users would not pay the renewal charge once the certificate expired [30].

B. Private Key and Digital Certificate Storage

The storage of digital certificates and their corresponding private keys is difficult for enterprises even under a full PKI

deployment. Asking end users to manage this information responsibly and securely is an impossible task. Bromby identifies the storage and security of the private key as the weakest link in PKI; he states that “if [the key is] exposed, allows other parties to both decrypt messages and to transmit fraudulently signed messages; and if lost, prevents the original owner from de-coding incoming messages” [31]. Bromby introduces the potential for biometrics to be used to tie a private key to an individual, in which “a unique key can be generated that does not require secure storage as it is encapsulated within the biological make-up [of the individual]” [31]. Revocation of a biometric key remains a barrier and is a focus of current research in the field.

Software based technologies such as digital wallets and lockboxes, and hardware solutions such as smart cards and token generators, are often provided by organizations to their employees to assist with key storage. The proliferation of smart phones may help extend solutions to the general population; however, the storage and use of personal digital certificates continues to carry inherent complexity and requires an educative component.

Most modern browsers (Chrome, Firefox, and IE) support direct installation of certificates via their certificate managers into PKCS #12 containers²; however the procedure is still too complex for the average user. This is readily confounded by the use of different digital certificate caches per browser. Not all browsers are required to package the same trusted CAs on deployment, and they do not use an OS specific / machine specific common store by default. Therefore, a CA trusted in one browser may not necessarily be pre-installed on a different one. The WebTrust seal [32] is used as a common standard for CAs to be accepted into browsers, but not all trusted CAs carry the seal.

Portability of client-side digital certificates is a concern for users. Whereas a server-side digital certificate is commonly tied to a single host, their client-side counterparts need to work across multiple devices: personal computers, laptops, smart phones, and even embedded devices such as gaming consoles. Server-side digital certificates often rely on a PKI solution for management across an enterprise. Client-side digital certificates on the other hand will not have access to expensive and complex PKI solutions nor will their users have the inclination to learn such systems. As a result, a multiplicity issue arises; server-side certificates can be bound one-to-one (1:1) to a device (i.e., a web server or a VPN router) while client-side certificates need to be bound to the user instead, in order to permit a one-to-many (1:∞) relationship to the user’s multiple devices.

C. Adoption

Due to the roll-out of PKI solutions at corporations, employees are more likely to be issued a digital certificate than a member of the general population [21, 22]. Despite being classified as personal certificates, these can be considered a

special case as they are usually the result of a corporate mandate and are packaged with training and support. The general web user on the other hand is left with a bewildering set of options for management.

Barriers to adoption include technical (complexity), social (education and awareness), economical (costs) and legal (compliance) factors. One study found the deployment of digital certificates to be a complex task even for several computer scientists holding PhDs [32]. A program in Denmark to offer every citizen a free digital certificate saw an uptake of less than 3% of the population after 3 years [33]. Legal compliance can be a deterrent for adoption, as it adds uncertainty and doubt into parties’ responsibilities. The use of digital signatures is legally binding in many countries. Since the passing of a digital signature act in the EU, adoption has stalled. Many users don’t believe the relative advantages outweigh the perceived usefulness [33].

Lim reviews a study conducted in Hong Kong in 2004 [30]. As part of a government initiative, smart cards were distributed to approximately 7 million residents. Afterwards, residents were offered a free personal digital certificate. The study sought to examine digital certificate adoption. When enabled with digital certificates, the smart cards could partake in a wide range of services covering email security, e-commerce, and government interactions. Despite being freely available, after the first year less than 6% of the population had opted for one. Lim determined that a high Internet connectivity rate or even digital certificate ownership did not lead to user acceptance of e-commerce [30].

The results matched other studies conducted in Finland and Germany. Even low costs (~\$15) for renewals were spurned. Technical audiences were no more likely to renew. In Hong Kong, 54% reported no understanding of PKI; 66% did not know how their digital certificate could be applied. Lim concluded that for there to be any traction of free digital certificates, the government would need to conduct training and awareness programs [30].

D. Cloud Based Security

The emergence of the cloud as a ubiquitous platform for information technology has started to redefine the application of security principles. The cloud is a group of services accessible to users remotely. When it comes to cloud security, there is often an immediate concern as to who owns the data, and whether a third party cloud-provider can be trusted with it [25]. To counter this, leading cloud-providers (such as Amazon, Microsoft and Google) have worked to make their data centers secure – usually more secure than the average enterprise could accomplish. The use of any service model requires a security model, and PKI is the ideal infrastructure to roll out as the cloud provider can niche their expertise and offer it as a commodity to the enterprise.

To enforce PKI policies, digital certificates can be used not only as trust assurance, but also as authentication and authorization mechanisms via attributes. Cloud services can simplify the distribution and management of digital certificates, removing this burden from the enterprise and user.

² Public Key Cryptography Standard #12 bundles private keys with an X.509 digital certificate.

Although HTTPS can be used for securing communications, encryption and signing operations face a concern over the location of private keys. Data encrypted at the provider site needs client keys stored remotely. However, encrypting locally may have exhaustive bandwidth requirements. Regardless, the cloud model offers new approaches to applying PKI with variable levels of (light-weight) assurance while protecting mobility and multi-device usability that may help kick-start adoption towards the majority, even if it lacks all the safeguards of a mature PKI implementation. In time, design principles of cloud deployments will orient towards controlling relevant vulnerabilities and threats while improving scope and scale of usability [34].

1) Model for Network Security

Stallings promotes a network security model which is subdivided into five main categories³ [35]:

- i. Confidentiality – Security by protecting data from unauthorized parties. This is accomplished via encryption.
- ii. Integrity – Security by ensuring the received data is the same as the transmitted data. This is accomplished via hashing.
- iii. Non-Repudiation – Security that the message was sent by the transmitting party. This is accomplished via digital signatures.
- iv. Authentication – Security that a source can be trusted. This is accomplished via digital certificates.
- v. Authorization – Security by ensuring a user has permission to act. This is accomplished via access control (and other means such as attribute certificates).

The combination of these categories provides a data security model suitable for e-business applications.

The model and its resultant architecture can be further extended by layering in PKI. The addition of PKI does not require a new security category. Instead, PKI offers a set of guidelines (and constraints) for how the model should be implemented. PKI solves the key distribution challenge and is built on public key (asymmetric) cryptography for key exchange and shared key (symmetric) cryptography for data transmission. It involves a suite of mathematical algorithms covering encryption, hashing, signing and trust-verification. As long as these mathematical approaches remain computationally infeasible to compromise, PKI provides a guarantee of security.

The PKI Model for Internet Security illustrates the five categories working in conjunction. The end result is a secure information channel. Once the secure information channel has been established with a degree of trust acceptable to both parties, business may be conducted. E-Business applications

³ Stallings also introduces a sixth category, “Availability”, but this category is not relevant to our discussion of PKI digital certificates.

range from secure communications to e-commerce to intellectual asset exchange [36].

E. Drivers and Barriers for Acceptance

Of the numerous drivers behind PKI, personal certificate adoption is influenced most by the following factors:

- Cybersecurity – the need for individuals to protect themselves from loss due to cyber breaches, loss, or theft, especially in the smartphone era;
- Privacy – the need to protect transactions and communications from other parties;
- Authentication and Non-Repudiation – the need to prove identity and conduct e-commerce; and
- Innovation – the forward evolution of PKI based solutions to meet the transforming needs of the Internet landscape.

The barriers to adoption however are numerous, and a powerful restraint. Technical complexity has left PKI inaccessible and requires the engagement of expert consultants to progress [37]. The sheer complexity of selecting, deploying, and managing a PKI solution is overwhelming to most enterprises, and the “simpler” elements of private key storage and personal certificate management are hieroglyphics to the general public [38, 39].

Economic factors have a significant impact on personal certificate adoption. As shown in the aforementioned studies, individuals were reluctant to pay even marginal amounts for renewal. Absent government subsidization, individuals are faced with complex fee structures and wildly varying licensing costs due to vendor focus on enterprise revenue.

Social factors are at play as well. The general user has little to no comprehension of the intricacies of personal certificates, nor do they have the inclination to learn about it. The PKI space lacks any simple methodology for un-trained adoption. Many users aren’t aware of the benefits; as a result many consumer applications bypass security needs, falsely reinforcing to the consumer that PKI is not essential. Furthermore, trust models are difficult to reconcile; why should a user trust another entity based on the word of an unknown CA? Finally, there is the one-to-many relationship between users and their multiple devices; this presents challenges not realized in server centric implementations.

The barriers are substantial enough to impact the driving forces. The result is a lack of significant change. A disruptive entry is required to push digital certificate and PKI further into the mainstream, and without the introduction of a seamless/transparent, “one-click” solution, client adoption will never happen at any significant level.

V. PROPOSAL: DIGITAL CERTIFICATE LITE

The current PKI approach is tightly integrated with a client-server model (responsibilities burden each side). There are two approaches for consideration: client centric (increased security

for the user at the expense of simplicity) and server centric (increased simplicity for the user at the expense of security).

The proposal is for a server centric approach: a web API enabled service which can provide higher risk, very low assurance certificates, called Digital Certificate Lite (DCL). Furthermore, the use of a web API for key management resolves the Key Storage problem (as it is CA managed) and the Multiple Device Problem (since any of the user's devices can access the key).

A DCL creates a new validation class as a subcategory of certificate level one. Whereas a Class 1 personal certificate is considered to be low-assurance, the DCL would be best considered "very-low-assurance". It foregoes extensive identity validation but gains transparent interoperability, enabling PKI security functions for end users with zero knowledge requirements.

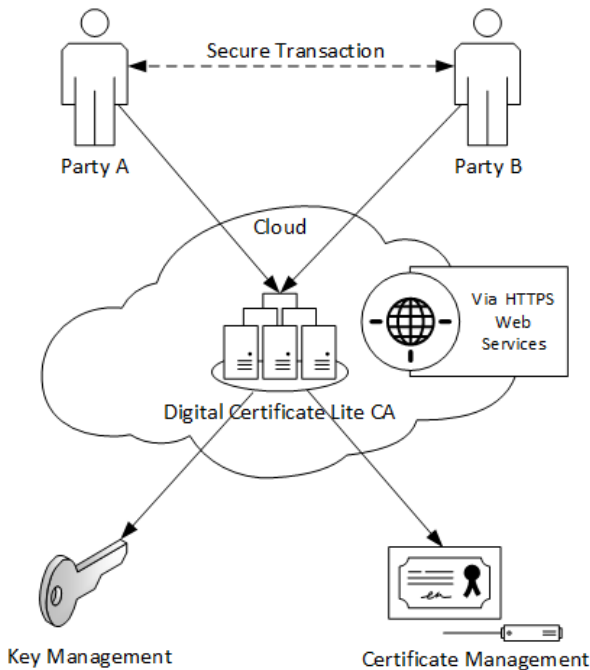


Fig. 4. Context Diagram for Digital Certificate Lite

A user, via a web service enabled user agent, can contact the DCL CA for a wide range of key management functions (such as public/private key pair generation, key storage, etc...) and certificate management (lifecycle and validation).

It is proposed that a WOA based approach be used, with the bulk of the responsibility borne by the service provider. User agents, such as JavaScript code in Rich Internet Applications (RIAs) can be delivered as code-signed modules for execution on the client side automatically when required. The web service provider can also perform all functions on behalf of the client. The increased risk can be considered worthwhile if it drives user adoption. The model can be reformed in future evolutions.

A. Interaction

Two parties wish to communicate securely. In this scenario, both parties are individuals lacking personal digital certificates. The parties can't trust each other to be who they say they are, and they can't solve the Key Distribution Challenge. It is assumed that both parties are using application agents that can consume RESTful Web Services (and which have an API key or pre-established credentials). Party A can obtain a certificate (either prior to the transaction or on demand) via the cloud from the DCL CA. Party B does likewise. Party A and Party B can now authenticate each other, using the other's DCL and the validation web service of the DCL CA.

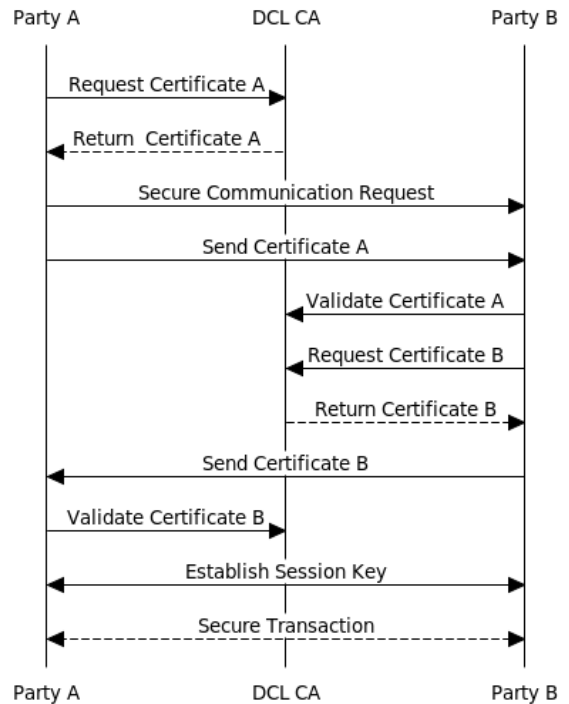


Fig. 5. Two Party Secure Communications

Note that the preferred transport is HTTPS, which not only keeps the web service calls confidential, but also serves as a method of authentication between the consumer agent and the provider service. The use of web services permits the creation of Enterprise Mashups, with the promise of leveraging core PKI functionality in long-tail issues, a realm formerly thought inapproachable. Furthermore, rich internet applications (RIAs) can be built overtop DCL web services to provide secure, confidential interactions between parties on an ad-hoc basis.

VI. CONCLUSIONS

PKI has been prevalent for three decades but technology diffusion has been slow, and PKI has failed to gain the necessary traction for adoption by the general Internet community. This paper has highlighted various reasons for this

lack of adoption, and proposed an alternative low-assurance digital certificate solution to alleviate some of the technology barriers. We contend that a web-services based identity verification and authentication solution is increasingly more suitable in today's environment and would integrate well with other cloud applications that end-users utilize on a regular basis.

To enter a show, one needs a ticket. It is no different with PKI; to take advantage of PKI's full feature set, one requires a digital certificate. Extending digital certificates to the masses through a Digital Certificate Lite approach trades barrier complexity for adoption simplicity, albeit at a loss of assurance. Such sacrifices may well be the only way for personal certificates to overcome the restraining forces they face and drive greater mainstream adoption.

REFERENCES

- [1] S. Chokhani and W. Ford, "RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," 1999.
- [2] S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, "RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," 2003.
- [3] C. Van Der Walt, "SSL - Rumours and Reality: A practical perspective on the value of SSL for protecting web servers," 2001.
- [4] Virtru, "'Why Aren't More People Using Email Encryption?'" The Virtru Blog: Email encryption and digital privacy news, tips, and insights, 2015, [Online]. Available: <https://www.virtu.com/blog/arent-people-using-email-encryption/>. [Accessed 29 July 2015].
- [5] M. Kovinić, "Securing Service Access with Digital Certificates," AMRES Security Group, Cambridge, UK, 2011.
- [6] D. Wagner and B. Schneir, "Analysis of the SSL 3.0 protocol," in Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce, 1996.
- [7] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0," 1996.
- [8] R. Bragg, K. Rhodes-Ousley and M. Strassberg, The Complete Reference: Network Security, New York: McGraw Hill Osborne Media, 2004.
- [9] RSA, "Understanding Public Key Infrastructure (PKI): An RSA Data Security White Paper," San Mateo, 1999.
- [10] M. R. Thompson, A. Essiari and S. Mudumbai, "Certificate-based authorization policy in a PKI environment," ACM Transactions on Information and System Security, vol. 6, no. 4, pp. 566-588, 2003.
- [11] Z. Hallock, J. Johnston, F. Macias, R. Saville, S. Tenneti, M. Jessup, S. Deshpande and T. Szigeti, "Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD," 2014.
- [12] S. Jaweed, "Could there ever be a unitary digital certificate?," Inf. Secur. Tech. Rep., vol. 8, no. 3, pp. 36-44, 2003.
- [13] P. Zimmerman, The Official PGP User's Guide, Cambridge: MIT Press, 1995.
- [14] B. Zajac, "Pretty Good Privacy," Computer Fraud & Security Bulletin, vol. 1994, no. 9, pp. 14-17, 1994.
- [15] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.
- [16] C. Cocks, "An identity based encryption scheme based on quadratic residues," in 8th IMA International Conference on Cryptography and Coding, 2001.
- [17] A. Herzberg, Y. Mass, J. Mihaeli, D. Naor and Y. Ravid, "Access control meets public key infrastructure, or: assigning roles to strangers," in Proceeding 2000 IEEE Symposium on Security and Privacy (S&P 2000), 2000.
- [18] A. Boldyreva, V. Goyal and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15th ACM Conf. Comput. Commun. Secur. - CCS '08, 2008.
- [19] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," IEEE Trans. Comput., vol. 64, no. 2, pp. 425-437, 2015.
- [20] R. Shirey, "RFC 2828: Internet Security Glossary," May 2000. [Online]. Available: <https://www.ietf.org/rfc/rfc2828.txt>.
- [21] R. Oppliger, Security Technologies for the World Wide Web, 2nd ed., Norwood: Artech House, 2003.
- [22] J. R. Vacca, Public Key Infrastructure, New York: CRC Press, 2004.
- [23] J. Davies, Implementing SSL/TLS Using Cryptography and PKI, Indianapolis: Wiley, 2011.
- [24] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, "RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008. [Online]. Available: <http://www.ietf.org/rfc/rfc5280.txt>.
- [25] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, vol. 28, no. 3, pp. p. 583-592, 2012.
- [26] CA / Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3," 16 October 2014. [Online]. Available: <https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf>.
- [27] E. Gerck, "Overview of Certification Systems: X.509, CA, PGP and SKIP," 1998. [Online]. Available: <http://www.blackhat.com/presentations/bh-usa-99/EdGerck/certover.pdf>.
- [28] N. Leavitt, "Internet Security Under Attack: The Undermining of Digital Certificates," Computer (IEEE), vol. 44, no. 12, pp. p. 17-20, 2011.
- [29] C. R. Davis, IPsec: Securing VPNs, New York: McGraw-Hill, 2001.
- [30] N. Lim, "Internet Security and Digital Certificates: How Much Do You Know About Them?," in The Fourth International Conference on Electronic Business, Beijing, 2004.
- [31] M. Bromby, "Identification, Trust and Privacy: How Biometrics can Aid Certification of Digital Signatures," International Review of Law, Computers & Technology, vol. 24, no. 1, pp. p. 133-141, 2010.
- [32] CPA Canada, "WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.0," 3 April 2014. [Online]. Available: <http://www.webtrust.org/homepage-documents/item79806.pdf>.
- [33] J. St.Sauver, "Client Cert Deployment Models an Hardware Tokens / Smart Cards," 23 January 2012. [Online]. Available: <http://pages.uoregon.edu/joe/client-cert-models/jt-louisiana.pdf>.
- [34] H. Rossnagel, "On Diffusion and Confusion - Why Electronic Signatures Have Failed," TrustBus, pp. p. 71-80, 2006.
- [35] W. Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed., Upper Saddle River: Prentice-Hall, 1999.
- [36] R. Oppliger, "Authorization Methods for E-Commerce Applications," in Proceedings of the 18th IEEE Symposium, 2000.
- [37] E. G. Carayannis and E. Tuner, "Innovation Diffusion and Technology Acceptance: The Case of PKI Technology," Technovation, vol. 2006, no. 26, pp. p. 847-855, 2006.
- [38] J. Lopez, R. Oppliger and G. Pernul, "Why Have Public Key Infrastructures Failed So Far?," Internet Research, vol. 15, no. 5, 2005.
- [39] N. Vratonjic, J. Freudiger, V. Bindschaedler and J.-P. Hubaux, "The Inconvenient Truth About Web Certificates," School of Computer and Communication Sciences, Switzerland, 2012.

Using parallel computing to implement security attack

Sedeeq Hassn Albana Ali Al-Khazraji

PHD Student in Computing and Information Sciences, Rochester Institute of Technology,
New York, USA

In 2003, Philip Oechslin invented a new technology to implement the security attack called Rainbow table. Rainbow table is time memory trade off which aims to reduce the calculation happened during the cryptanalysis. Rainbow table reduce the required time for the attack, but generating of the Rainbow table required long time. In this paper we try to achieve parallel implementation for Rainbow table using Message Passing Interface (MPI) with the frame work Intel Cluster Suite. The proposed system support five hashing algorithms, yet our case study was two windows hashing algorithms lm and ntlm. We used Linux operating system in RC computing lab and made our parallel implementation using 201 processing unit to generate Rainbow table. We decrease the time to generate table from 7.1 days in sequential implementation to 46.4 minutes in parallel implementation; as a result we achieve 221.5 speedup.

Keywords- Parallel processing, Security, Privacy & login, Rainbow tables.

I. INTRODUCTION

In the last few years, security represent on the most important challenges in computer world. The need of security increases directly proportional to the increases to the attack. As everybody know there are different types of attacks, and one of the most important attacks is the attack on passwords. The password always encrypted using an encryption algorithm and the general idea of encryption algorithms is to make the required time to break the encrypted information not worth the value of the information. In the other words, the power of attack on password different in the required time to break the password; for example brute force attack considered a guaranteed method to break the password. The problem in the brute force attack it's required a long time to break the password. As a result, many algorithms appeared to decrease the required time to breaking the password. One of these interesting algorithms is proposed by Philippe Oechslin in his paper "Making a Faster Cryptanalytic Time-Memory Trade-Off", Oechslin algorithm made a tread between time and memory space. This algorithm try to reduce the cryptanalysis time dramatically using Rainbow tables [1] [2] [6].

Rainbow tables simply is precomputed table contain many passwords calculated in a specific method this table used to cryptanalysis passwords instead of trying to attack the password one by one like brute force attack[7]. There are many implementation for Oechslin algorithm for example RainbowCrack [3] and Cryptohaze GPU Rainbow Cracker [4], but these implementation considered basic implementation of

Oechslin's algorithm. These implementations normally use normal personal computer or sometime GPU in the computer.

II. RELATED WORKS

One of the previous work is the RainbowCrack considered one of the most popular rainbow table cracker it is a general purpose implementation of the Oechslin's algorithm. RainbowCrack project is software to crack hashes using rainbow table in this implementation rainbow table are sorted and saved in the hard disk. RainbowCrack consist of many software for example rtgen program which used to create rainbow table, rtsort program which used to sort the given rainbow table after loading it to memory and rtcrack which used to crack a specific hash or hashes list using the sorted rainbow table. RainbowCrack is efficient implementation to rainbow table but it need a long time to generate the table days or weeks depending on the options for creating the table which depend on the types of passwords want to cracks[3][8].

Another interesting work in this field is the thesis of Michael S. Taber, "Distributed Pre-computation for a Cryptanalytic Time-Memory Trade-Off" in his work Taber made parallel implement for RainbowCrack using local network on windows operating system. This implementation include three hashing algorithms lm, md5 and SHA1 [9]. However this thesis present an efficient implementation for RainbowCracker, but it not supports some important hashing algorithms for example ntlm.

Edward R. Sykes in his paper "An improved parallel implementation of RainbowCrack using MPI" shows another implementation for RainbowCrack. He made parallel implementation of RainbowCrack using SHARCNET supercomputer. And he showed the implementation of generating windows hash of length 14 characters by decreasing the required time to generate the table [10].

In this paper we made a development for Taber thesis we make generation rainbow table for supporting more algorithms, then support sorting and cracking features. With support other operating system for example Linux. Then after sequential and parallel implementation for rainbow table completed we test the generated tables and get the same result. Our test achieved by cracking windows 7 and windows 8 login passwords which encrypted using ntlm algorithm.

III. SOLUTION DESIGN

Our solution will focused on using parallel processing to generate Rainbow table. first we will describe the sequential implementation then the parallel approach.

A. Rainbow Table sequential generation

In our solution we focused on generating rainbow table using MPI. The algorithm of creating rainbow table is illustrate in the following steps:

List (1): Generating rainbow table.

- 1- Start
- 2- Generate password plain text rang space.
- 3- Pick a random location in plain text rang space and get the real value for plain text
- 4- Calculate hash value for selected text
- 5- Reduce hash to a new location
- 6- if not reached chainlength go to step 3
- 7- store first plain text and last hash value in rainbow table

generating rainbow table is a complex process figure (1) can help to simplified this process:

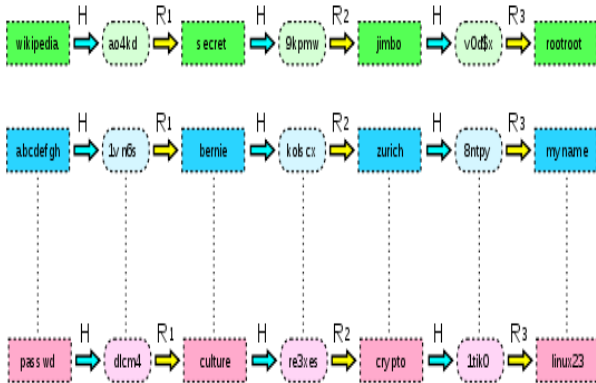


Figure generating rainbow table [1]

Where the simple H represent a specific hashing algorithm. Our solution support five algorithms: md4, md5, sha1, lm and ntlm. And the symbols R1, R2 and R3 represent reduction function; the only condition for reduction function is that to return value within the range of the password plain text. The process start from the beginning of the chain and repeated number of times equal to chain length. And finally only two values will be stored in rainbow table which is chain start and last hashed. RainbowCrack consists of the following components [9] [3]:

rtgen: program to generate rainbow tables.

rtsort: program to sort rainbow tables generated by rtgen.

rcrack: program to lookup rainbow tables sorted by rtsort

All these programs can run either sequential or multithread and rtgen is the program required the longest time of Oechslin's algorithm this program take the largest ratio of the time.

The last section represent the sequential implementation for Oechslin algorithm for generating rainbow table. Our work is to enhance this implementation we use Master-Worker parallel implementation for this algorithm. In our implementation the

master as specific function and the workers (slaves) has different function. We will summarize these function as following

B. Master does the following functions:

1. Send task to a worker: sending a start of the chain and the client will do the calculation.
2. Get next task and
3. Until complete the total number of chains.
4. Receive task result from any worker: it mean the master receive portion of the rainbow table from each client then combine these portions to single rainbow table.

C. Worker does the following functions:

1. Receive task from the master.
2. Compute task results: by creating temporary file and each row this file contains tow values represent the start point and the end point of the chain. The calculating of the end point explained in List (1).

Send results to the master by sending the generated rainbow table portion to the master.

After generating rainbow table it need to sort the table to reduce the searching time. Then we use the generated rainbow table to crack the windows 7 and windows 8 hashed passwords. We obtain windows password using "quarkspwdump" software, which is open source program we can easily configure and use to obtain the password to be cracked.

IV. RESULT ANALYSIS

The sequential implementation in our work was done using Windows 7 operating system and the specification of the computer was CPU used "Intel Xeon E312xx (Sandy Bridge) 2.6 GHz" and the memory size is 4G. While in parallel implementation we used Research Computing Laboratory (RC computing lab) which is a computing environment provide by RIT used to provide high resources and make parallel processing experiments. According to their website the specification of RC computing lab is [5]:

- 250 core HPC cluster with 1.3 TB of RAM and 10 Gig interconnect
- 64 port 10 Gigabit switch
- 70 TB of network attached storage

We implement different algorithms using different parameter. The parameters we used in our implementation is

hash_algorithm: represent the algorithm used to create the table we support five algorithms they are md4, md5, sha1, lm and ntlm

charset: represent all possible characters for the plaintext of the password we want to crack.

minlen: Minimum number of characters of the password.

maxlen: Maximum number of characters of the password.

table_index: the Index value refers to a number between 0 and key space max -1, and it is used to prevent collisions between different rainbow tables.

chain_len: Chain length which represent the number of hashes stored in each chain.

chain_count: Number of Chains can be stored inside Rainbow Tables. The more chains we create, the more hashes we can crack.

After making different type of experiments we get the different results here we try to focus on ntlm algorithm because we used this algorithm to crack windows 7 password.

The result of sequential implementation using single core is:

#	Algorithm	Charset	Min len	Max len	Chain len	Chain count	Generation Time		Generated file size
							Minutes	Days	
1	Ntlm	alpha	1	7	10000	10000000	816.62	0.22	152 MB
2	Ntlm	ascii-32-95	1	14	10000	100000000	10290.65	7.14	1.48 GB

The result of parallel implementation using 201 core one for Master and 200 workers is:

#	Algorithm	Charset	Min len	Max len	Chain len	Chain count	Generation Time		Generated file size
							Minutes	Days	
3	Ntlm	alpha	1	7	10000	10000000	3.38		152 MB
4	Ntlm	ascii-32-95	1	14	10000	100000000	46.45		1.48 GB

V. DISCUSSION

From the previous results we see huge decreasing of the generating time of the rainbow table because the calculation of each chain is independent of calculation of other chains i.e. this rainbow table generation is massively parallel problem.

We can reduce the Generation Time of 152 MB of data from 816.62 Minutes in sequential implementation to 3.38 in parallel implementation. And reduce the Generation Time of 1.48 GB of data from 7.14 days in sequential implementation to 46.45 Minutes in parallel implementation

The Speed up and the efficiency in this implementation is:

Case	Sequential time	Parallel time	Speed up	Eff
#1 & #3	816.62	3.38	241.19	1.19
#2 & #4	10290.65	46.45	221.53	1.10

Some difficulties in such programs is the debugging problem which is one of the hardest difficulties in this work; Microsoft supports MPI debugging in Visual Studio 2010 but it stops supporting MPI debugging in Visual Studio 2013. And there are many developer ask to return this feature in the following versions of visual studio.

VI. CONCLUSIONS

Rainbow Table represent an efficient method to attack passwords, it reduces the time of breaking the hashed password because it is precomputed and stored in memory. Creating the rainbow table needs a large amount of time. We use parallel processing to decrease the required time to generate rainbow table. As a recommendation we suggest after our experiment in this work we suggest:

- Using longer password
- Using more complex password
- We need more advanced login technique.

VII. FUTURE WORK

As a future work for this work we are planning to implement the crack operation in parallel using MPI. Beside, making this system support other algorithms. And create better user interface to provide easier use for the program for example design web based application for this program.

REFERENCES

[1] Wikipedia, Rainbow Table, Retrieved Jun 13, 2015, from http://en.wikipedia.org/wiki/Rainbow_table

[2] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off", in Advances in Cryptology – CRYPTO 2003 (D. Boneh, ed.), vol. 2729 of Lecture Notes in Computer Science, pp. 617–630, Springer-Verlag, 2003.

[3] RainbowCrack Project. RainbowCrack project - Rainbow Table Generation and Sort. Retrieved Aug 8, 2015, from <http://www.project-rainbowcrack.com/generate.htm>.

[4] Cryptohaze, GPU Rainbow Cracker, Retrieved Jul 20, 2015, from <http://www.cryptohaze.com/gpuRainbowCracker.php>

[5] RCLab, Research Computing Laboratory, Retrieved Mar 1, 2015, from <http://rc.rit.edu/rclab.html>

[6] H. Mathur and Z. Alam, "Analysis In Symmetric And Asymmetric Cryptology Algorithm," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 4, no. 1. January-February 2015.

[7] D. Melber, "ATTACKING WINDOWS PASSWORDS", Internal Auditing, vol. 26, no. 4, pp. 42-5. Jul-Aug 2011

[8] S. Marechal, "Advances in password cracking", Journal in Computer Virology, vol. 4, no. 1, pp. 73-81. October 2007.

[9] M. S. Taber, "Distributed Pre-computation for a Cryptanalytic Time-Memory Trade-Off", Master thesis, Rochester Institute of Technology, October 2008.

[10] E. R. Sykes, and W. Skoczen, "An improved parallel implementation of RainbowCrack using MPI", *Journal of Computational Science*, vol. 5, no. 3, pp. 536-541, 2014.

Sedeeq Hasan Albana Ali Al-Khazraji is a lecturer in Computer Sciences Department, College of Computers and Mathematics. University of Mosul. he received his MSC degree in computer sciences in 2011 in the specialty of operating system and computer networks. Currently he is a PH.D. student in B. Thomas Golisano College of Computing and Information Sciences, Rochester Institute of Technology. He interest with Distributed systems, Databases, Security and Privacy issues.

Access Model with the checking of scenarios “AMWCS”

Samir TAHIRI
*Hassan II University
ESTC,RITM Lab
Casablanca Morocco*

Nadia AFIFI
*Hassan II University
ESTC,RITM Lab
Casablanca Morocco*

Hicham BELHADAOUI
*Hassan II University
ESTC,RITM Lab
Casablanca Morocco*

Reda FILALI HILALI
*Hassan II University
ESTC,RITM Lab
Casablanca Morocco*

Mohammed Ouzzif
*Hassan II University
ESTC,RITM Lab
Casablanca Morocco*

Abstract— The safeguarding of the confidentiality of information and data in an information system has become a major factor nowadays. Indeed with the omnipresence of data processing, the setting on line of the applications, the challenges of security have also become considerable.

The access control is a mechanism which governs the way in which data or information must be exploited. It defines and gives authorizations and prohibited accesses. To define or adapt a model of access becomes impossible to circumvent in order to guarantee an optimal security for an information system.

With the growth, the diversity and the wealth of information systems, the traditional models of access control show considerable limits. These limits contributed to the birth of other models that are more adapted to our needs.

In this article we propose a model of access control that we will set up for in order to deal with the progression of a flow in information system. This model is based on a cutting of the way traversed by a flow in several stages. The passage of a stage has another east governed by rules and conditions. This model makes it possible to challenge the abnormal behavior during the execution of an operation. It is based on the checking of the legitimacy of the presence of an entity in one of the stages of the system.

Keywords— Security, Authentication, control, model, scenario, transaction.

I. INTRODUCTION

The access to the resources and data of a system is regarded as a very important and critical act. It is authorized only by the people having necessary and eligible rights. These

rights of access to the resources are granted to the users, and they are governed and controlled by models of security measures in order to intercept any intrusion.

The model of security is a process which aims to fulfill the requirements of information systems in terms of security. It consists of setting up means to guarantee its security and its reliability. A wide range of organizations lay and set up security policies governing their information systems in order to control the risks related to any eventual intrusion.

In this context, the installation of the models of access control is often governed by legislative texts [15]. One can quote for example the Directive 95/46/EC of the European Parliament on the protection of the individuals taking into consideration treatment carried out on personal data [16] and the American directive HIPAA (federal Health Insurance Portability and Accountability Act) which is particularly more concerned with data protection of health [17] [15].

Several access controls were suggested, we present in this article certain traditional models, and we show their limits compared to the attacks. Thereafter we propose a model of access control which perfectly meets our needs, in order to guarantee the security of progression of flow during a banking transaction. This model aims at intercepting the attempts that target the access of both the resources and the significant data that is not authorized.

We are interested in this case study by (I) authentication “to check the identity of the user who reaches the system”, (II) the authorization “to check the rights of access that are deemed necessary and enabling to exploit the resources of the system”, (III) the traceability to fight against the impostures of right.

This article will be presented as follows: in the second section we will present a forceful review of literature about various models of access control. In the third one we will present the model that we propose. Finally we will finish by concluding and giving some proposals for further research and investigation.

II. BACKGROUND

The information system security makes it possible to tally the environment of users of its resources. It guarantees that a resource (hardware or software) is not used within the framework envisaged. It represents the whole array of means deployed for, at the same time to guarantee, to preserve, and to restore an information system.

Several techniques are used to guarantee security, among which is the cryptography and access control, during the information flow. We are basically interested in this work in the access control.

The monitoring system of access is a process of control of attempts at access. It guarantees the following properties of security [22]:

- Integrity: The data must be the same as one might expect it to be, and do not have to be faded in a fortuitous or voluntary ways.
- Discretion: Only the authorized people have access to information which is intended to them. Any undesirable access must be prevented.
- The availability of service: The system must function without errors during the limits of use envisaged, to guarantee the access to the services and resources installed with the response time expected.[ITS 91, CTC].

In order to reinforce the protection of the resources, various entities intervene. Initially the **subjects** which are human users or the processes of data-processing which work for them [1]. Also called active entity, it has rights of access to objects and requires to reach them. A subject can be regarded as object since it is likely to be handled by another subject [ITS 91, CTC].

We also quote the **objects**. They are passive entities of the system. They contain or receive information [1], from wherever the need for being protected arises [ITS 91, CTC].

In this literature, we have found out several models of access that exist; we can classify them in three main families of security models. Discretionary model DAC (Discretionary Access Control) [10], the obligatory model MAC (Mandatory

Access Control) and the model containing roles RBAC (Role-Based Access Control) [3].

Discretionary model DAC grants the person in charge of “information” property the rights of access, of handling and the possibility of propagating information with the others according to its discretion.

The rights can be granted by this person in charge to each user to groups’ user, or to both. A subject which holds the rights of handling an object has the freedom “with its discretion” to share the authorizations at its disposal with other subjects [3].

Among the discretionary models most known we find:

The Model of Lampson, it is based on three principal components to define the access control [4]:

- A set of objects “O”: These are the properties of the system protected. Each object with a single identifier;
- A set of fields “D”: In fact the properties have access to objects;
- A matrix of access “M”: Stamp operations of access.[4]

The components (Object, Field and Matrix) are controlled by a set of rule determining the way in which the entries of the matrix can be exploited [4].

The **HRU** model uses a matrix of traditional access similar to that of Lampson, and then it adds orders in order to carry out, under condition, the basic operations for the automated updates of the matrix of access [12].

The model of Graph privileges was proposed in 1994 by Mr. Dacier [13]. Its principle is simple, a node X represents the whole of the privileges granted to a user. An arc of a node X with a second Y represents the right for the user having privileges X to extend them to obtain those of the node Y, by applying the rules of access controls [6].

Although model DAC represents the advantage of being extremely flexible, it nonetheless shows an important disadvantage. Indeed the DAC allows an insurance on the protection of flows in a system, it is possible also that certain access control indicated in the authorizations is to be deviated. This failure is due to the fact that a user having certain access authorization can thereafter communicate a resource with other users who do not have the necessary authorizations to reach there. Moreover, it is very useful to make the distinction between the users and the subjects. A user is a passive entity which generates subjects or processes which are in fact active entities having authorizations, and which carry out operations. To do without this distinction, it makes the system vulnerable to malevolent attacks such as Trojan horses.

Thus, DAC is more likely to be adapted for the systems having the resource sharing that is more important than protection.

The model of obligatory access control **MAC** defines the rules impossible to circumvent, governing the rights of access to the objects by subjects. These rights are not defined

by the creator of the data but by the administrator of the system [7]. This fact restricts the privileges of a subject on the objects which belong to him [2].

Among the MAC models, we can quote the **Bell-LaPadula** model. This model was proposed for the first time by David Bell and Leonard Lapadula in 1973 [11]. It was elaborated in 1975 by the American Department of Defense [14]. It is based on an approach which takes care to protect information against the disclosure in an information system. The objective of this model is to preserve the confidentiality of an object protected against the unauthorized accesses of the subjects [6]. It defines constraints to supervise applications in order to prevent the attack by Trojan horse against confidentiality [8].

In this model the subjects and the objects are classified according to a level of security measures. For each object one grants a security level in form (Level of classification, Ensemble of categories). The subjects are characterized by a maximum security level and a current security level likely to be changed dynamically. The various levels of classification are ordered by the relation " $<$ ", example: not classified $<$ confidential $<$ secret $<$ secret signal.

The obligatory model MAC shows serious limits because of restrictions on the actions imposed by its system. It does not allow modification dynamics of the rights and requires that the system and its user be worthy of confidence beyond the framework of the model [14].

In the model containing roles RBAC, the role is the central concept of the security policy [19]. For each role, one grants a set of rights and permissions, and the users see themselves allotting one or more roles, which makes it possible thereafter to reach the right given to their roles (figure1). Contrary to the model of the discretionary access control, the policy based on RBAC does not apply directly to the users [18].

RBAC was criticized for the following reasons:

- The generic absence of structure of permissions. Those are regarded as dependent on the concrete application of the model [2.19].
- The concept of hierarchy of role is somewhat ambiguous. In general, the hierarchy of the roles does not correspond completely to the organizational hierarchy. For example, the director of the hospital plays an administrative role higher than the role of doctor. For as much, a director of the hospital is not necessarily a doctor, thus he is not feasible to grant to the director the permissions of the doctor [2.19].
- The distinction between the concept of role and that of group is fuzzy [2.19].
- Impossibility of expressing permissions and in particular permissions which depend on the context. Consequently, it would be difficult to specify that a doctor has the permission to reach the medical record of a patient only if the latter is its patient [2.19].

To conclude, although these models offer an important security level for certain systems. In very significant operations such as banking transactions, not only the attribution of a right to an entity must be controlled but also, the presence of this entity in this stage of the operation is legitimate. The model that we will propose defines a control mechanism of access which at the same time allows to control the attribution of the authorizations and to check the legitimacy of the presence of an entity in a stage of the system.

