IJCSIS Vol. 11 No. 8, August 2013
ISSN 1947-5500

International Journal of Computer Science & Information Security


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

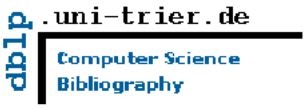

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


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 2013 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 Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.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, Cornell University Library, ScientificCommons, EBSCO, ProQuest and more.

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

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

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

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

Editorial
Message from Managing Editor

International Journal of Computer Science and Information Security *(IJCSIS – established since May 2009), is an English language periodical on research in information security which offers prompt publication of important technical work, whether theoretical, applicable, or related to implementation. As scholarly open access, peer reviewed international journal with a primary objective to provide the academic community and industry for the submission of original research related to Computer Science and Security. The goal is to bring together researchers and practitioners from academia and industry to focus on computer science issues and advancement in these areas. It also provides a place for high-caliber researchers, practitioners and PhD students to present ongoing research and development in computer science areas.*

Authors are solicited to contribute to this journal by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the Computer Science & Security. IJCSIS archives all publications in major academic/scientific databases; abstracting/indexing, editorial board and other important information are available online on homepage. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported a large amount of cited papers published in IJCSIS. IJCSIS supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

IJCSIS editorial board consisting of international experts solicits your contribution to the journal with your research papers, projects, surveying works and industrial experiences. IJCSIS appreciates all the insights and advice from authors and reviewers.

We look forward to your collaboration. 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. 11, No. 8, August 2013 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

size, without the appearance of any effect on the resulting image. The results shows no change in the image size after embedding the text, and any increase or decrease in the text size does not represent a major factor in hiding, but whenever the size of the image is greater, the hiding will be secure.

Keywords- Steganography; Canny Edge Detection, True Color Image.

4. Paper 31071313: Image Integrity based on HMAC Structure (pp. 19-24)

Shahd Abdul-Rhman Hasso
Department of Software Engineering, College of Computer Sciences and Math., University of Mosul, Mosul, Iraq

Abstract— With the increasing of the online applications and aggravation of dealing with official papers via the Internet that is send by images. It has become very necessary to add ways to make sure of the reliability of the transmitted image. The presented work is a design of algorithm for the integration and authentication of the image by adding it's hash message authentication code (HMAC) of the original image after encryption code using triple DES to it. The proposed algorithm depends on applying the HMACSHA-512 for finding the 512-bit HMAC code of an input (secured and must be integrated) image, then encrypt the resultant hash code by 3DES algorithm , forming it as an icon (small) image and send the resultant image icon attached. The receiver will receive the original and icon image, he wants to insure that the original is integrated and authenticated, Therefore , the HMAC-SHA-512 will applied on the original, decrypt the icon image to obtain the hash code, then matching codes to check the integrity and make sure of the reliability of the transmitted image. Results proved high precision and reliable images whatever the size of the image slight change the image pixel affect the output code which increases the reliability of the image.

Keywords- HMAC; 3DES; Image Authentication; Image Integrity.

5. Paper 31071321: Security Issues on Cloud Computing (pp. 25-34)

Harit Shah, Sharma Shankar Anandane, Shrikanth

Abstract - The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection sphere of the data owner. Most of the discussions on these topics are mainly driven by arguments related to organisational means. This paper focuses on various security issues arising from the usage of Cloud services and especially by the rapid development of Cloud computing arena. It also discusses basic security model followed by various High Level Security threats in the industry.

Keywords — Cloud Computing, Security, Threats

6. Paper 31071323: Extraction of Pupil Region from Iris Image Using a Scheme Based On Gamma Transform and Contrast Stretching (pp. 35-38)

Suhad A. Ali, Dept. of Computer Science, Babylon University, Babylon/ Iraq
Dr. Loay E. George, Dept. of Computer Science, Baghdad University, Baghdad/ Iraq

Abstract — Iris region extraction is almost the most challenging part in iris recognition system. The correctness of iris segment allocation is affected by the pupil localization accuracy. In this paper, a new method is developed for pupil region detection using a combination of gamma transform and contrast enhancement techniques. The proposed method is tested on 2639 iris images from CASIA v4.0 database (Interval class). The results prove the efficiency of the proposed method.

Keywords- Gammas transform, Iris segmentation, Seed filling, Enhancement techniques.