III. APPROACHES AND MODEL PROPOSED

Let us recall that the model of access defines rules which govern good performance and the transmission of flows in the system. These rules are specified in terms of instructions. The installation of a model of access control requires a milked multiphase approach each one with a different level of design, while being based on the following concepts [2]:

- Security policies: It consisted of the whole laws, rules and practices which govern the treatment of the sensitive information and the use of the resources by the hardware and the software of the system [1]. Within the framework of our work we are interested in logical security policies achieved by the system itself.
- A model of security: It is composed of a formal expression of the rules of the security policy, it makes it possible to show theorems concerning the security of information [1].
- Mechanisms of security: those define the low functions level (software and hardware) making it possible to implement the controls imposed by the security policy [2].

The development of a monitoring system of access is based on the three concepts quoted above, which offers different security level with several advantages [6]. Consequently, on the one hand, it offers the possibility of making a comparison between the various security policies, and on the other hand, it enables us to combine the implementation of multiple security policies, which brings more flexibility [2].

The evaluation of the security of an entity will always be done according to the known criteria of security, namely confidentiality, integrity, availability and traceability.

A. Presentation of the access model with the checking of scenarios "AMWCS":

1) Stage and Scenarios:

An action in an information system can be regarded as a set of phases of progression. A **stage** can be a phase or set of phases progression of a flow in an information system. The succession of these stages of progression defines a **scenario**. This latter makes it possible to represent any action or

progression of flow. In a system one can count the operations authorized and thereafter the possible and authorized scenarios. **The graph of scenarios** is the chart of the scenarios of legitimate access in an information system.

The model that we will propose is based on a mathematical modeling of the graph of scenario, in order to detect abnormal behaviors of the system.

B. Development of model “AMWCS”:

Model AMWCS is based on a procedure which takes care of making sure that the behavior of a subject is authorized and that all the rights it has in the course of its progression in the system have been acquired legitimately.

The AMWCS shares the access to the system in several stages; the rights and privilege of access are not to be allotted directly to the users. They are generated in the stages in which these rights are necessary. Consequently, the acquisition of a right of access passes through the activation of the stages which hold them. **The activation** of a stage is the acquisition of the authorizations to be there. These rights are created by the administrator of the system.

C. The principle of the “AMWCS”:

The development of the AMWCS is based on a chart of the stages of progression of the flow defined by the administrator of the system. It offers paramount information, which of the possibilities, predefined to us, passage or progression between the stages. This information makes it possible to check, at a given moment, if a subject S, in a stage I.E.(internal excitation) respects the way it is authorized either to be there or not. The following figure represents a graph of stages

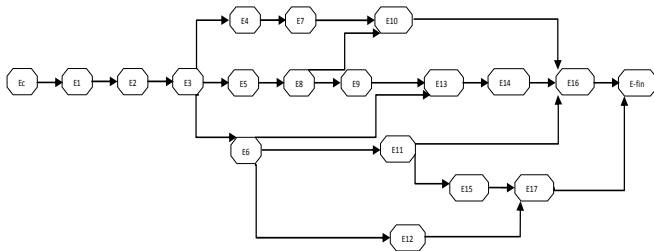


Figure 1. Stages of graph

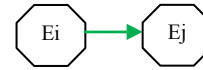
The root of graph “EC.” represents a slap of confidence, it is considered without possible hazard, stage of starting, with privileges and authorizations. These authorizations make it possible thereafter to reach other stages according to the predefined scenarios, by guaranteeing a correct operation and an authorized system.

D. Formal representation of the Model:

In order to better be able to exploit this approach which is based on a graph of scenarios, we have converted this latter into a matrix “Stamps access” with same information offered by the graph of stages.

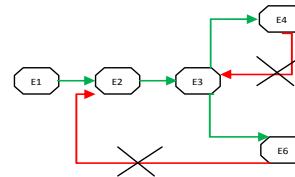
Property of the matrix:

It is said that there is a direct way of E_i to E_j if $M(I, J) = 1$;



Information passes in only one direction \Rightarrow si $M(i, j) = 1$ alors $M(j, i) = 0$

And if $\exists K$ such as $M(J, K) = 1$ then $M(K, I) = 0$



The following figure represents the matrix of access of the graph of stages defines:

	Ec	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	EFin
Ec	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E3	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
E4	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
E5	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
E6	0	0	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	0
E7	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0
E8	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0
E9	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
E10	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
E11	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0
E12	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
E13	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
E14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
E15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
E16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
E17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Figure 2. Access matrix

The development of a matrix approach enables us to develop a mathematical model which defines the rules of checking of the progression of a flow.

E. Mathematical approach of checking of the scenario of access

The AMWCS consists of checking if the progression of a flow in a system is legitimate according to the predefined scenario

To traverse a scenario amounts successively activating stages one after the other. A user of the system cannot activate more than only one stage at the same time.

An activated stage I.E.(internal excitation) makes it possible as a consequence to activate the following stage E_j on condition of having a direct way in-between. The activation of E_j decontaminates I.E.(internal excitation) automatically.

A course or a scenario is legitimate if and only if, the passage of a stage I.E.(internal excitation) has another E_j , in this same scenario that is authorized. In other words there should exist a direct way between I.E.(internal excitation) and E_j .

Activation of a state:

- So Active (I) =0 ↔ stage I.E.(internal excitation) is decontaminated.
- So Active (I) =1 ↔ stage I.E.(internal excitation) is activated.
- So Active (I) =1 ↔ $\forall j \neq i$ Activates (J) =0
 - Function of activation of I via J:
 - $f(i/j) = M(J, I) * Active(Ej)$
 - $Active(Ei) = f(i/j)$
 - $Active(Ej) = 0$
 - A stage I.E.(internal excitation) can be activated (Activated) ↔ activates (I.E.(internal excitation)) =0 and $\exists J$ such as active (Ej) =1 and $M(J, I) =1$

The figure above represents a progression of flow governed by the AMWCS. A user holding a set of privileges can reach a stage. In this latter case, the user can carry out a set of operations generated by this stage. The successful execution of these operations enables the acquisition of another privilege and thereafter the activation of the following stage of the scenario.

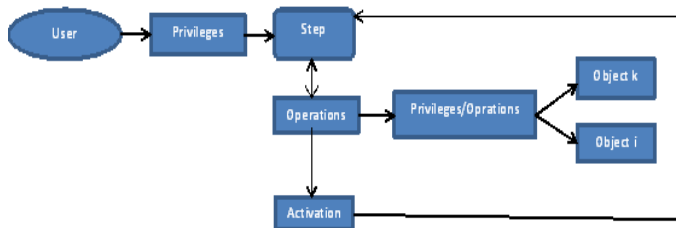


Figure 3. Progression of flow

F. Application of the model to the E-banking transaction:

With the increase of frauds related to the payment on Internet, the banks deploy solutions to reinforce strong authentication of these customers online. During our former work, we suggested a solution which consists of combining an application which exploits the EMV functionality of a smart card, with a card reader BASIC [20] which allows the customer to authenticate himself on the Web site of the bank and to sign transactions online, either on this same site or on a trader site.

To reinforce Security with the turns of our solution using AMWCS for its implementation in order to interception of intrusion which seeks to remove a passage of authentication.

1) Operating process of the software one:

The solution that we proposed operates in the following way. A user who wishes to authenticate himself on a website in order to carry out purchases, has to be redirected towards the website of his bank, this latter shows him the instructions to be followed in using the software. The user first invites to connect his BASIC reader card and to insert his chart inside. Then he is asked to provide both his PIN and supplementary data provided by the page of the bank “Challenge”. The software provides an answer in the form of a token, “One Time Password” (OPT). The latter must be introduced into the website of the bank in order to validate this answer and to accept the authentication of the holder of the chart, and to accept the transaction. The following figure shows the operation of the software:

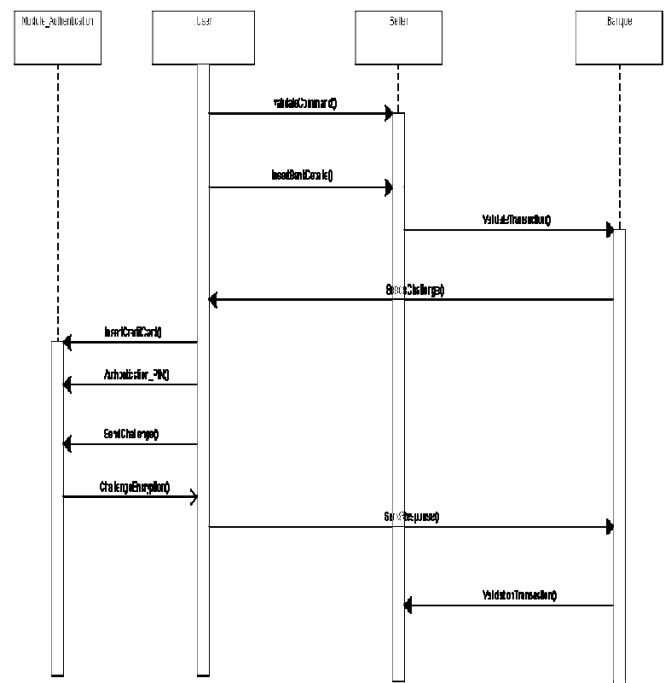


Figure 4. Application diagram

1) Stages of progression of access of the application:

In this section we will cut out the operations of our software in succession of a progressive stage. In order to make an enumeration of the functions of the application, a description of the scenario of use of the system is essential.

Scenario of use:

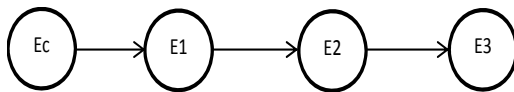
The user starts with the insertion of his bank card in the reader. The system detects the chart and checks the organization from which it emanates. Once the chart is detected, the system controls its validity by checking its expiration date. Once the chart is judged valid, we proceed to

control the holder by asking for the chaPIN. In end if the PIN is correct the system provides the user with an answer and proceeds to the cryptic process and returns an answer which makes it possible to the financial organization to validate the transaction. The chart below represents the distributions of the functions on the stages:

TABLE I. DISTRIBUTIONS OF THE FUNCTIONS

Stages	Functions
EC.	1. Card detection
	2. RESET Application
E1	3. RED RECORD
	4. Checking expiry dates
E2	5. Get Dated
	6. Checking PIN COUNT
	7. Verify PIN
E3	8. Challenge encryption /Response

In our system there is only one scenario to respect in order to validate a transaction, below, figure 7 presents the graph of the scenarios and the matrix of access which corresponds to him.



	Ec	E1	E2	E3
Cc	1	1	0	0
E1	0	1	1	0
E2	0	0	1	1
E3	0	0	0	1

Figure 5. Graph of scenarios and its matrix of access

- ✓ **First stage EC** contains useful functions for the detection of the chart in the reader, it is the stage of starting of our application.

- Starting data:
Activate (EC.) =0
- Conditions of activation:

Execution successfully of the functions generated by EC.

- Activation of EC.:
Activate (EC.) =1

- ✓ **The E1 second phase**, activated by stage EC. It is reserved for the reading of public information, which is readable also on the chart. During this stage the software checks the validity of the chart which carries out the transaction. The risk during this stage is to use

a nonoperational purchasing card, this can be done by eliminating this operation by a jump from code. The AMWCS can detect this jump, which means also the jumping of stage and by consequence one cannot activate the following stage E2.

- Starting data:
Activate (E1) =0 and Active (EC.) =1
- Conditions of activation:

If $\exists J$ such as Active(Ej)=1 and M(Ej, E1) =1

Then execution successfully of the functions generated by E1.

- Activation of E1:
 $f(c/1) = M(C, 1) * \text{Active}(EC.)$
 $\text{Active}(E1) = f(c/1)$
 $\text{Active}(Ec) = 0$

- ✓ **The E2 stage** can be activated only by E1. The checking of the validity of the expiration date carried out previously in the E1 stage enables us to go up in the scale of sensitivity of information. During this stage one will exploit very significant and very important functions such as the checking of the PIN. This passage is very critical for the continuation of the operations. Indeed the checking of the PIN is the means which one has for the authentication of the card holder, before exploiting the functions of decoding existing in the bank card. The activation of the E3 stage is conditioned primarily by the validation of this stage "E2".

- Starting data:
Activate (E2) =0 and Active (E1) =1

- Conditions of activation:

If $\exists J$ such as Active (Ej) =1 and M(Ej, E2) =1
Then execution successfully of the functions generated by E2.

- Activation of E2:
 $f(1/2) = M(1,2) * \text{ACTIVE}(E1)$
 $\text{Active}(E1) = f(1/2)$
 $\text{Active}(E1) = 0$

- ✓ **The E3 stage** is only activated it was preceded by E2. During this stage one will exploit functions of encoding which lies in the chart. These functions allow us to crypt the challenge provides at the time of the transaction, and an answer returns, which makes it possible the bank to check our authentication.

- Starting data:
Activate (E3) =0 and Active (E2) =1

- Conditions of activation:

If $\exists J$ such as $Active(E_j) = 1$ and $M(E_j, E_3) = 1$

Then execution successfully of the functions generated by E_3 .

- Activation of E_3 :

$$f(2/3) = M(2,3) * ACTIVE(E_2)$$

$$Active(E_2) = f(2/3)$$

$$Active(E_2) = 0$$

IV. CONCLUSION

In this article, we presented a model of access being based on an original concept that is not approached yet by the existing models. This model that we proposed, is called *AMWCS*, and it focused on the attribution of the rights such as the concept of scenario checking in order to legitimate the presence of an entity in a stage of progression of the system. Indeed the existing models have focused on the manner of attribution of the rights to an entity, without taking into account if its presence in the system is authorized. This model is based on a matrix representation of the authorized scenarios, of progression of flow in the system. This one has enabled us to formulate a function which starts from the vectors of the matrix at a given stage, to extract the former and latter stages. This information is essential in order to authorize our progression. The attribution of the rights on the objects, in our model, is done in an evolutionary way in the system. Indeed each stage generates the whole necessary rights and authorizations in order to exploit these functions. Consequently to have a right it is necessary to activate the stage which has that right. From our point of view, one plans to include the notion of the roles in combination with the matrix of access and a matrix of right in order to improve the requirement in Security, and to cover the property of availability of the objects.

REFERENCES

- [1] Analyse de sécurité pour la certification d'applications Java Card.
- [2] DEA Modelisation et vérification de politique de sécurité MODELISATION ET VERIFICATION DE POLITIQUES DE SECURITE. Amal HADDAD. Université Joseph Fourier 2005.
- [3] ANALYSE FORMELLE DES POLITIQUES DE SÉCURITÉ. IKHLASS HATTAK. UNIVERSITÉ DU QUÉBEC 2010.
- [4] Bulter W. Lampson. Protection and access control in operating systems. In Operating Systems, Infotech State of the Art Report 14, 1972, pp 309-326, 1972.
- [5] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. Commun. ACM, 19(8):461-471, 1976.
- [6] Pierangela Samarati and Sabrina de Capitani di Vimercati, Access Control: Policies, Models, and Mechanisms, FOSAD 2000, LNCS 2171, pages 137-196, 2001
- [7] Pierre KONOPACKI UNIVERSITE PARIS-EST Thèse de doctorat Une approche événementielle pour la description de politiques de contrôle d'accès 4 mai 2012
- [8] Artille Les modèles de sécurité. Frederic Cuppens et Nora Cuppens-Boulahia.
- [9] Methods for Access Control: Advances and Limitations. Ryan Ausanka-Cruets Harvey Mudd College 301 Platt Blvd Claremont, California. [CTC] CTCPEC - Canadian Trusted Computer Product Evaluation Criteria, <ftp://ftp.cse.dnd.ca/pub/criteria/>, 2001. [ITS 91] ITSEC - Information Technology Security Evaluation Criteria, juin 1991, <http://vespa.cru.fr/securite/Documents-generaux/ITSEC.ps>, 2001.
- [10] Butler W. Lampson, Protection, In 5th Princeton Symposium on Information Science and Systems, pages 437-443, 1971. Reprinted in ACM Operating Systems Review 8(1): 18-24, 1974.
- [11] [BL73a] D. E. Bell and L. J. Lapadula, Secure computer systems: Mathematical foundations, Technical Report ESD-TR-73-278, vol. 1, The Mitre Corp., Bedford, MA, 1973.
- [12] Michael A. HARRISON, Walter L. RUZZO et Jeffrey D. ULLMAN. Protection in operating systems. Commun. ACM, 19 :461-471, August 1976
- [13] M. Dacier. Vers une évaluation quantitative de la sécurité informatique PhD thesis, décembre 1994.
- [14] thèse : Une approche événementielle pour la description de politiques de contrôle d'accès. Pierre KONOPACKI UNIVERSITE PARIS-EST
- [15] Thèse : Modèle de contrôle d'accès pour XML : "Application à la protection des données personnelles" Saïda MEDJDOUB Le 8 décembre 2005. Université de Versailles Saint-Quentin-en-Yvelines.
- [16] Directive 95/46/CE du Parlement européen et du conseil, de 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Journal officiel n° L 281 du 23/11/1995 p. 0031 - 0050 http://www.privacy.fgov.be/nieuw%2029-8-2002/directive_95_46_fr.pdf.
- [17] Haut-Commissariat aux droits de l'homme "principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel" Adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies. http://www.unhchr.ch/french/html/menu3/b/71_fr.htm.
- [18] ORBAC : un modèle de contrôle d'accès basé sur les organisations. Anas Abou El Kalam Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, 7 avenue du Colonel Roche, 31077 Toulouse Cedex 4.
- [19] S. I. Gavrila et J. F. Barkley. Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management. Third ACM Workshop on Role-Based Access Control, pages 81-90, 22-23 Octobre 1996.
- [20] Samir TAHIRI "Implementation of Software Alternative Equivalent to the EMV-CAP for Banking Transactions Security" University Hassan II ESTC. IJARCSSE January 2014.

Facial Expression Recognition Using Gabor Wavelet & Neural Networks

Amira Elsir Tayfour
King Khalid University
Abha, Saudi Arabia

Dr. Altahir Mohammed
Sudan University of Science & Technologies
Khartoum, Sudan

Dr. Moawia Yahia
King Faisal University
Saudi Arabia

Abstract— This paper presents methods for identifying facial expression. The objective of this paper is to present a combination texture oriented method with dimensional reduction for identifying facial expressions. Conventional methods have difficulty in identifying expressions due to change in the shape of the cheek. By using simple two dimensional image analysis, the accuracy of the expression detection becomes difficult. Without considering the three dimensional analysis, by using texture extraction of the cheek, we are able to increase the accuracy of the expression detection. In order to achieve the expression detection accuracy, Gabor wavelet is used in different angles to extract possible texture of the facial expression. The texture dimension is further reduced by using Fisher's linear discriminant function for increasing the accuracy of the proposed method. Fisher's linear discriminant function from transforming higher dimensional feature vector into two-dimensional vector training and identifying expressions. Different facial expressions considered are angry, disgust, happy, sad, surprise and fear are used. These expressions can be used for security purposes.

Keywords-component; Fisher's linear discriminant function, Wavelet Gabor filter.

I. INTRODUCTION

Man communicates to another person using expressions. In this expression, words are mixed along with facial muscle movements. Computers are "emotionally challenged". The universal expressions are classified based on Love-fear. Some of the basic expressions are angry, happy, fear, disgust, sad, surprise and neutral. There can be many types of unlimited expressions which can be observed from the face of actors and actresses. They are embarrassments, interest, pain, shame, shy, anticipation, smile, laugh, sorrow, hunger, curiosity. Different techniques can be adapted for expressing anger. This can be like Enraged, annoyed, anxious, irritated, resentful, miffed, upset, mad, furious, and raging. Similarly, Happy can be through joy, greedy, ecstatic, fulfilled, contented, glad, complete, satisfied, and pleased.

In addition, Disgust can be presented by contempt, exhausted, peeved, upset, and bored. The angry can be shown through brows by lowering and drawing together, with

Vertical lines appearing between the brows, lower lid highly tensed, eyes hard stare or bulging, lips can be pressed firmly together with corners down. During happiness, the corners of the lips appear to be drawn back and up. The mouth is parted with teeth exposed. A wrinkle runs from the outer nose to the outer lip. Meanwhile, the cheeks are raised, and the lower lid shows wrinkles.

II. RELATED WORK

Standard methods like static and dynamic techniques have been used earlier by researchers in identifying expressions. Bayesian technique has been used as an important static method. Ravi et al, 2011, gave a comparative study and analysis of 'Facial Expression Recognition Technology' along with its progressive growth and developments. Oliveira et al., 2011, proposed a novel method called two-dimensional discriminant locality preserving projections (2D-DLPP) is proposed that can best discriminate different pattern classes. Cheng et al., 2011, proposed a Gaussian Process model for the facial expression recognition in the Japanese female facial expression dataset and found successful classification of facial expression.

Klaus and Ursula, 2011, report the development of a rapid test of expression recognition ability, the Emotion Recognition Index (ERI), consisting of two subtests: one for facial and one for vocal expression recognition. Ruffman, 2011, presents that recognition of expression in still photos provides important information about young-old differences, and has sufficient ecological validity to explain age differences in a number of social insights. Bänziger et al., 2012, discusses an overview of some of the major emotion expression (EE) corpora currently available for empirical research and introduces a new, dynamic, multimodal corpus of expression expressions, the Geneva Multimodal Emotion Portrayals Core Set (GEMEP-CS). Schlegel et al., 2012, studied on expression recognition ability (ERA) that can inform the measurement of the expression perception component in emotional intelligence.

III. PROBLEM DEFINITION

Many techniques have been developed over a period of facial expression recognition and applied for various situations. In

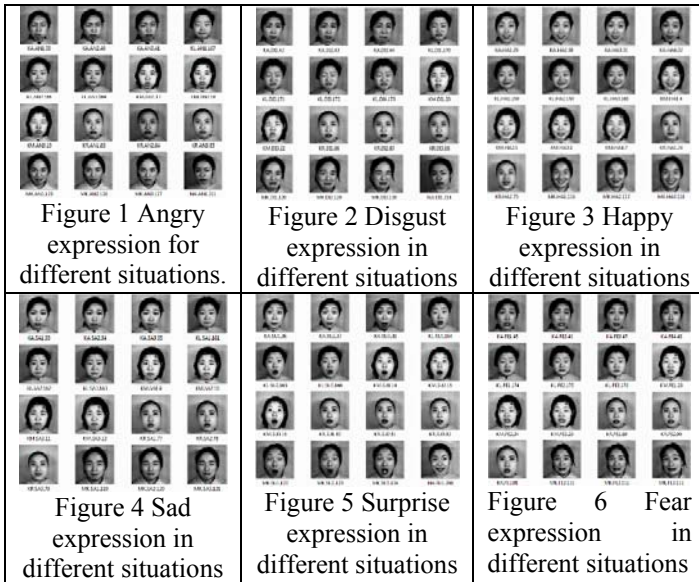
this paper, an effort is made to know the feasibility of identifying expressions from South Indians.

IV. THE SYSTEM SETUP

The implementation of the expression identification system includes detection of the image, training the images for recognition and testing the image for identification

1. Image Detection

A face has to be detected in a captured image. Once detected, the image region containing the face is extracted and geometrically normalized. Images have been acquired using a standard digital camera. The expression of a person under different conditions are presented in Figures 1-6 shows some of the training images.



The statistical values of the frames of each facial expression are presented in Figures 7-12. The summed difference between adjacent frames is plotted for the expression “Angry” in Figure7.

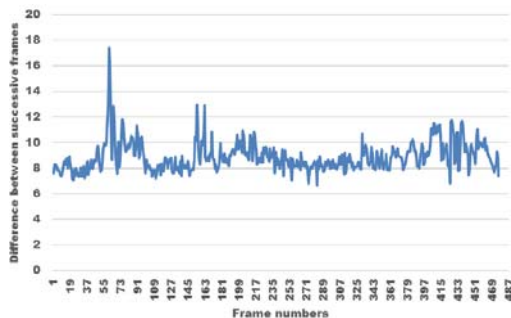


Figure 7 Difference values for the expression ‘Angry’

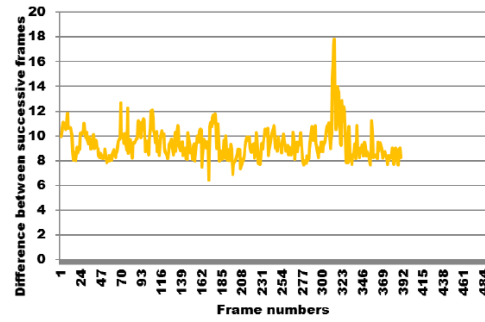


Figure 8 Difference values for the expression ‘Disgust’

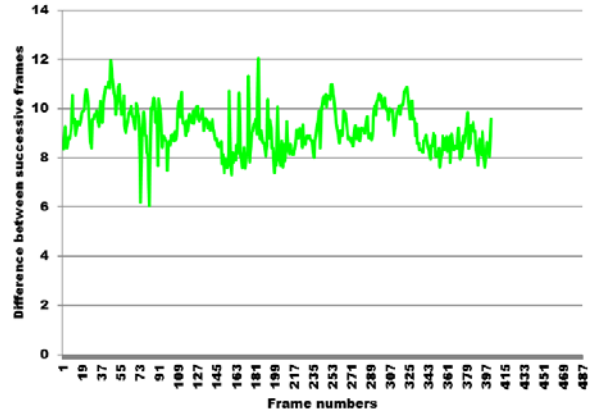


Figure 9 Difference values for the expression ‘Fear’

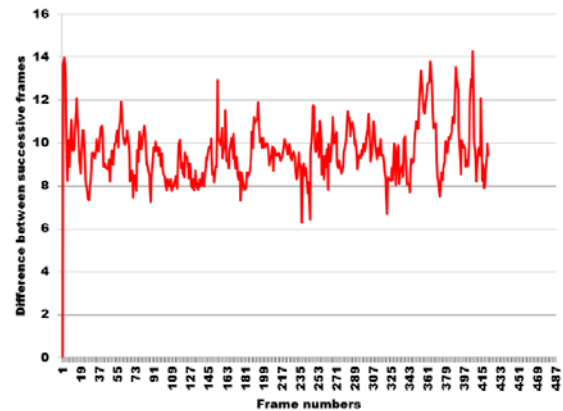


Figure 10 Difference values for the expression ‘Happy’

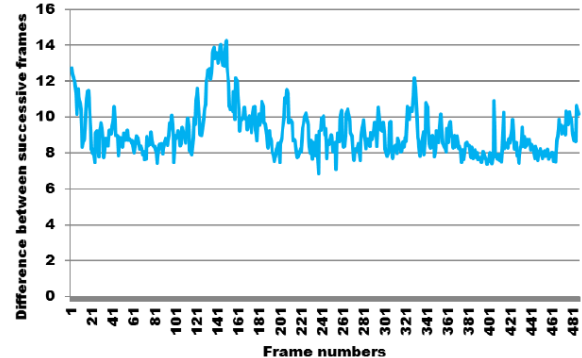


Figure 11 Difference values for the expression ‘Sad’

2. Feature Extraction by Rotational Wavelet Gabor Filter

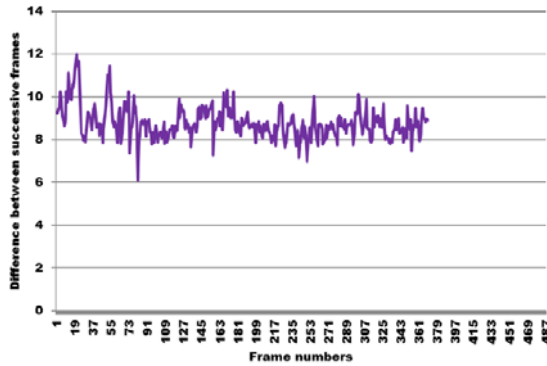


Figure 12 Difference values for the expression ‘Surprise’

The Figures 6-12 show that there are some variations of information in the successive frames. In reality, the variations can be due to change in the lighting conditions, or other factors. However, we have assumed that the lighting conditions are constant. Hence, the difference in variations of the graph indicates some movements in the skin of the face and movement in the lips. The person does not move her head rather than the only face.

The Figure 13 indicates there is overlapping of the difference values calculated for the successive frames for all the six expressions. The plot shows there is a variation in the contents of the frames.

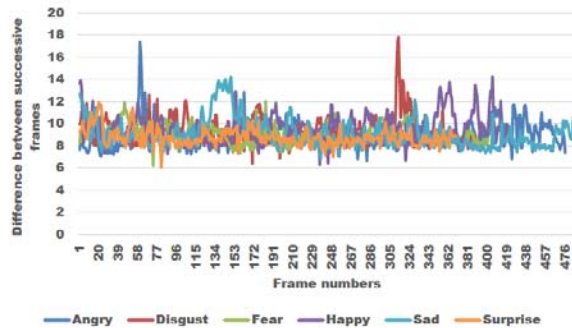


Figure 13 Comparisons of the difference values of the successive frames for six facial expression expression (FEE)

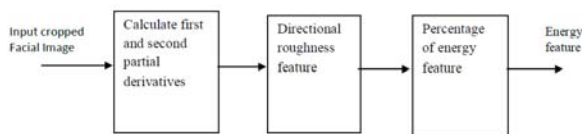


Figure 14 Design of feature extraction

Facial texture segmentation plays an important role in recognizing and identifying a material, type of characteristic for particular image. Wavelets are employed for the computation of single and multi-scale roughness features because of their ability to extract information at different resolutions. Features are extracted in multiple directions using directional wavelet obtained from partial derivative of Gaussian distribution function. The first and second derivative wavelets are used to obtain the features of the textured image at different orientations like 0°, 45°, 90° and 135° and scales such as 1, 2 and 4.

Facial segmentation procedure partition an image into constituent object that is used to find the regions of interests using K-means algorithm. The schematic flow of the extracting energy feature from the textured image is given in figure 14.

2.1. PREPROCESSING

Preprocessing is done for the removal of noise from image using Gaussian smoothing function. In designing Gaussian filters the mask weights are computed directly from the Gaussian distribution, given by equation (1)

$$\phi(x, y, s) = \exp\left\{ -\frac{x^2 + y^2}{2s^2} \right\} \tag{1}$$

Where x, y are directions, and s is the scale

An overlapping moving window size of NxN is used for preprocessing. The coefficient value at the center of the mask is made equal to one by a suitable multiplication factor. When performing the convolution, the output pixel values must be normalized by the sum of the mask weights to ensure that regions of uniform intensity are not affected.

2.2 Directional roughness feature

A wavelet from the exponential wavelet family is used for the computation of roughness features. The 2-D Gaussian smoothing function from equation (1) is partially differentiated with respect to x and y to calculate the first order partial derivatives of the smoothing function along x-axis and y-axis.

Along x-direction (0°)

$$W_0(x, y, s) = \frac{\partial \phi(x, y, s)}{\partial x} = \frac{-x}{s} \exp\left\{ -\frac{x^2 + y^2}{2s^2} \right\} \tag{2}$$

Along y-direction (90°)

$$W_{90}(x, y, s) = \frac{\partial \phi(x, y, s)}{\partial y} = \frac{-y}{s} \exp\left\{ -\frac{x^2 + y^2}{2s^2} \right\} \tag{3}$$

Gradient component or the filtered version of the original image in direction 0° and 90° is calculated by convolving the

original image $f(x,y)$ with the partial derivative filters along x and y directions.

$$W_0(x,y,s) * f(x,y) = \frac{\partial \phi(x,y,s)}{\partial x} * f(x,y) \quad (4)$$

$$W_{90}(x,y,s) * f(x,y) = \frac{\partial \phi(x,y,s)}{\partial y} * f(x,y) \quad (5)$$

The filtered version of the original image along other directions other than 0° and 90° is calculated by using the linear combination of equations 4 and 5 and is given in equation (6)

$$W_\theta(x,y,s) * f(x,y) = [W_0(x,y,s) * f(x,y)] \cos \theta + [W_{90}(x,y,s) * f(x,y)] \sin \theta \quad (6)$$

Where θ - is the directional angle

Similarly, the second order partial derivatives of the smoothing function is calculated along the directions $(0^\circ, 90^\circ)$, $(0^\circ, 0^\circ)$ and $(90^\circ, 90^\circ)$. The second order partial along the direction $(0^\circ, 90^\circ)$ is obtained by partially differentiating $W_0(x, y, s)$ with respect to x as given in equation (7)

$$W_{0,90}(x,y,s) = \frac{\partial^2 \phi(x,y,s)}{\partial x \partial y} = \frac{xy}{s^4} \exp\left\{\frac{-x^2 + y^2}{2s^2}\right\} \quad (7)$$

The second order partial along the direction $(0^\circ, 0^\circ)$ is obtained by partially differentiating $W_0(x, y, s)$ with respect to x as given in equation (8)

$$W_{0,0}(x,y,s) = \frac{\partial^2 \phi(x,y,s)}{\partial^2 x} = \left(\frac{x^2}{s^4} - \frac{1}{s^2}\right) \exp\left\{\frac{-x^2 + y^2}{2s^2}\right\} \quad (8)$$

The partial along the direction $(90^\circ, 90^\circ)$ is obtained by partially differentiating

$W_{90}(x, y, s)$ with respect to y as given in equation (9)

$$W_{90,90}(x,y,s) = \frac{\partial^2 \phi(x,y,s)}{\partial^2 y} = \left(\frac{y^2}{s^4} - \frac{1}{s^2}\right) \exp\left\{\frac{x^2 + y^2}{2s^2}\right\} \quad (9)$$

The filtered version of the original image along other directions is obtained by the linear combination of the equations 7, 8 and 9 as given in equation (10)

$$W_{\theta, \theta+90}(x,y,s) * f(x,y) = [W_{0,90}(x,y,s) * f(x,y)] * \cos 2\theta + 0.5 * \left\{ [W_{0,0}(x,y,s) * f(x,y)] - [W_{90,90}(x,y,s) * f(x,y)] \right\} \sin 2\theta \quad (10)$$

The gradient component along any directions is found by using the equations 6 and 10. The two wavelet transforms of a function $f(x,y)$ at scale s and direction θ are calculated as given in equation (11)

$$W_1 T_f^\theta(x,y,s) = W_0(x,y,s) * f(x,y)$$

$$W_2 T_f^\theta(x,y,s) = W_{\theta, \theta+90}(x,y,s) * f(x,y) \quad (11)$$

where

$W_1 T_f^\theta(x,y,s)$ – is the first derivative wavelet

$W_2 T_f^\theta(x,y,s)$ – is the second derivative wavelet.

Figure 15-17 show the directional values along y -axis for different angles of rotations of Gabor filter. The x -axis shows the different locations of the image. Figure 18 shows the final output of the Gabor wavelet output.

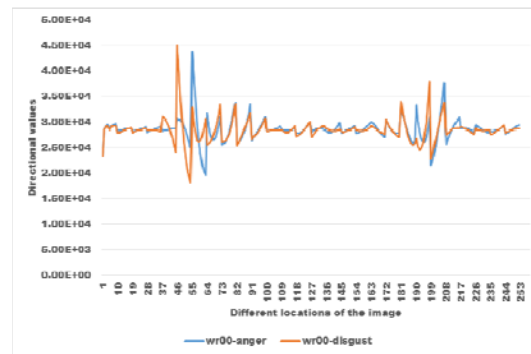


Figure 15 Directional values along wr00

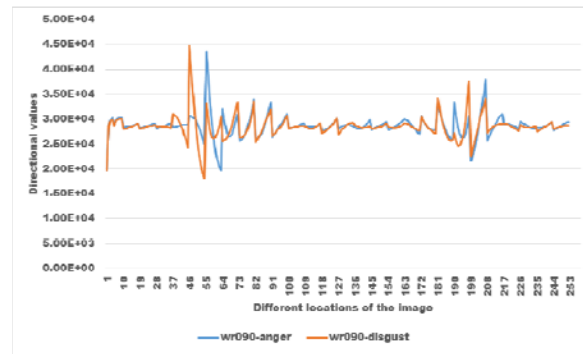


Figure 16 Directional values along wr090

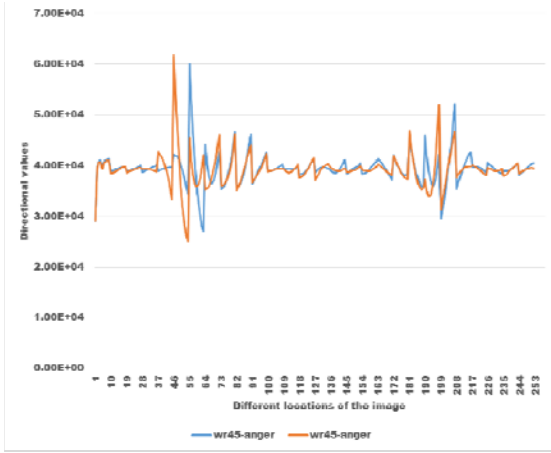


Figure 17 Directional values along wr45

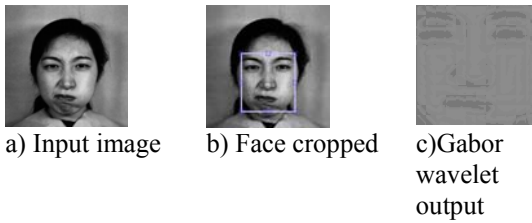


Figure 18 Final output of wavelet Gabor texture extraction

2.3 The directional roughness features (R_s^θ)

The directional roughness features is obtained by finding the arithmetic average in a 9×9 window for the two wavelet transforms given in the equations 11 and 12 with different orientations and scales. The wavelet with the maximum is selected as given in equation (13)

$$R_s^\theta \approx \langle \max |W_i T_f^\theta(u, v, s)| \rangle_{N \times N} \quad (13)$$

$\langle \rangle$ $N \times N$ – arithmetic average in an $N \times N$ window
 $i = 1, 2$ (1 and 2 derivative wavelet)

2.4 Percentage of energy feature

The effect of roughness depends on the relative texture energy between different directions. The roughness features are weighted with the percentage of textural energy existing in the corresponding direction. The energy computed in direction θ using an s -scale wavelet is given by equation (14).

$$E_{s,i}^\theta = \langle |W_i T_f^\theta(x, y, s)| \rangle_{N \times N} \quad (14)$$

Total Energy

The total energy at scale s is obtained from equation (15)

$$E_{s,i}^{total} = \sum_{\theta} \langle |W_i T_f^\theta(x, y, s)| \rangle_{N \times N} \quad (15)$$

4.2.5.1 Percentage of Energy

The percentage of energy feature computed in direction θ and scale s is given by equation

$$\text{Per}_{s,i}^\theta = \frac{E_s^\theta}{E_s^{total}} \quad (16)$$

where

E_s^θ is the energy computed in direction θ

E_s^{total} is the total energy

The percentage of energy $\text{Per}_{s,i}^\theta$ is insensitive to the absolute image illumination because energy is computed using exponential wavelets where the dc component is removed. It is also insensitive to contrast changes, because E_s^θ and E_s^{total} is multiplied by a constant multiplicative term.

The output of wavelet Gabor filter is used as input for Fisher's linear discriminant function for obtaining transformed higher dimensional feature vector into two dimensional vector by computation of discriminant vectors ϕ_1 and ϕ_2

The Fisher's criterion is given by

$$J(\phi) = \frac{\phi^T S_b \phi}{\phi^T S_w \phi} \quad (17)$$

$$S_b = \sum_{i=1}^m P(\omega_i) (m_i - m_o)(m_i - m_o)^T \quad (18)$$

$$S_w = \sum_{i=1}^m P(\omega_i) E[(x_i - m_i)(x_i - m_i)^T / \omega_i] \quad (19)$$

Where

S_b is the between class matrix, and

S_w is the within class matrix which is non-singular.

$P(\omega_i)$ is a priori the probability of the i^{th} pattern, $P(\omega_i) = 1/m$,

m_i is the mean vector of the i^{th} class patterns, $i=1, 2, \dots, m$;

m_o is the global mean vector of all the patterns in all the classes.

$X = \{X_i, i=1, 2, \dots, L\}$ is the n -dimensional patterns of each class.

The discriminant vector that maximizes J in equation (17) is denoted by ϕ_1 . The vector ϕ_1 is found as a solution of the Eigenvalue problem given by equation (20).

$$S_b \varphi_1 = \lambda_{m1} S_w \varphi_1 \quad (20)$$

Where λ_{m1} is the greatest non-zero eigenvalue of $S_b S_w^{-1}$. The eigenvector corresponding to λ_{m1} is φ_1 . Another discriminant vector φ_2 is obtained by using the same criterion of equation (17). The vector φ_2 should also satisfy the equation given by equation (21).

$$\varphi_2^T \varphi_1 = 0.0 \quad (21)$$

The equation (21) indicates that the solution obtained is geometrically independent. The discriminant vector φ_2 is found as a solution of the Eigen value problem, which is given by equation (22).

$$Q_p S_b \varphi_2 = \lambda_{m2} S_w \varphi_2 \quad (7 \quad 22)$$

Where

λ_{m2} is the greatest non-zero eigenvalue of $Q_p S_b S_w^{-1}$ and Q_p is the projection matrix given by equation (23).

$$Q = I - \frac{\varphi_1 \varphi_1^T S_w^{-1}}{\varphi_1^T S_w^{-1} \varphi_1} \quad (23)$$

Where, I is an identity matrix. Figure 19 shows the effect of eigenvalue in differentiating the different expressions. Eigen value for three different frames of three different expressions are plotted in Figure 19 that indicate distinguished difference among different facial images, This is an indication that, eigenvalue process can be applied for facial image identification.

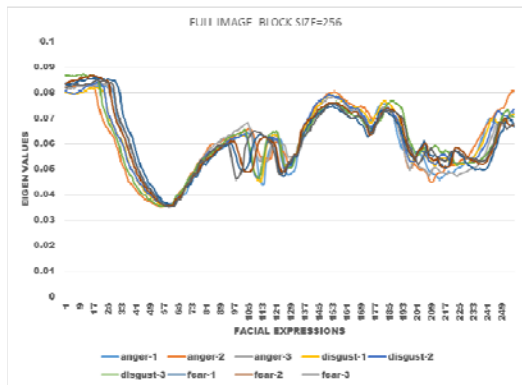


Figure 19 Eigen value plot for different frames

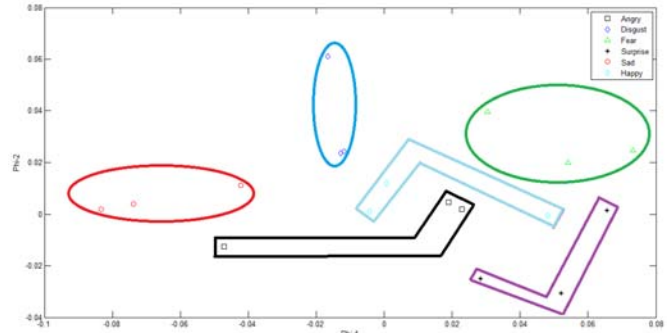


Figure 20 Plot of discriminant vectors for all six expressions

In equation (22), S_w should be non-singular. It is necessary that S_w should be non-singular, even for a more general discriminating analysis and generating multi orthonormal vectors, If S_w is singular, S_w should be made on-singular, by using singular value decomposition (SVD) method and perturbing the matrix. By using equations (20 and 22), the values of φ_1 and φ_2 discriminant vectors are obtained and presented in Figure 20. In this figure, the expressions happy and sad are scattered and not cluttered. The other expressions are cluttered.

The 2-dimensioal vectors set are denoted by Y_i . The vector Y_i is given by equation (24).

$$Y_i = (u_i, v_i) = \{ X_i^T \varphi_1, X_i^T \varphi_2 \} \quad (24)$$

The vector set Y_i , is obtained by projecting the original vector 'X' of the patterns onto the space spanned by φ_1 and φ_2 by using equation 24.

V. CONCLUSION

In this paper, sample images with expressions are used for training and testing the proposed system of expression identification. Wavelet Gabor filter, Fisher's linear discriminant function are used to implement the system. The performance of the system is purely based on the quality of the images. The future work includes in analyzing the proposed system and its suitability for people with different origins.

REFERENCES

- [1] Bänziger, T., Mortillaro, M., & Scherer, K. R. (2012). Introducing the Geneva Multimodal expression corpus for experimental research on emotion perception. *Emotion*, 12, 1161–1179. doi:10.1037/a0025827.
- [2] Cheng, F. , Yu, J. , & Xiong, H. (2010). Facial expression recognition in jaffe dataset based on Gaussian process classification. *IEEE Transactions on Neural Networks*, 572 21(10), 1685–1690.
- [3] Klaus R. Scherer and Ursula Scherer, 2011, Assessing the Ability to Recognize Facial and Vocal Expressions of Emotion: Construction and Validation of the Emotion Recognition Index, *J Nonverbal*

- Behav., Vol.35, pp.305–326., DOI 10.1007/s10919-011-0115-4.
- [4] Oliveira, L. E. S. , Koerich, A. L. , Mansano, M. , & Britto, A. S. Jr. , (2011). 2d principal component analysis for face and facial expression recognition. *Computing in Science and Engineering*, 13(3), 9–13.
- [5] Ravi S., and Mahima S., 2011, Study of the Changing Trends in Facial Expression Recognition, *International Journal of Computer Applications* (0975-8887), Vol.21. No.5, pp.10-16.
- [6] Ruffman, T. (2011). Ecological validity and age-related change in emotion recognition. *Journal of Nonverbal Behavior*, 35, 297–304. doi:10.1007/s10919-011-0116-3
- [7] Schlegel, K., Grandjean, D., & Scherer, K. R. (2012). Emotion recognition: Unidimensional ability or a set of modality- and emotion-specific skills? *Personality and Individual Differences*, 53, 16–21. doi:10.1016/j.paid .2012.01.026.

Reduce collision in assigned tree slotted aloha anti-collision protocol in the RFID anti-collision systems

Akram Shangi ghahi¹, Mohammad Ali Pourmina²

Abstract—Radio Frequency Identification (RFID) is a wireless technology that has replaced barcodes.

The major advantages of radio frequency identification (RFID) technology over barcodes are that the RFID-tagged objects do not require to be in line-of-sight with the reader for their identification and multiple objects can be read simultaneously. But when multiple objects are read simultaneously there is always a problem of collision which reduces the efficiency of the system. But when multiple objects are read simultaneously there is always a problem of collision which reduces the efficiency of the system. In this study new algorithms called DyATSA (Dynamic Assigned Tree Slotted Aloha) and DyImATSA (Dynamic Improved Assigned Tree Slotted Aloha) have been proposed to the third category of Hybrid-based. These two proposed algorithms have been made dynamic by adding new method to ATSA protocol to determine the F0 value prior to the identification of tags.

To evaluate the proposed method, two of the most important network parameters including the number of collision slots and idle slots rate were studied in constant tags. By comparing the results of the diagrams, it can be concluded that DyImATSA protocol toward ImATSA protocol, show network performance improvement in tag identification process in simulations.

Index Terms—RFID, Anti-Collision, ATSA protocol, Radio Frequency Identification (RFID), Slotted Aloha protocol.

I. INTRODUCTION

An RFID system consists of three components: the tag, the reader, and the middleware.

Tags can have different sizes, shapes, and capabilities, but there are mainly two types: active and passive. An active tag contains a battery, the energy of which operates the tag. A passive tag does not have a battery and operates from the radio frequency signal that comes from the RFID reader. Compared to a passive tag, an active tag is larger in size since it comes with a battery. In today's market, passive tags are inexpensive compared to active tags, and they last longer. Data contained in the tag is used to identify an object. This data can be simply an identification number or it can be information about the

object. Also we have two types of tags: constant and movable. In this paper, common systems of RFID that consist of a reader and some constant Passive tags are considered.

Anti-collision occurs when multiple RFID tags respond to a query that the RFID reader sends to identify tags in its range. Anti-collision protocols are used to avoid tag collision. There are basically two types of anti-collision protocols: probabilistic and deterministic. Protocols of a probabilistic nature do not guarantee the time required to read all tags. The Aloha protocol is probabilistic in nature, and the Binary Tree protocol is deterministic in nature. Binary Tree protocols are capable of identifying tags by querying different levels of the tree based on the tag prefix distributed on the tree [1].

Anti-collision protocols, such as SDMA (space division multiple access), FDMA (frequency division multiple access) and CDMA (code division multiple access) are not applicable to the RFID environments [2]. A variety of anti-collision protocols (also called collision resolution or arbitration protocols) have been proposed in the literature, which can be categorized into three classes, namely tree-based [3], [4], Aloha-based [5] and hybrid protocols [6], [7].

If collision occurs, before the identification tags process is completed, these protocols need to identify all tags in the area precisely and fast, because it is likely that the tags go out of range of the reader.

In Aloha-based protocols with estimation, dynamic frame slotted Aloha [8] is widely applied. Dynamic FSA configures an identification process with some continuous frames consisting of slots, and dynamically adjusts a frame length. Compared with fixed framed slotted Aloha, Dynamic FSA can achieve a higher efficiency value of 0.37. To improve the identification efficiency, someone integrates tree algorithms into Aloha-based protocols, and proposes several hybrid protocols likes TSA protocol [9].

In tree-based protocols, colliding tags are recursively split into disjoint subgroups until there is at most one tag in each group. These protocols have the advantage of successfully recognizing all the tags even when the number of tags is vast [10]. The query tree algorithm (QT) uses binary splitting strategy to identify tags. Also, if the received tag IDs collide, the extended prefix attached '0' or '1' to the prefix is retransmitted. Furthermore, if there is no collision, the reader identifies one of the tags.

In [11], [12], some hybrid protocols have been proposed by combining the advantages of tree-based and Aloha-based protocols. Most of them first implement a tree-based

¹ Corresponding Author: Akram Shangi Ghahi is with the Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran (a.shangi@srbiau.ac.ir).

² Mohammad Ali Pourmina is with the Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran (Pourmina@srbiau.ac.ir)

procedure or an estimation procedure to obtain an approximate number of tags, then combine a variation of Aloha or tree protocol to reduce the identification delay. In general, hybrid protocols can provide relatively better performance than tree-based and Aloha-based protocols. So we have used hybrid protocols in this study.

II. THE PROPOSED PROTOCOLS

Now in this article presents two new simple but efficient hybrid tag anti-collision protocols, termed dynamic assigned tree slotted Aloha (DyATSA) and dynamic improved ATSA (DyImATSA), respectively. And a new method is added to ATSA protocol which determines F_0 value prior to the tags identification process. In fact, by adding this to ATSA and ImATSA, the identification process is made more dynamic.

These protocols combine the idea of the traditional QT protocol with that of the DFSA protocol. The collision resolution idea of QT is that the reader repeatedly queries tags' ID prefixes so as to split tags into small subgroups until there is at most one tag in each subgroup. It can provide deterministic identification via easy implementation, however, the reading process is very slow [10].

In ATSA protocol, a special prefix is used for each frame and slot that the reader assumes QT empty at the beginning and then begins the first frame with the Query (pre, F) command. (It should be noted that F is the length of the frame and a number of square 2 and pre prefix records collision slots and the first frame pre is an empty string). At this stage, the tags in the reader range receive this order and compare it with their own ID. It means they compare received pre prefix with their own tpre prefix and if they are the same, respond the reader [13]. Tpre for each tag is obtained from the following equation:

$$P = \log_2^F (F \text{ should be chosen from numbers of } S_2) \text{ that } P \text{ is the number of bits which are obtained from left side of ID address to obtain tpre.}$$

At the beginning of algorithm, F_0 is considered as a random number that shows the quantity of slots, which exist in any frame and is a number of S_2 . Our goal in this study is to present a method for primitive selection of F.

In a frame, tags first match their ID with the frame prefix. When matched, tags then match their tpre with the slot prefix and reply in the matching slot. During the frame, the reader records the prefixes of every collision slots. Since the length of the frame changes in any stage and the reader is not aware of the number of the tags so, the number of the tags is found through the number of collided, unemployed, and successful slots of previous stages and it determines the length of frame via this method. In this paper, the Vogt estimation algorithm is applied. [14]

The ATSA protocol can be further improved by using Manchester encoding to reduce the influence of tag density. That is called ImATSA. [10]

In this paper by making an algorithm, we will determine the length of the frame and send them to the tags. That's why we use the flow diagram in Fig 1. This section will propose a dynamic ATSA protocol, whose procedure involves dynamic

frame length adjustment and ATSA algorithm. The benefit of dynamic ATSA is that its adjustment procedure is very simple because a reader can obtain a reasonable frame length by judging only the first slot type.

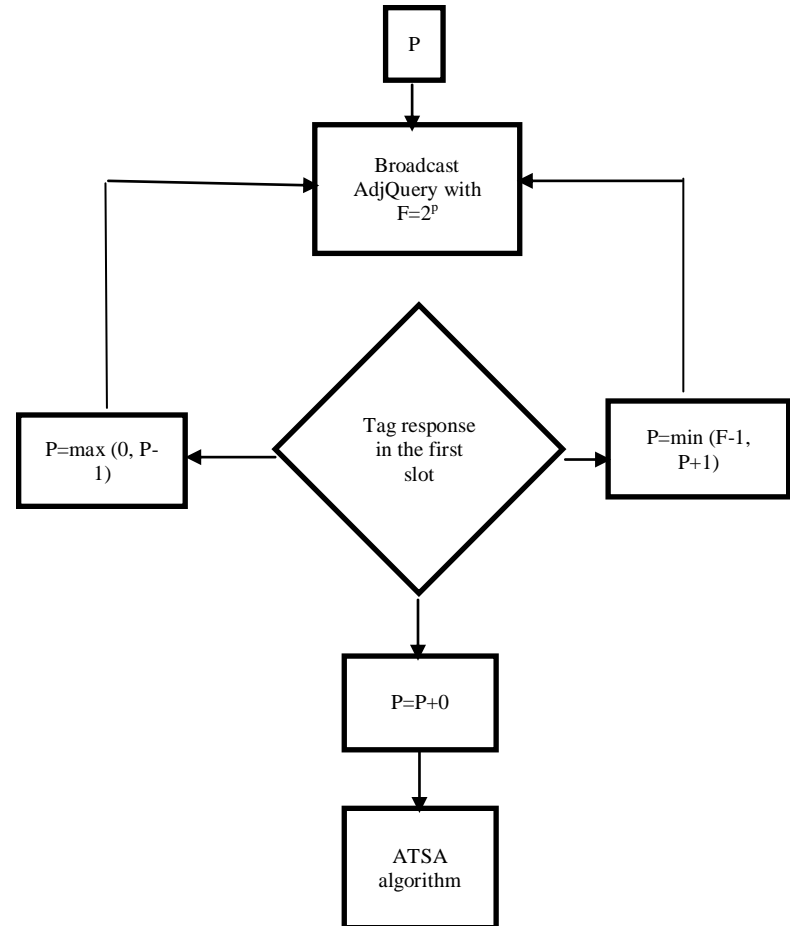


Fig 1. DyATSA protocol Flow diagram

Initially, a frame length is $F = 2^P$. Then, a reader broadcasts an AdjQuery command with F. After a tag receives the command with F, the tag's Counter selects a random integer from 0 to F - 1. Tags whose Counters select 0 can transmit their IDs, and the reader will detect the tags responses in the first slot. If the first slot is collisional, $P = P + 1$, and the reader will broadcast a command with a new F and then detect tags responses in the first slot of next frame. If the first slot is idle slot, by choosing $P=P-1$, reader sends a new value of P and waits for tag's response and If the first slot is successful, P will not be changed and the reader's operation will transit to ATSA algorithm.

III. SIMULATION

In this study, the Simulator NS2, 2.35 Version was used. The type of the net is wireless net in this simulator. common systems of RFID that consist of a reader and some constant Passive tags are considered.

1. Simulation Configuration

Received energy is 0.76 MW and sent energy is 0.28 MW. The number of tags is considered as 5000 tags and the number of readers as 1.

In the simulation process of this study, at first, the results of simulation in some diagrams named collision and idle slots are shown and the results are normally obtained after 150 times. We also focus on the length of the ID (12 and 96 bit) in order to simplify everything. However, For the 96-bit ID, we cannot simulate all the 2^{96} tags. We only test a subset of 2^{16} tags at most.

2. Implementation of DyATSA and ImDyATSA methods (length of ID = 12Bit)

In this part of the simulation, the length of ID was considered as 12 bits and the two suggested methods were simulated and the results were compared with together.

Fig 2. Diagram of the collision slots in DyImATSA and DyATSA methods (length of ID = 12bits)

As the diagrams in Fig 2 indicate, between the methods with tag quantity of below 2500, the DyATSA method and DyImATSA acted the same but in high quantity of tags the difference between DyAtSA and DyImATSA is obvious.

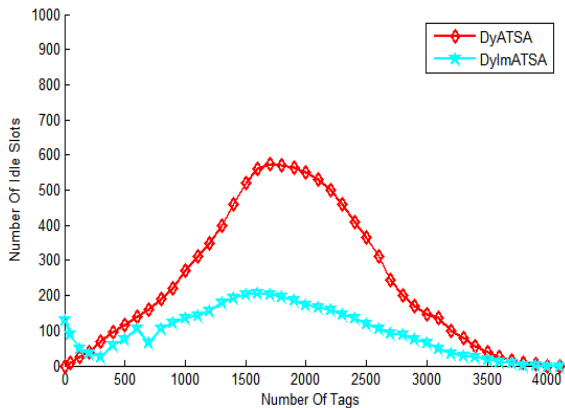
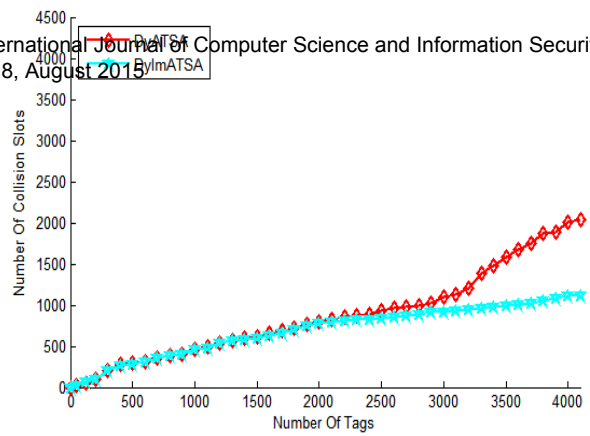


Fig 3. Diagram for the number of idle slots in DyImATSA and DyATSA methods (length of ID = 12bits)

If the number of idle slot is less than the optimum, it means that the reader can finish the identification process in less number of frames and finally less energy is consumed. So, by comparing the number of idle slots in different methods we can analyze their function. The diagram for the number of idle slots in identification process is presented in Fig 3. If the quantity of the tags is more than 3500, it will have the same function. Now it is the time to look into the effect of frame length activation in protocols as well as applying Manchester Encoding in the process of identification. Concerning the comparison of the red diagram (DyATSA) with the green one (DyImATSA), it can be revealed that the Manchester Encoding method and the activation of ATSA method seem to be more effective.



3. Implementation of DyATSA and ImDyATSA methods (length of ID = 96Bit)

Here in this section, the simulations of tags ID with 96 bits are done. Regarding the diagram of the Fig 4 and 5 changes in the number of collision slots and idle slots at diagnosis labels proposed by the two methods, the difference in the number of 96 bits to 12 bits ID is more evident.

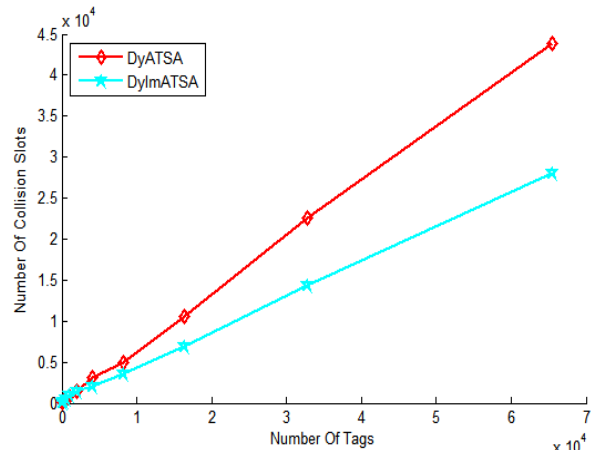


Fig 4. Diagram of the collision slots in DyImATSA and DyATSA methods (length of ID = 96bits)

Especially when the number of tags is more than 2^{14} the number of collision and idle slots in the protocol DyATSA with large steep rises, that indicate the DyImATSA protocol is better than DyATSA.

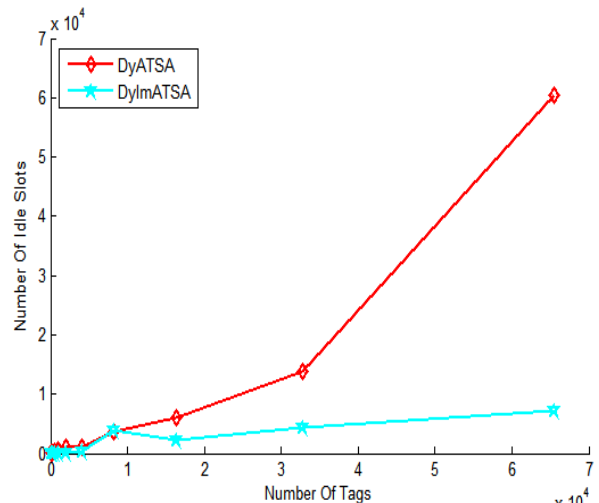


Fig 5. Diagram for the number of idle slots in DyImATSA and DyATSA methods (length of ID = 96bits)

IV. CONCLUSION

When an RFID system identifies multiple tags, tag collisions will happen. The RFID system generally applies a tag anti collision protocol to resolve the multi tag collisions. This paper utilizes ATSA algorithm to propose two protocols: dynamic ATSA protocol and dynamic ImATSA protocol. The proposed protocols not only have higher efficiency but also require no estimation of the number of tags, and hence can avoid the computational cost of the estimation. Furthermore, since the proposed protocols always can adjust a frame to a reasonable length for the number of tags, their efficiency will not be affected by the variance of the number of tags. When the number of tags suddenly increases or decreases much, the underutilization of channel and low efficiency will not happen. Regarding the comparison of the diagrams, it can be concluded that the protocol of DyImATSA outperformed DyATSA in simulations and improvement of network performance in case of efficiency increase in the process of tag identification. Hence, the present research presented two mixed methods, which successfully led to system collision decrease in relation to other previous comparable methods.

REFERENCES

- [1] Namboodiri, V., and Gao, L., "Energy-Aware Tag Anti-Collision Protocols for RFID Systems," PerCom '07, Fifth Annual IEEE International Conference on Pervasive Computing and Communications, 19 March 2007, pp. 23-36.
- [2] D. K. Klair, K. W. Chin, and R. Raad, "A survey and tutorial of RFID anti-collision protocols," IEEE Commun. Surveys Tuts. vol. 12, no. 3, pp. 400-421, 2010.
- [3] C. Law, L. Lee, and K. Y. Siu, "Efficient memoryless protocol for tag identification (extended abstract)," C. Law, K. Lee, and K.-Y. Siu, "Efficient Memoryless Protocol for Tag Identification (Extended Abstract)," Proc. ACM Discrete Algorithms and Methods for Mobile Computing and Comm. (DIALM '00), pp. 75-84, 2000.
- [4] L. Pan and H. Y. Wu, "Smart trend-traversal protocol for RFID tag arbitration," IEEE Trans. Wireless Commun., vol. 10, no. 11, pp. 3565-3569, 2011.
- [5] M. V. Bueno-Delgado, J. Vales-Alonso, and F. J. Gonzalez-Castaño, "Analysis of DFSA anti-collision protocols in passive RFID environments," in Proc. IEEE Conf. Industrial Electron., pp. 2630-2637, 2009.
- [6] J. Vales-Alonso, V. Bueno-Delgado, E. Egea-Lopez, F.J. Gonzalez-Castaño, and J. Alcaraz, "Multiframe Maximum-Likelihood Tag Estimation for RFID Anticollision Protocols," IEEE Trans. Industrial Informatics, vol. 7, no.3, pp. 487-496, Aug. 2011.
- [7] T. F. L. Porta, G. Maselli, and C. Petrioli, "Anticollision protocols for single-reader RFID systems: temporal analysis and optimization," IEEE Trans. Mobile Comput., vol. 10, no. 2, pp. 267-279, 2011.
- [8] S.R. Lee, S.D. Joo, and C.W. Lee, "An Enhanced Dynamic Framed ALOHA Algorithm for RFID Tag Identification," Proc. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services, pp. 1-5, 2005.
- [9] M.A. Bonuccelli, F. Lonetti, and F. Martelli, "Tree Slotted ALOHA: A New Protocol for Tag Identification in RFID Networks," Proc. Int'l Symp. World of Wireless, Mobile and Multimedia Networks, pp. 1-6, 2006.
- [10] Zhang, Lijuan; Zhang, Jin; Tang, Xiaohu, "Assigned Tree Slotted Aloha RFID Tag Anti-Collision Protocols," IEEE Transactions on Wireless Communications, vol.12, no.11, pp.5493,5505, November 2013.

- [11] M.K. Yeh, J.R. Jiang, and S.T. Huang, "Adaptive Splitting and Pre-Signaling for RFID Tag Anti-Collision," Computer Comm., vol. 32, no. 17, pp. 1862-1870, Nov. 2009.
- [12] Y. Lai, L. Hsiao, H. Chen, C. Lai, and J. Lin, "A novel query tree protocol with bit tracking in RFID tag identification," IEEE Transactions on Mobile Computing, vol.12, no. 10, pp. 2063-2075, Oct. 2013.
- [13] Chiu-Kuo Liang; Hsin-Mo Lin, "Using Dynamic Slots Collision Tracking Tree Technique Towards an Efficient Tag Anti-collision Algorithm in RFID Systems," Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on , vol., no., pp.272,277, 4-7 Sept. 2012.
- [14] H. Vogt, "Efficient Object Identification with Passive RFID Tags," Proc. First Int'l Conf. Pervasive Computing, pp. 98-113, Jan. 2002.



Akram Shangi Ghahi was born in Tehran, Iran, in 1988.

She acquired the B.Sc. degree in Electronics Engineering from Adiban University, Garmsar, Iran in 2011. She is a M.S. student in

Communications Engineering at science and Research Branch, Islamic Azad University, Tehran, Iran, now. Her major fields of interest are networks communications and RFID systems. She is currently working as a RFID expert.



Mohammad Ali Pourmina is associated professor in electrical engineering (Telecommunication) in Science and research Branch, Islamic Azad University, Tehran, Iran.

He received his Ph.D. degree in electrical engineering (Telecommunication) at Science and research Branch, Islamic Azad University, Tehran, Iran, in 1996 and joined to this university 1996. He has been a member of Iran Telecommunication research center since 1992. He has performed research in the areas of packet radio networks and digital signal processing systems since 1991. His current research interests include spread-spectrum systems, cellular mobile communications, indoor wireless communications, DSP processors and wireless multimedia networks.

Enhanced Secure Hash based Client Puzzle approach to defend against Cyber Attacks

M.Uma
Ph.D Research Scholar
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore -641043

Dr.G.Padmavathi
Professor and Head
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore -641043

ABSTRACT

Game theory is a widely used technique for network security. As technology grows, the cyber worlds are more vulnerable to unknown cyber attacks. There are many cyber attack detection methods available for known attacks; however, efficient methods are essential to detect the unknown cyber attacks. In this research work, an enhanced hash based game theory approach is introduced to defend against cyber attacks. The proposed method is tested in a simulated environment and the method is evaluated using the performance metrics like Throughput, End to end delay, Packet delivery ratio, routing overhead, energy consumption and latency.

KEYWORDS: Game theory, Client puzzle, Hash Chain, Cyber Attacks, Elliptic curve cryptography

1. INTRODUCTION

Passive attack is a process of hacking the communicated data without giving any alerts [1]. There will not be any mess up in the network. There are still more challenges in detecting the passive attacks. Traffic monitoring, Eavesdropping, Traffic analysis and Syn flooding are the termed as passive attacks [2] [3]. Though many methods are available some more efficient techniques are still needed to handle unknown cyber attacks.

Now a days, as technology grows the vulnerability also higher for hacking the data or information. In the year 2009, in cyber leap year summit it is suggested that game theory plays a

major role in network security. Game theory is nothing but a security game played by the attacker and the defender [12]. In the game theory approach the attacker and the defender can play a game as single stage, two player and non-zero sum games [13]. The existing game theory approach for network security problem and the author [14] classifying the solution into two categories namely attack-defense analysis and security measurement. Moreover the game theory based solution for network security is commonly classified [15] into two categories namely cooperative game models and non-cooperative game models. In the game theory approach consists of four basic elements say Players, Actions, Payoff and Strategies. The games applied in game theory approach are broadly classified into three various methods and they are based on the number of stages, Based on perfect information or not and Based on complete information or not. The classification of game theory applications in network security, the notions are System, Attacker, Attack target, Intrusion Detection System, Virtual sensor and Defender.

Client puzzle protocol (CPP) is an algorithm [16] which is used to harden the process of hacking the network resources. The basic concept of this CPP is requesting all the clients which are connected to the server to solve the mathematical puzzle in a given time to establish a connection. Each client will send the solution to the server after solving the puzzle. After that, the server will verify the solution and will decide to establish a connection or to drop a connection.

Client puzzle protocol plays a vital role in network security, developed in the year 1992 against email spam. Client puzzle is basically based on hash function; hardly one or two hash function is required to generate a puzzle [6]. Nash equilibrium [10] is also used for client puzzle to defend against flooding attacks. Puzzle generation is the most important process in game theory as it should contain few uniqueness [15] in its future and they are the puzzle must be easier for the server to generate and it should be harder for the client to solve. And the puzzle computational cost must be lesser for the server than the client. Every client must be allotted only a short time to solve the puzzle.

The paper is organized as follows. Related works are discussed in Section 2. In Section 3 overview of the proposed methodology is given 5. Experimental setup, simulation parameter along with experimental results in Section 4. Finally, conclusion in Section 5.

2. RELATED WORKS

Some of the related works of the method proposed is given below

Brent Waters et al., (2004) introduced a new technique to handle denial of service attacks. They use a robust external service called bastion for distribution. The author aims to provide unique puzzle solution, per-channel puzzle distribution, per-channel puzzle solution, random-beacon property, Identity-based key distribution and Forward security. The author declares that the method developed by them is more resistant in handling over 80% DoS over the existing methods. This method is cheap in applying at the IP level and at higher level of the protocol stack. The method also provides an opportunity to solve the puzzle in offline. Diffie – Hellman agreement is used for puzzle generation.

Mehran S. Fallah (2010) proposed a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios. The author proposed four methods namely PDM1 for open-loop solution and which is not applicable when the payoff is higher, PDM2 proposed for closed loop solution but which is not capable in handling the single-source attacks, PDM3 for known coalition size is an extension of PDM2 which deals with distributed attacks and PDM4 in which the size of the attack coalition is assumed unknown.

Lakshmi Kuppusamy et al., (2012) proposed a number theoretic puzzle against denial of service attacks. They introduced a new variant of the interval discrete logarithm assumption problem and showed the hardness of this new problem under the factorization and composite interval discrete logarithm assumptions. The author declares that the puzzle proposed is much faster to verify than the existing number theoretic puzzles. for the 512-bit RSA modulus, the solution verification time of proposed is approximately 89 times faster when compared with Rivest et al. puzzle and by approximately 50 times faster when compared with Karame- Capkun puzzle.

T. Shanmugapriya et al., (2013) in their research work the optimal puzzle-based defense strategies are developed. The proposed method provides a complete flooding attack solution is likely to require some kind of defense during the attack traffic identification.

Vancha Maheshwar Reddy et al., (2013) suggest a Game theory based strategy to create a series of defense mechanisms using puzzles to defend against flooding attacks. Author used the concept of Nash equilibrium is used to handle sophisticated flooding attack to defend distributed attacks from unknown number of sources.

3. OVERVIEW OF THE PROPOSED METHODOLOGY

The proposed method consists of few steps and they are discussed in detail in this section. The flow of the proposed method is given in figure.1

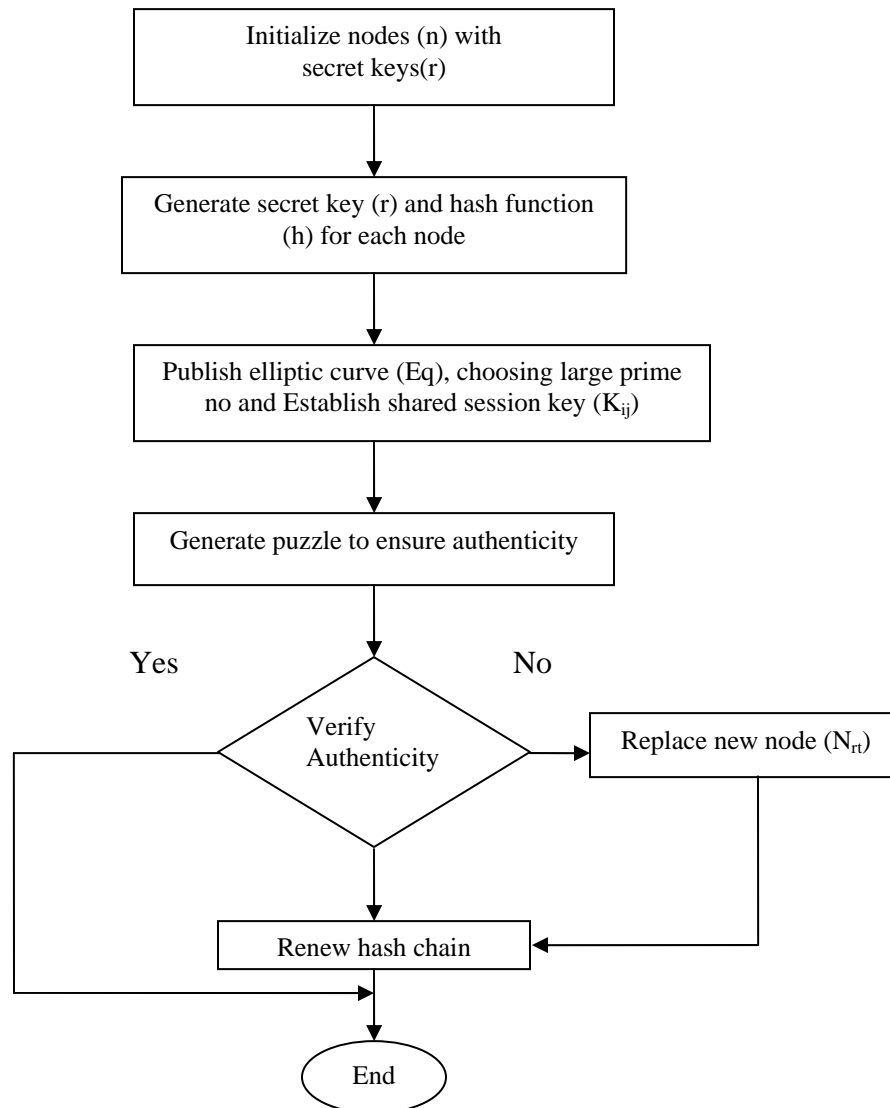


Figure.1 Flow of the proposed method

3.1. Steps of the Proposed Method

The proposed method consists of some phases which are discussed below in various sections. The notations used in the proposed method are given in following table:

Step.1 Initialization Phase

Initiates secret keys and hash function for the nodes of a designated are

Step.2 Authentication

Each node solves puzzle for authentication and key establishment between nodes.

Client puzzle is the process of sending the puzzle by the server to client before executing the client request. Upon receiving the puzzle, every client has to solve the puzzle within the given period of time in order to access the server. The puzzle generated by the server must be harder for the client to solve. The steps involved in client process are

- Step 1 C → S: sending service request*
- Step 2 S: generation of a puzzle*
- Step 3 S → C: sending a description of the puzzle*
- Step 4 C: solving the puzzle*
- Step 5 C → S: sending solution to the puzzle*
- Step 6 S: verification of the solution. If the solution is correct:*
- Step 7 S: continue processing a service request*

Step.3 Key establishment phase

Generate session key randomly to verify the authenticity of the node.

Step.4 Elliptic Curve Cryptography on new node failure phase

Add new node on failure of any existing node with secret key, random number and ECC parameter.

Elliptic Curve Cryptography (ECC) is popular nowadays for key generation. The key will be generated using ECC is a shorter one. The benefits of using ECC help in reducing the energy consumption, lower bandwidth usage and execution will be faster when compared with other algorithms. ECC can be defined as

$$E: y^2 + xy = x^3 + ax^2 + b$$

a, b ---> finite binary fields

x, y ----> set of all points on E

Step.5 Game theory on hash chain renewal phase

Renew the hash chain for the new node updated.

3.2. Proposed Method Algorithm

Game theory plays a major role in security in recent years. In this phase the cyber attack is handled using game theory approach. The proposed method consists of few steps and they are discussed in detail in the following sections:

Table.1 Proposed Method Algorithm

<p><i>Input:</i></p> <p><i>S</i> → <i>Source Node</i> <i>D</i> → <i>Destination Node</i></p> <p><i>Procedure:</i></p> <p><i>repeat</i></p> <p> <i>for each neighbor nodes</i></p> <p> <i>S sends a RREQ to all nodes</i></p> <p> <i>check sequence number</i></p> <p> <i>check key</i></p> <p> <i>sends puzzle</i></p> <p><i>do if nodes solves puzzle</i></p> <p> <i>establish connection</i></p> <p> <i>forward packets</i></p> <p> <i>then stop</i></p> <p> <i>end if</i></p> <p><i>else</i></p> <p> <i>exit</i></p> <p><i>end</i></p> <p><i>until end of the node</i></p>

4. RESULTS AND DISCUSSIONS

The simulated environment, simulation parameter, performance metrics and results are discussed in detail in this section.

4.1 Simulation environment

The proposed methodology is simulated under Linux Fedora, using the Network Simulator NS2 version ns-allinone-2.35.

4.2 Simulation Parameter

The below table shows the simulation parameters used in this method:

Table.1. Simulation Parameter

Parameter	Value
Simulator	NS-2
Channel Type	Wireless
Number of nodes	20,40,60,80,100
Traffic Model	CBR
Maximum mobility	60 m/s
Terrain area	1000m x 1000m
Transmission Range	250m
Routing Protocol	AODV
MAC protocol	802.11
Observation Parameter	End to end delay, Packet loss, Throughput, Latency, Routing Overhead

4.3 Performance Metrics

The proposed methodology is evaluated for its efficiency using the following parameters.

Throughput

The network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in data packets per second or data packets per time slot i.e. number of bytes of data that is transferred per second between source and destination.

Routing Overhead

The total number of routing packets generated and forwarded at the time simulation

Average Packet Delivery Ratio

Average Packet Delivery Ratio is calculated for every 10 seconds. This performance metrics shows the efficiently the packets are delivered between the source and the destination. The packet delivery ratio is calculated using the following equation:

$$\text{Packet delivery ratio} = \frac{\text{receivedpackets}}{\text{sentpackets}} * 100$$

Average End to End Delay

The performance of the proposed method is evaluated in terms of end-to-end delay. Total time utilized to transmit the data from source to the destination.

False Acceptance Rate

The false acceptance rate is a fraction of negative entry or unauthorised user was incorrectly identified as positive entry or unauthorised user and it will be calculated using the following formula:

$$FAR = \frac{\text{number of false rejections}}{\text{number of client accesses}}$$

False Rejection Rate

The false rejection rate is a fraction of positive entry or unauthorised user that was correctly identified as negative entry or unauthorized user and it will be calculated using the following formula:

$$FRR = \frac{\text{number of false accep tan ces}}{\text{number of client accessses}}$$

4.4. Results

The results of the proposed method are presented in this section. The graphical representation of the results is also given below:

Table.2 Results of Throughput

Node	Existing Method	Proposed Method
20	1432	3987
40	3438	8908
60	7898	14343
80	14879	17809
100	21233	24569

Table.3 Results of Overhead

Node	Existing Method	Proposed Method
20	70	67
40	102	97
60	146	123
80	189	154
100	213	193

Table.4 Results of Packet Delivery Ratio in Percentage

Node	Existing Method	Proposed Method
20	14	17
40	33	39
60	48	45
80	68	78
100	92	98

Table.5 Results of Delay

Node	Existing Method	Proposed Method
20	0.4522	0.3452
40	0.8431	0.6431
60	0.9272	0.8272
80	1.213	0.7563
100	1.33	1.1243

Table.6 Results of Packet Drop

Node	Existing Method	Proposed Method
10	14	12
20	35	26
30	46	38
40	52	43
50	65	56
60	77	63
70	82	78
80	92	86
90	121	108
100	156	138

Table.7 Results of Average No of claims (Based on time)

Time (Seconds)	True Positive	True Negative	False Positive	False Negative
10	2.3	4.0	6.5	9.0
20	2.4	4.2	6.3	8.9
30	2.5	4.3	6.3	8.9
40	2.5	4.4	6.1	8.7
50	2.6	4.5	6.0	8.6
60	2.9	4.6	5.9	8.6
70	3.0	4.6	5.8	8.6
80	3.2	4.7	5.6	8.5
90	3.7	4.9	5.5	8.5
100	4.1	5.2	5.4	8.4

The average number of claims of the attacker and the defender is calculated and the results are given in the table. 7.

Cyber Attacks	Enhanced Game Theoretic Approach	Existing Method	% of Improvement
Active Attacks	75%	78%	3%
Passive Attacks	69%	71%	2%

The above table.8 shows the accuracy of the proposed method in detecting the cyber attacks.

5. CONCLUSION

In this research work secure hash based game theory approach is introduced to detect the unknown cyber attacks. Hash based client puzzle protocol is used along with elliptic curve cryptography. Every data or information communicated in this method is encrypted. The efficiency in detecting the unknown cyber attacks of the proposed method is evaluated in a simulated environment using network simulator NS2 ns2allinone 2.35. The proposed method detects the unknown cyber attacks and it also evaluated using performance metrics namely Throughput, Routing Overhead, Packet Delivery Ratio, End to end delay, Packet drop ratio, Average No of claims (Based on time and distance). Based on the evaluation result, the proposed method outperforms the existing method.

REFERENCES

- [1].Abhay Kumar Rai et al., “Different Types of Attacks on Integrated MANET-Internet Communication” *International Journal of Computer Science and Security (IJCSS)* Volume (4): Issue (3), pp.265 – 274.
- [2].Priyanka Goyal et al., “A Literature Review of Security Attack in Mobile Ad-hoc Networks” *International Journal of Computer Applications (0975 – 8887)* Volume 9– No.12, November 2010, pp.11-15.