7. Paper 31071325: Quadrate Design of Linear System for Color Image Encryption (pp. 39-47)

Ashwaq T. Hashem, MSc., Computer Science Department, Babylon University, Hilla, Iraq
Loay E. George, Ph.D, Computer Science Department, Baghdad University, Baghdad, Iraq

Abstract — Nowadays the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. This paper attempts to design a simple and safer cryptographic algorithm. It is a new secret-key block cipher using type-3 Feistel network. The original image has been divided into 4×4 pixels blocks, which were rearranged into a permuted image using a linear system in quadrate design with mixing of operation from different algebraic group. The test results confirmed its security; which are shown in terms of statistical analysis using histograms, entropy and correlation. The test results showed that the correlation between image elements has been significantly decreased, and the entropy has been very close to the ideal value.

Keywords-: Image encryption, Linear system, quadrate design, type-3 Feistal network.

8. Paper 31071332: Coin based Untraceable Incentive Mechanism for Multi-hop Cellular Networks (pp. 48-52)

Vishnu Subramonian P, Department of Electronics and Communication Engg., Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India
Parameshachari B D, Department of Electronics and Communication Engg., Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India.
Rahul M Nair, Department of Electronics and Communication Engg., Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India.
H S DivakaraMurthy, Department of Electronics and Communication Engg., Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India.

Abstract — The multihop cellular network uses nodes to relay packets of data which helps in enhancing the network performance. Selfish node do not usually take part and this increases the load on cooperative nodes. This paper provides a fair charging policy which also includes hashing operations, public key cryptography, authentications to provide a secure and efficient communication.

Keywords- cryptography; fescim; hashing; selfish nodes; checks; networks;

9. Paper 31071335: Multidimensional Analysis applied to WSN Case study: routing Protocol (pp. 53-56)

Ziyati Elhoussaine, Rachid Haboub, Mohammed Ouzzif, and Khadija Bami
RITM laboratory, Computer science and Networks team, ENSEM - ESTC - UH2C, Casablanca, Morocco

Abstract — Mobile Ad-hoc Network is a kind of wireless adhoc network where nodes are connected wirelessly and the network is self configuring [1]. This paper shows the use of data warehouse as an alternative for managing data collected by Wireless Sensor Networks. In general Wireless Sensor Network is used to produce a large amount of data that need to be analyzed and normalized, so as to help researchers and other people interested in the information. These data managed and compared with information from other sources and systems could contribute in technical decision processes. This paper proposes a model to extract, transform and normalize data collected by Wireless Sensor Networks by implementing a multidimensional warehouse for comparing many aspects in WSN such as (routing protocol[4], sensor, sensor mobility, cluster ….). Hence, data warehouse applied to the context

above is detached as a useful alternative that helps specialists to obtain information for decision processes and navigate from one aspect to another.

Keywords- WSN, Data Warehouse, multidimentional design, OLAP, Routing Protocol

10. Paper 31071337: "People Are the Answer to Security": Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization (pp. 57-64)

Oyelami Julius Olusegun, Norafida Binti Ithnin
Department of Information systems, University Technology Malaysia, Faculty of Computing, Skudai, Johor Bahru 81310,

Abstract - Educating the users on the essential of information security is very vital and important to the mission of establishing a sustainable information security in any organization and institute. At the University Technology Malaysia (UTM), we have recognized the fact that, it is about time information security should no longer be a lacking factor in productivity, both information security and productivity must work together in closed proximity. We have recently implemented a broad campus information security awareness program to educate faculty member, staff, students and non-academic staff on this essential topic of information security. The program consists of training based on web, personal or individual training with a specific monthly topic, campus campaigns, guest speakers and direct presentations to specialized groups. The goal and the objective are to educate the users on the challenges that are specific to information security and to create total awareness that will change the perceptions of people thinking and ultimately their reactions when it comes to information security. In this paper, we explain how we created and implemented our information security awareness training (ISAT) program and discuss the impediment we encountered along the process. We explore different methods of deliveries such as target audiences, and probably the contents as we believe might be vital to a successful information security program. Finally, we discuss the importance and the flexibility of establishing a sustainable information security training program that could be adopted to meet current and future needs and demands while still relevant to our current users.

Keywords: Information Security, Awareness, End-User, Education and Training

11. Paper 31071338: Enhancing the Conventional Information Security Management Maturity Model (ISM3) in Resolving Human Factors in Organization Information Sharing (pp. 65-76)

Oyelami Julius Olusegun, Norafida Binti Ithnin
Department of Information systems, University Technology Malaysia, Faculty of Computing, Skudai, Johor Bahru 81310,