- [3].Dr. G. Padmavathi and Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks” *International Journal of Computer Science and Information Security*,. 4, No. 1 & 2, 2009, pp.1-9.
- [4].Brent Waters et al., “New Client Puzzle Outsourcing Techniques for DoS Resistance” *CCS'04*, ACM, pp. 246-256.
- [5].Mehran S. Fallah, “A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory” *IEEE Transactions on dependable and secure computing*,Vol.7,No.1, p.5-19.
- [6].Lakshmi Kuppusamy et al., “Practical Client Puzzles in the Standard Model” *ASIACCS '12*, ACM.
- [7]. Raju Neyyan, “Game Theory based Defense Mechanism against Flooding Attack using Puzzle” *Emerging Trends in Computer Science and Information Technology - 2012(ETCSIT2012)*, pp.5-10.
- [8].T. Shanmugapriya et al., “Computational puzzles for repudiation of misbehaving users in anonymizing network”, *International Journal of Advances in Engineering & Technology*, May 2013, Vol. 6, Issue 2, pp. 1032-1036.
- [9].Douglas Stebila et al., “Stronger difficulty notions for client puzzles and denial-of-service-resistant protocols” *CT-RSA 2011, The Cryptographers' Track at the RSA Conference*, LNCS, Springer, 2011volume 6558, pp. 284- 301.
- [10]. Vancha Maheshwar Reddy, “Game Theory based Defense Strategy against Denial of Service Attack using Puzzles” *International Journal of Engineering Research and Applications (IJERA)* ISSN: 2248-9622 Vol. 3, Issue 1, January -February 2013, pp.751-757.
- [11]. Animesh Patcha and Jung-Min Park, “A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks” *International Journal of Network Security*, Vol.2, No.2, Mar. 2006, PP.131–137.
- [12]. Tansu Alpcan and Tamer Basar, “A Game Theoretic Analysis of Intrusion Detection in Access Control Systems” *43rd IEEE Conference on Decision and Control*, 2004, pp.1568 – 1573.
- [13]. Martin Rehak et al., “Game Theoretical Adaptation Model for Intrusion Detection System” *Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems – Innovative Applications Track (AAMAS 2011)*, 2011, pp. 1123-1124.

- [14]. Xiannuan Liang and Yang Xiao, “Game Theory for Network Security” IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, 2013, pp.472 – 486.
- [15]. J.Jaikumar, “A Defense Strategy Against Flooding Attack using Puzzles By Game Theory” *International Journal of Computer Trends and Technology (IJCTT) - volume4Issue4 –April 2013*
- [16]. Ari Juels and John Brainard, “Client puzzles: A cryptographic countermeasure against connection depletion attacks” *Proceedings of NDSS '99 (Networks and Distributed Security Systems)*. pp. 151–165.

BIOGRAPHIES



M.Uma is a Ph.D. research scholar of Avinashilingam Deemed University, currently doing research on cyber security. Her areas of interest include Information and communication Security. She has 5 publications in her research work. She is currently the principal investigator for one project funded by DST (WOS-A). She is a reviewer for WSEAS, IJSET and TIJCSA.



Dr.G.Padmavathi is the Professor and Head of computer science of Avinashilingam Deemed University for women, Coimbatore. She has 23 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has 100 publications in her reascher area .In presently she is guiding M.phil researcher and PhD’s Scholar .She has been profiled in various Organizations her academic contributions. She is currently the principal investigator of four projects funded by UGC and DRDO.She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.

fMRI slice registration using Hilbert-Huang transform

¹Magesh, ²S.Purushothaman and ³P.Rajeswari

¹Magesh, Research scholar, Department of MCA, VELS University, Chennai-600117,

²Associate Professor,

²Lecturer, Department of Electrical and Computer Science Engineering,

^{2,3}Institute of Technology, Haramaya University, DireDawa, Ethiopia

ABSTRACT

In this paper, brain image slices are considered for registration task. The Fuzzy logic algorithm is used for registration of the brain image slices. As a convention, floating image has misalignment. The floating image has to be transformed and aligned with the target image. Two approaches can be used to create floating image. The first approach is to use the actual image obtained in scanning and it is considered as the target image. The second approach is to introduce misalignment in an existing image slice to obtain a floating image. The application area considered is, registration of image slices of human brain acquired using magnetic resonance imaging scanner. This paper presents implementation of Hilbert Huang transform for fMRI slice registration.

Keywords: medical image registration, fmri slice, Hilbert-Huang Transform (HHT)

1. Introduction

The field of medical imaging requires registration of images to view the entire 3D shape of the human organs. The location of organ, tissues with different information have to be correctly visualized in the 3-dimensional (3D) model of the reconstructed volume. Visualization helps in identification of tumors, lesions and in performing surgery. It has become a common task in using more than one medical scanning equipment for understanding the anatomical structure and functionality of the human organs. When a scanning equipment is used, it is single modality. When many equipment is used, then it is multimodality. The images acquired from different equipment of the same organ, will have different intensity representations in the acquired images. This is due to inherent capabilities of the machine and the type of file used for storing the images.

The field of medical image analysis includes a variety of image acquisitions that are used for diagnostic and interventional purposes. There has been a significant growth in scanner performance computational power and storage facilities. It is possible to process large size data sets with improved speed and accuracy with the technological advances.

With the growing number of available imaging modalities, a more detailed and complete characterization of the imaged anatomies and functional properties are attainable. The analysis of multiple acquisitions of the same subject, comparisons of images across subjects or groups of subjects are done by the doctors.

The medical experts rely on manual comparisons of images, but the abundance of information available makes this task difficult. The image coordinate system describes how an image was acquired with respect to the anatomy. The 'i' axis increases to the right, the 'j' axis to

the bottom and the 'k' axis backwards. The origin represents the position of the first voxel (0,0,0) in the anatomical coordinate system. The spacing specifies the distance between voxels along each axis. Figure 1 shows the acquisition of a 3D Volume of data related to the patient. The 3D volume is sampled on a 3D grid in the acquisition coordinate system (I,J,K).

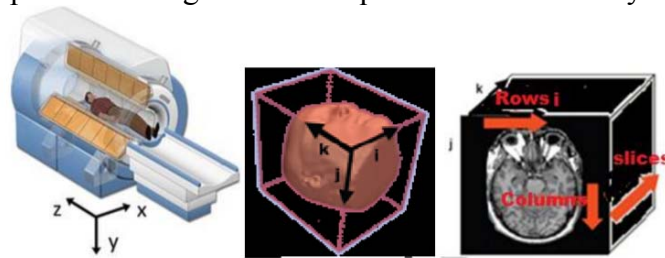


Fig.1 Presentation of patient head data in the acquisition coordinate system (i,j,k)
(Courtesy, http://www.slicer.org/slicerWiki/index.php/Coordinate_system)

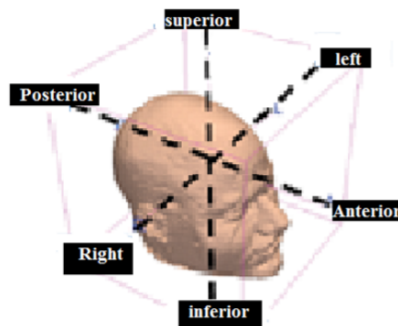


Fig.2 Head image directions

The coordinate system for medical imaging techniques is the anatomical space called patient coordinate system. This space consists of three planes to describe the standard anatomical position of a human:

- 1) The axial plane is an X-Z plane, parallel to the ground and separates the head (Superior) from the feet (Inferior).
- 2) The coronal plane is a Y-X plane, perpendicular to the ground and separates the front from (Anterior) the back (Posterior).
- 3) A sagittal plane is a Y-Z plane, perpendicular to the ground that separates the Left from the Right.

The anatomical coordinate system is a continuous three-dimensional space in which an image has been sampled.

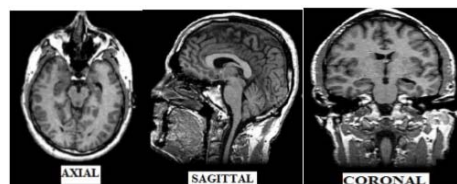


Fig.3 Magnetic resonance images of human brain
Courtesy: Visible human project

2. Review of literature

Dipankar Ray et al., 2010, stated that synergistic studies of anatomical to functional imaging provide some additional information which is not always available in either of the two

individual images. Alzheimer disease, the synergistic study of Magnetic resonance Positron emission tomography (MR-PET) or Magnetic resonance Single photon emission computed tomography (MR-SPECT) brain images provides clinical information of functional behavior of effected brain regions with the pathological status of corresponding tissues. It requires alignment and fusion of two different types of imaging modalities. They have suggested a shape based generalized transformation model for the brain image registration and implemented it with radial basis function (RBF) neural network.

Benzheng et al., 2010, used a basic concept from spatial information, mutual information, and relative entropy, as a new matching criterion. The feature characteristics like location, edge strength and orientation are taken into account to compute a joint probability distribution of corresponding edge points in two images. The mutual information based on this function is minimized to find the best alignment parameters. The translation parameters are calculated by using Powell algorithm. The experiment results showed that the method have achieved a good performance.

Min Chen et al., 2011, described deformable registration techniques that play vital roles in a variety of medical imaging tasks such as image fusion, segmentation, and post-operative surgery assessment. Mutual information loses much of its effectiveness when there are poor statistical consistency and a lack of structure. This is especially true in areas of images where the intensity is homogeneous and information is sparse. They presented a method designed to address the problem by integrating distance transforms of anatomical segmentations as part of a multi-channel mutual information framework within the registration algorithm.

Liu et al., 2012, developed a technique to automate landmark selection for point-based interpolating transformations for nonlinear medical image registration. Interpolating transformations were calculated from homologous point landmarks on the source (image to be transformed) and target (reference image). Point landmarks are placed at regular intervals on contours of anatomical features, and their positions are optimized along the contour surface by a function composed of curvature similarity and displacements of the homologous landmarks.

3. Data generation

Data has been collected from the standard database available in statistical parametric mapping (SPM) website. The website presents PET and fMRI data collected for single subject and multiple subjects. Rest condition and task related images have been presented with realignment, co-registration, normalization, smoothing wherever applicable.

Patterns are generated for the inputs and targets from the floating and target images. The patterns are created using statistical features of the regions of interest (ROI) of an image or in the corresponding images of interest obtained using HHT.

4. Hilbert-Huang transform (Empirical mode decomposition (EMD) and Hilbert transform (HT))

The features of the images are extracted using HHT. These features are used to align the images. Instead of taking the representative points of the floating image and representative points of the target image. If the entire floating image has to be aligned with the target image then HHT can be preferred.

An image is formed from the quantized values of continuous signals based on the intensity value recognized. A signal can be analyzed in details for its frequency, amplitude and phase contents by using EMD followed by Hilbert Transform (HT) (Jayasree et al. 2010 and

Stuti et al. 2009), The EMD produces the mono components called intrinsic mode functions (IMFs) from the original signal. In a given frame of the signal, there can be many IMFs. Each IMF will contain a wave form of different amplitude. Hilbert Transform is applied on an IMF to obtain, instantaneous frequency (IF) and instantaneous amplitude (IA). It is mandatory that a signal be symmetric regarding the local zero mean, and should contain same number of extreme and zero crossings.

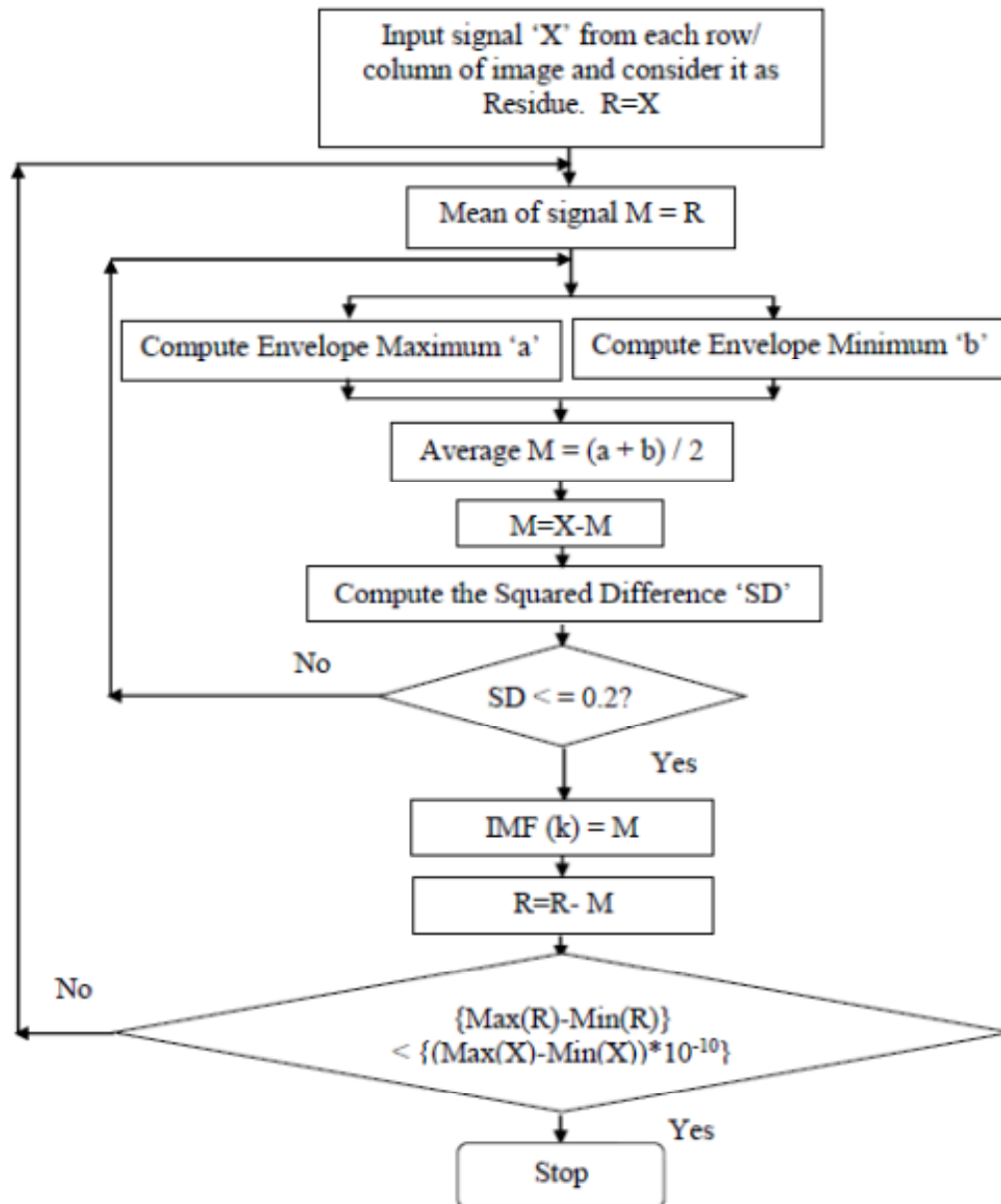


Fig.4 Flow chart for Empirical Mode Decomposition to obtain Intrinsic Mode Function

4.1 Feature Extraction from EMD

In a given frame of signal, there can be many IMFs. Each IMF will contain a waveform of different amplitude. The HT is applied on an IMF to obtain Instantaneous Frequency (IF) and Instantaneous Amplitude (By using IF and IA, features are obtained. They are mean, standard

deviation, norm, maximum and instantaneous frequencies of an IMF. Similarly mean, standard deviation, norm, maximum and minimum of instantaneous amplitudes of an IMF, energy of fine to coarse (F2C) and coarse to fine (C2F) waveforms of an IMF.

Figure 4 presents the EMD process. For a signal 'X', all the local maxima and minima have been identified. The upper and lower envelopes have been obtained using these local maxima and minima by cubic spline interpolations. The point by point local mean value 'M' has been calculated using these envelopes. The Extractions of the details have been calculated by subtracting the mean value 'M' from the signal. The Squared Difference 'SD' between two successive extractions has been checked and iterated 'k' times to identify the IMF present in the signal. It is designated as first IMF. Normally, the value of SD has to be set as 0.2 to 0.3.

The Residue 'R' has been found by subtracting the IMFs from the signal. This residue is taken as the new signal and further IMFs are calculated till conditions are satisfied. The steps involved in EMD of a signal X(t) into a set of IMFs are as follows:

Read the intensity values of a row / column. Sample intensity values of first row of the original image is shown in Figure 5.

The intensity values are modified based on equation (1)

$$\text{New value} = I - \frac{\text{maximum}(I)}{2} \quad (1)$$

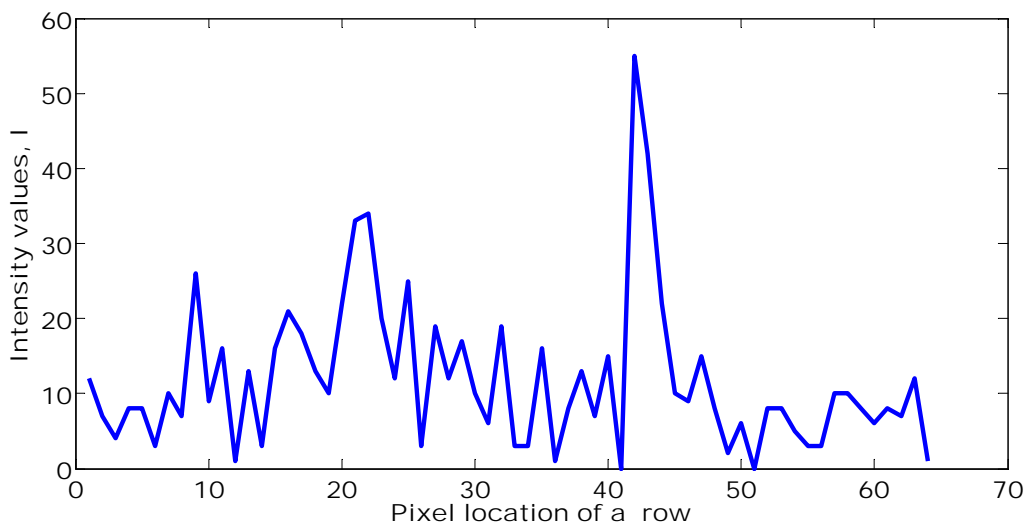


Fig.5 Intensity values of row 1 in original image

The new values are obtained for processing through EMD.

1. All local maxima of X (t) are identified by the equations (2 to 10).

Let the signal 'X' has 'm' sampling points.

$$X = X(i) \quad (2)$$

Where $i = 1, 2, \dots, m$.

$$X_1 = X(i)$$

Where $i = 1, 2, \dots, m - 1$.

$$X_2 = X(i) \quad (3)$$

Where $i = 2, 3, \dots, m$.

Multiply the signal 'X₁' and 'X₂', and find out the places of sampling points where the result is less than zero to determine the zero crossings 'X₀' by equation (4).

$$X_0 = \text{Places} ((X_1 * X_2) < 0) \quad (4)$$

Difference between two consecutive sampling points of signal 'X (t)' is 'X_{Dff}' and it has n sampling points. Therefore,

$$n = m - 1 \quad (5)$$

$$X_{Dff} = \text{Diff}(X(t)) \quad (6)$$

$$X_{Dff1} = X_{Dff}(i) \quad (7)$$

Where $i = 1, 2 \dots n$.

$$X_{Dff2} = X_{Dff}(i) \quad (8)$$

Where $i = 1, 2 \dots n-1$.

Multiplying the signal equation (7) and (8), and find out the places if the result is less than zero and X_{D1} is greater than zero to determine the indices of maximum of the signal by the equation (9).

$$X_{\text{Ind_Max}} = \text{Places} \left(((X_{Dff1} * X_{Dff2}) < 0) \& (X_{Dff1} < 0) \right) + 1 \quad (9)$$

Since the signal X_{Dff1} and X_{Dff2} has the sampling points $m-1$, Equation (9) is added with 1 to determine the perfect place of the signal. Connect these sampling points using a cubic spline. The interpolated curve obtained is the cubic spline. The upper line is called the upper envelope (Env_Max).

2. All local minima of 'X (t)' are identified by equation (10). Indices of minimum of the signal are calculated by the equation (10).

$$X_{\text{Ind_Min}} = \text{Places} \left(((X_{Dff1} * X_{Dff2}) < 0) \& (X_{Dff1} < 0) \right) + 1 \quad (10)$$

Connect the sampling points using a cubic spline.

The lower line (dash-dotted lines) is called the lower envelope (Env_Min).

3. The average is computed by equation (11)

$$M = \frac{(a+b)}{2} \quad (11)$$

Where $a = \text{Env_Max}$ and $b = \text{Env_Min}$.

4. Extract the details from the signal called a new signal using equation (12).

$$h_1(t) = X(t) - M_1 \quad (12)$$

Determine if $h_1(t)$ is an IMF. In order to check this condition, normalized Squared Difference (SD) between two successive sifting processes has to be calculated.

5. h_1 becomes asymmetric. h_1 is taken as the new signal and determines the envelope using steps 1 to 4.

By using equation (13), k^{th} iteration can be obtained.

$$h_{1k}(t) = h_{1(k-1)}(t) - M_{1k} \quad (13)$$

Where,

M_{1k} is the mean envelop after the k^{th} iteration,

$h_{1(k-1)}$ is the difference between the signal and the mean envelope at the $(k-1)^{\text{th}}$ iteration.

The step (5) is repeated until all the IMFs and residual is obtained. Equation (14) has been used to check this condition.

$$(\text{Max}(R) - \text{Min}(R)) < (\text{Max}(X) - \text{Min}(X)) * 10^{-10} \quad (14)$$

Figure 6 shows the IMFs of signal.

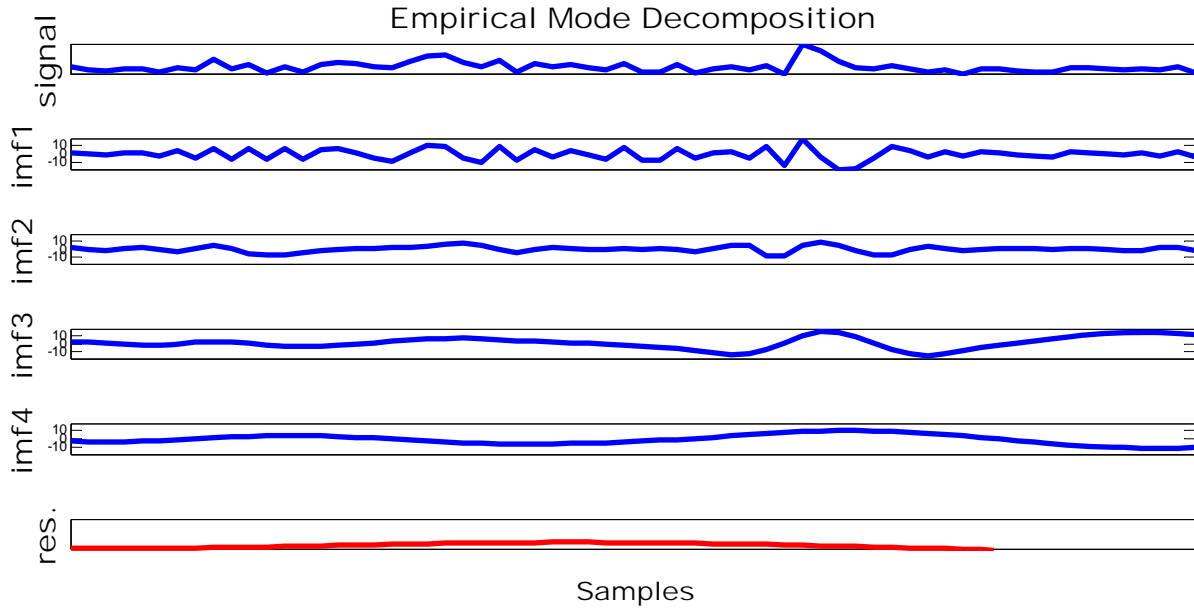


Fig.6 Intrinsic Mode Functions

6. C2F is calculated using equations (15-17)

$$C2F_1 = IMF_k \quad (15)$$

Where IMF_k = final IMF obtained.

$$C2F_2 = IMF_k + IMF_{(k-1)} \quad (16)$$

Similarly,

$$C2F_k = IMF_k + IMF_{(k-1)} + \dots + IMF_1 \quad (17)$$

Where $C2F_k$ is the original signal.

7. F2C is calculated using equations (18-20).

$$F2C_1 = IMF_1 \quad (18)$$

$$F2C_2 = IMF_1 + IMF_2 \quad (19)$$

$$F2C_k = IMF_1 + IMF_2 + \dots + IMF_k \quad (20)$$

8. Hilbert transform (HT) is applied for each IMF and discrete time analytical signal is obtained. HT is a convolution integral, of $IMF(t)$ and $\frac{1}{\pi t}$. It is a mathematical tool used to calculate analytical signal from real signal as in equation (21) and (22).

$$X_H(t) = \frac{1}{\pi} \int_{-\alpha}^{\alpha} \frac{IMF(\tau_{sh})}{t - \tau_{sh}} d\tau_{sh} \quad (21)$$

Where, τ_{sh} is the shifting operator and $X_H(t)$ is HT of $IMF(t)$. $X_H(t)$ consists of passing $IMF(t)$ through a system which leaves the magnitude unchanged, but changes the phase of all frequency components by $\frac{\pi}{2}$.

From this, Analytical signal has been calculated by

$$X_{analytic}(t) = IMF(t) + \text{imag}(X_H(t)) \quad (22)$$

Instantaneous phase of $IMF(t)$ is calculated by equation (23).

$$\theta(t) = \tan^{-1} \left(\frac{X_H(t)}{\text{IMF}(t)} \right) \quad (23)$$

6. Instantaneous frequencies are obtained from analytical signal by equation (24). It is the time derivative of $\theta(t)$.

$$\text{IF} = \frac{0.5 * (\text{angle}(-X_{\text{analytic}}(t+1) * \text{conj}(X_{\text{analytic}}(t-1))) + \pi)}{2 * \pi} \quad (24)$$

$$\text{IA} = \sqrt{\text{IMF}(t)^2 + \text{imag}(X_H(t))^2} \quad (25)$$

From the IF and IA, the following statistical properties are obtained to create training pattern.

(i) Mean: Mean is divided by the number of values. The mean is expressed as equation

$$\text{IF}_{\text{Mean}} = \frac{\sum \text{IF}(i)}{n_{\text{sfr}}} \quad (26)$$

Where, n_{sfr} = Number of samples in a frame, IF_{Mean} = Mean value of IF and $i = 1, 2, \dots, n_{\text{sfr}}$.

(ii) Standard Deviation: Standard deviation is widely used in measurement of variability or diversity. It can be calculated by equation (27).

$$\text{IF}_{\text{Std}} = \frac{\sum (\text{IF}(i) - \text{IF}_{\text{Mean}})}{n_{\text{sfr}}} \quad (27)$$

Where

IF_{Std} = Standard Deviation of IF. $i = 1, 2, \dots, n_{\text{sfr}}$.

(iii) Maximum and Minimum: Maximum and Minimum value of each IMF are calculated using equation (28) and equation (29)

$$\text{IF}_{\text{Max}} = \text{Maximum (IF)} \quad (28)$$

$$\text{IF}_{\text{Min}} = \text{Minimum (IF)} \quad (29)$$

(iv) Norm: calculates several different types of matrix norms. It is calculated for each IMF using equation (30)

$$\text{IF}_{\text{norm}} = \text{norm}(\text{IF})^2 \quad (30)$$

Where, IF_{norm} = Energy value of frequency

Just like equation (26) to equation (30), Mean of IA, 'Std' of IA, Maximum of IA, Minimum of IA and norm of IA are calculated using instantaneous amplitude.

$$\text{IA}_{\text{Mean}} = \frac{\sum \text{IA}(i)}{n_{\text{sfr}}} \quad (31)$$

Where, IA_{Mean} = Mean value of Instantaneous amplitude, $i = 1, 2, \dots, n_{\text{sfr}}$. $\text{IA}_{\text{Std}} = \frac{\sum (\text{IA}(i) - \text{IA}_{\text{Mean}})}{n_{\text{sfr}}}$ (32)

Where,

IA_{Std} = Standard Deviation of Instantaneous amplitude, $i = 1, 2, \dots, n_{\text{sfr}}$.

$$\text{IA}_{\text{Max}} = \text{Maximum (IA)} \quad (33)$$

$$\text{IA}_{\text{Min}} = \text{Minimum (IA)} \quad (34)$$

$$\text{IA}_{\text{norm}} = \text{norm (IA)}^2 \quad (35)$$

Where,

IA_{norm} = Energy value of Amplitude (35)

(v) Log2: It is base 2 logarithm and dissects floating point number. Log2 value of F2C and C2F are calculated using equation (36) and equation (37).

$$\text{F2C}_{\text{Log2}} = \sum \text{Log}_2(\text{abs}(\text{F2C})^2) \quad (36)$$

$$\text{C2F}_{\text{Log2}} = \sum \text{Log}_2(\text{abs}(\text{C2F})^2) \quad (37)$$

Where, F2C_{Log2} = Log 2 value of F2C, and C2F_{Log2} = Log2 value of C2F.

5. Results and Discussions

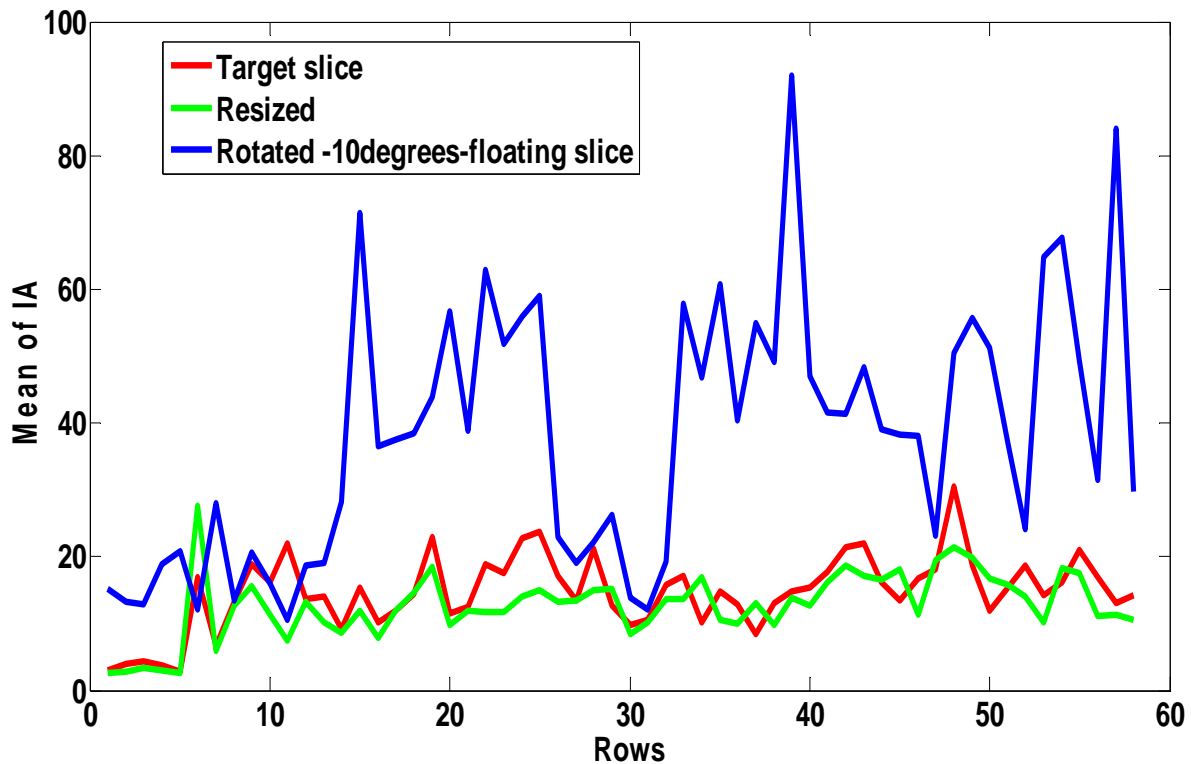


Fig. 7 Mean value for each row for IA

Figures 7 and 8 present plots of the statistical features obtained through equations (26-37). These plots are obtained for one position of floating image. Many such plots can be generated based on number of rotation and translation steps required for correct registration.

Figure 7 shows three curves. X-axis shows row number of the target image, resized image (floating) and rotated image (floating) and y-axis shows the mean value of instantaneous amplitude (IA) for each row for all the three images. The registration of the floating image with the target image is perfect when the red color or green color lines are closer to the blue color line. This indicates that, the floating image has been transformed to match the target image.

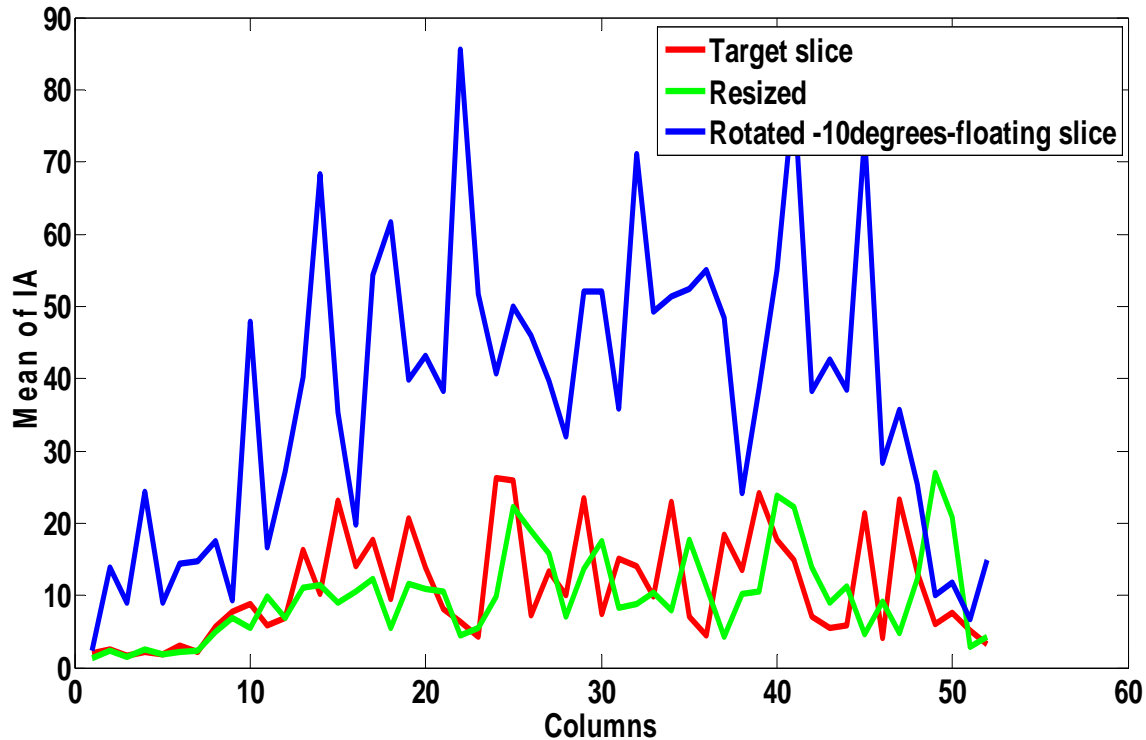


Fig.8 Mean value for each column for IA

Figure 8 shows three curves. X-axis shows column number of the target image resized image (floating) and rotated image (floating) and y-axis shows the mean instantaneous amplitude (IA) for each column for all the three images. The registration of the floating image with the target image is perfect when the red color or green color lines are closer to the blue color line. This indicates that, the floating image has been transformed to match the target image.

6. Conclusion

Hilbert-Huang transform has been used for extracting features from the fMRI slices. Statistical feature were extracted. Based on the statistical features, alignment of images were carried out until close alignment of images slices are obtained.

7 References

- Benzheng Wei, Zaitao Liu, and Xin Peng, 2010, Spatial Information Based Medical Image Registration Using Mutual Information, Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10), pp.174-177.
- Dipankar Ray, Dutta Majumder, Amit Das, 2010, Synergistic Study of Alzheimer Diseased Brain MRI with PET and SPECT Images using Shape based Registration and Fuzzy-Dempster Shafer Evidence Accumulation Model, International Journal of Computer Applications, Vol.12, No.7, pp.18-25.
- Jayasree T., Devaraj D., and Sukanesh R., 2010, Power quality disturbance classification using Hilbert transform and RBF networks, Neurocomputing , Vol. 73 Issue 7-9, pp. 1451-1456.
- Min Chen, Aaron Carass, John Bogovic, Pierre-Louis Bazin, Jerry L., Prince., 2011, Distance transforms in multichannel MR image registration, Proc. SPIE 7962, Medical Imaging 2011: Image Processing, 79621D.

Liu Y., Sajja B.R., Uberti M.G., Gendelman H.E., Kielian T., Boska M.D., 2012, Landmark optimization using local curvature for point-based nonlinear rodent brain image registration, International Journal of Biomedical Imaging, Vol.2012, No.1, pp.1-8.

Shukla Stuti, S. Mishra, and Bhim Singh, 2009, Empirical-Mode Decomposition With Hilbert Transform for Power-Quality Assessment, IEEE transactions on power delivery, Vol.24, No.4, pp.2159–2165.

Data Security Protocol for Wireless Sensor Network using Chaotic Map

Haider M. Al-Mashhadi, Hala B. Abdul-Wahab, Rehab F. Hassan
Computer Science Dept., University of Technology, Baghdad, Iraq

Abstract

In last years, many cryptosystems relay on the chaotic maps have been proposed. Many significant features of chaotic systems can be exploited in cryptography like: ergodicity, instability to initial condition, and confusion feature. These features lead to a significant relationship between cryptography and chaos. Because of widely usage of WSNs in variety environments, it is important to save the transferred messages from unwanted access. Security of these data while transferring through the network happens to be more critical. In this study, a new cryptosystem called Hybrid Chaotic Cryptosystem Tent-PWLCM (HCCTPWLCM) have been suggested, based on two chaotic methods to create keys and encrypt the WSN's data in a multistep manner to enhance the security of WSN's. The analysis and experimental results show that the execution time and the security achieved by the proposed method are very suitable for securing communications in a variety of WSNs applications, and real-time applications.

Keywords- Block cipher; cryptography; skew tent map; PWLCM; Wireless Sensor Networks (WSNs).

INTRODUCTION

Wireless sensor networks (WSNs) are employed in various fields and important purposes like warlike fields, manufacture, house networks, and so on. The disadvantage of WSNs is the limited resources including limited storage, limited calculation capability, variable topology, and limited power, the conventional networks uses security protocols that are difficult implemented in WSN, they are need memory for key storage, processing overhead for encryption/authentication, and do not really consider limited power applications [1, 2].

Chaotic processes include many of significant features like instability to initial condition and system parameter, ergodicity and confusion feature, etc. Due to these features the chaotic systems are good option for designing the cryptosystems the instability to the initial status/system parameter and mixing features respectively, are identical to the confusion and diffusion features of a perfect cryptosystem [3].

There are numerous chaotic maps have been exploited to create chaotic key systems: Forré utilized two-dimensional Hénon system [4], Pareek et al. applied generic logistic map system [5], Behnia et al. utilized Piecewise Linear Chaotic Map (PWLCM) [6]. The output of such chaotic systems can

be used to generate the key streams by processing them in different methods. This is done by using multiple chaotic systems in a sequential manner [7], or by conjunction chaotic systems [8].

A chaos-based cryptosystem uses a chaotic generator to generate the keys that can be used in the cryptosystem. A chaotic series is created depend on a primary value, and the series, used as a key, is mixes with the plaintext to obtain the ciphertext. The same chaotic series is used for decipherment [9]. This cryptosystem is convenient for wireless applications with restricted resources due to it can provide a better security and low of time and space [10].

The purpose of this research is to introduce and implement a secure encryption algorithm using chaotic skew tent map and PWLCM methods to encrypt the data message that transmit between sensor nodes in Wireless sensor networks to enhance the security and energy consumption. A new method creates keys using in encryption algorithm to improve the strength of security with a less execution/run time. The simulation results show that proposed scheme provides good security due to their ability to achieve diffusion confusion effects, needed in any cryptosystem. To explain the performance of the proposed technique, the paper performs a set of tests. The detailed quantitative analysis and experiment show that, our scheme is greatly superior in terms of security and time execution of WSNs.

The paper is arranged as follows. Section 2 presents the related works. Related concepts of the chaotic systems are presented in section 3. The proposed cryptosystem is given in section 4,. In section 5 the performance analysis for the cryptosystem is presented. Finally, conclusion and discussion are presented in section 6.

Related Works

Many cryptosystem using chaotic maps have been proposed from these methods:

Chen et al [11] proposed a block cipher algorithm depends on feistel frame and logistic chaotic mapping, this method uses a block length of 8 bits, without using any tabulation, it has a high security feature with high speed computing, but the distribution of the sequence generated by the chaotic logistic mapping is nonuniform. And the power and modular calculation of large numbers in the process of key generating will increase the burden of the WSN nodes.

Yanbing et al. [12] proposed a block cipher depends on chaotic S-box. By uses the cross-calculations mod as similar to RC5 algorithm.

Wang et al. [13] proposed a new security gateway depends on chaotic sequences. Using Logistic mapping, generates an infinite binary sequence to encrypt the data information to achieve a real sense of "one-time pad."

Jiandong et al. [14] proposed a cryptographic algorithm using coupled extended integer tent maps, with Feistel structure, to generate the key sequence, one byte plain text block, extended integral tent mapping, and avoid the floating point.