Abstract - Information sharing in organization has been considered as an important approach in increasing organizational efficiency, performance and decision making. With the present and advances in information and communication technology, sharing information and exchanging of data across organizations has become more feasible in organization. However, information sharing has been a complex task over the years and identifying factors that influence information sharing across organization has becomes crucial and critical. Researchers have taken several methods and approaches to resolve problems in information sharing at all levels without a lasting solution, as sharing is best understood as a practice that reflects behavior, social, economic, legal and technological influences. Due to the limitation of the conventional ISM3 standards to address culture, social, legislation and human behavior, the findings in this paper suggest that, a centralized information structure without human practice, distribution of information and coordination is not effective. This paper reviews the previous information sharing research, outlines the factors affecting information sharing and the different practices needed to improve the management of information security by recommending several combinations of information security and coordination mechanism for reducing uncertainty during sharing of information .This thesis proposes information security management protocol (ISMP) as an enhancement towards ISM3 to resolve the above problems. This protocol provides a means for practitioners to identify key factors involved in successful information sharing. The first one is the identification of all stakeholders to be incorporated into information flow. The second is the integration of the existing information sharing legal frameworks, information sharing protocols, information security

standards from the ISO/IEC 27001 and management standard ISO9001 with the existing information security management model (ISM3). An experiment was conducted to evaluate the performance of the proposed protocol. The results revealed that interoperability, culture and behavior towards information sharing improved by an average of 10 percent.

Keywords: Information Security Management, Information Sharing and Human Factors.

12. Paper 31071346: Robinson Edge Detector Based On FPGA (pp. 77-81)

Farah Saad Al-Mukhtar, M. Sc. Student in Computer Science Dept. / College of Computer Sciences and Mathematics / University of Mosul. Mosul, Iraq
Dr. Maha Abdul-Rahman Hasso, Computer Science Dept. / College of Computer Sciences and Mathematics / University of Mosul. Mosul, Iraq

Abstract — Edge detection is one of image enhancement techniques that are used to extract important features from the edges of an image (e.g., corners, lines, curves). The aim of image enhancement is to improve the interpretability of information in images for human viewers, or to provide "better" input for other automated image processing techniques. The proposed work presents Programmable Gate Array (FPGA) based architecture for Edge Detection using Robinson edge detection operator in respect of both time and space complexity. The algorithm are implemented using MATLAB 2010 language code as well as the VHDL language to deal with use of FPGA device, which was of a kind (Xilinx XC3S500E Spartan-3E), and it implemented on 8 bit grayscale image data, Robinson edge detection algorithm is produced using the pixel windows (3×3 windows) to calculate its output, make a comparison between the resultant image in MATLAB and VHDL by calculate the Peak Signal-to-Noise Ratio (PNSR), Root Mean Square error (RMSE) and the correlation between resultant images from MATLAB and VHDL.

Keywords - component; FPGA; Robinson Edge Detectot, VHDL, Windowing.

13. Paper 31071318: Profile Cloning in Online Social Networks (pp. 82-86)

Fatemeh Salehi Rizi, Department of Computer and IT, Sheikh Bahaei University of Isfahan, Isfahan, Iran
Mohammad Reza Khayyambashi, Department of Computer, Faculty of Engineering, University of Isfahan, Isfahan, Iran

Abstract — Today, Online Social Networks (OSNs) are becoming important due to the recent explosive growth in online interactions. They allow their users to express their personality and to meet people with similar interests. Meanwhile, there are also many potential privacy threats posed by these websites, such as identity theft and the revealing of personal information. However, many users have not yet been made aware of these threats, and the privacy setting that is provided by OSNs'service providers is not flexible enough to preserve users' data. Furthermore, users do not have control over what others share about them. One of the recently emerging attacks is the impersonation of a real user, instead of creating a fake account for a non-existing user, which is called Identity Theft Attack (ICA) or profile cloning. The purpose of cloned profiles is to try to steal real users' identities by making contact with their friends in order to financially abuse them or misuse their reputation. In this paper profile cloning attacks and some possible ways of detecting them are discussed. Then, based on the recent techniques and attack strategies further directions in research are proposed.

Keywords - Profile Cloning, Online Social Networks, Security

14. Paper 31071343: Software Cost Estimation using Fuzzy-swarm Intelligence (pp. 87-91)

Mustafa shakir mahmood Al-Sabaway, Software Engineering Dept., University of Mosul, Mosul, Iraq
Dr.Jamal Salahaldeen Majeed Al-Neamy, Assistant professor, Software Engineering Dept., University of Mosul, Mosul, Iraq

Abstract — Estimation is the most challenging and emerging field in software engineering development life cycle. Software cost estimation is a part of it. In this paper, Software cost estimation techniques were used to estimate cost of software development, the proposed system was built from four phases, Fuzzification, Fuzzy Inference, Parameter Tuning (using PSO) & Defuzzification, compute Cost.

Index Terms— Lines of Code, Fuzzy Logic System, Particle Swarm Optimization, Software cost Estimation.