Al-Mashhadi et al. [15] proposed a new encryption scheme called Chaotic Block Cipher (CBC) to encrypt the message digest MD for WSNs data. The proposed method uses logistic chaotic method to create a number of chaotic values and treats these values to obtain the encryption/decryption keys then mixing them with a plaintext to get a ciphertext.

CHAOTIC SYSTEMS

a. The Logistic map

It can be show very responsive to the system and control variable together. Beside, other aspects like ergodicity, pseudo-randomness and unpredictable behavior. The logistic map can be shown as [16]:

$$x_{i+1} = \alpha x_i (1 - x_i) \quad (1)$$

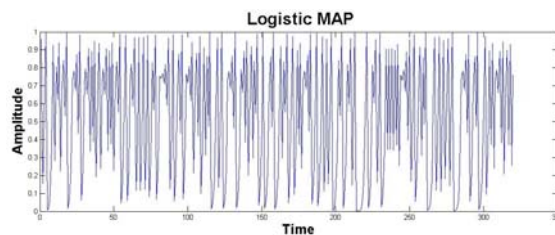
Where " x_i " is the system variable ($0 < x_i < 1$) and α is the control parameter ($3.56 \leq \alpha \leq 4$), respectively, and i is the number of repetition.

b. The Skew Tent Map

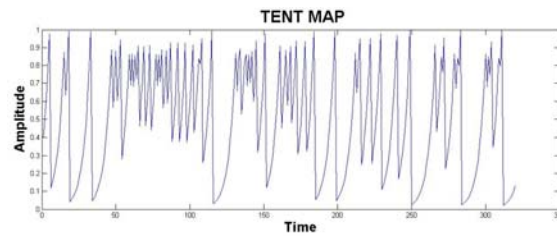
It is ergodic and has uniform invariant density function in its definition interval [17]. It can be defined as [18]:

$$x_{i+1} = F(w, x_i) = \begin{cases} x_i/w, & x_i \in [0, w) \\ (1-x_i)/(1-w), & x_i \in (w, 1] \end{cases} \quad (2)$$

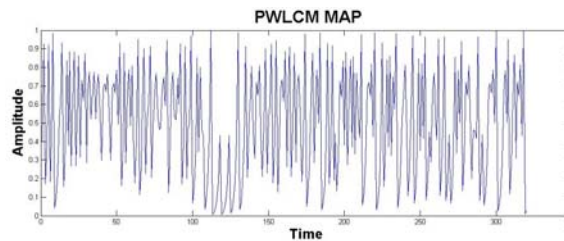
Where, w is the system parameter and x_i is the initial state of the map. It is a non-reversible transformation of unit epoch onto itself and have only one system parameter w , which determines status of the top of the tent in the period $[0,1]$. A series computed by repeating $F(w, x)$, is expansionary everywhere in the period $[0,1]$ and distributed uniformly in it.



(a)



(b)



(c)

Fig. 1): (a) Logistic map result; (b) Skew Tent map, and (c) PWLCM results.

Figure 1 (a), (b), and (c) shows the chaotic results of logistic map and tent map equations when using $x_0=0.4$ and $\alpha=3.99996$ for logistic map, using $x_0=0.4$, $w=0.8$ for skew tent map, and $x_0=0.4$, $w=0.4321$ for PWLCM map, for $n=320$ iteration. To show the effective of initial condition and system parameter.

c. Piecewise Linear Chaotic Map (PWLCM)

It is a map consists of numerous linear fragments. This mapping is used by Zhou [19, 20]. The PWLCM is defined as:

$$F(x_i, w) = \begin{cases} x_i / w & 0 \leq x_i < w \\ (x_i - w) / (0.5 - w) & w \leq x_i < 0.5 \\ F(1 - x_i, w) & 0.5 \leq x_i \leq 1 \end{cases} \quad (3)$$

where w is the control parameter and $0 < w < 0.5$, and $0 \leq x_i \leq 1$.

The PWLCM is widely used in chaotic cryptosystems due to the following features [21]:

- A regular and steady density.
- Perfect dynamical characterizes.
- Can be implements in hardware and software in a simple way.

The proposed Chaotic cryptosystem

The proposed scheme consists of two phases: chaotic sequence generation phase and encryption phase. Here, we describe the scheme in detail.

Chaotic key generator

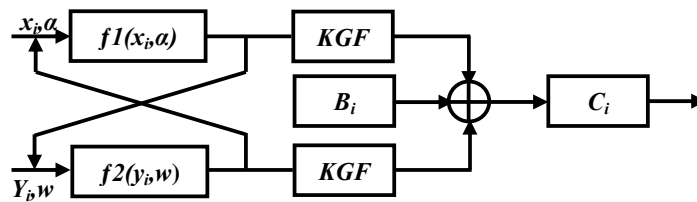


Fig. (2): The diagram of Hybrid Chaotic Cryptosystem Tent Map-PWLCM (HCCTPWLCM).

Figure (2) shows the diagram for all stages of HCCTPWLCM, in which:

- $f1(x_i, a)$ is a skew tent map function that implements eq. (2), $f2(y_i, w)$ is a PWLCM function that implements eq. (3).
- The two functions produce chaotic values that enter to Key Generator Function (KGF).
- The KGF handles the values produce from eq. (2) and eq. (3) by enters it to eq. (4) to produce the K_i . Then take the fraction part of value as the key K_i . The length of each K_i is equal to data block size 32 bits. And the number of K_i is equal to number of message blocks.

$$K_i = 2^{16} * (x_i) \quad (4)$$

where K_i is the i^{th} key, x_i the i^{th} chaotic value generated by eq. (2) and eq. (3). Then implement eq. (5) to produce the final Keys KW_i and KL_i :

$$\left. \begin{aligned} KW_i &= (KW_i \text{ xor } KW_{i-1}) \\ KL_i &= (KL_i \text{ xor } KL_{i-1}); \end{aligned} \right\} \quad (5)$$

- After produce the chaotic keys K_i , then it enters to keys vectors depending on its order, that are get it during runs of $f1$ and $f2$.
- Using Xor for the message blocks with the keys to produce the encrypted block as the eq. (6)

$$C_j = K_r \oplus (K_i \oplus B_j) \quad (6)$$

Where C_j is the ciphertext, K_i is the i^{th} key, K_r is the r^{th} key, and B_j is the j^{th} message block. The eq. (6) is performed until end of all message blocks.

- The algorithm use two chaotic maps in parallel and each chaotic map produce her private keys that can be use in encryption/decryption of data blocks.

Figure (3) shows the flow chart diagram of the current method.

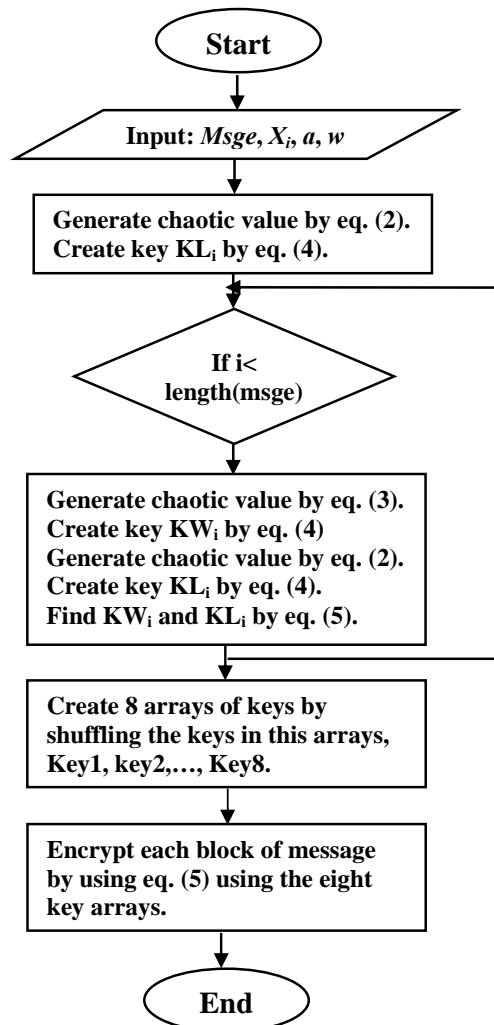


Fig. (3): Flow chart of the HCCTPWLCM algorithm.

Table I. The run time/ms Results of cryptosystem experiments compared with RC5.

Seq.	Input	Output		RC5
	Plaintext	Ciphertext	Run time/ms	Run time/ms
(a)	F86AF1C4BCFD6216B 2B75765CF42BD8635 7FAD1F	75F30BE6E822363C428691 7F448C7645D6F6284C	0.0470	0.0739
(b)		6382A35B452A4244FDDB0E 35B7F516ABBAACF685	0.0486	0.0756
(c)		5C7ACD3AA869596B78BA7 3B8A7CB17BABFA7F7B7	0.0457	0.0743
(d)	AF81A71412DF6FC32 6AAEC0578DC724794 B381E7	F2185D36B6003BE9D69B2A 1FF312B9847C3A0453	0.0434	0.0744
(e)		E469F58B1B084F9169C6B5 55006BD96A1060DA9A	0.0465	0.0768
(f)		DB919BEAF64B54BEECA7 C8D81055D87B156BDBA8	0.0471	0.0745
(g)	55307885C4C2EE41C FF168D4CF9D9C156B 70FA5F	78A982A7401DBA6B3FC0A ECE445357D681F97FA8	0.0443	0.0733
(h)		6ED82A1AED15CE13809D3 184B72A3738EDA3A161	0.0462	0.0735
(i)		5120447B0056D53C05FC4C 09A7143629E8A8A053	0.0434	0.0757

Performance Analysis for the Cryptosystem

The Security and execution time/run time is the most important for any cryptosystem designed for WSNs. So we focus on these two features in the performance analysis that is made on the proposed cryptosystem.

Several experiments have been implemented to examine the performance of the proposed algorithm on three different text samples and three different values of x_0 , a and w for each text sample as shown in Table I.

The system parameters x_0 , a , w shown in Table II.

Table II: the system parameters values.

No.	x_0	a	w
1	0.4	0.8	0.4321
2	0.41	0.8	0.321
3	0.42	0.8	0.21

The security protocol is performing by using Matlab R2010a, and the evaluation is performing by using Crypt-X'98 [22] statistical analysis tool that is used to inspect the randomness of resulting ciphertext. This statistical analysis include frequency test, change point, sub-block, runs, binary derivative, sequence complexity and linear complexity [23, 24, 25, 26].

Table III: The statistical analysis for the new method.

Test	RC5	HCCTPWLCM
Frequency	0.3750	0.3789
Binary derivative	Ok	Ok
Change point	Ok	Ok
Sub block	No	No
Runs	No	No
Sequence complexity	No	No
Linear complexity	Ok	Ok

Table III shows the statistical analysis results for the new method. The statistical test for the two method is very close. From these tests we can conclude that the new method can be used to secure the messages of WSN with less encryption run time and high security and then low power consumption depends on the above tests.

Conclusion

In this paper a new cryptosystem based on two chaotic methods used to create number of keys that equal to number of data blocks. Encrypt the WSN's data in a multistep manner to enhance the security of WSN's. The cryptosystem used a cipher block of 32 bit length, the chaotic key generator provides randomness and security features. Several experiments have been taken to prove the suitable of the algorithm for WSN nodes. The experimental results shows that the sensitivity of cryptosystem's output to the initial values of x_0 , α , and w , and the small amount of the run time that required to execute the system.

The new cryptosystem performance is examined from the security and time consuming. The proposed method is evaluated to demonstrate the effectiveness of the new approach with regards to enhancement of the run time and security of message in wireless sensor networks.

References

- [1] Wang Y., Attebury G., and Ramamurthy B., "A survey of security issues in wireless sensor networks," *IEEE Comm. Surveys & Tutorials* vol. 8, no. 2, pp 2–23, 2006.
- [2] Trevatha J., Ghodosi H., and Myers T., "Efficient batch authentication for hierarchical wireless sensor networks," in *IEEE ISSNIP*, pp. 217–222, 2011.

- [3] Narendra K Pareek, Vinod Patidar, and Krishan K Sud, "A Random Bit Generator Using Chaotic Maps," *International Journal of Network Security*, vol.10, no.1, PP.32-38, 2010.
- [4] Forre R., "The Henon Attractor as A Keystream Generator," In *Advances in Cryptology-EuroCrypt'91*, vol. 0547, pp. 76-81, Berlin, Springer-Verlag, 1991.
- [5] Pareek N., Patidar V., and Sud K., "Image Encryption Using Chaotic Logistic Map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006.
- [6] Behnia S., Akhshani A., Ahadpour S., and Mahmodi H., "A Fast Chaotic Encryption Scheme Based on Piecewise Nonlinear Chaotic Maps," *Physics Letters A*, vol. 366, no. 4-5, pp. 391-396, 2007.
- [7] He X., Zhu Q., and Gu P., "A New Chaos-Based Encryption Method for Color Image," *Springer Berlin/Heidelberg*, vol. 4062, pp. 671-678, 2006.
- [8] Shujun L., Xuanqin M., and Yuanlong C., "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography," in *Proceedings of the Second International Conference on Cryptology in India: Progress in Cryptology*, vol. 2247, pp. 316-329, 2001.
- [9] Zhu C. and Chen Z., "A fast combined chaotic cryptographic method fitting mobile computing," *Comput. Engrg.* Vol. 31, no. 1, 138–140, 2005.
- [10] Plitsis G., "Performance of the application of chaotic signals in IEEE 802.11b and wireless sensor networks," In: *Proc. Seventh IEEE Internat. Symposium on Computer Networks*, 2006.
- [11] Chen Shuai, Zhong Xianxin, Wu Zhongzheng, "Research on Chaos blockcipher for wireless sensor network [j]," *Science in China*, vol. 39 no. 3, pp 357-362, 2009.
- [12] Yanbing Liu, Simei Tian, "Design and statistical analysis of a new chaos block cipher for WSN," *IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp 327-330, 2010 .
- [13] Wang Hai-Chun, Huang Tao, " Design of security gateway based on chaotic encryption," *IEEE International Conference on Internet Technology and Applications (iTAP)*, pp 1-4, 2011 .
- [14] Jiandong Liu, Kai Yang, Xiahui Wang, Chen Zhao, "Research on chaotic block cipher algorithm applied to wireless sensor networks," *IEEE 4th International Conference on Digital Manufacturing and Automation (ICDMA)*, pp 1029 – 1038, 2013,
- [15] Al-Mashhadi Haider, Abdul-Wahab Hala, and Hassan Rehab, "Chaotic Encryption Scheme for Wireless Sensor Network's Message," In *proc. International Conference on Communication and Networking Security 2014, (ICCNS'2014)*, Tunisia, 2014.

- [16] Kanso A., Smaoui N., "Logistic chaotic maps for binary numbers generations," *Chaos, Solutions and Fractals*. Vol. 40 , pp: 2557-2568, 2009..
- [17] Stojanovski T., Pihl J., and Kocarev L., "Chaos-based random number generators - Part II: Practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 382-385, 2001.
- [18] Zhang, G.J., Liu, Q. "A novel image encryption method based on total shuffling scheme," *Optics Communications* vol. 284, pp. 2775–2780, 2011.
- [19] Zhou H., Ling X.-T., "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits and Systems–I* 44 (3): 268–271, 1997.
- [20] Zhou H., Ling X.-T., Yu J., "Secure communication via one-dimensional chaotic inverse systems," in: *Proc. IEEE Int. Symposium Circuits and Systems*, Vol. 2, pp. 9–12, 1997.
- [21] Chen G., Mou X. and Li S., "On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps," *International Journal of Bifurcation and Chaos*, Vol. 15, no 10, pp. 3119-3151, 2005.
- [22] Information Security research Center, "Crypt-X'98 User Manual: a graphical package for the statistical testing of stream ciphers, block ciphers and key generator", Queensland University of Technology, Australia, 1998.
- [23] A. Rukhin, J. Soto ,J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, "A statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology, Apr. 2010.
- [24] A. Menezes, P. van Oorschot, and S. Vanstone, "Ch: 5; Pseudorandom Bits and Sequences", in *Handbook of Applied Cryptography*, 5th Ed., CRC Press, pp. 169-187, 2001.
- [25] N. Davies, Ed Dawson, H. Gustafson, A. N. Pettitt , "Testing for Randomness in Stream Ciphers Using the Binary Derivative", *Stat. Comput.*, vol. 5, no. 4, pp 307-310, Dec. 1995.
- [26] J. M. Carroll, y. Sun, "The Binary Derivative Test for the Appearance of Randomness and its Use as a Noise Filter", Report no. 221, Nov. 1989.

Reducing the effects of interference in multi-user multi-antenna systems using pre-coder in the wireless system

Ghodsie Ghalamkarian¹, Mohammad Ali Pourmina²

Abstract—From the perspective of the information theory, the capacity of multi-user “multiple-input multiple-output” (MIMO) channels is attainable using the “dirty paper coding” (DPC) technique. Due to its high computational load in practical systems, using this technique can be quite complex. Therefore, linear pre-coding techniques such as “zero forcing co-channel interference” (ZF-CCI) and “block Diagonalization” (BD), which are less complex in nature, are proposed in order to remove “multi-user interference” (MUI). These two methods were initially proposed to remove the interference between users in a multi-user system and did not address the “other cell interference” (OCI) that can reduce the performance of cellular communications systems, especially for users that are located at the edge of cells. Two balancing techniques for inter-cell interference and the use of the “minimum mean-squared error” (MMSE) in receivers were proposed in order to reduce OCI without taking MUI into account. An improved version of the BD algorithm, which uses a whitening filter in the receiver, is proposed in multi-user MIMO channels with OCI. However, just like the original BD technique, this technique also faces with the restriction of limited transmitting antennas in most practical applications. Therefore, in order to solve the problem of limited transmitting antennas in the base station, OCI’s elimination or control problem should be examined, using the GCI algorithm. Since this technique cannot eliminate the whole multi-user interference, unlike the BD technique, and leaves some amount of interference behind in the system, we propose an optimization problem in the present study in order to allocate energy among users of a weighted set with maximum optimization. The energy allocation problem is a convex one and, therefore, solvable by the “water filling” (WF) technique. The limitation of both these techniques is that the transmitter should be aware of the covariance matrix of the aggregate noise and interference, which may lead to user feedback.

Index Terms—MIMO, BD algorithm, precoding, GCI algorithm.

I. INTRODUCTION

Multi-input multi-output (MIMO) systems have drawn a lot of attention in the past few years due to their great potential to achieve high throughput in wireless communication systems [1][2][3]. More recently, the investigation of the capacity region has been of concern in multi-user MIMO broadcast channels (BC) [4][5].

In [6] and [7], it was shown that the maximum sum rate in multi-user MIMO BC can be achieved by dirty paper coding (DPC). However, the DPC is difficult to implement in practical systems due to high computational burden of successive encoding and decoding in linear processing systems where each user has multiple antennas, transmitter and receiver design methods have normally been developed in two different ways. The first approach employs an iterative method of canceling out multi-user interference (MUI), allowing multiple data sub channels per users as in classical MIMO transmission techniques. For single user MIMO channels, the optimum joint linear transmitter and receiver design was investigated in [8]. Also, authors in [9], [10] and [11] expanded the work in [8] to multi-user MIMO downlink channels by adopting a joint iterative algorithm. However, the iterative nature of these algorithms typically results in a high computational cost.

II. THE PROPOSED PROTOCOLS

A. The improved BD technique’s drawback and defining the research problem

To make sure that there are at least L_k rows in $V_k^{(0)}$ and so L_k interference-free paths for the user k , the number of antennas in the base station must hold in the equation $N_T \geq \sum_{l=1, l \neq k}^K n_l + L_k$ [12]. This limitation makes providing service by the improved BD method possible only for a limited number of users whose number of antennas fulfill the required conditions. Therefore, in the present study, we use a pre-coder based on the extended reverse channel method proposed for channels without OCI in the system being examined.

B. The design of the pre-coder based on the extended reverse channel method

In this way, the limitations of the modified BD will be removed. Then, we remove the OCI again using the whitening filters that are installed in every user’s receiver [13]. The equation of the retrieved signal after passing through the whitening signal is as follows:

$$\begin{aligned} \mathbf{r}_k &= \mathbf{W}_k \mathbf{H}_k \mathbf{x}_k + \mathbf{W}_k \mathbf{H}_k \sum_{i=1, i \neq k}^K \mathbf{x}_i + \mathbf{W}_k \mathbf{z}_k \\ &= \mathbf{H}_{r,k} \mathbf{x}_k + \mathbf{H}_{r,k} \sum_{i=1, i \neq k}^K \mathbf{x}_i + \mathbf{z}_{r,k} \end{aligned}$$

The above relation shows that, with the presence of the whitening filter, the multi-cellular system will be equivalent to the single-cellular system.

In order to achieve the pre-coder matrix, the matrix $\bar{\mathbf{H}}_s$ should be defined as follows:

$$\bar{\mathbf{H}}_s = (\mathbf{H}_s^H \mathbf{H}_s + \alpha \mathbf{I})^{-1} \mathbf{H}_s^H = [\bar{\mathbf{H}}_{r,1}, \dots, \bar{\mathbf{H}}_{r,K}]$$

¹ Corresponding Author: Ghodsie Ghalamkarian is with the Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran (gh_ghalamkarian@yahoo.com).

² Mohammad Ali Pourmina is with the Electrical and Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran (Pourmina@srbiau.ac.ir)

In this equation, $H_s = [H_1^T H_2^T \dots H_K^T]^T$ and α are the ratio of the variance of the system's total noise to the whole transmission power, that is $\alpha = N_r \sigma_z^2 / P_T$ which means $N_r = \sum_{j=1}^K n_{rj}$. Now in order to make \bar{H}_{rj} orthogonal, using the QR decomposition, we have:

$$\bar{\mathbf{H}}_{r,j} = \bar{\mathbf{Q}}_j \bar{\mathbf{R}}_j, \quad j = 1, \dots, K$$

It should be noted that $\bar{R}_j \in C^{n_j \times n_j}$ is an upper triangular matrix and that \bar{Q}_j also forms n_{rj} orthogonal bases for \bar{H}_j . The proposed method solves the noise problem and, as a result, the total ratio of the system increases linearly with the number of users and the number of transmitting antennas.

$$\bar{\mathbf{y}}_j = \mathbf{H}_j \bar{\mathbf{Q}}_j \mathbf{T}_j \mathbf{s}_j + \mathbf{H}_{r,j} \sum_{k=1, k \neq j}^K \bar{\mathbf{Q}}_k \mathbf{T}_k \mathbf{s}_k + \mathbf{w}_j$$

Matrices U_j^H and V_j are used in the receiver and the pre-coder block, respectively, in order to split the block channel $H_j \bar{Q}_j T_j$ into parallel sub-channels.

Matrices U_j^H and V_j were obtained through the "singular value decomposition" (SVD) of the matrix $H_j \bar{Q}_j T_j$. It should be noted, however, that, since the matrix T_j has not been defined yet, the values of these two matrices cannot be estimated, and it is only known that these two matrices are unitary matrices, which can be determined using the method below.

C. Methods to determine the composition matrix:

Suppose $T_j = \beta \bar{T}_j$ is the composition matrix of user j , where β is a positive integer. Thus, the mean square error for user j will be defined as follows.

$$E \left\{ \left\| \mathbf{U}_j^H \mathbf{G}_j \mathbf{V}_j \mathbf{s}_j - \frac{1}{\beta} \mathbf{x}_j \right\|^2 \right\}$$

Where $G_j \in C^{n_j \times n_j}$ is the objective channel based on MMSE criterion. The problem of minimizing the MMSE based on the power constraint is as follows [14].

$$\min_{T_j} \sum_{j=1}^K E \left\{ \left\| \mathbf{U}_j^H \mathbf{G}_j \mathbf{V}_j \mathbf{s}_j - \frac{1}{\beta} \left(\mathbf{U}_j^H \mathbf{H}_j \sum_{k=1, k \neq j}^K \bar{\mathbf{Q}}_k \mathbf{T}_k \mathbf{V}_k \mathbf{s}_k + \mathbf{U}_j^H \mathbf{w}_j \right) \right\|^2 \right\}$$

$$\text{s.t.} \quad \sum_{j=1}^K \text{Tr}(\mathbf{V}_j^H \mathbf{T}_j^H \bar{\mathbf{Q}}_j^H \bar{\mathbf{Q}}_j \mathbf{T}_j \mathbf{V}_j) = P_T$$

The above approach has no control over the allocation of power to users. It is needed in some conditions and applications to control the power allocated to different users. For example, we can allocate more power to a user whose channel is weaker in order to decrease the mean error of system's overall frame. Thus, it would be better to be able to design the composition matrices of transmission with power constraints dedicated for each user.

Therefore, the allocated power to user j will be:

$$\text{tr}(\mathbf{T}_j^H \mathbf{T}_j) = n_j p_j^2$$

In this approach, the composition matrix is determined by minimizing the power of the interference caused by the pre-coder matrix of user j along with the receiver noise power of this user [13].

$$\min_{T_j} p_j^2 \left[\text{tr} \left(\bar{\mathbf{T}}_j^H \left(\bar{\mathbf{Q}}_j^H \sum_{k \neq j} \mathbf{H}_{r,k}^H \mathbf{H}_{r,k} \bar{\mathbf{Q}}_j + \frac{\sigma^2}{p_j^2} \mathbf{I}_{n_j} \right) \bar{\mathbf{T}}_j \right) \right]$$

In a multi-user system, the output signal can be obtained through the following steps:

$$\begin{aligned} \mathbf{y}_k &= \mathbf{H}_k \mathbf{M}_k \mathbf{s}_k + \mathbf{H}_k \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \underbrace{\mathbf{H}_{1,k} \mathbf{x}_{1,k} + \mathbf{n}_k}_{\mathbf{z}_k} \\ &= \mathbf{H}_k \mathbf{M}_k \mathbf{s}_k + \mathbf{H}_k \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \mathbf{z}_k \rightarrow \text{Whitening} \\ \mathbf{r}_k &= \underbrace{\mathbf{W}_k \mathbf{H}_k}_{\mathbf{H}_{r,k}} \mathbf{M}_k \mathbf{s}_k + \mathbf{W}_k \mathbf{H}_k \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \underbrace{\mathbf{W}_k \mathbf{z}_k}_{\mathbf{z}_{r,k}} \\ &= \mathbf{H}_{r,k} \mathbf{M}_k \mathbf{s}_k + \mathbf{H}_{r,k} \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \mathbf{z}_{r,k} \rightarrow \text{Precoding+ decoding} \\ \hat{\mathbf{r}}_k &= \mathbf{U}_k^H \underbrace{\mathbf{H}_{r,k} \bar{\mathbf{Q}}_k \mathbf{T}_k}_{\text{SVD: } \mathbf{H}_{r,k} \bar{\mathbf{Q}}_k \mathbf{T}_k = \mathbf{U}_k \mathbf{\Lambda}_k \mathbf{V}_k^H} \mathbf{V}_k \mathbf{s}_k + \mathbf{U}_k^H \mathbf{H}_{r,k} \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \mathbf{U}_k^H \mathbf{z}_{r,k} \xrightarrow{\text{SVD}} \\ \hat{\mathbf{r}}_k &= \underbrace{\mathbf{U}_k^H \mathbf{U}_k}_{\mathbf{I}} \underbrace{\mathbf{\Lambda}_k \mathbf{V}_k^H \mathbf{V}_k}_{\mathbf{I}} \mathbf{s}_k + \mathbf{U}_k^H \mathbf{H}_{r,k} \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \mathbf{U}_k^H \mathbf{z}_{r,k} \rightarrow \text{Simplifying} \\ \hat{\mathbf{x}}_k &= \mathbf{\Lambda}_k \mathbf{s}_k + \mathbf{U}_k^H \mathbf{H}_{r,k} \sum_{i=1, i \neq k}^K \mathbf{M}_i \mathbf{s}_i + \mathbf{U}_k^H \mathbf{z}_{r,k} \end{aligned}$$

D. Defining the power problem

After the problem of minimizing inter-user and inter-cellular interference being solved using the GCI algorithm, we present the optimization problem below that has practical applications [15]. The similarity problem and pre-coder BD has been presented without taking into account the OCI.

To solve this problem, a priority for power allocation for different users can be presented by the weighted rate of different users. Given this, in practice, more versatile services can be provided in a cellular network based on the share of allocated power to users. In this optimization problem, every user's share corresponding to the allocated power to that user can be determined by the factor Q_k . The total power P_T is split among each user and their antennas based on the pre-coder matrix M_k among users with the condition of maximizing a weighted set.

$$\begin{aligned} \max_{R_k} \quad & \sum_{k=1}^K \theta_k R_k \\ \text{s.t.} \quad & R_k = \log_2 \left(\mathbf{I} + \mathbf{H}_{r,k} \mathbf{M}_k \mathbf{M}_k^H \mathbf{H}_{r,k}^H \right) \\ & \sum_{k=1}^K \text{Tr}(\mathbf{M}_k \mathbf{M}_k^H) = P_T \\ & \mathbf{M}_k = \bar{\mathbf{Q}}_k \mathbf{T}_k \mathbf{V}_k \in C^{N_T \times n_k} \end{aligned}$$

The cost function can be reformulated as follows based on the allocated power to each of the user's antennas.

$$\begin{aligned}
 R_k &= \log_2(\mathbf{I} + \mathbf{H}_{r,k} \mathbf{M}_k \mathbf{M}_k^H \mathbf{H}_{r,k}^H) \\
 &= \log_2(\mathbf{I} + \mathbf{H}_{r,k} \bar{\mathbf{Q}}_k \mathbf{T}_k \mathbf{V}_k \mathbf{V}_k^H \mathbf{T}_k^H \bar{\mathbf{Q}}_k^H \mathbf{H}_{r,k}^H) \\
 &= \log_2(\mathbf{I} + p_k^2 \mathbf{H}_{r,k} \bar{\mathbf{Q}}_k \bar{\mathbf{T}}_k \mathbf{V}_k \mathbf{V}_k^H \bar{\mathbf{T}}_k^H \bar{\mathbf{Q}}_k^H \mathbf{H}_{r,k}^H) \\
 &= \log_2(\mathbf{I} + p_k^2 \mathbf{H}_{r,k} \bar{\mathbf{Q}}_k \bar{\mathbf{T}}_k \bar{\mathbf{T}}_k^H \bar{\mathbf{Q}}_k^H \mathbf{H}_{r,k}^H) \xrightarrow{\text{SVD: } \mathbf{H}_{r,j} \bar{\mathbf{Q}}_j \mathbf{T}_j = \mathbf{U}_j \Lambda_j \mathbf{V}_j^H} \\
 &= \log_2(\mathbf{I} + p_k^2 \boldsymbol{\Sigma}_k^2) \\
 &= \sum_{i=1}^{n_k} \log_2(1 + p_k^2 \lambda_k^2(i))
 \end{aligned}$$

$$\begin{aligned}
 \sum_{k=1}^K \text{Tr}(\mathbf{M}_k \mathbf{M}_k^H) &= \sum_{k=1}^K \text{Tr}(\bar{\mathbf{Q}}_k \mathbf{T}_k \mathbf{V}_k \mathbf{V}_k^H \mathbf{T}_k^H \bar{\mathbf{Q}}_k^H) \\
 &= \sum_{k=1}^K p_k^2 \text{Tr}(\bar{\mathbf{Q}}_k \bar{\mathbf{T}}_k \mathbf{V}_k \mathbf{V}_k^H \bar{\mathbf{T}}_k^H \bar{\mathbf{Q}}_k^H) \xrightarrow{\text{Tr}(AB) = \text{Tr}(BA)} \\
 &= \sum_{k=1}^K p_k^2 \text{Tr}(\bar{\mathbf{T}}_k \bar{\mathbf{T}}_k^H) \xrightarrow{\text{Tr}(\bar{\mathbf{T}}_k \bar{\mathbf{T}}_k^H) = n_k} \\
 &\stackrel{(a)}{=} \sum_{k=1}^K p_k^2 n_k
 \end{aligned}$$

$$\begin{aligned}
 &\max_{P_k, R_k} \sum_{k=1}^K \theta_k R_k \\
 \text{s.t. } &\sum_{i=1}^{n_k} \log_2(1 + p_k^2 \lambda_k^2(i)) \\
 &\sum_{k=1}^K p_k^2 n_k = P_T
 \end{aligned}$$

Now that it has been verified that the cost function is a convex one, the problem can be easily solved using algorithms such as WF and the share of each user can be calculated.

III. SIMULATION

In this section, we compare the efficiency of the proposed pre-coding method with the BD method using computer simulation. In all simulations, it is assumed that all channels are uncorrelated and modeled using complex Gaussian variables. Thus, the size (amplitude) of channel coefficients has a Rayleigh distribution and the phase of channel coefficients has a uniform distribution. In the curves shown, GCI and BD were used to show the extended reverse channel and block diagonalization, respectively.

Figure 1 compares the overall ratio of the multi-user MIMO system for situations where channel mode information is completely in possession of the base station, for different pre-coding methods. The OCI in this figure was set to zero and the result was $W = R^{-1} = I$. The WF power allocation was used for efficient power allocation. In figures 1 and 2, the assumption is that the base station has 4 antennas that transmit information in the downward path for two users who have two antennas each. The results, which have been obtained without taking into account the OCI, show that the GCI method in both cases of even distribution and efficient allocation of power has a better performance compared to the BD method. The trade-off for this is gaining access to the information of the noise covariance matrix in the base station, which is necessary for the GCI method. It is also evident in the figure that the GCI method shows a better performance compared to the BD method without efficiently allocating power to weaker noises in signal.

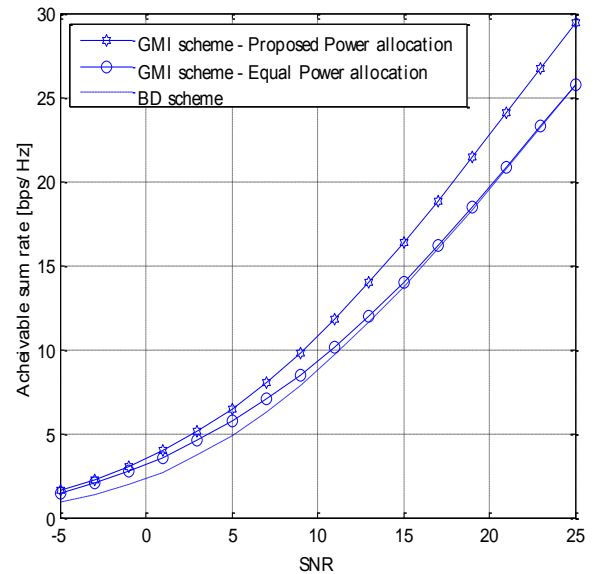


Figure 1. A comparison between the GCI and BD methods without OCI for both even distribution and efficient power allocation for GCI

Figure 2 shows the performance of pre-coding methods with OCI and the interference power is equal to $INR = 20$ dB. The two different $N_{I,k} = 1$ and $N_{I,k} = 2$ cases have been assumed for the OCI.

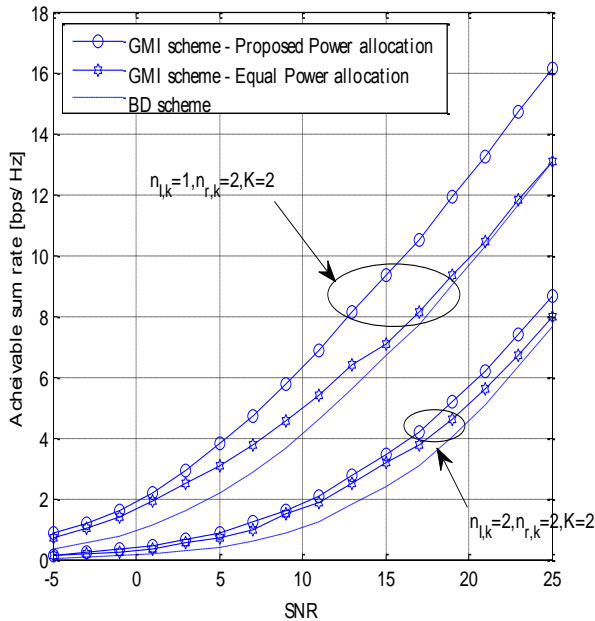


Figure 2. A comparison between the GCI and BD methods with OCI for both even distribution and efficient power allocation for GCI

As expected, in situations where the OCI is lower, all of the methods show a good performance. It can be seen in the figure that, in the presence of OCI, the GCI and the efficient power allocation among users show a better performance in all signal to noises.

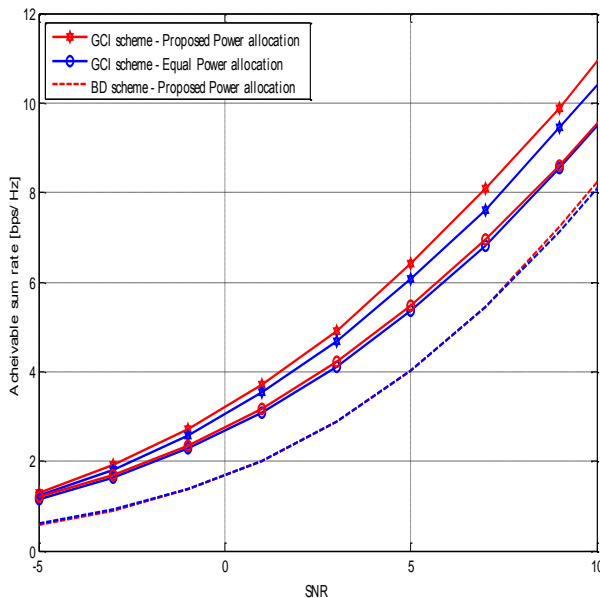


Figure 3. A comparison between the GCI and BD methods with OCI for different powers of interference signal

It is assumed in figure 3 that the base station has 6 antennas which transmit information for $K = 3$ users who have two antennas each. In this figure, the red curves were obtained for

$INR = [0,0,0]dB$ and the blue ones for $INR = [-10,0,10]dB$ which highlights the negative effects of the OCI.

Figure 4 compares the total ratio of the BD method and the GCI method. The two power allocation modes for the GCI have been compared as well. In the first case, power allocation was done using the WF method and in the second case, power allocation was done evenly and equally among users. The assumptions in the figure are $N_{R,k} = 3$, $K = 3$ and $\alpha_k = \frac{N_{I,k}}{N_{R,k}} = \left\{ \frac{1}{3}, \frac{1}{2}, 1 \right\}$.

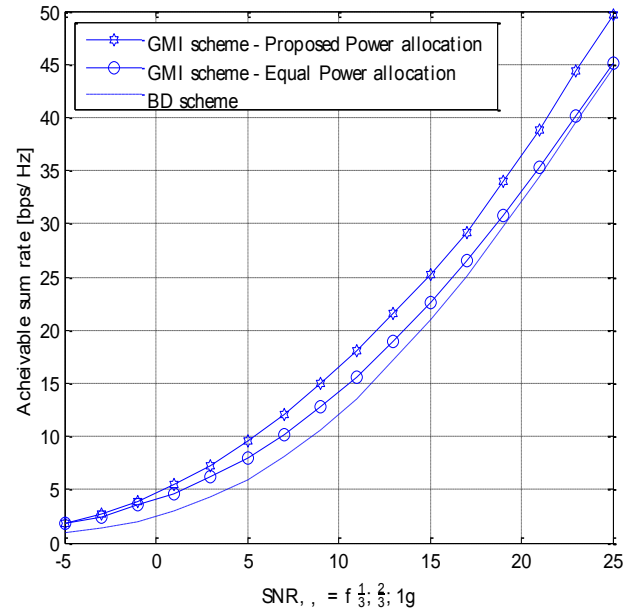


Figure 4. A comparison between the GCI and BD methods with OCI for the number of different interference users

IV. CONCLUSION

In the present study, we examined the issue of pre-coder design for a multi-user cellular system. According to the available resources, we assumed that the channel mode information will be transmitted to the base station through the right feedback channel and the base station designs the pre-coder and decoder. In the present study, in addition to removing the inter-user interference, which is the goal in most studies on the pre-coder design, we also took into account the other cell interference in the design of the two matrices. After minimizing the other cell interference in the improved BD method, which was done using the whitening filter, we used the extended reverse channel method in order to remove the limitations of the improved BD, which uses QR decomposition in order to find spatial orthogonal bases. We examined two methods for finding the composition matrix suitable for combining these spatial bases and realized that not both of the methods allow for total deletion of inter-user interference. However, in order to compensate for the lost ratio due to left interference, we introduced a power allocation problem that, instead of distributing power evenly among users, distributes the total available power among users efficiently to maximize the total ratio. The performance

improvement caused by the efficient power allocation method was supported by the simulations in MATLAB™.

REFERENCES

- [1] G. J. Foschini and M. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Commun.*, vol. 6, pp. 311-335, Mar. 1998.
- [2] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, pp. 585-595, Nov. 1999.
- [3] I. Lee, A. Chan, and C.-E. W. Sundberg, "Space-time bit-interleaved coded modulation for OFDM systems," *IEEE Trans. Signal Process.*, vol. 52, pp. 820-825, Mar. 2004.
- [4] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2658-2668, Oct. 2003.
- [5] P. Viswanath and D. N. C. Tse, "Sum capacity of the vector Gaussian broadcast channel and uplink-downlink duality," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1912-1921, Aug. 2003.
- [6] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, pp. 439-441, May 1983.
- [7] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian MIMO broadcast channel," in *Proc. IEEE International Symp. Inform. Theory*, June 2004.
- [8] D. P. Palomar, J. M. Cioffi, and M. A. Lagunas, "Joint Tx-Rx beam forming design for multicarrier MIMO channels: a unified framework for convex optimization," *IEEE Trans. Signal Process.*, vol. 51, pp. 2381-2401, Sep. 2003.
- [9] A. J. Tenenbaum and R. S. Adve, "Joint multiuser transmit-receive optimization using linear processing," in *Proc. IEEE International Commun. Conf.*, vol. 3, pp. 588-592, June 2004.
- [10] J. Zhang, Y. Wu, S. Zhou, and J. Wang, "Joint linear transmitter and receiver design for the downlink of multiuser MIMO systems," *IEEE Commun. Lett.*, vol. 9, pp. 991-993, Nov. 2005.
- [11] J. Joung and Y. H. Lee, "Regularized channel diagonalization for multiuser MIMO downlink using a modified MMSE criterion," *IEEE Trans. Signal Process.*, vol. 55, pp. 1573-1579, Apr. 2007.
- [12] L. Tran, M. Juntti, and E. Hong, "On the precoder design for block diagonalized MIMO broadcast channels," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1165-1168, Aug. 2012.
- [13] H. Sung, S. R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489-3499, 2011.
- [14] H. Sung, S.-R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, Nov. 2009.
- [15] L. M. C. Hoo, B. Halder, J. Tellado, and J. M. Cioffi, "Multiuser transmit optimization for multicarrier broadcast channels: asymptotic FDMA capacity region and algorithms," *IEEE Trans. Commun.*, vol. 52, no. 6, pp. 922-930, June 2004.

Ghodsie Ghalamkarian was born in Isfahan, Iran, in 1982. She acquired the B.Sc. degree in Telecommunication Engineering from Najafabad University, Isfahan, Iran in 2005. She is a M.S. student in Communications Engineering at science and Research Branch, Islamic Azad University, Tehran, Iran, now. Her major fields of interest are DSP processors, wireless multimedia networks and signal processing systems. She is currently working as a MIMO expert.



Mohammad Ali Pourmina is associated professor in electrical engineering (Telecommunication) in Science and research Branch, Islamic Azad University, Tehran, Iran. He received his Ph.D. degree in electrical engineering (Telecommunication) at Science and research Branch, Islamic Azad University, Tehran, Iran, in 1996 and joined to this university 1996. He has been a member of Iran Telecommunication research center since 1992. He has performed research in the areas of packet radio networks and digital signal processing systems since 1991. His current research interests include spread-spectrum systems, cellular mobile communications, indoor wireless communications, DSP processors and wireless multimedia networks.

An Improved Multiple-level Association Rule Mining Algorithm with Boolean Transposed Database

Ruchika Yadav

Research Scholar,

*Department of Computer Science and Application,
Kurukshetra University, Kurukshetra, Haryana, India*

Dr. Kanwal Garg

Assistant Professor,

*Department of Computer Science and Application,
Kurukshetra University, Kurukshetra, Haryana, India*

Abstract- Mining of multiple level association rules is a process of data mining, in which significant implication relationship of useful items can be extracted in the form of knowledge at different levels of abstraction. It determines interesting relations between data items through various levels. Association rules with multiple levels of abstraction are more practical and superior as compare to single level association rules. Numerous algorithms had been proposed by the researchers for finding multilevel association rules. The majority of the presented algorithms in this direction relied upon Apriori, and FP-growth, which are based on tire-out explore methods and face problems with large databases. To facilitate multilevel association rules searching, from large databases, a novel algorithm named as “MLTransTrie” is proposed in this paper which is based on bottom-up approach. This newly developed algorithm helps in reducing number of iterations of database as well as it takes less space in computer memory due to transposed representation of database.

Keywords- Frequent Itemsets; Minimum Support; Multiple Level Association Rule; Transposed Database; Trie;

1. INTRODUCTION

Association rules [1, 2] mining is a significant technique of data mining. It is basically used for finding the relationship between items of a transactional database. The association rules mining is applicable in the area of sensor network data mining [3], gene ontology mining [4], cloud computing [5], spatial data mining [6, 7], and network intrusion detection [8, 9]. Principally, association rules are the correlation among items of database in the form of $X \rightarrow Y$, where X and Y are the set of items. The validity of association rules is based on two essential parameters: support and confidence. The frequency or occurrence of an itemset in the database is known as support of that item. The confidence is the ratio of support of itemset (XUY) to support of itemset(X). An Itemset is known as frequent if it qualifies the condition of minimum support and a rule is valid if it satisfies the user defined minimum support and minimum confidence. The frequent item set generation is an initial step in the process of mining association rules. For generation of frequent itemsets, numerous algorithms were proposed in last few decades; nearly all of them were based on two approaches: with candidate set generation and without candidate set generation approach. Apriori [10] was the first algorithm which generated the frequent itemsets on the basis of candidate set generation. After that many researchers presented extensions of the algorithm which were AprioriTID [10], AprioriHybrid [11], DHP [12], FDM [13], DIC [14], CARMA [15], Éclat [16], Scaling Apriori [17] and many more. Another kind of approach based algorithm was FP-growth [18], which proposed without candidate set generation method. Further improvements to the FP-growth algorithm were FPMMax [19], GIT-tree [20], COFI [21], Minimum effort [22]. Above mentioned approaches were intended to produce association rules at single level of abstraction, which contain extremely general information. To find more comprehensible and interpretable facts, multiple level association rules came into existence. The concept hierarchy of items is essential to mine multiple level association rules. These hierarchies characterize the relationships among the items, and categorize them at more than a few levels of abstraction. These concept hierarchies are offered, or created by specialists in

the application field. Remaining Paper is organized as follow: Section 2 contains Theoretical Background & Related Work. The proposed algorithms MLTransTrie is presented in section 3. Section 4 contains the conclusion and future work.

2. RELATED WORK

There are some kinds of associations that particularly grab the attention. These associations arise between hierarchies of items. These items usually can be divided into different hierarchies based on domain nature. For example, things in a department store, beverages in a supermarket, or objects in a sports shop can be grouped into classes and subclasses that can lead to creation of hierarchies, which plays an important role of providing relationship among items. These relations are necessary for mining multiple level association rules. For finding these rules two phases are required: Initially, it generates the frequent itemsets at each level of hierarchy on the basis of minimum support value and then on the basis of these frequent item sets useful association rules are generated. Many researchers have focused on multiple level association rules mining. The one category of algorithms is based on Apriori [10] method. Firstly, multiple level association rules concept was given by Han & Fu [23]. Authors built up a top-down dynamic developing procedure for mining multiple-level association rules that expands the prevailing single-level association rule mining algorithms and discovers techniques for sharing information structures. In [24], a hash tree based method PRUTAX was introduced for mining multiple level frequent itemsets. The algorithm PRUTAX calculates count for only those candidate itemsets where all subset itemsets are frequent. The experimental results show the numbers of support computations were reduced by this method. A relatively different approach was introduced by Han and Fu in [25]. The researchers had analyzed the methods proposed in [23], and presented enhanced and optimized algorithms. Starting with the topmost level of the taxonomy, the rules on all level are extracted with decreasing support value as going down in the taxonomy. The extraction of rules, including items of different levels is not possible by this method. Another algorithm, MLAPG (Multiple-Level Association Pattern Generation) was presented in [26]. In order to extract all multiple-level frequent itemsets MLAPG scanned the database once and built a bit vector for each item. Furthermore, the size of the database is gradually reduced by pruning the items which are not frequent at the prior concept level. The association rules are generated by construction of an association graph by using the AGC algorithm [26]. But in case of large database, this algorithm is not able to perform well because related information may not fit in the main memory. In order to reduce memory requirements a new algorithm LWFT (Level wise filter table) was introduced in [27] for mining multiple level association from large transactional database. This method was the extension of [23] which was based on top-down dynamic developing procedure. In this algorithm the number of passes over database at each concept level is reduced due to itemsets counting implication approach, which is based on the notion of key patterns of equivalence class of itemset. The size of database is reduced at each concept level by filtration of encoded table. Experimental results proved that LWFT performed superior in terms of execution time and memory. Researchers in [28] explored a new model (MLBM), for mining multilevel association rules which was based on Boolean matrix. In that method only one scan of database was required. It adopted Boolean vector relation calculus, to extract frequent item sets at lower level and Boolean logic operations were used to produce association rules.

Another category of algorithms is based on FP-growth [18] approach. The key motive of pattern-growth approach is to store large database with the help of tree. In this method, number of scans of large database is not required. Consequently, this technique was fast as compare to candidate set generation approach. A fast algorithm for mining multiple level association rules was FAMML_FPT presented in [29]. This algorithm was based on frequent pattern tree. The concept of the repaired items and the cross-level repaired items is introduced, which is promising to create FP-tree from lower levels to higher levels. In [30] author offered a new method ADA-AFOPT to resolve the problem associated mining multiple level frequent itemsets. This method uses top-down, depth-first traversal and items are stored according to their support value in increasing order. Another approach with FP-tree structure was proposed in [21]. In this approach FP-Growth tree was combined (used) with COFI (co-occurrence frequent item) to generate rules at multiple levels of abstraction. This algorithm builds COFI-tree for extraction of frequent itemsets which utilizes the memory in

efficient way. A complete set of frequent items can be produced by straightforward traversal of COFI-tree, so there was no requirement of repetitive mining process. An improved multi-level association rule mining algorithm was presented in [31], which employed a secondary storage structure. In that algorithm, efficiency of searching items was enhanced by use of hash table. By the help of experimental results it was proved that performance of the improved algorithm was increased by about 10%. In order to enhance the frequent itemset extraction process efficiency, another method of multi-level association rules mining was proposed in [3]. Multi-Level Association Rules Algorithm (MLAR algorithm) was designed in order to find valuable information in diverse information granularity level.

The above mentioned approaches towards multiple level association rules are based on exhausting exploration techniques. Nevertheless, these algorithms can suffer for tremendous computational cost in finding association rules while they are applied to large transactional databases. To accelerate generation of multiple levels association rules and to reduce the unnecessary computation, a novel genetic-based method was introduced in [32]. In this algorithm, the tree encoding schema was used, which significantly decrease the association rule exploration space. The empirical outcomes show the efficacy and competence of the given algorithm in big data. Existing algorithms that accomplish the task of mining association rules at multiple levels of abstraction with Apriori based methods are not efficient to achieve time efficiency. The repetitive numbers of database scan are required to generate the candidate sets. Proposed methods that employ FP-growth approach are inefficient in the way that they use a large amount of computer memory to store conditional trees for frequent itemsets mining. Most kind of methods produce redundant multiple levels association rules in association rule discovery process. To encounter these problems an efficient algorithm is proposed which will overcome the problem associated with repetitive database scans and space requirement.

3. PROPOSED ALGORITHM

A new algorithm, *MLTransTrie* is proposed for mining multi-level association rules. The new method works on bottom-up approach. The lowest level contains rules with specific information, and it may be possible that no rules may match the constraints. But the rules at higher levels are enormously general. So, the value of user defined minimum support will vary according to the level. The algorithm will use an encoded transaction database. This encoded database is prepared by applying the positional encoding scheme on the concept hierarchy as explained in [27]. The method finds frequent 1-itemsets with their support at each level and on the basis of that, it filters the encoded database to remove infrequent items and also, transactions with only infrequent items. Then database is represented in transposed form and sorted, in descending order, according to support value of items. The presence of item in transactions of sorted transposed database is stored in bit format. Due to its structure as well as reduced form, it takes less space in memory and also less time for scanning.

Subsequently, this database is represented by Trie[33], which is appropriate for candidate set generation because transactions that have similar items uses the same prefix tree. Now simply trie traversal is required, to obtain candidates sets.

3.1. Case Study

MLTransTrie accomplish its task in two steps at each level of concept hierarchy. Initially, it converts the encoded database into reduced transposed database and then, it represents the database in Trie for frequent item set generation. A sample transactional database is shown in Table 1.

Table 1: Sample Transactional Database

Transaction Id	Items
T1	{211, 212, 313, 111, 122}
T2	{112, 122, 211, 225, 321, 313}
T3	{211, 311, 111, 456}
T4	{122, 132, 555, 231, 212, 311}
T5	{211, 212, 311, 111}
T6	{131, 112, 211, 322, 311}
T7	{121, 211, 221, 212, 132, 413}

T8	{111, 211, 323, 524, 212, 132}
T9	{411, 524, 121}
T10	{111, 211, 222, 411}

The Process of scanning will start from lowest level and then goes up to first level. Level wise explanation and Trie representation is given below:

Level: 3

Scan the encoded database given in Table1 and compute the presence of each item at level 3. At this level all items are represented by three digits as 211, 111, 212 and so on. On the basis of their occurrence, items are arranged in descending order which is show in Table 2.

Table 2: Transaction Items at Level 3 with Frequency

Item	Frequency in Transactions	Item	Frequency in Transactions
211	7	131	1
111	6	221	1
212	5	222	1
311	4	225	1
122	3	231	1
132	3	321	1
112	2	322	1
121	2	323	1
313	2	413	1
411	2	456	1
524	2	555	1

To proceed further, assume the value of minimum support (M_Supp) as 3. The sporadic items and the transactions in which all items are infrequent are not considered for the transposed database. The presences of items in a transaction are represented by 1. In this way a reduced sorted transposed database is created which is shown in Table 3.

Table 3: Reduced Transposed Database at Level 3

Items	T1	T2	T3	T4	T5	T6	T7	T8	T10
211	1	1	1	0	1	1	0	1	1
111	1	0	1	0	1	0	1	1	1
212	1	0	0	1	1	0	1	1	0
311	0	0	1	1	1	1	0	0	0
122	1	1	0	1	0	0	0	0	0
132	0	0	0	1	0	0	1	1	0

After the creation of transposed database only one scan of this database is required to make Trie, which takes less effort to generate frequent itemsets. In Trie, there are two kinds of nodes. The root node, which is initialize to NULL and the child nodes, which have three fields: Item name, Frequency of item (occurrence count of item) and link of next item of a transaction.

1) *Transaction T1: {211,111, 212, 122}*.

The ROOT is created and then adds 211 as child of ROOT and it will contain 211 as item name, Frequency of item as 1 and link of next item i.e. 111. Add 111 as child of 211 and it will contain 111 as item name, Frequency of item as 1 and link of next item i.e. 212. Add 212 as child of 111 and it will contain 212 as item name, Frequency of item as 1 and link of next item i.e. 122. Add 122 as child of 212 and it will contain 122 as item name and there is no link for this because 122 is a leaf node for this transaction. This formation is shown in Figure 1.

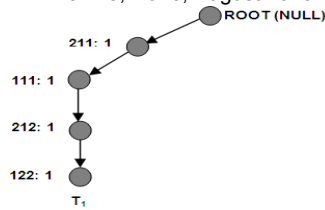


Figure 1

2) Transaction T2: {211, 122}.

The item 211 of this transaction is part of same prefix path which is already exists in Trie. So, just increase the frequency of 211 by 1. 122 is not the part of this prefix path so make it child of 211 with frequency. This formation is shown in Figure 2.

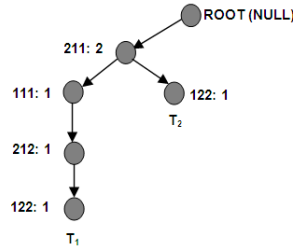


Figure 2

3) Transaction T3: {211, 111, 311}.

Two items of this transaction i.e. 211 and 111 are part of same prefix path which is already exists in Trie. So, just increase their frequency by 1. 311 is not the part of this prefix path so make it child of 111 with frequency 1. This formation is shown in Figure 3.

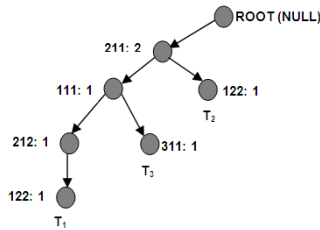


Figure 3

4) Transaction T4: {212, 311, 122, 132}.

Add 212 as another child of ROOT and it will contain 212 as item name, Frequency of item as 1 and link of next item i.e. 311. Then 311 is making the child 212 with frequency 1. and so on. This formation is shown in Figure 4.

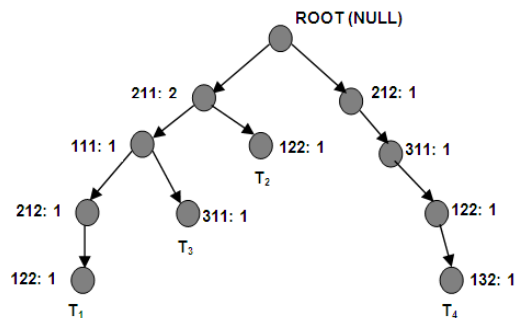


Figure 4

As there are total 10 transactions in the example so, it will be sufficient to show the precise parts of the proposed algorithm.

5) Transaction T10: {211, 111}.

Finally, Trie is formed. All the frequent items are shown with their frequency in Figure 5.

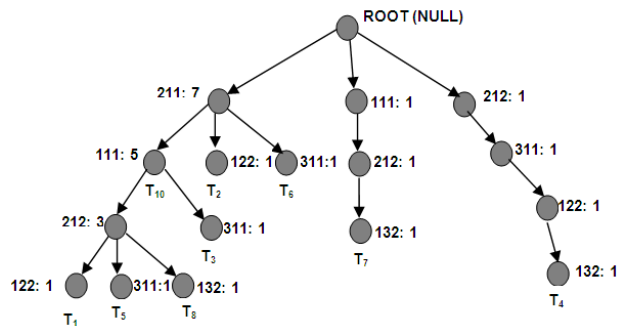


Figure: 5

Level 2:

Again examine the encoded database given in Table1 and compute the presence of each item at level 2. At this level all items are represented by two digits followed by symbol ‘*’ as 21*, 11*, 21* and so on. Table 4 is designed by inserting the items in decreasing order of their frequency.

Table 4: Transaction Items with Frequency at Level 2

Item	Frequency in Transactions	Item	Frequency in Transactions
21*	9	22*	2
11*	7	32*	2
31*	6	52*	2
12*	5	23*	1
13*	4	45*	1
41*	3	55*	1

The minimum support is increased at level 2, because as going to upper levels the information is not specific. So frequency of all items is higher than lower level. Let the minimum support (M_Supp) at level 2 is 4. The items with frequency less than minimum support are not considered. The reduced transposed database is given in Table 5.

Table 5: Reduced Transposed Database at Level 2

Items	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
21*	1	1	1	1	1	1	1	1	0	1
11*	1	1	1	0	1	1	0	1	0	1
31*	1	1	1	1	1	1	0	0	0	0
12*	1	1	0	1	0	0	1	0	1	0
13*	0	0	0	1	0	1	1	1	0	0

After the creation of transposed database at level 2 with minimum support 4 again make Trie by repeating the process (steps) as at level 3.

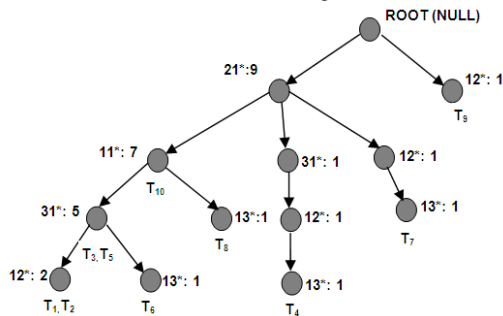


Figure: 6

Figure 6 shows the final representation of the database after generating the Trie at level 2.

Level 1:

For level 1 same procedure is followed as for lower levels used. The Table 6 is generated by the help of Table 1. At this level all items are represented by only one digit and two ‘**’ as 1**, 2**, 3** and so on. Table 6 is considered by inserting the items in decreasing order of their frequency.

Table 6: Transaction Items with Frequency at Level 1

Item	Frequency in Transactions
1**	10
2**	9
3**	7
4**	4
5**	3

Let the minimum support (M_Supp) at level 1 is 6. The items with frequency less than minimum support are not considered. The reduced transposed database is given in Table 7.

Table 7: Reduced Transposed Database at Level 1

Items	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
1**	1	1	1	1	1	1	1	1	1	1
2**	1	1	1	1	1	1	1	1	0	1
3**	1	1	1	1	1	1	0	1	0	0

After the creation of transposed database at level 1 with minimum support 6 build Trie by repeat the process (steps) as at level 3.

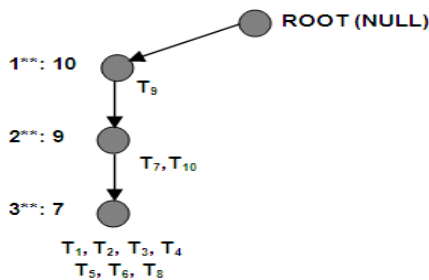


Figure: 7

Figure 7 illustrate the final representation of the database at level 1. Now, with the help of Tries at each level the task of generation of frequent itemsets is performed. This paper explains the process of mining of frequent itemsets at level 3. For that, first of all, using depth first search, it will traverse the Trie in Figure 5. After traversal the Maximal itemset with their frequency are given below: -

- {211, 111, 212, 122: 1}, {212, 311, 122, 132: 1},
- {111, 212, 132: 1}, {211, 111, 212, 311: 1}, {211, 122: 1},

{211, 111, 212, 132: 1}, {211, 111, 311: 1}, {211, 311: 1}

Now takeout the maximal itemset of any single path one by one and compare its frequency with M_Supp of that level i.e. 3 for this level. If it qualifies the condition then put all the subsets of maximal itemset in the Frequent Itemset Table i.e. Table 8 otherwise, put all the subsets in the Suspected Itemset Table i.e. Table 9. While putting the subsets in the concerned table, find the frequency of each subset from Trie. To find the frequency of subsets take their values and after confirming the minimum value from these items, assign that to the subset. As it is possible that different paths may contain same itemset so, add the frequency of same itemsets of a table. After completion of this step, takeout itemset from suspected table which qualifies the condition of M_Supp and put them in Frequent Itemset Table and add the frequency of same itemsets.

Table 4: Frequent Itemset

Item	Frequent item Set
211	{211: 7}
111	{111: 6}, {111, 211: 5}
212	{212: 5}, {212, 111: 4}, {212, 211: 3}
311	{311: 4}, {311, 211: 3}
122	{122: 3}
132	{132: 3}, {132, 212: 3}

Table 5: Suspected Itemset

Infrequent Itemsets
{311, 212: 2}, {311, 111: 2}, {311, 211: 2}, {311, 212, 111: 1}, {311, 212, 211: 1}, {311, 111, 211: 1}, {311, 212, 111, 211: 1}
{122, 311: 1}, {122, 212: 2}, {122, 211: 1}, {122, 311, 212: 1}, {122, 212, 111: 1}, {122, 111, 211: 1}
{132, 311:1}, {132, 111:2}, {132, 211:1}, {132, 122, 311:1}, {132, 122:1}, {132, 111, 212:1}, {132, 311, 212: 1}, {132, 212, 111:2}, {132, 212, 211:1}, {132, 111, 211:1}, {132, 122, 311, 111:1}, {132, 212, 111, 211:1}, {132, 122, 311, 212:1}

3.2 Algorithm *MLTransTrie*

Input: 1) D a transactional database in the format of (Tid, items). 2) Concept hierarchy CH to support the items in transactional database. 3) User defined minimum support value M_supp .

Output: Frequent itemsets at multiple levels.

Method: A bottom-up dynamic developing procedure which generates frequent itemsets at different levels of concept hierarchy. This method uses non-uniform support for all levels, so it starts with lowest level (max_level) of hierarchy and goes up to highest level.

1. For $level = max_level$ to $level = 1$ do
2. $Trie[level] = CREAT_TRIE(TD[level]);$
3. $Frequent[level] =$
 $GET_FREQUENT_ITEMSETS(Trie[level], M_supp[level]);$
4. End

Procedure *CREAT_TRIE*

Input: 1) Transposed database TD in the format of (items, Tid).

Output: Trie with frequency of each item.

1. *CREAT_TRIE (TD) do*
2. *Trie=NULL; Item.support=0;*
3. *For all Tid ∈ TD do*
4. *Insert (Trie, Tid);*
5. *For each item ∈ Tid do item.support++;*
6. *End*
7. *return Trie;*
8. *End*

Procedure GET_FREQUENT_ITEMSETS

Input: 1) Trie with frequency of each item and minimum support value M_supp .

Output: All frequent and infrequent itemsets.

1. *GET_FREQUENT_ITEMSETS(Trie, M_supp) do*
2. *Frequent_itemsets=NULL; Suspected_itemsets= NULL;*
3. *For all (paths) routes in Trie do*
4. *Maximal_itemsets= DFS Traversing(Trie);*
5. *For all subset of Maximal_itemsets do*
6. *If itemset.support ≥ M_supp than do*
7. *Frequent_itemsets =Frequent_itemsetsU itemset;*
8. *End*
9. *Else than do Suspected_itemsets= Suspected_itemsetsU itemset;*
10. *End*
11. *For all itemset of Suspected_itemsets do*
12. *If itemset.support ≥ M_supp than do*
13. *Frequent_itemsets =Frequent_itemsetsU itemset;*
14. *Itemset.support++;*
15. *End*
16. *End*
17. *End*
18. *return Frequent_itemsets;*
19. *return Suspected_itemsets;*
20. *End*

4. CONCLUSION AND FUTURE WORK

The necessity of multiple-level association rule mining algorithms is rapidly increasing due to the need of advanced and precise knowledge in all fields. In this research work, a novel multiple-level association rule mining algorithm *MLTransTrie* is proposed which is based on advanced data structure Trie and transposed database. This new algorithm overcomes the problem associated with existing algorithms by improving the time efficiency as well as space requirements. The proposed algorithm counts the supports of itemsets based on the supports of other itemsets. The redundancy of association rules is an untouched issue. Although this *MLTransTrie* method is proficient in dealing with some key challenges related to multilevel association rule mining, but some issues are left for further research. Some effective optimization techniques are required to reduce the useless association rules.

1. Agrawal R, Imielinski T. and Swami A., "Mining Association Rules between Sets of Items in Large Databases". Proceedings of the 1993 ACM SIGMOD Conference Washington DC, USA, 1993.
2. Savasere A., Omiecinski E. and Navathe S., "An Efficient Algorithm for Mining Association Rules in Large Databases". Proceedings of the 21st VLDB conference Zurich, Switzerland, 1995.
3. Han D., Shi Y., Wang W., "Research on Multi-Level Association Rules Based on Geosciences Data". Journal of Software, vol. 8, no. 12, pp.3269–3276, 2013.
4. Guzzi p. H., Milano M. and Cannataro M., "Mining Association Rules from Gene Ontology and Protein Networks: Promises and Challenges". In Proceeding 14th International Conference on Computational Science, Published by Elsevier Vol.29, pp.1970-1980, 2014.
5. Lin K.W. and Deng D.J., "A Novel Parallel Algorithm for Frequent Pattern Mining with Privacy Preserved in Cloud Computing Environments". International journal of Ad Hoc and Ubiquitous Computing, Inderscience publication, pp.205-215, 2010.
6. Petelin B., Kononenko I., Malaocioc V., and Kukar M., "Multi-level association rules and directed graphs for spatial data analysis". Expert Systems with Applications, vol. 40, no. 12, pp.4957–4970, 2013.
7. Appice A., Berardi M., Ceci M., and Malerba D., "Mining and Filtering Multi-level Spatial Association Rules with ARES". Proceedings in 15th International Symposium, ISMIS 2005, Saratoga Springs, NY, USA, pp.342-353, 2005.
8. Han H., Lu X. L., and Ren L. Y., "Using Data Mining to Discover Signatures in Network-Based Intrusion Detection". Proceedings of the First International Conference on Machine Learning and Cybernetics, Beijing, vol. 1, 2002.
9. Zhengbing H., Zhitang L., and Jungi W., "A Novel Intrusion Detection System (NIDS) Based on Signature Search of Data Mining". WKDD First International Workshop on Knowledge discovery and Data Ming, pp. 10-16, 2008.
10. Agrawal R. and Srikant R., "Fast Algorithms for Mining Association Rules". In Proc. 20th International Conference of Very Large Databases (VLDB), pp.487-499, Santiago, Chile, 1994.
11. Bica M., "Apriori Error Estimation in Terms of The Third Derivative for The Method of Successive Approximations Applied to ODE'S". Journal of Applied Mathematics and Computing, vol. 22, pp.199-212, 2006.
12. Park J.S., Chen M.S. and Yu P.S., "An Effective Hash Based Algorithm for Mining Association Rules". In Proceeding 1995 ACM SIGMOD International Conference on Management of Data, pp.175-186, 1995.
13. Cheung C., Han J., Ng V.T., Fu A.W. and Fu Y., "A Fast Distributed Algorithm for Mining Association Rules". In Proceeding of 1996 International Conference on Parallel and Distributed Information Systems (PDIS'96, Miami Beach, Florida, USA), 1996.
14. Brin S., Motwani R., Ullman J.D., and Tsur S., "Dynamic Itemset Counting and Implication Rules for Market Basket Data". In Proceedings of the 1997 ACM SIGMOD International Conference on Management of Data, Vol.26 No. 2, pp.255–264, 1997.
15. Hidber C. "Online Association Rule Mining". In Proceeding of the 1999 ACM SIGMOD International Conference on Management of Data, Vol. 28, No.2, pp.145–156, 1999.
16. Zaki M.J., "Scalable Algorithms for Association Mining". IEEE Transactions of Knowledge and Data Engineering, Vol.12, pp.372–390, 2000.
17. Prakash S., Parvathi R.M.S., "An Enhanced Scaling Apriori for Association Rule Mining Efficiency". European Journal of Scientific Research, Vol. 39, pp.257-264, 2010.
18. Han J., Pei J. and Yin Y. "Mining Frequent Patterns without Candidate Generation". In Proceeding 2000 ACM SIGMOD International Conference on Management of Data, 2000.
19. Grahne G. and Zhu G., "Fast Algorithms for Frequent Itemset Mining Using FP-trees". In IEEE transactions on knowledge and Data engineering, Vol.17, No.10, pp.1347-1362, 2005.
20. Vo B., Nguyen H., Ho T. B. and Le B., "Parallel Method for Mining High Utility Itemsets from Vertically Partitioned Distributed Databases". Proceedings of the 13th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, pp.28-30, 2009.
21. Shrivastava V. K., kumar P. and pardasani K. R., "FP-Tree and COFI Based Approach for Mining of Multiple Level Association Rules in Large database". International Journal of Computer Science and Information Security (IJCSIS), Vol.7, No. 2, 2010.
22. Rajalakshmi M., Purusothaman T. and Nedunchezian R., "International Journal of Database Management Systems". Proceeding in IJDMIS, Vol. 3, No. 3, pp.19-32, 2011.
23. Han J. and Fu Y., "Discovery of Multiple-Level Association Rules from Large Databases," in Proceedings of the 21st International Conference: Very Large Data Bases, vol. 95, pp.420–431, 1995.
24. Hipp, J., Myka, A., Wirth, R. and Guntzer, U., "A New Algorithm for Faster Mining of Generalized Association Rules". In 2nd International Conference PKKD, 1998.
25. Han J. and Fu Y., "Discovery of Multiple-Level Association Rules from Large Databases". Proceeding in IEEE Trans. on Knowledge and Data Eng. Vol. 11 No. 5, pp.798- 804, 1999.
26. Jane S. and Chen Arbee L.P., "A Graph-Based Approach for Discovering Various Types of Association Rules". Proceeding in IEEE Transactions on Knowledge and Data Engineering Vol. 13 No. 5, pp.839-845, 2001.
27. Vishav M., Yadav R. and sirohi D., "Mining Frequent Patterns with Counting Inference at Multiple Levels". Proceeding in International Journal of Computer Applications Vol. 3, No.10, 2010.
28. Gautam P. and Pardasani K. R., "A Fast Algorithm for Mining Multilevel Association Rule Based on Boolean Matrix". International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 03, pp.746-752, 2010.
29. Cao H., Jiang Z., and Sun Z., "Fast Mining Algorithm for Multilevel Association Rules Based on FP-tree," Computer Engineering, vol. 19, no. 25, 2007.
30. Mirela P. and Popescu D. E., "Multi-Level Database Mining Using AFOPT Data Structure and Adaptive Support Constrains". Proceeding in International Journal of Computers, Communications & control, Vol. 3, pp.437-441, 2008.
31. Tang H., Wu M., and He Y., "Improved multilevel Association Rule Mining Algorithm". Computer Engineering, vol. 16, No. 16, 2011.
32. Xu Y., Zeng M., Liu Q. and Wang X., "A Genetic Algorithm Based Multilevel Association Rules Mining for Big Datasets". Hindawi Publishing Corporation Mathematical Problems in Engineering, Vol.9, 2014.
33. Bodon F. and Ronyal L., "Trie: An Alternative Data Structure for Data Mining Algorithms". Proceeding in Mathematical and Computer Modeling, Elsevier Ltd., Vol. 38, pp.739-751, 2003.

A Review on Development of GIS and m-Health Based Patient Registration System to Enhance Support for Epidemiological Analysis: A Case Study of Tanzania Hospitals

Judith Leo, Kisangiri Michael, Khamisi Kalegele
*School of Computational and Communication Science and Engineering
Nelson Mandela African Institution of Science and technology
P. O. Box 447, Arusha, Tanzania*

Abstract- Over the past decades, there has been great advances in ICTs, which has led to the evolution and deployment of mobile phone application technology and GIS in the health sector. Despite of the expanded use of advanced ICT in the health sector, there is still ineffective data collection and presentation of patient and general health data in Tanzanian HIS. This paper shows different proposed and used GIS and mobile applications in perfecting HIS systems. It further proposes the best way on how these technologies can be used to provide effective data collection and presentation. Based on the discussions, a module is proposed to be integrated into the HIS. The ultimate goal of this paper is to improve collection and presentation of health/patient data, in order to enable enhancement of epidemiological analysis.

I. INTRODUCTION

Healthcare services access, quality and affordability are major problems all around the world especially in developing countries, including Tanzania [1]. These problems are due to ineffective performance of the existing Health Information Systems (HIS). The health systems are no longer adequate for dealing with effective health data collection and presentation. The resulting effect is that epidemiological analyses are wrongly done due to poor data collection and presentation in the HIS [2]. Epidemiology involves studying the distribution and determinants of health-related states or events in a specific population, and the application of this in controlling health problems [3].

Most developing countries, especially Tanzania are reforming their health systems to provide expanded and equitable access to quality services [4] despite the low number of available health workers as reported by Kwesigambo et al. [5]. Figure 1 below shows the number of workers required and available in government healthy facilities in Tanzania.

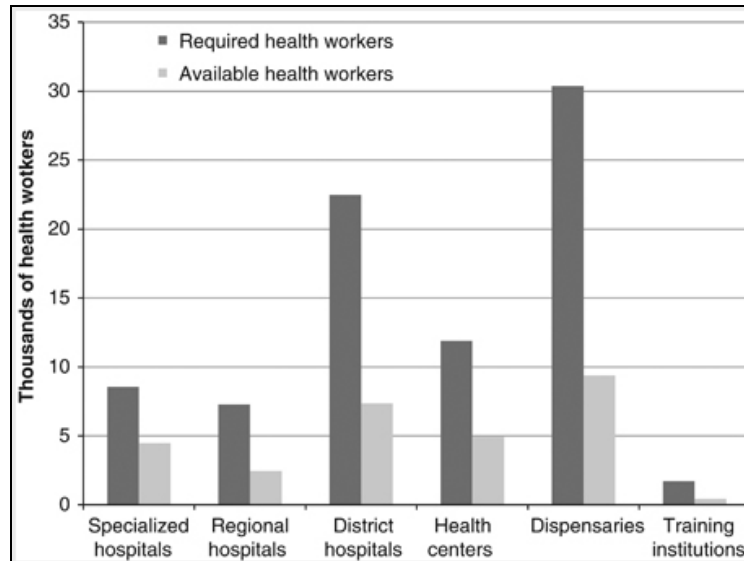


Figure 1. Number of health workers required and available in government facilities in Tanzania

Despite the health sector reforms in Tanzania that aim at reducing the workloads of the available health workers in hospitals, the World Health Organization (WHO) reports that the healthy system still encounters many problems [6] as shown in Table 1 below. However, different studies have been done to solve the health issues but still ineffective data collection and presentation persists in HIS.

Table 1. Problems encountered in existing HIS

Type of Problems Encountered	Village	District	Province	National
Duplication of forms	✓			
Too many record books/forms being filled out at this level	✓			
Lack of constant supply of forms				
Reports not submitted on time				
Inadequate training of health workers on how to fill out forms	✓	✓		
High degree of inaccuracy in data collected	✓	✓		
Lack of technical expertise of staff to properly analyze the data collected	✓	✓	✓	✓
Lack of utilization of data being collected	✓	✓	✓	✓

Taking advantages of the current growing ICT, mobile phone application and Geographical Information System (GIS) have the potential to offer major contribution towards improving the existing HIS services. Therefore, the objective of this paper is to propose the best GIS and mobile based integrated HIS, after reviewing different systems with regard to the use of mobile and GIS applications, whether they are used independently or in combination to improve data collection and presentation in HIS.

II. REVIEW OF DIFFERENT HIS IN TANZANIA

The Health Information System (HIS) is as a set of components and procedures of the healthy system organized to generate information used in improving management decisions involving health care services delivery at all levels [7]. The main components and standards of HIS as described by World Health Organization (WHO) [8] are provided in the Figure 2 below. HIS allows for transparent decision making supported by evidence, and hence improve the health status of the population. Thus, HIS produces relevant and quality information to support decision making in the health sector [6].

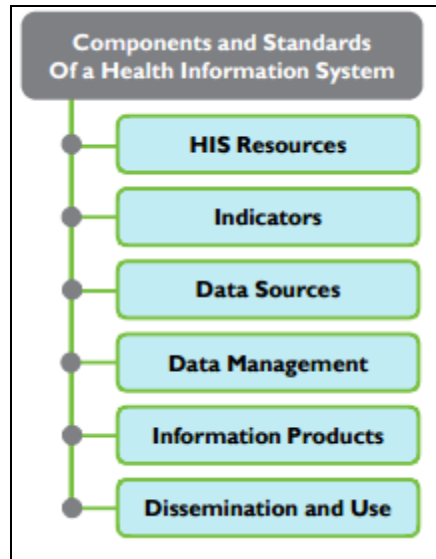


Figure 2. Health Information System's Components and Standards

However, WHO has contributed to positive progress in the health sector by putting up components and standards for all HIS designs to follow, but still the Tanzanian's HIS is currently not sufficiently responsive or effective in general [9]. Figure 3 below shows the topology of the existing HIS in Tanzania, whereby after visiting the hospital for treatment, the patient starts with the registration process then is asked the payment modality as to whether it is by the National Health Insurance Fund (NHIF) card/other insurance card or cash. The patient pays some amount for doctor's consultation and other treatment procedures will follow accordingly. The doctor documents the diagnosis results into the patient's profile. Most of the time, nurses or public officers will compile reports in paper format, which are then submitted to the district health office for analysis. This shows the ineffectiveness of the existing HIS in terms of patient data collection and presentation.

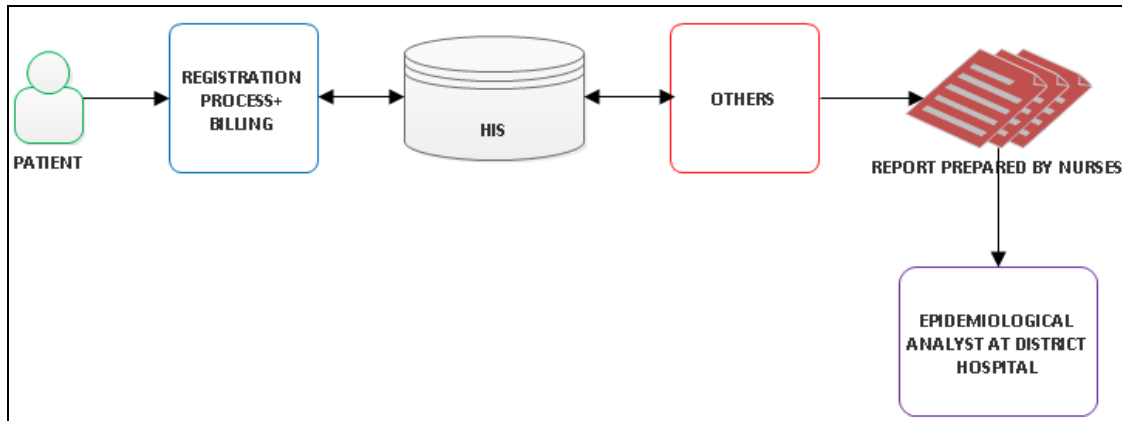


Figure 3. Topology of existing HIS in Tanzania

Many studies have attempted to find the optimal solution for counteracting the existing HIS. We now carry out a fair review of the different studies on mobile application and GIS in health care systems.

A. Mobile application based HIS

Mas et al. [10] proposed an enhanced healthcare multi-collaborative system operation over Third Generation (3G) mobile network. The proposed m-health system's architecture and sub-systems are presented in the block diagram shown in Figure 4 below.

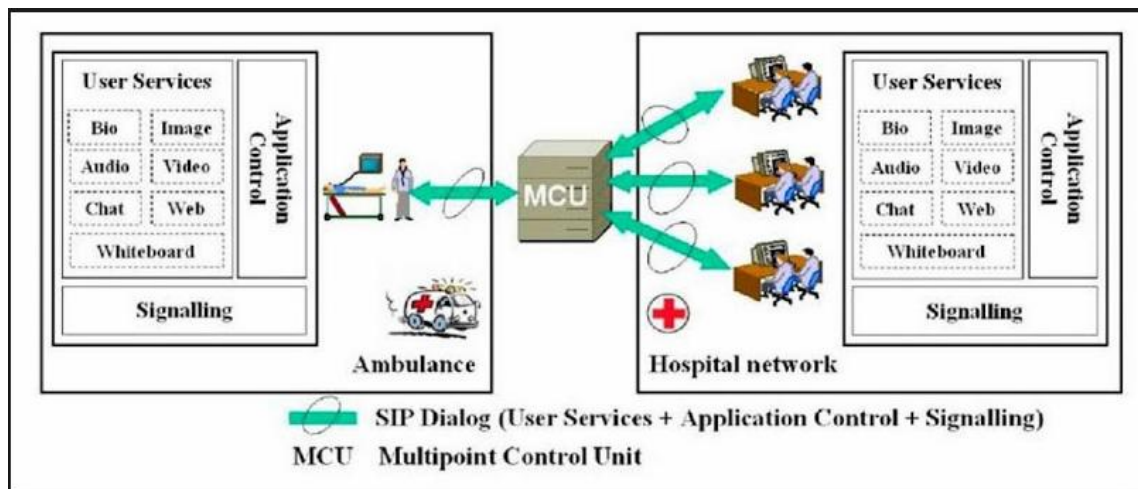


Figure 4. The m-Health System's Architecture and Sub-systems

Another related work as proposed by Ruotsalainen et al. [11] involved the use of personal doctors in a prescribed community in which they adopted the use of trust information-based architecture as shown in Figure 5.



Figure 5. The Architecture of the Trust Information Based-Privacy for Ubiquitous Health

However, the reviewed mobile based applications in healthcare have some limitations in the health sector Tanzania. From Figure 4, we see that the m-Health system architecture and sub-systems are only used between healthcare works and therefore it lacks community participation or involvement. Also Figure 5 shows the architecture of trust information based-privacy for ubiquitous health whereby patient calls his/her personal doctor for treatment. This architecture in Figure 5 is also not suitable for developing countries where the number of available healthcare workers is very low; this system can effectively work in developed countries where the number of available healthcare workers is very large.

B. GIS based HIS

Otto et al. [12] proposed the development of health monitoring system network architecture, whereby each user/patient wears a number of sensors through personal network implemented by ZigBee or Bluetooth. The personal server provides graphical or audio interface to the user, and transfer the information about health status to the medical server through the internet or mobile telephone networks such as the GPRS, 3G etc. It can be implemented on a personal digital assistant (PDA), home personal computer or cell phone, and it is used to set up and control WBAN. Figure 6 shows proposed health monitoring system network architecture by Otto, Chris et al.

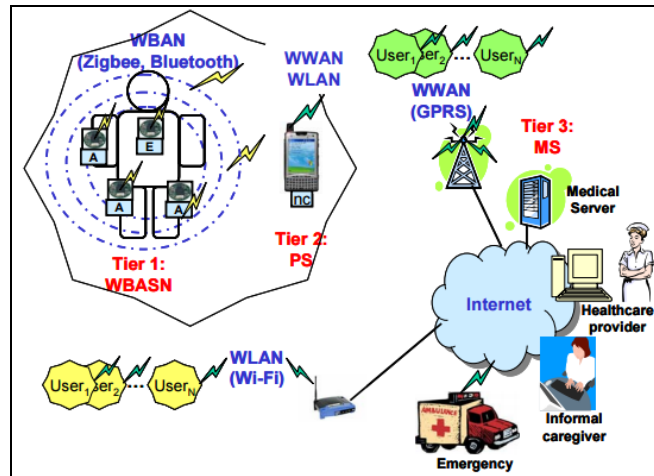


Figure 6. Health Monitoring System Network Architecture

Another use of GIS is the ArcGIS software, which is mostly used in developing countries especially in public health. The ArcGIS Server as explained by Huaqing, et al. [13] is a platform on which enterprise WebGIS applications are built. Figure 7 below shows the architecture for ArcGIS server system.

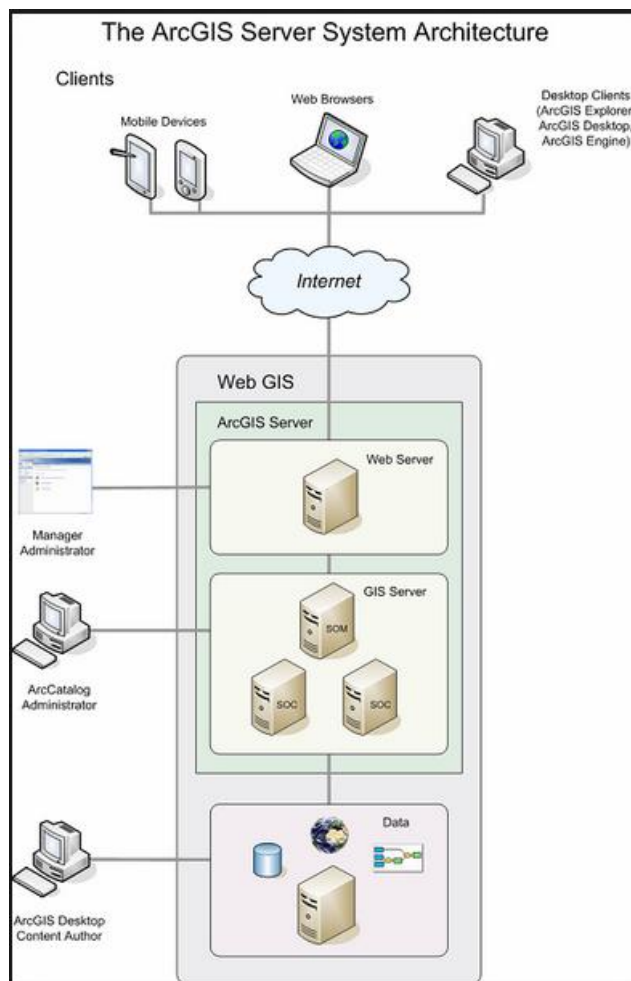


Figure 7. Architecture for the ArcGIS Server System

However, the reviewed GIS architecture in healthcare has limitations in Tanzania. The health monitoring system is very expensive as it depends on sensor and internet to run its activities full time whereas the ArcGIS is a commercial software, which is also expensive to purchase.

C. Benefits of integrating Mobile application and GIS into HIS

GISs are useful in compiling and presenting data at regional and national levels. They are particularly useful in compiling data for environmental and health outcomes for recording and measuring to the use and impact of health services. Nowadays, GIS is seen to have the potential for improving the population's health and contribute to policy development, implementation and research in public health [14]. On the other hand, the mobile application in HIS has many uses ranging from remote data collection and monitoring, education and awareness, diseases and epidemic outbreak training, diagnostic and treatment support as well as communication and healthcare workers' training [15].

In viewing the benefit of integrating GIS and Mobile application in HIS, the objectives of epidemiology in healthcare systems can be realized. These include identification of the priority health problems in the affected community, determination of the extent to which diseases exists in the community, identification of the causes of diseases and the risk factors, determination of the priority health interventions, determining the capacity of the local infrastructure and the extent of damage, monitoring the health trends of the community, and health programmes' impact evaluation [16].

III. THE PROPOSED SYSTEM

A review of various studies shows that many researchers have used mobile application technology and GIS to enhance health information systems. However, no studies have attempted to integrate the mobile application technology and GIS into the health information infrastructure to provide the basis for data collection and presentation for effective data analysis and decision support [17].

We therefore, propose to develop a system which integrates the mobile application technology and GIS to be used specifically on wireless computing devices, such as smartphones and tablets [18]. Using this system, patients can register for treatment with a hospital. After the registration form is submitted, the data goes into the staging database, which is used to store all submitted patient data. Then from the staging database, the data is pulled into the HIS database only if the patient has visited the hospital for treatment. And then patient treatment procedures take place, whereby the doctor documents the results/status of the patient into the patient profile, and finally the epidemiological analyst is able to automatically view the data in different summaries, reports and visualization using GIS. The GIS is online software, which is free to use; there will be no additional cost for purchasing it. Figure 8 below shows topology of the proposed system.

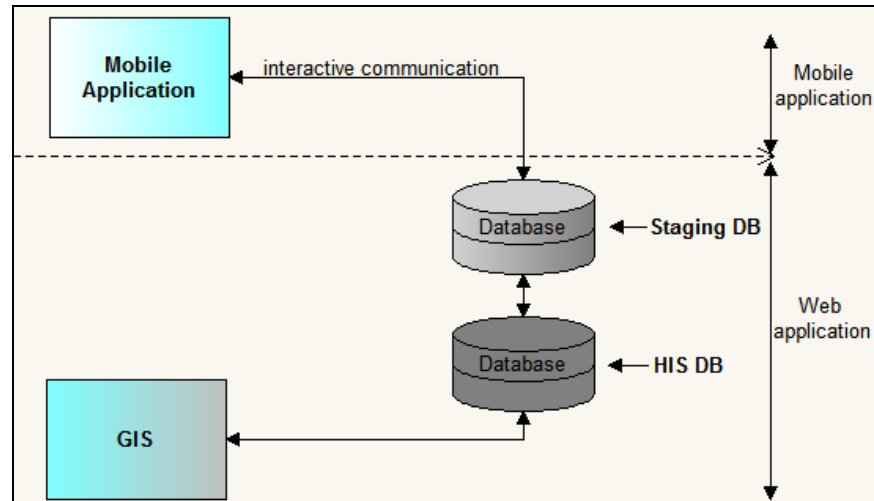


Figure 8. Protocol of the proposed system

IV. CONCLUSION AND RECOMMENDATION

This study has reviewed and analyzed various methods related to the integration of the mobile application technology and GIS with the aim of improving HIS. We have discussed different methods that help to remove inefficiencies in data collection and presentation to enhance decision making in HIS. Although some of the methods are good but very difficult to implement in the Tanzanian environment, we propose the introduction of another method that can match with the Tanzanian context. The method proposed is the use of interactive remote patient registration and integration on GIS in HIS. We recommend that the same system should be further researched using USSD mobile phones and also the related security issues in m-Health application should be research further.

ACKNOWLEDGMENT

We extend our sincerely appreciation to The Nelson Mandela African Institution of Science and Technology (NM-AIST) and the School of Computational and Communication Science and Engineering (CoCSE) for supporting this work.

REFERENCES

- [1] D. M. West, "Improving health care through mobile medical devices and sensors," *Brookings Institution Policy Report*, 2013.
- [2] S. N. Weingart, R. M. Wilson, R. W. Gibberd, and B. Harrison, "Epidemiology of medical error," *BMJ: British Medical Journal*, vol. 320, p. 774, 2000.
- [3] G. M. Stirrat, "Recurrent miscarriage I: definition and epidemiology," *The Lancet*, vol. 336, pp. 673-675, 1990.
- [4] D. R. Gwatkin, A. Bhuiya, and C. G. Victora, "Making health systems more equitable," *The Lancet*, vol. 364, pp. 1273-1280, 2004.
- [5] G. Kwesigabo, M. A. Mwangi, D. C. Kakoko, I. Warriner, C. A. Mkony, J. Killewo, *et al.*, "Tanzania's health system and workforce crisis," *Journal of public health policy*, pp. S35-S44, 2012.
- [6] W. H. Organization, "Developing Health Management Information Systems," *A Practical Guide for Developing Countries*. WHO, 2004.
- [7] T. Lippeveld, R. Sauerborn, and C. Bodart, *Design and implementation of health information systems*: World Health Organization Geneva, 2000.
- [8] W. H. Organization, "Framework and standards for country health information systems," 2008.
- [9] H. Kimaro and J. Nhamposha, "The challenges of sustainability of health information systems in developing countries: comparative case studies of Mozambique and Tanzania," *Journal of Health Informatics in Developing Countries*, vol. 1, 2007.
- [10] J. R. Mas, E. A. V. Navarro, C. H. Ramos, Á. A. Iglesias, J. F. Navajas, A. V. Bardají, *et al.*, "Design of an Enhanced 3G-Based Mobile Healthcare System," *Idea Group Publishing, USA*, 2006.
- [11] P. S. Ruotsalainen, B. Blobel, A. Seppälä, and P. Nykänen, "Trust Information-Based Privacy Architecture for Ubiquitous Health," *JMIR mHealth and uHealth*, vol. 1, 2013.
- [12] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, pp. 307-326, 2006.
- [13] K. L. F. J. W. Huaqing and C. Jinsong, "Development of WebGIS Based on ArcGIS Server [J]," *Water Resources and Power*, vol. 1, p. 007, 2007.
- [14] P. Wilkinson, C. Grundy, M. Landon, and S. Stevenson, "GIS in public health," *GIS and Health (GISDATA Series 6)*, pp. 179-189, 2003.

- [15] C. Liu, Q. Zhu, K. A. Holroyd, and E. K. Seng, "Status and trends of mobile-health applications for iOS devices: A developer's perspective," *Journal of Systems and Software*, vol. 84, pp. 2022-2033, 2011.
- [16] D. J. P. Barker and A. J. Hall, *Practical epidemiology*: Churchill Livingstone, 1991.
- [17] J. A. Nhavoto and Å. Grönlund, "Mobile technologies and geographic information systems to improve health care systems: a literature review," *JMIR mHealth and uHealth*, vol. 2, 2014.
- [18] M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer, "Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage," in *Proceedings of the 13th international conference on Human computer interaction with mobile devices and services*, 2011, pp. 47-56.

Radio Frequency Identification based Drug Management and Monitoring System: A Case of Public Hospitals in Tanzania,

Review Paper

Prisila Ishabakaki

Department of Communicational Science and Engineering
Nelson Mandela AIST
Arusha, Tanzania

Shubi Kaijage

Department of Communicational Science and Engineering
Nelson Mandela AIST
Arusha, Tanzania

Abstract— RFID is an automatic identification technology that enables tracking of people and objects. Recently, the RFID technology has been deployed in hospitals for patient and equipment tracking, surgical equipment monitoring, medication monitoring, and improving health record access in emergency cases. The pharmacy department in public hospitals faces challenges due to manual record keeping and inventory management, which result in theft and diversion of the drugs by unfaithful workers. This work identifies the potentials behind use of the RFID technology in addressing these challenges. The paper focuses on reviewing the current situation at the hospitals to identify loopholes causing these problems and later suggests the solution based on RFID to counteract the challenges. The case study methodology is used where 5 public hospitals in Tanzania were visited to obtain data based on real situation. It was discovered that the drug management and monitoring process is done manually, involves paper based record keeping, manual counting of stock during each staff shifting time, which is hard to track in case of any loss. Therefore, there is need to develop a technological solution to manage the process and secure the drugs.

Keywords: RFID, UHF Radio Frequency, Drug management and monitoring, public hospital

I. INTRODUCTION

The health sector uses different technologies in healthcare services delivery, including the Radio Frequency Identification (RFID). The RFID is an automatic identification technology that enables tracking of people and objects [1]. It utilizes electromagnetic waves for transmitting and receiving information stored in a tag to or from a reader [2]. A typical RFID system is made of at least three components: the radio frequency transponder (tag), the reader, which is basically a transceiver controlled by a microprocessor used to inquire a tag, and client software to communicate with a reader through a reader protocol, collecting, storing and/or processing codes retrieved from the tags.

Public hospitals are all healthcare service providers owned and operated by the government to serve the citizenry.

Pharmacy departments at hospitals coordinate drug orders from suppliers and distribute the drugs to patients and other hospital units. In Tanzania, all public hospitals receive or purchase drugs/medications from the Medical Stores Department (MSD) and few drugs from other suppliers or distributors. The pharmacists in healthcare institutions are increasingly burdened with handling complex manual work involving record keeping and inventory management as hospitals serve a large number of patients every day [3].

The pharmacists in hospitals are responsible for a range of work activities including filling in patients' medical prescriptions, daily maintenance of drug inventories making sure that the hospital has enough quantity for each drug for administering to patients, accounting for the hospital's purchase and usage of drugs and for provision of drugs to individual patients, and distributing the drugs to the appropriate nursing stations and wards within the hospital to suit each station's daily demands. Hospital pharmacists are also responsible for tracking of drug lot numbers and expiration dates to get rid of expired drugs, and reporting to the hospital management on all matters concerning drug ordering, dispensing and delivery.

However, there have been several instances reported on theft and loss of drugs in hospitals. For instance, the MSD's Internal Audit investigation report of October 2007 indicated that medicines valued at USD 133,000 (163.2 million TZS) were missing or stolen [4]. Another reported case [4] revealed that some medicines meant for public hospitals have been diverted to private hospitals and pharmacies. Our preliminary survey of the drugs market discovered that medicines intended for free dispensing in public health facilities are sold at varying market rates in the private sector. These drugs may have been acquired through donations by countries or manufacturers as part of aid programs, or sold at very good discounts to support public health service delivery in Tanzania [5]. Our study revealed loopholes in the information management system in relation to pharmacists' duties and responsibilities of purchasing, distribution and dispensing of medicines, which result into some medicines being channeled from the public

health facilities to the private markets. Despite the fact that these duties can be simplified by integrating the information management system, we found that there is no electronic system deployed in public hospitals in Tanzania. Various attempts have been made to assist hospitals' pharmacy departments with maintaining accurate records and reduce challenges in managing drug distribution information. Thus, developing a technological solution for monitoring drugs supplied to hospitals to reduce losses and unintended use of drugs is essential. This paper provides a review of different technologies, which are used for drug monitoring and management.

The rest of this paper is organized as follows: Section II covers overview of the RFID technology and its potential in enhancing information management in the health sector, Sections III and IV present reviews on the RFID technology basics and various research work done to counteract the hospital pharmacy challenges and their limitations respectively. Section V explains the proposed solution to the challenges facing pharmacy information management in hospitals, while Section VI concludes the paper.

II. OVERVIEW OF THE RFID TECHNOLOGY

RFID is a generic technology that uses radio waves to identify objects [6]. Other identification technologies related to RFID include barcodes, biometrics, magnetic stripe, optical card readers, voice recognition etc. The difference between RFID and these other technologies is that RFID is an automatic identification technology, which utilizes radio waves to transfer its information. Furthermore, it doesn't require line of sight for communication, and it can sustain harsh physical environments, allows simultaneous identification, has excellent data storage, wide read range, and it is efficient in terms of cost and power [7], [8]. In the health sector, the RFID has been deployed for various applications such as patient identification, anti-counterfeiting, hospital inventory management, staff and patient location and medication adherence enhancement [9]–[11].

A. RFID System Architecture

Basically, the RFID system has three components: the RFID tag or transponder, the RFID reader device or transceiver, and a backend information system (servers). Figure 1 shows the main components of the RFID system. The RFID tag typically has an electronic chip that holds a certain amount of data, and an antenna used to communicate with the reader. There are also RFID tags with no chips; these utilize certain Radio Frequency (RF) reflecting properties of materials. RFID tags can be characterized as active, passive or semi-passive. An active tag uses a battery to power the microchip's circuitry and broadcast signals to the reader. It has more memory capacity and provides wide read range. A passive tag does not use batteries and is powered by electromagnetic waves sent by a reader to induce a current in the tag's antenna. The passive tag has less memory capacity; it can store little basic information such as identification number and short coverage range. A

semi-passive tag uses both the battery and waves sent by the reader. Cost of RFID tags depends on the type; active tags are more cost than passive ones. The choice of tag depends on the kind of application where the aspects like read range, amount of information to be stored on tags and cost should be considered.

The communication between RFID reader device and the RFID tag is through RF waves. This communication with the RFID reader device with the tag differs between the types of RFID tags. The RFID reader communicates with tags through inductive coupling method. The tag's read range depends on both the reader's power and the frequency used to communicate. Radio-frequency communication between the tag and reader may occur on the following frequency bands: Low frequency (LF) band is in the range of 125–134 kHz and 140–148.5 kHz channels, high frequency (HF) band is at 13.56 MHz, and ultra-high frequency (UHF) band is in the range of 868–928 MHz [12]. The RFID system operates in Industrial-Scientific Medical (ISM) band, which is freely used by low-power, short-range systems. A higher frequency results into a longer communication range and a faster communication means that more data can be transmitted, but requires more energy output from the readers. In addition to these components, the RFID system receives large amounts of data generated from the movement of physical goods in a real world setting; the data is rarely clean and it is often noisy, erroneous, and may be unusable in its native form [13]. As a result, it was necessary to develop an intelligent component, called middle ware, to filter, aggregate, sort and add missing information in the data before it is sent to the host system.



Figure 1: RFID System components

B. RFID Tagging Levels

The RFID tag is placed at the item for identification. Level of tagging depends on the application. The RFID tagging can essentially happen at three granularity levels. First, in supply chain the RFID tagging can take place at the pallet level, where the tag is attached to a pallet. In this case, the tag ID is programmed into the tag and attached on the pallet when the pallet is ready for shipment. Typically, the tag ID is cross-referenced to a list of inventory on the pallet and the purchase order. Once the shipment arrives at its destination, the cross-referencing of the tag ID can be done again to the database record containing the pallet information. The second level of granularity is case level tagging, in which the tag is attached to the case. The tag typically cross references information for the purchase order and inventory. The case level tagging has a primary advantage over pallet-level tagging, which is that

Identify applicable sponsor/s here. (Sponsors)

more detailed tracking can be done. Case-level tagging allows for full inventory visibility as the inventory can be moved in case quantities. The automatic reporting of case counts means that case level tagging saves labor time and it makes manual case counting unnecessary.

Thirdly, item level tagging is where the tags are on the packaging of the items. The tags are attached to each product item during the manufacturer's packaging. Item level tagging provides the highest visible granularity. Depending on the RFID application environment, tagging can be at item level, case level or pallet level. In this intended application, the best tagging position will be at the case level since the item level and the distribution at pharmacy store is basically through carton boxes. And this will also reduce the tag cost as item level tagging is the costliest solution [12]. However, the cost of RFID tags was expected to be 5 cents by 2007 [14]. According to RFID journal, the volume, amount of memory on the tag and the packaging determines the cost of cost tag; thus this cost would much lower for high volume requirement [15].

C. The Potential of RFID Technology in the Health Sector

One of reasons for slow deployment of the RFID technology in many sectors is its potential in solving the intended problem due to its cost of implementation. However, making the cost benefit analysis informs the importance of the technology; that is, consideration of the cost to the hospital, government, and donor and indirectly to patients who miss treatment will eventually conclude that the cost for implementation is much less compared to the loss incurred. Studies have been conducted in different countries with the aim of examining the potential of RFID implementation in hospitals. Some of the studies include those done in Taiwan, USA [16] [17], and Taiwan [18] [19]. In our review, we found that [13] conducted a study on how information technology can be used to initiate change and improve the healthcare. The results of this study showed that implementation of the RFID in the health industry can help to measure, control, and improve workflow processes. A study by Wang et.al involved implementation of the RFID at the Taiwan Medical University Hospital. In their work, the authors explain the growth in use of the RFID in improving monitoring and management of drugs as well as the RFID planning and related strategy for implementing the RFID projects in hospitals.

A study by [18], investigated the impact of implementing the RFID technology in the hospitals and how it affects the hospital staff and the society. The findings of this study showed that the nursing staff at the hospital had signs of worries as the technology involved close scrutiny and supervision. However, these findings basically apply to the tracking application of the technology where the nurses had to be directly involved. We believe this feeling will not be experienced on pharmacy staffs since the application intends to serve their burden by automating the work. Another study [14] used case studies of 5 hospitals to find the value of using RFID in business. The case hospitals had implemented the RFID technology in 2003 with the specific aim of minimizing the impact of the Severe Acute Respiratory Syndrome (SARS). In the study, measuring the value of the RFID technology at the execution stage involved

identifying a number of intentions. The researchers concluded that including the RFID technology in the whole business framework can result into successful implementation of the technology. These studies prove that integration of the RFID technology in the health sector is very promising provided that the whole business environment is considered at early stages.

III. CURRENT DRUG MANAGEMENT ISSUES IN PUBLIC HOSPITALS IN TANZANIA

The significant cost of purchasing and storing pharmaceutical products and their respective control requirements largely contributes to the healthcare industry costs [15]. Although the health industry is seen as one the most important industries in the world, both in developed and developing countries, little attention has been given to the area of drug management and monitoring which is at the core of effective healthcare delivery. Pharmacies in Tanzania's public hospitals use traditional paper-based processes to document disbursed drugs, order drugs from suppliers, follow up on orders before delivery and receive the ordered drugs. Moreover, they also need to verify the orders, keep received drugs in stores, maintaining them in the storage facility till they got dispatched to the intended public health unit. Also, pharmacists are responsible for keeping records on all pharmacy related matters, keep track on drugs and carefully dispose the expired drugs. Furthermore, pharmacists spend most of their time on paper work to ensure all drug records are updated. The pharmacy stores receive drugs and medical equipment from suppliers in bulk, and thus have to maintain them in stores until they are dispatched to the intended public health facilities.

At the dispensing unit where patients obtain drugs from, the records are kept by filling in individual patient prescriptions and amount of money paid for the drugs on paper forms. Basically, the whole procedure is done by filling in information on the papers and monitoring activities need to be done manually. In 2007, the Global Pharma Health Fund established the protocol on assessing the quality of anti-malaria drugs in private health sectors. Unfortunately during sample collection, they found some public intended drugs being sold in private retails. This was followed by the study by [5] in which they identified the anti-malaria medicines being diverted into the African markets, especially in such countries as Nigeria, Tanzania, the Central African Republic, Senegal and Zambia. This might be due to the current management process where no one is held responsible for the government or donor supplied drugs to public hospital. A study by [16] identified that inefficiency and inaccuracy in the inventory operations and controls of pharmaceuticals is among the major challenges facing management of the operations and processes in public hospitals.

IV. RELATED WORKS

The problem involving pharmacy management and monitoring has been noted by many researchers. In addressing the hospital pharmacy management problems, several studies from academia and industry have been carried out. This section

discusses some literatures addressing pharmaceuticals research problems and we review how these can provide a better solution to similar challenges faced by public hospitals in Tanzania. This section reviews related works on pharmaceutical supply chain management, drug dispensing systems, and medication monitoring systems.

A. Pharmaceutical supply chain management

The works on pharmaceutical supply chain management concentrated on establishing the protocols and procedures to manage and monitor drugs in the hospital environment. Work done in [15] developed a model for proper utilization of resources at the pharmacy store. The study came out with order and refill levels of drugs in the information systems. This provides the basis for system designing whereby the proposed refill level could be used as reference stock level to alert users to reorder prior to total stock out.

Other researches focused on drug counterfeit detection systems. Among the major challenge in the pharmacy industry worldwide is the counterfeit drug penetration to the market. This affects both manufacturers and consumers of the pharmaceutical products. The manufacturers are affected through business loss since the counterfeit drugs are much cheaper as the traders avert paying tax and the drugs are manufactured with low quality. As for the consumers, the counterfeit drugs are dangerous to their health. Therefore, different researchers have attempted to investigate the application of the RFID technology in pharmaceutical supply chain to detect counterfeit products [17][10][18][19]. The RFID based anti-counterfeit drug tracking system is designed to provide a drug verification mechanism. Figure 8 shows the manufacturer to hospital drug distribution control system.

However, the limitation for this system is the unrealistic assumption that all the key stakeholders in the drug supply chain, such as the manufacturers, distributors, wholesalers, and pharmacies, have the necessary hardware and computing ability to read and process RFID equipment information. Furthermore, the solution is not ideal for developing countries like Tanzania where the electronic system has not been introduced and hospitals do not have internet connectivity, for referral hospitals. Implementing this solution in Tanzania will be not feasible due to high cost of implementing information systems across the hospitals and interlink with manufacturers' systems. Therefore the development of a simple but effective solution feasible to the economic status of the country yet solving the problem is important.

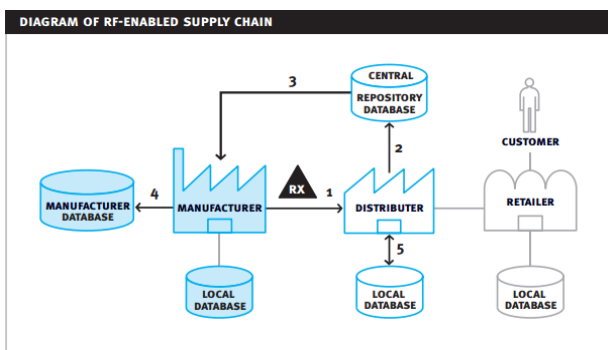


Figure 2: RFID enabled pharmaceutical supply chain [17]

B. SMS based drug monitoring systems

Novartis Company developed an SMS-based system for monitoring anti-malarial drug distribution in the sub-Saharan Africa. The technology was developed to prevent stock-out of anti-malarial drugs in remote areas by taking advantage of the coverage of the expansive mobile phone network, which has reached rural areas. The system automatically sends weekly text messages using the SMS to mobile phones at public health facilities requesting updated information on their stock levels [20]. The major challenge on the effectiveness of this system is that the remote health centers are served by the district hospital where the automated drug monitoring and ordering system is not in place. Thus, even if the SMS from the remote health center will be received, it will be difficult to process the request since even the district level can get out of stock without notification. This necessitates the need for developing an information system for drug monitoring and management at the hospital level.

C. Medication monitoring systems

Errors in administration of medication are a leading cause of patient morbidity and mortality and excessive costs; thus the development of an information system that assists in monitoring medication is vital for efficient

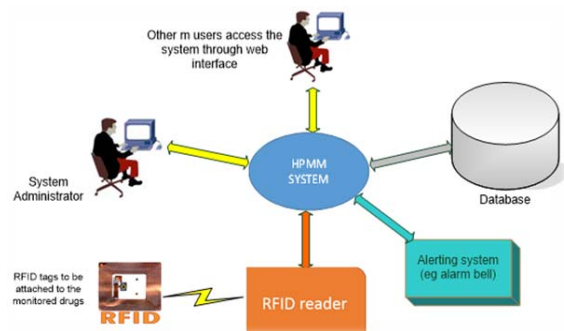


Figure 3: Proposed system architecture

health care provision [21]. Study by [22] developed a system used in maintaining drug information and communicating with medication delivery devices. The system includes software for use in the hospital pharmacy and biomedical environments. Also, ref [23] designed and developed the medication error control system, which was a RFID-based prototype software that can be used to monitor and administer medication in hospital environments. The pitfall with this system is that it is limited to medication error control and thus does not extend to pharmaceutical monitoring and management. And it also needs a well information technology networked hospital.

V. PROPOSED DRUG MONITORING AND MANAGEMENT SYSTEM

Despite the fact that barcode labeling is an inexpensive technology, offers reliability, and is widely used, the technology's limitations including the line-of-sight requirement and short-range reading distance. This makes it a slow and labor-intensive technology [2]. Receiving, storing, sorting, and shipping processes will all benefit from this wireless technology and become more efficient and effective [24]. Our proposed system intends to utilize the RFID technology to manage and monitor drugs in the hospital environment for the case of public hospitals. The system will be of low cost as it utilizes UHF RFID tags to tag the drug to be monitored. The system comprises of the central database, the RFID network, and user/administration interfaces. The proposed system will offer several benefits including preventing unexplained drug loss, saving the government's expenditure on hospital supplies by ensuring the available resources are well spent, and it will simplify stock keeping, prevent stock-out by integrating re-ordering notification on preset stock level. Furthermore, the system will improve record keeping, health service delivery and eliminate manual work performed by pharmacy staff. Figure 3 shows the proposed system architecture.

Traditionally, the RFID technology has been thought to be used in health care service delivery just for diagnosis of patients in emergency situations, measuring patient's vital signs, recording significant medical information and transferring to an electronic monitoring device, and monitoring the elderly. It has also been used in monitoring of goods and equipment, as well as controlling drugs administration and blood transfusions, thereby reducing medical errors in hospitals [9]. This study investigated the use of RFID in healthcare service delivery, especially in drug monitoring and management. The RFID technology is classified as a wireless automatic identification technology that uses electronic tags to store identification data and other specific information, and a reader to read and write the tags. The motivation for using the RFID technology in this research is the automatic identification and tracking capability of the objects with RFID tags which when utilizes can counteract unexplained drug loss and theft in the hospital environments.

VI. CONCLUSION

The application of RFID technology in the health industry can provide significant benefits in improving the pharmaceuticals supply chain management in hospital environments. This paper has presented a review on the actual situation of pharmacy management practices using the case of public hospitals in Tanzania. A review on the RFID technology has been presented where the feasibility of the technology in solving the identified challenges is done. It has been revealed that there is high potential and return on investment for applying the RFID technology in the health sector.

Lastly, we introduced and proposed the RFID technology and its application in pharmacy management systems, which can be adopted to mitigate problems faced by most public hospitals in Tanzania. The proposed system intends to be of low cost by utilizing passive Ultra High Frequency RFID tags to tag the monitored drugs, which will counteract drug diversion or loss in the government owned hospitals to the private sector and therefore ensure drug availability at the hospitals.

REFERENCES

- [1] M. Bouet and A. L. Dos Santos, "RFID tags: Positioning principles and localization techniques," in *Wireless Days, 2008. WD'08. 1st IFIP*, 2008, pp. 1–5.
- [2] A. Rida, L. Yang, and M. Tentzeris, *RFID-Enabled Sensor Design and applications*. LONDON: British Library, 2010.
- [3] L. Broadfield, S. Colella, H. T. Daft, D. D. Lester, and D. D. Swenson, "System and method for drug management." Google Patents, 2000.
- [4] Global-Fund, "Audit Report on Global Fund Grants to Tanzania," The Office of the Inspector General, 2009.
- [5] R. Bate, K. Hess, and L. Mooney, "Antimalarial medicine diversion: stock-outs and other public health problems," *Res. Reports Trop. Med.*, pp. 19–24, 2010.
- [6] R. Angeles, "RFID Technologies: Applications and Implementation Issues," *Inf. Syst. Manag. winter*, pp. 51–66, 2005.
- [7] A. Lozano-Nieto, *RFID Design fundamentals and applications*. London: CRC press, 2011.
- [8] C. Turcu, *DEPLOYING RFID – CHALLENGES , SOLUTIONS , Edited by Cristina Turcu .*
- [9] C. Turcu, T. Cerlinca, C. Turcu, M. Cerlinca, and R. Prodan, "An RFID and multi-agent based system for improving efficiency in patient identification and monitoring," *WSEAS Trans. Inf. Sci. Appl.*, vol. 6, no. 11, pp. 1792–1801, 2009.
- [10] Z. Hamid and R. Asher, "Counterfeit Drugs Prevention in Pharmaceutical Industry with RFID: A Framework Based On Literature Review," *Int. J. Medical, Heal. Biomed. Pharm. Eng.*, vol. 8, no. 4, pp. 198–206, 2014.
- [11] T. I. Cerlinca, C. Turcu, C. Turcu, and M. Cerlinca, "RFID-based Information System for Patients and Medical Staff Identification and Tracking," *Sustain. Radio Freq. Identif. Solut.*, no. February, 2010.
- [12] G. M. Gaukler, R. W. Seifert, and W. H. Hausman, "Item level RFID in the retail supply chain," *Prod. Oper. Manag.*, vol. 16, no. 1, pp. 65–76, 2007.
- [13] J. a. Fisher and T. Monahan, "Tracking the social dimensions of RFID systems in hospitals," *Int. J. Med. Inform.*, vol. 77, no. 3, pp. 176–183, 2008.
- [14] S. F. Tzeng, W. H. Chen, and F. Y. Pai, "Evaluating the business value of RFID: Evidence from five case studies," *Int. J. Prod. Econ.*, vol. 112, no. 2, pp. 601–613, 2008.
- [15] P. Kelle, J. Woosley, and H. Schneider, "Pharmaceutical supply chain specifics and inventory solutions for a hospital case," *Oper. Res. Heal. Care*, vol. 1, no. 2–3, pp. 54–63, 2012.
- [16] I. Bose, E. W. T. Ngai, T. S. H. Teo, and S. Spiekermann, "Managing RFID projects in organizations," *Eur. J. Inf. Syst.*, vol. 18, no. 6, pp. 534–540, 2009.
- [17] R. Koh, E. W. Schuster, I. Chackrabarti, and A. Bellman, "Securing the pharmaceutical supply chain," *White Pap. Auto-ID Labs, Massachusetts Inst. Technol.*, pp. 1–19, 2003.
- [18] E. Sultanow and C. Brockmann, "An Information Technology Model for Pharmaceutical Supply Chain Security," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 57, no. 2, pp. 1–13, 2013.
- [19] M. S. Matalka, J. K. Visich, and S. Li, *Reviewing the drivers and challenges in RFID implementation in the pharmaceutical supply chain*, vol. 7, no. 5, 2009.
- [20] J. Barrington, O. Wereko-Brobby, P. Ward, W. Mwafongo, and S. Kungulwe, "SMS for Life: a pilot project to improve anti-malarial

- drug supply management in rural Tanzania using standard technology," *Malar J.*, vol. 9, no. 298, pp. 1–9, 2010.
- [21] A. F. Merry, C. S. Webster, and D. J. Mathew, "A new, safety-oriented, integrated drug administration and automated anesthesia record system," *Anesth. Analg.*, vol. 93, no. 2, pp. 385–390, 2001.
- [22] G. A. Howard, F. Assadi, Y. Xin, N. Okasinski, T. Canup, S. Engebretsen, R. P. Silkaitis, G. N. Holland, P. B. Keely, and M. H. Awan, "System for maintaining drug information and communicating with medication delivery devices." Google Patents, 2013.
- [23] Z. Zhou, "RFID Usage for Monitoring Drug Dispensing in Hospitals," Auckland University of Technology, 2012.
- [24] A. Lozano-Nieto, *RFID design fundamentals and applications*. CRC press, 2011.

AUTHORS PROFILE

Prisila Ishabakaki is a Student pursuing masters in Information Communication Science and Engineering at Nelson Mandela African Institutions of Science and Technology. Undertaking masters

Shubi Kaijage, is a lecturer at is a lecture at Nelson Mandela African Institution of mScience and Technology school of Computational and Communication Sciences and Engineering (CoCSE).

Cloud-Aware Web Service Security

Information Hiding in Cloud Computing

Okal Christopher Otieno
Department of Information Technology
Mount Kenya University
Nairobi, Kenya

Abstract: This study concerns the security challenges that the people face in the usage and implementation of cloud computing. Despite its growth in the past few decades, this platform has experienced different challenges. They all arise from the concern of data safety that the nature of sharing in the cloud presents. This paper looks to identify the benefits of using a cloud computing platform and the issue of information security. The paper also reviews the concept of information hiding and its relevance to the cloud. This technique has two ways about it that impact how people use cloud computing in their organizations and even for personal implementations. First it presents the potential to circulate harmful information and files that can adversely affect the data those users upload on those platforms. It is also the basis of the strategies such as steganalysis and cryptographic storage architecture that are essential for data security.

1. INTRODUCTION

Cloud computing is still an evolving paradigm of information technology, but it has received much attention because of the capabilities it can assure the users [13]. In summary, this is a subscription-based service that allows people to use storage spaces on a network that enables them to keep and retrieve computing resources [10]. Primary examples of cloud computing technologies are emailing and social media platforms that allow a person to store different bits of information in a virtual internet space. The various enablers about cloud computing are, for example, access to one's information from anywhere in the world at any time just as long as they have an internet connection.

The scope of operation of a cloud computing services determines its type. Public Clouds are the most popular type that requires someone to use the internet to access a storage space [10]. These are the types that email users can access and also in other services that businesses have established online and any person can access their use. The private cloud consists of a small group of individuals who limit the access to space just to themselves [10]; it can involve a small organization that opens its storage for its workers only. The scope grows and develops to a community cloud that allows access between groups

of organizations. When users make a combination of any of the above types, it becomes a hybrid cloud.

There are different challenges that associate with the platforms of cloud computing. They are most common in the Internet-based service providers. These internet service models have the most widespread use of the cloud [13]. Due to the higher number of persons that use the internet as a virtual storage space, there are many different risks that come up. Most of them are about managing space while ensuring the safety and efficiency of every user's operations.

These challenges open up to the research that is the primary concern of this paper. Security is one of the major problems that cloud users face around the globe [16]. It is mainly the reason that most people fear using this platform despite the benefits it promises for different enterprises. Most would prefer to meet the high costs and develop their clouds instead of taking the advantages of the cheaper Internet-based infrastructure. The author will focus on the causes of insecurity in the web-based cloud computing services. It will then outline the practices that lead to a web-aware security strategy for the providers and users that can ensure they get the best experiences. This research will focus on information hiding as a safety issue for Internet-based cloud computing applications. The researcher will take a look at various techniques of hiding data such as steganography and cryptography and how they can be dangerous or significant. The significance of different methods of ensuring that clients can experience minimal damage from these techniques is also another important consideration.

2. LITERATURE REVIEW

2.1 Definition of Web-Based Cloud Computing

There is always a common misconception that cloud computing has its scope only on the internet. It is more of a network-based strategy that enables people to share computing resources and other information without the need of setting them up on their computers [4]. These settings allow the people to perform computations on this network using standard infrastructure like software and storage spaces that are not on their computers but rather in a central location for that connection.

Web-based cloud computing provides the capability to host files and resources on an internet platform and allows the users to implement all their activities online [20]. It allows people to access a pool of these resources that they can share their connections. There are various characteristics that define web-based cloud computing [6]; first is the access to the services on demand at anytime from anywhere in the world with just an internet connection. This ability equally allows people to load the information into the system independent of their location. The cloud also provides rapid elasticity from the natures of its systems to adapt and handle the shift in workloads and storage capacity requirements from the users [9]. Another feature of these services is their measurability; it provides an easy method to estimate the value that the implementation of this strategy brings to an organization [18].

2.2 Benefits of Cloud Computing

There are different benefits of implementing a cloud for an organization or even an individual. Lower costs of infrastructure and operation are among the advantage that one will witness through the use of this platform [15]. The group does not need to purchase very robust infrastructure and computers to provide the ability to handle their resources [15]. There is the need to purchase on the central network equipment that will host all the services and software the people will use with any form of computing device they launch into it. The systems that use Internet clouds need a connection and perform all their functions in the virtual spaces through the websites [3]. All this capabilities lower the costs of operation for that organization and are a big gain. They also extend their scope to reduce costs in software operation and maintenance costs as the providers of the services will handle them as part of their activities [15].

Another advantage comes to a reduction in the worry about the maintenance of infrastructure and other enablers of the group's operations [14]. There is the benefit of lower dependencies on the organizational hardware and actually, they even need much less that they would if the set up their facilities [15]. This requirement reduces the probability of too much maintenance requirements of the hardware and software in the organization.

There are always issues that organizations have to handle about software licensing and updates every time. The cloud reduces the need for such requirements in an organization and defines another benefit of its implementation [12]. The service providers have to ensure that all the resources in their scope receive regular updates by allowing the internet based operations to input these changes into the

system [15]. Therefore, the cloud serves the advantage that people will always use the latest version of the software if the implement the web-based services.

Using the cloud assures the clients that they have access to limitless capabilities in computing power and storage capacity [15]. The power of the entire cloud is at the disposal of the user as all they can share all the functions and abilities that all the other people on the platform can access. The need for larger storage capacities is always growing, and the providers are always expanding their facilities to accommodate the demands of their customers [15]. The segment of performance also mirrors this trend and, therefore, every user benefits from these capabilities as the access is standard to those who require high computing and storage capacities and those who do not. The clients can access much more capacities than they have on their smaller computers if they can access the cloud [15].

Data safety is another assurance that cloud computing provides to those who implement it in their operations [5]. There are different challenges that using personal computers can bring to the users. For example, there would be hardware breakdowns that endanger the data that people store in them [15]. Using the cloud eliminates these risks because the providers take care of the information in their system and can afford to conduct regular backups to secure it [5].

Compatibility is another advantage that cloud computing allows for its clients [15]. The issue of compatibility arises in the areas of operating systems, applications and document formats [15]. For example, there is no way on regular computing that an application for Windows operating systems can work in Mac personal computer. This issue does not exist in the cloud as the customers can use all the apps on any computer operating systems [15]. There is a duplication of this capability to all document formats that observe the OS boundaries and, therefore, it increases the amount of computing flexibility, unlike the other platforms. It also enables the universality of access to documents and applications which is another advantage that the users can get benefits [15].

2.3 Security as a Threat to Web-Based Cloud Computing

Despite the increase in popularity of cloud computing, there are different challenges in its way and one of them is data safety [25]. The use of the cloud involves complex structures of databases, networks, operating systems and the control of various other infrastructures that are mostly vulnerable [7]. The security of the information that clients put on the cloud and the different support

system that enable its operations has created a great hindrance to the progress of this avenue [22]. The virtualization paradigm opens the Cloud to various problems especially in the processes of mapping the virtual space to the physical machines on the user's end [21]. There are also other challenges such as inconsistencies that are prone to arise from the processes of resource allocation and management [1]. The process also extends to the division of roles and responsibilities between the people in the organization that can lead to the same challenges [24]. These strategies determine how different users access and utilize the amenities of that cloud system. Most users will avail very sensitive information on the cloud that raises their concerns for its safety in that environment [1]. These concerns are a significant cause for lower client turnouts on the internet platforms. Since their access is public it is equally more vulnerable [8]. Security is the biggest source of worry even for the providers as it relates directly to the way that customers choose their services against competing strategies.

2.4 Information Hiding in Cloud Computing

Different organizations have developed various methodologies that can help reduce the impacts of the security threats. Information hiding has grown its significance in the computing arena over the recent periods [19]. It is a traditional programming method that developers use to segregate the components of a program into smaller modules to protect the whole system from the operations of a single segment [17]. There are different applications of this technique in other areas of computing such as in communication. This method is both a challenge and a savior to the security problems that different people experience in the scope of cloud computing.

Among the methods of information, hiding is steganography. It involves the practice of hiding one file behind another one of a different format to conceal the former from any monitoring in the channel of transfer [23]. The aim of this strategy is to hide a message or other data behind another probably harmless event to conceal it from all other people except for the one the sender intends it for [23]. Malicious people can use steganographic techniques to implement attacks on different computing systems or to necessitate communications that have an ill intention [13]. The most popular file formats that people use to conceal other files are graphics such as pictures and videos [13].

Regarding the steganographic procedures that people employ on different communication platforms, there is the probability of use in the cloud computing platform. It also raises the concern on how threat this cunning techniques can cause on the users

of the cloud and by what scale of impact. There have been different applications of steganography in different areas to create and spread harmful files to computer systems. It has also been an efficient technique for tracking the use of copyright materials and their violations in different markets [13]. Therefore, it presents both a challenge and a way to handle some security issues in cloud computing.

The second technique for data hiding is cryptography that is a way of establishing secret codes of writing for communication between two parties to an agreement [13]. It differs from steganography in that, involves a secret for of writing whereas, steganography refers to the cover-up of different forms of information in other standard ones [13]. Therefore, one can make a cryptographic message and use the steganographic methodology to circulate it in the cloud and prevent third parties from accessing it. Cryptography also presents a dual face in the form of a problem and solution to the cloud infrastructure.

Steganography and Cryptography are the most popular forms that people sue to prevent third parties from accessing the information that their communication contains. These techniques can also be necessary for the service providers in securing the information that their clients load onto their systems in different manners of application. Most customers use these techniques to protect their data from malicious cloud users by hiding it in the storage facilities [11]. Although most people can point that this is dangerous, the providers have different ways of ensuring that their customers do not misuse this privilege to circulate damaging data in their systems.

2.5 Protection Procedures Using Information Hiding

Steganalysis is one of the techniques that providers use to detect if a file that a user uploads to the system has any form of hidden message within it [13]. This method does raise issues on the providers' commitment to the privacy and confidentiality of the customer and their information on the cloud [11]. But most providers implement strategies that do not violate this provisions. There are different regulatory policies that they use to develop these strategies and also ensure that the data stays in protection after analysis [11]. These techniques are in line with those of cryptographic storage services.

Steganalysis is the detection method that involves the system looking at files that have outlying characteristics such as vast sizes [2]. The primary reason for conducting this exercise is to identify the files that have steganographic codes within their structures and rendering them incapable of performing any unauthorized activity [2]. The process then proceeds to analyze the fingerprints of each file to determine the best way to handle it in the

system [23]. It is not easy to develop a service that is stringent enough to deal with the shifting patterns that the cloud experiences; therefore, there is always the possibility of a threat from this forms of information hiding.

Cryptographic storage services are another technique that cloud providers use to secure the information on the facilities [11]. This method involves regular checks on the information that the users send to the cloud storage to determine if any person has tampered with it. It has an architecture that enables the system to detect and record the nature of the data that each client uploads into the cloud [11]. This section allows the cloud providers' systems to analyze and determine if the files that the customer generates are safe and appropriate to the system. When the client accesses that data in the future, the system will provide an overview of any changes or access that other people made to it during its period of existence in their storage space [11]. The systems will notify the user of how the other people that they share resources with accessed their files and inform them to reverse any undesirable changes that they made for their backups. It also enables the providers to detect any malicious activities on their system by retrieving feedback from their customers.

There are different difficulties that providers and their systems encounter in outlining these methodologies. They depend on techniques that analyze outlying file attributes that may not be unique to those that users encrypt [2]. It also takes a greater challenge in assessing the records as some of them may have irrelevant data or noise in them [2]. It also takes further effort to enable that they can decrypt the file to retrieve the information in it. It is hard to establish as standard decoding strategy; therefore, each data presents a new challenge and an increase in the workload [2]. The current methods just provide a stream of suspect files without the information on what they contain.

3. CONCLUSION

The biggest threat to cloud computing that this paper identifies is security. Most organizations worry about the safety of the information that they send and share on the cloud, especially ones that are sensitive to certain operations. There are different benefits that people can get from implementing the cloud by the threat of their information is a shadow to all of them. This trend has motivated the development of various methods and practices that can ensure the minimal possibility of such breaches.

Information hiding is both a problem and solution to the security issues in cloud computing. People can use this technique to launch attacks on customer data, and this has enormous implications that hinder the popularity of the cloud. The methods

of steganalysis and cryptographic storage systems present solution to these problems as they are capable of detecting any files that contain hidden information. The only challenge remaining is to establish a universal algorithm that can detect and decrypt the information that the files contain.

REFERENCES:

- [1]. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud Computing and Security Issues in the Cloud." *International Journal of Network Security & Its Applications (IJNSA)* 6.1, 2014, 25-36.
- [2]. Al-Khanjari, Z., and A. Alani. "Developing Secured Interoperable Cloud Computing Services." *European Scientific Journal* 10.24, 2014.
- [3]. Apostu, Anca, et al. "Study on Advantages and Disadvantages of Cloud Computing—the Advantages of Telemetry Applications in the Cloud." In: *Recent Advances in Applied Computer Science and Digital Services*. New York: Wseas LLC, 2013, 118-123.
- [4]. Babitha, Pallaty, and Ravi Mathey. "Measurable, Safe and Secure Data Management for Sensitive Users in Cloud Computing." *International Journal of Research in Engineering and Technology*, 2014, 171-174.
- [5]. Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze. "Secure Cloud Computing: Benefits, Risks and Controls." *Information Security South Africa (ISSA)*, 2011. IEEE, 2011.
- [6]. Claycomb, William R. "Tutorial: Cloud Computing Security." Lead Research Scientist CERT Enterprise Threat and Vulnerability Management Team, 2007.
- [7]. Hamlen, Kevin, et al. "Security Issues for Cloud Computing." *Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies*, 2012, 150.
- [8]. Hashizume, Keiko, et al. "An Analysis of Security Issues for Cloud Computing." *Journal of Internet Services and Applications* 4.1, 2013, 1-13.
- [9]. Herbst, Nikolas Roman, Samuel Kounev, and Ralf Reussner. "Elasticity in Cloud Computing: What It Is, and What It Is Not." *ICAC*. 2013.
- [10]. Huth, Alexa, and James Cebula. "The basics of cloud computing." *United States Computer*, 2011.
- [11]. Kamara, Seny, and Kristin Lauter. "Cryptographic cloud storage." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2010. 136-149.
- [12]. Kondo, Derrick, et al. "Cost-Benefit Analysis of Cloud Computing Versus Desktop Grids." *Parallel & Distributed Processing*, 2009. IPDPS 2009. IEEE International Symposium on. IEEE, 2009.
- [13]. Mazurczyk, Wojciech, and Krzysztof Szczypiorski. "Is Cloud Computing Steganography-proof?." *Multimedia Information Networking and Security (MINES)*, 2011 Third International Conference on. IEEE, 2011.
- [14]. Merrill, Toby, and Thomas Kang. "Cloud Computing: Is Your Company Weighing Both Benefits & Risks?" *Ace Group*, 2014.
- [15]. Miller, Michael. *Cloud computing: Web-Based Applications That Change the Way You Work and Collaborate Online*. Que Publishing, 2008.
- [16]. Mosher, Richard. "Cloud Computing Risks." *ISSA Journal*, July Issue, 2011, 34-38.
- [17]. Ostermann, Klaus, et al. "Revisiting Information Hiding: Reflections on Classical and Nonclassical Modularity." *ECOOP 2011—Object-Oriented Programming*. Springer Berlin Heidelberg, 2011. 155-178.
- [18]. Papadopoulos, Alessandro Vittorio. "Design and Performance Guarantees in Cloud Computing: Challenges and

- Opportunities." 10th International Workshop on Feedback Computing, 2015.
- [19]. Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information Hiding - A Survey." *Proceedings of the IEEE* 87.7, 1999, 1062-1078.
- [20]. Rewatkar, Liladhar R., and U. L. Lanjewar. "Implementation of Cloud Computing on Web Application." *International Journal of Computer Applications* 2.8, 2010, 28-32.
- [21]. Sen, Jaydip. "Security and Privacy Issues in Cloud Computing." *Architectures and Protocols for Secure Information Technology Infrastructures*, 2013, 1-45.
- [22]. So, Kuyoro. "Cloud computing security issues and challenges." *International Journal of Computer Networks* 3.5, 2011.
- [23]. Thampi, Sabu M. "Information hiding techniques: A tutorial review." *ISTE-STTP on Network Security & Cryptography*, LBSCE, 2004.
- [24]. Wang, Cong, et al. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing." *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010.
- [25]. Zhang, Shuai, et al. "Cloud Computing Research and Development Trend." *Future Networks, 2010. ICFN'10. Second International Conference on*. IEEE, 2010.

Managing & Analyzing Large Volumes of Dynamic & Diverse Data

Okal Christopher Otieno
Department of Information Technology
Mount Kenya University
Nairobi, Kenya

Abstract: This study reviews the topic of big data management in the 21st-century. There are various developments that have facilitated the extensive use of that form of data in different organizations. The most prominent beneficiaries are internet businesses and big companies that used vast volumes of data even before the computational era. The research looks at the definitions of big data and the factors that influence its access and use for different persons around the globe. Most people consider the internet as the most significant source of this data and more specifically on cloud computing and social networking platforms. It requires sufficient and adequate management procedures to achieve the efficient use of the big data. The study revisits some of the conventional methods that companies use to attain this. There are different challenges such as cost and security that limit the use of big data. Despite these problems, there are various benefits that everyone can exploit by implementing it, and they are the focus for most enterprises.

1. INTRODUCTION

The growth of businesses around the globe has always motivated the owners and managers to try and ensure their enterprises keep up with the technological trends that are equally developing at a fast pace. This progress is especially important in the field of business analytics according to past research. These studies reveal that 97% of the companies whose revenues exceed \$100 million are embracing technology into their practices of analysis on their operations [3].

These developments have provided the background for using information technology (IT) in organizations around the world. Computational techniques are necessary for

every sector as they provide an avenue that quickens the operations as well as ensuring the efficiency and precision of the outcomes [10]. This action is equally significant in the management of data structures in the organizations and any other operations that involve the sourcing, analysis and use of information [14].

These changes in business trends open up to the topic of this research that is, the management and analysis of big data. These practices involve the management of the strategies that companies use to get the data from the fields and create databases where they can manage it [3]. They also define the methodologies that the companies will use to achieve the best outcomes from their data.

In this research paper, the investigation focuses on the definition of the contexts that describe big data systems. It will also outline the importance of these systems in business operations and indulge into their management. The aim is to determine the processes that define the management and analysis of large volumes of data that is diverse and dynamic in nature. The study will provide an overview of the challenges that businesses go through to attain the efficiency that is their target in using this type of structures.

2. LITERATURE REVIEW

2.1 What is Big Data?

Big Data refers to data sets of vast volumes that can provide for computational manipulations and analysis to reveal the trends and associations between various variables of organizational operations [22]. There is an association between these forms of data with the Internet and cloud computing platforms especially proposing it as a 21st-century technology. This relationship goes to these avenues providing the ground for the use and

growth of big data systems. It occurs through the online platforms and small internet startups that have practiced it in very extensive use [6]. This connection originates from the ability of a business to operate a standalone infrastructure that big data provides. Some examples of companies that use these types of information in their systems are internet search engines and social networking websites [19].

Big data is the information that organizations use to determine most aspects of consumer and stakeholder behavior [8]. The size that defines the context of big data keeps growing with the advances in the infrastructure and the technologies that people use to handle it [8]. In the past people used mainframe computers whose storage capacities limited their capabilities and, therefore, their definition for big data would be just a small fraction of the current systems. In some instances, startups and the Internet platforms can see this as an innovation but larger companies have been doing big data from their inception (Davenport & Dyché, 2013). These enterprises have been handling large volumes of information in traditional ways that technology has improved tremendously.

The management and analysis of big data rely on the IT infrastructure to exploit the information that unstructured data contains and it is the form that dominates the globe [23]. To counter on the recent definitions of big data, some point that there is no sense of the distinction between any other forms. On the description of its size, some argue that data will continue growing and, therefore, one cannot distinguish big data in terms of size [7]. Therefore, the exact limits of the size that defines the term 'Big Data' lack any clarity as the amounts will keep changing with the advancements in technology. According to some research, one considers any information as large if they cannot handle it using the tools and software that they count as of ordinary use [7]. The infrastructural inadequacy to handle this form of data arises from the complexity that it contains and requires better methodologies to handle the larger scales that it presents.

2.2 Big Data Mining

One of the primary attributes of big data is that its sources have independent events that

no one can monitor at any particular instances [24]. This nature presents different challenges that necessitate complicated methods of sourcing the information in the fields into the data sets. The name given to this exercise is data mining and in summary, it is the process of extracting pertinent information from those big datasets that are autonomous [7]. The sets consist of high levels of variability, velocity and gigantic volumes that are hard to predict due to the manner of growth they exhibit. The heterogeneous state of the variables is among the factors that increase this problem [17].

The growth of IT and the use of the internet have always had an excellent association with big data in the current society (Davenport & Dyché, 2013). This relationship has established cloud computing as one of the areas that organizations source their big data [12]. The development of the technologies in this sector has enabled people and organization to interconnect and share information on various platforms. Social media is among the top enablers of big data mining strategies for different groups especially information on human behavior [17]. Improvements in parallel programming are also an important development that facilitates various techniques of sourcing large data sets [18]. Some of the tools that are in common use for this purpose are software applications like Hadoop and MapReduce. They are in a position to handle the exponential growth of data in the globe [11].

2.3 Management and Analysis of Large Volumes of Data

There are different benefits that the access to big data has brought to various enterprises including the elimination of guesswork in decision-making [20]. The growth that data structures are growing around the world has enabled the possibility of accessing any information through different platforms. This expansion in the amounts of information people can access requires them to establish a system that allows proper monitoring and analyzing the data and this demand keeps growing [21]. Therefore, large-volume data management involves the processes of dealing with both structured and unstructured datasets. They include properly organizing, governing and administering vast volumes of such data sets

for efficient utilization [4]. Most enterprises use database management systems (DBMS) to outline this function in their operations [1].

2.3.1 Best Practices in Big Data Analysis and Management: It requires proper management techniques to ensure that an organization can benefit from its adoption of big data strategies, especially in the computing platforms. These practices concern all the aspects of an enterprise's operations revolving around their culture and implementation methodologies. They also ensure that the organization can cope with the different changes that the environment of activity can send its way from period to another.

Establishing governing standards for the usability of the big data infrastructure is one of the practices to ensure efficiency in the organization [16]. The managers should ensure that they establish stringent policies that can enable the people in the business to observe a particular order in using the databases. The business should have policies that govern the access that every level of employee in the organization has to the data sets. The scope of these guidelines should begin from the basic oversight exercises right up to the overall monitoring processes of information use [16]. The aim of outlining these policies is to ensure that the people in the organization are only able to make the changes that the managers authorize. Therefore, it lowers the probability that people can just tamper with the data as it is likely to increase the variability that makes it harder to analyze. It is also one of the ways that they can make sure their database is secure from manipulation. It is also important to establish the difference between these policies and those of other operations in the enterprise [22].

Planning for quality in a big data system is also another important practice in analyzing and managing large volumes of information [13]. The use of big data in an organization has the potential to mislead decision-makers. It results from the lack of adequate opportunities to perform quality checks and simultaneously ensuring real-time access to the events that are occurring in the relevant perspectives [13]. The best management practices should aim to optimize between the two areas. It takes precious time to check data for credibility and

reliability and this may hinder the operations of acquiring more from the field. It is wiser, therefore, for the enterprise to establish a link between the two activities. They should ensure that they perform tests and corrections on the data at the fastest possible rates of processing to enable them to continue with the activities of mining [13]. The organization requires the establishment of methods that can allow them to cleanse the information on the go, for example, using information filters and sorting techniques that work alongside data mining [13].

Agility to the changing trends in the data platforms is an important consideration in managing its larger volumes [13]. The changes are too rapid and require that the analysts be keen on the shifts; therefore, there is no sufficient time to build a long-lasting strategy to handle the information [13]. The users have to stay alert and focus on obtaining newer facts and analytical methods instead of focusing their energy on the current structures [22]. The implementation of management decisions should focus on the foreseeable future as the patterns are shifting rapidly and would be difficult to predict their long-term outcomes [13]. It also requires that the people in charge are ready for any disruptions that are likely from various sources in their environments. The interruptions may arise from a change in the technology that they use, a shift in the variables of focus, or even the evolution of programming methodologies that are available [13]. These events demand high levels of flexibility to accommodate the shifts that the personnel may experience in outlining their mandates of big data management.

Efficiency and reliability the storage capabilities an enterprise has at its dispensation is also a very significant consideration in managing large volumes of data [13]. This segment also goes hand-in-hand with the requirement of infrastructural flexibility. It is good to ensure that one has the best facilities that can handle the volume of information that they are likely to access and keep in their systems. The users must establish the use of flexible technologies in the form of hardware and software to manage their information, both in accessing and storing it [13]. In this aspect, the organization should ensure they are

operating in compliance with the legal frameworks of their territories. For example, they should have sufficient licensing for their activities and materials or opt for the open source equipment and software to reduce these costs. It is also important that they maintain a good schedule on backing up their data and archiving other valuable information in their operations [13]. Security is another concern that is pertinent to this practice, but the solution can be in ensuring proper policy implementation and constant monitoring of the activities.

Data modeling is another important aspect of big data management for different users [13]. It refers to the activities that are likely to influence the logical and physical characteristics of the information in the enterprise [13]. The best proposal on data modeling for large-volume operations is to divide it into dimensions and deal with it in those subdivisions. Matching the information to the real world situation can be a challenge if one does not consider proper models for their data. This process is also important in ensuring that the analysis procedures have a sufficient facilitation and that the results have a higher precision capacity [13]. The dimensioning strategy is also important in ensuring good governance of big data, especially in handling the policies of access to different segments of a database.

2.4 Challenges in Big Data Management

The first problem in the analysis and management of big data derives from the nature of the information it contains [9]. The datasets are in vast scales that include heterogeneous rules and patterns whose characteristics exhibit high variability [9]. These issues present a challenge right from the exercises of data mining up to its distribution and usage in the relevant areas. Sometimes it will require sophisticated algorithms and programming procedures to enable the organizations to use this form of data efficiently. The amount of variation in the source variables makes it difficult for managers and developers to make any predictions about the data they have due to its enormous scale as well [9]. The algorithms are especially important in establishing searches for particular information. If the procedures are not adequate in terms of speed and accuracy, they will slow

down the processes and reduce the precision of the data that the organization has [9]. Developing these methods for use in an organization is time-consuming and also very costly and in turn poses a constraint for implementation in smaller scales of business [9].

The amounts of variability pose another challenge of the increase of workload in the organization. The heterogeneity of the variables from the sources of big data implies that an organization cannot use a single database structure to monitor and analyze the activities [25]. Therefore, it has to administer more labor into creating a newer infrastructure to adjust to the changes in patterns of the raw data. This trend also calls for a change in analytical methods every time they experience a particular shift in the sources. These events will increase the amount of work that the workers have to handle and also its diversity. It then requires the enterprise to increase its investment into these processes, and that equally raises the cost of operation [5].

Security is another challenge that is very frequent in the arena of implementation and management of large volumes of data [2]. The information that most big data infrastructures contain is highly sensitive and can motivate cyber attacks from different people to gain access to it. Most of the information is very critical for organization processes such as marketing and finances that people can develop an interest in to complete malicious events [15]. The diversity of sources that companies get their data also brings the challenge of its legitimate use and the protection of privacy for its customers [15]. The access to an enterprise's information in such situation can cause havoc as it usually has the personal data about employees and customers. The process of protecting the databases from cyber attacks that can lead to dangerous manipulations comes with many implications. It leads to an increase in the managerial workload and costs of operation for the business in question.

Cost is another challenge that overlaps through all the above limitations to big data. The cost of implementing the infrastructure necessary to handle these operations is high. In each of the activities and the various challenges that come up, the organization will always need

to expend funds to deal with the problems. Though, the advances in technology and social applications of large data, there is a promise that all this will become affordable at a particular period [20]. In the meantime, such technologies as cloud computing can fill in the gap by lowering the infrastructural expenses that most organizations have to incur.

3. CONCLUSION

There are different benefits that people can get from implementing and using large volumes of data. It is beneficiary to both educational engagements and business decision-making for various environments of application around the globe. The only way to ensure that one exploits these benefits is if they practice the best methodologies for analysis and management of the information that is under their mandate. These actions are specifically significant for business operations as the data they have exhibits a lot about their target markets. It also has the potential of influencing consumer behavior and is wise if they can perform proper managerial techniques on it.

There are different challenges in the sourcing, implementation and usage of big data in the current environment. The largest problem is the cost of adoption for such data especially for people who have not established the cases for business use of the data. Other challenges are in the nature of the variables that the persons have to observe with the primary focus on the variability, velocity and volume of the information that is available. Rapid changes do not allow the users to establish a standard way of sourcing and measuring the information, and this is a big challenge especially on cost.

There is an advantage to the diversity of the sources of big data despite the challenges they pose. This diverse nature of the information can be a significant source of decision-making data in an organization primarily because it reveals the variations in consumer behavior. With proper analysis of the findings in the target markets, the enterprise can benefit from such information. There is the challenge of ensuring that one is up to date about the different events about their sources and the rapid shift in their nature. It brings the difficulty of predictions that long-term decision-makers requires. Therefore, it is through proper implementation of the best

management practices that an entity can benefit from such events to make decisions for the foreseeable future.

References

- [1]. Borkar, Vinayak, Michael J. Carey, and Chen Li. "Inside Big Data management: ogres, onions, or parfaits?." *Proceedings of the 15th International Conference on Extending Database Technology*. ACM, 2012.
- [2]. Cardenas, Alvaro A., Pratyusa K. Manadhata, and Sreeranga P. Rajan. "Big Data Analytics for Security." *IEEE Security & Privacy* 6, 2013, 74-76.
- [3]. Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." *MIS quarterly* 36.4, 2012, 1165-1188.
- [4]. Chen, Jinchuan, et al. "Big data challenge: a data management perspective." *Frontiers of Computer Science* 7.2, 2013, 157-164.
- [5]. Chen, Yanpei, Sara Alspaugh, and Randy Katz. "Interactive Analytical Processing in Big Data Systems: A Cross-Industry Study of Mapreduce Workloads." *Proceedings of the VLDB Endowment* 5.12, 2012, 1802-1813.
- [6]. Davenport, Thomas H., and Jill Dyché. "Big Data in Big Companies." May 2013.
- [7]. Fan, Wei, and Albert Bifet. "Mining Big Data: Current Status, and Forecast to the Future." *ACM SIGKDD Explorations Newsletter* 14.2, 2013, 1-5.
- [8]. Fisher, Danyel, et al. "Interactions with Big Data Analytics." *Interactions* 19.3, 2012, 50-59.
- [9]. Fujimaki, Ryohei, & Satoshi Morinaga. "The Most Advanced Data Mining of the Big Data Era." *NEC Technical Journal* 7.2, 2012, 91.
- [10]. Ivan, Ion, Cristian Ciurea, and Sorin Pavel. "Very Large Data Volumes Analysis of Collaborative Systems with Finite Number of States." *Journal of Applied Quantitative Methods* 5.1, 2010, 14-28.
- [11]. Jaseena, K. U., and Julie M. David. "Issues, Challenges, and Solutions: Big Data Mining." 2014, 132-140.

- [12]. Kepes, Ben. "How to Utilize Cloud Computing, Big Data and Crowdsourcing for an Agile Enterprise." *Gigaom Research*, 2014, 1-17.
- [13]. Kimball, Ralph. "Newly Emerging Best Practices for Big Data." *Kimball Group*, 2015, 1-13.
- [14]. Knobbe, Arno, et al. "InfraWatch: Data Management of Large Systems for Monitoring Infrastructural Performance." *Advances in Intelligent Data Analysis IX*. Springer Berlin Heidelberg, 2010. 91-102.
- [15]. Lafuente, Guillermo. "The Big Data Security Challenge." *Network Security* 2015.1 (2015): 12-14.
- [16]. LaValle, Steve, et al. "Big Data, Analytics and the Path From Insights to Value." *MIT SLOAN Management Review* 21, 2013.
- [17]. Lin, Jimmy, and Dmitriy Ryaboy. "Scaling big data mining infrastructure: the twitter experience." *ACM SIGKDD Explorations Newsletter* 14.2, 2013, 6-19.
- [18]. Moens, Sandy, Emin Aksehirli, and Bart Goethals. "Frequent itemset mining for big data." *Big Data, 2013 IEEE International Conference on*. IEEE, 2013.
- [19]. Pearson, Travis, and Rasmus Wegener. "Big Data: The Organizational Challenge." *Bain Co*, 2013.
- [20]. Purdue University. Challenges and Opportunities with Big Data. *Purdue University*, 2015, 1-17.
- [21]. Rabl, Tilmann, et al. "Solving Big Data Challenges for Enterprise Application Performance Management." *Proceedings of the VLDB Endowment* 5.12, 2012, 1724-1735.
- [22]. Russom, Philip. "Managing big data." *TDWI Research. TDWI Best Practices Report*, 2013.
- [23]. Shelley, Phil. "Big Data Spectrum." *Infosys*, 2012, 1-57.
- [24]. Wu, Xindong, et al. "Data mining with Big Data." *Knowledge and Data Engineering, IEEE Transactions on* 26.1, 2014, 97-107.
- [25]. Zhu, Yuqing, et al. "Bigop: Generating Comprehensive Big Data Workloads as a Benchmarking Framework." *Database Systems for Advanced Applications*. Springer International Publishing, 2014.

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 LENGILIZ, 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 Gnana 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. Wongyos 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, Soongsil 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. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktresh 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
Prof. Syed S. Rizvi, University of Bridgeport, USA
Dr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India
Dr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Dr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Dr. S. Mehta, Inha University, Korea
Dr. Dilip Kumar S.M, Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Dr. Saqib Saeed, University of Siegen, Germany
Dr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Dr. J. Komala Lakshmi, SNR Sons College, Computer Science, India
Dr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Dr. M. Azath, Anna University, India
Dr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Dr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr Suresh Jain, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Dr. Hanumanthappa. J. University of Mysore, India
Dr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Dr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Dr. Santosh K. Pandey, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation
Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India

Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar, Gujarat
Mr Jitendra Agrawal, : Rajiv Gandhi Proudhyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai
Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of
Technology, Durban, South Africa
Prof. Mydhili K Nair, Visweswaraiyah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies, Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India
Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh
City
Dr. Mary Lourde R., BITS-PILANI Dubai, UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan

Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, Taibah University, Madinah Munawwarah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institutiion of Engg. & Tech. CHD, India
Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand
Dr. P. Chakrabarti, Sir Padampat Singhanian University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India

Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS College of Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhanian University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan
Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F.Sagayaraj Francis, Pondicherry Engineering College, India
Dr. Ajay Goel, HIET , Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded , India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia
Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhanian University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh

Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India
Dr. V V S S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjana Reddy, P, KITS, Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A.Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordan
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen, Aberystwyth University, UK
Dr. Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praakash Singh, Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT)Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath, ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan
Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale, SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, Karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh
Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha, R&D Software Engineer, Gemalto, Singapore

Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India
Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya
Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India

Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman
Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt
Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CeINet security, India

Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dharendra Mishra, SVKM's NMIMS University, India
Prof. Shapoor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India
Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia
Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India

Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE, Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India
Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India

Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India
Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRT's College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Soner, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University, Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India
Mr. Masoud Rafighi, Islamic Azad University, Iran
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India

Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institute of Engineering and Technology for Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode
Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technology, India
Mr. Srikantha Kumar Mohapatra, NMIET, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elbouxhari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericsson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abdullallah Alsafi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan
Mr. R. Balu, Bharathiar University, Coimbatore, India
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India

Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhania University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abdullallah Alsafi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, N S S College, Pandalam, India
Assoc. Prof. K. Seshadri Sastry, EILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India

Assistant Prof. Sunish Kumar O S, Amalijothe College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India
Mr. Roohollah Etemadi, Islamic Azad University, Iran
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria
Mr. Sumit Goyal, National Dairy Research Institute, India
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur
Dr. S.K. Mahendran, Anna University, Chennai, India
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab
Dr. Ashu Gupta, Apeejay Institute of Management, India
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus
Mr. Maram Balajee, GMR Institute of Technology, India
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria
Mr. Jasvir Singh, University College Of Engg., India
Mr. Vivek Tiwari, MANIT, Bhopal, India
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India
Mr. Somdip Dey, St. Xavier's College, Kolkata, India
Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh
Mr. Sathyapraksh P., S.K.P Engineering College, India
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India
Mr. Md. Abdul Ahad, K L University, India
Mr. Vikas Bajpai, The LNM IIT, India
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai
Mr. A. Siles Balasingh, St. Joseph University in Tanzania, Tanzania
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India
Mr. Kumar Dayanand, Cambridge Institute of Technology, India
Dr. Syed Asif Ali, SMI University Karachi, Pakistan
Prof. Pallvi Pandit, Himachal Pradesh University, India
Mr. Ricardo Verschueren, University of Gloucestershire, UK
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India
Dr. S. Sumathi, Anna University, India

Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India
Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat
Mr. Sivakumar, Codework solutions, India
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA
Mr. Varadala Sridhar, Varadhman College Engineering College, Affiliated To JNTU, Hyderabad
Assist. Prof. Manoj Dhawan, SVITS, Indore
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India
Dr. S. Santhi, SCSVMV University, India
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh
Mr. Sandeep Reddivari, Mississippi State University, USA
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal
Dr. Hazra Imran, Athabasca University, Canada
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India
Ms. Jaspreet Kaur, Distance Education LPU, India
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India
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. Sathishkumar, 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. Sinthuja, 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, Interl 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. Poornima Girish Naik, Shahu 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
Assistant Prof. Sanjay Sharma, Roorkee Engineering & Management Institute Shamli (U.P), India
Assistant Prof. Panem Charan Arur, Priyadarshini Institute of Technology, India
Dr. Ashwak Mahmood muhsen alabaichi, Karbala University / College of Science, Iraq
Dr. Urmila Shrawankar, G H Raisonni College of Engineering, Nagpur (MS), India
Dr. Krishan Kumar Paliwal, Panipat Institute of Engineering & Technology, India
Dr. Mukesh Negi, Tech Mahindra, India
Dr. Anuj Kumar Singh, Amity University Gurgaon, India
Dr. Babar Shah, Gyeongsang National University, South Korea
Assistant Prof. Jayprakash Upadhyay, SRI-TECH Jabalpur, India
Assistant Prof. Varadala Sridhar, Vidya Jyothi Institute of Technology, India
Assistant Prof. Parameshachari B D, KSIT, Bangalore, India
Assistant Prof. Ankit Garg, Amity University, Haryana, India

Assistant Prof. Rajashe Karappa, SDM CET, Karnataka, India
Assistant Prof. Varun Jasuja, GNIT, India
Assistant Prof. Sonal Honale, Abha Gaikwad Patil College of Engineering Nagpur, India
Dr. Pooja Choudhary, CT Group of Institutions, NIT Jalandhar, India
Dr. Faouzi Hidoussi, UHL Batna, Algeria
Dr. Naseer Ali Husieen, Wasit University, Iraq
Assistant Prof. Vinod Kumar Shukla, Amity University, Dubai
Dr. Ahmed Farouk Metwaly, K L University
Mr. Mohammed Noaman Murad, Cihan University, Iraq
Dr. Suxing Liu, Arkansas State University, USA
Dr. M. Gomathi, Velalar College of Engineering and Technology, India
Assistant Prof. Sumardiono, College PGRI Blitar, Indonesia
Dr. Latika Kharb, Jagan Institute of Management Studies (JIMS), Delhi, India
Associate Prof. S. Raja, Pauls College of Engineering and Technology, Tamilnadu, India
Assistant Prof. Seyed Reza Pakize, Shahid Sani High School, Iran
Dr. Thiyagu Nagaraj, University-INOUE, India
Assistant Prof. Noreen Sarai, Harare Institute of Technology, Zimbabwe
Assistant Prof. Gajanand Sharma, Suresh Gyan Vihar University Jaipur, Rajasthan, India
Assistant Prof. Mapari Vikas Prakash, Siddhant COE, Sudumbare, Pune, India
Dr. Devesh Katiyar, Shri Ramswaroop Memorial University, India
Dr. Shenshen Liang, University of California, Santa Cruz, US
Assistant Prof. Mohammad Abu Omar, Limkokwing University of Creative Technology- Malaysia
Mr. Snehasis Banerjee, Tata Consultancy Services, India
Assistant Prof. Kibona Lusekelo, Ruaha Catholic University (RUCU), Tanzania
Assistant Prof. Adib Kabir Chowdhury, University College Technology Sarawak, Malaysia
Dr. Ying Yang, Computer Science Department, Yale University, USA
Dr. Vinay Shukla, Institute Of Technology & Management, India
Dr. Liviu Octavian Mafteiu-Scail, West University of Timisoara, Romania
Assistant Prof. Rana Khudhair Abbas Ahmed, Al-Rafidain University College, Iraq
Assistant Prof. Nitin A. Naik, S.R.T.M. University, India
Dr. Timothy Powers, University of Hertfordshire, UK
Dr. S. Prasath, Bharathiar University, Erode, India
Dr. Ritu Shrivastava, SIRTHS Bhopal, India
Prof. Rohit Shrivastava, Mittal Institute of Technology, Bhopal, India
Dr. Gianina Mihai, Dunarea de Jos" University of Galati, Romania
Assistant Prof. Ms. T. Kalai Selvi, Erode Sengunthar Engineering College, India
Assistant Prof. Ms. C. Kavitha, Erode Sengunthar Engineering College, India
Assistant Prof. K. Sinivasamoorthi, Erode Sengunthar Engineering College, India
Assistant Prof. Mallikarjun C Sarsamba Bheemna Khandre Institute Technology, Bhalki, India
Assistant Prof. Vishwanath Chikaraddi, Veermata Jijabai technological Institute (Central Technological Institute), India
Assistant Prof. Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, India

Assistant Prof. Mohammed Noaman Murad, Cihan University, Iraq
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Dr. Parul Verma, Amity University, India
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Assistant Prof. Madhavi Dhingra, Amity University, Madhya Pradesh, India
Assistant Prof.. G. Selvavinayagam, SNS College of Technology, Coimbatore, India
Assistant Prof. Madhavi Dhingra, Amity University, MP, India
Professor Kartheesan Log, Anna University, Chennai
Professor Vasudeva Acharya, Shri Madhwa vadiraja Institute of Technology, India
Dr. Asif Iqbal Hajamydeen, Management & Science University, Malaysia
Assistant Prof., Mahendra Singh Meena, Amity University Haryana
Assistant Professor Manjeet Kaur, Amity University Haryana
Dr. Mohamed Abd El-Basset Matwalli, Zagazig University, Egypt
Dr. Ramani Kannan, Universiti Teknologi PETRONAS, Malaysia
Assistant Prof. S. Jagadeesan Subramaniam, Anna University, India
Assistant Prof. Dharmendra Choudhary, Tripura University, India
Assistant Prof. Deepika Vodnala, SR Engineering College, India
Dr. Kai Cong, Intel Corporation & Computer Science Department, Portland State University, USA
Dr. Kailas R Patil, Vishwakarma Institute of Information Technology (VIIT), India
Dr. Omar A. Alzubi, Faculty of IT / Al-Balqa Applied University, Jordan
Assistant Prof. Kareemullah Shaik, Nimra Institute of Science and Technology, India
Assistant Prof. Chirag Modi, NIT Goa
Dr. R. Ramkumar, Nandha Arts And Science College, India
Dr. Priyadharshini Vydhialingam, Harathiar University, India
Dr. P. S. Jagadeesh Kumar, DBIT, Bangalore, Karnataka
Dr. Vikas Thada, AMITY University, Pachgaon
Dr. T. A. Ashok Kumar, Institute of Management, Christ University, Bangalore
Dr. Shaheera Rashwan, Informatics Research Institute
Dr. S. Preetha Gunasekar, Bharathiyar University, India
Asst Professor Sameer Dev Sharma, Uttaranchal University, Dehradun
Dr. S. Preetha Gunasekar, Bharathiyar University, India
Dr. Zhihan Lv, Chinese Academy of Science, China
Dr. Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, Amritsar
Dr. Umar Ruhi, University of Ottawa, Canada
Dr. Jasmin Cosic, University of Bihac, Bosnia and Herzegovina

CALL FOR PAPERS

International Journal of Computer Science and Information Security

IJCSIS 2015

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 2011 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

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity 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

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://sites.google.com/site/ijcsis/authors-notes> .



© IJCSIS PUBLICATION 2015

ISSN 1947 5500

<http://sites.google.com/site/ijcsis/>