15. Paper 31071312: An Operating System-based Model for Mobile Agent Deployment (pp. 92-96)

Oyatokun B.O. , Department of Mathematical Sciences, Redeemer's University, Mowe Ogun State, Nigeria
Osofisan A. O., Department of Computer Science, University of Ibadan, Ibadan, Nigeria
Aderounmu G.A, Obafemi Awolowo University, Ile-Ife, Osun State Nigeria

Abstract — Mobile agent technology has grown in acceptance over the years for distributed applications, but it is yet to be adopted as ubiquitous solution technique. This is due to its complexity and lack of interoperability. Mobile agent executes on mobile agent platform, these platforms from different vendors are design, and language specific, and are thus non interoperable. In other words mobile agent built on one platform cannot interact with or execute on any other platform. There is a need to provide a common base on which agents from different vendors can interact and interoperate. This work presents a framework for mobile agent interoperability by providing an Embedded Mobile Agent (EMA) system into the Windows Operating System kernel so that it can run as a service; this was done to eliminate the overheads associated with the agent platforms and enhance mobile agents' interoperability. The targeted OS were Windows XP, Windows Vista and Windows7.

Index Terms— embedded mobile agent, mobile agent platform, interoperability, operating system service.

16. Paper 31051333: Pre-SOA Models (pp. 97-100)

Safa Talal Hasan Al-Ramadani
Software engineering. Mosul University, Mosul University, Mosul, Iraq

Abstract — In this paper I propose a number of steps as a starting point to any SOA project. First we talk about SOA and its importance in nowadays, then listing other researches opinions in the first step to SOA. After that I'll lists my proposed practical approach to start the way toward any SOA system, and enforce that by a practical case study for a technical institution system.

Keywords-component; formatting; SOA : Service Oriented Architecture, Pre-SOA Model.

17. Paper 31071324: Performance Analysis of Call Admission Control Schemes in WCDMA Network (pp. 101-104)

Syed Foysol Islam, Faculty of Engineering, University of Development Alternative (UODA), Dhaka, Bangladesh
Mohammad Shahinur Islam, Faculty of Engineering, University of Development Alternative (UODA), Dhaka, Bangladesh

Abstract — The main objective of this research is to derive a numerical model of call admission control in WCDMA network and examines its performance. Three important call admission algorithms: wideband power based (WPB), throughput based (TB) and adaptive call admission control (ACAC) algorithms are investigated along with their performance analyzed throughout this paper and a little comparison between them is presented.

Key Words: Wide Band Code Division Multiple Access (WCDMA), Wideband power based (WPB), Throughput based (TB) and Adaptive call admission control (ACAC)

Optimizing Key Distribution in Peer to Peer Network Using B-Trees

Abdulrahman Aldhaheri
School of Engineering and Technology
Computer Science and Engineering
University of Bridgeport
Email: aaldhahe@my.bridgeport.edu

Hammoud Alshammari
School of Engineering and Technology
Computer Science and Engineering
University of Bridgeport
Email: halshamm@my.bridgeport.edu

Majid Alshammari
School of Engineering and Technology
Computer Science and Engineering
University of Bridgeport
Email: maalsham@my.bridgeport.edu

***Abstract*—Peer to peer network architecture introduces many desired features including self-scalability that led to achieving higher efficiency rate than the traditional server-client architecture. This was contributed to the highly distributed architecture of peer to peer network. Meanwhile, the lack of a centralized control unit in peer to peer network introduces some challenge. One of these challenges is key distribution and management in such an architecture. This research will explore the possibility of developing a novel scheme for distributing and managing keys in peer to peer network architecture efficiently.**

I. Introduction

Peer to peer network architecture allows peers to share available resources with each other in a decentralized way [1]. It's done efficiently using IP multicasting, which raises concerns about the security of system [2]. To provide security to the system, data transmitted has to be encrypted using a key that is known only to peers authorized to access the information. This motivated researchers to find the most efficient way to distribute those keys in order to improve the overall efficiency of the peer to peer system.

On the other hand, B-tree is a very fast and efficient data structure that is used to store and search large block of data is a logarithmic time. It achieves this by maintaing its balance, and avoiding have great hight. The worst case hight is:

$$h \quad \leq \quad \left\lfloor \log_d \quad (\frac{n \quad + \quad 1}{2}) \right\rfloor \qquad (1)$$

Where, h is the B-tree hight, d is the maximum number of children a node could have, and n is the number of nodes. This, in fact, provides a feature that could be of great benefit to peer to peer. Having a shallow and balanced tree hierarchy could improve the efficiency of the key management and distribution in peer to peer network.

Because of some characteristics i.e. the small average of failures and laking in central controlling, Peer to Peer (P2P) has been become most popular during these days. However, since there is no such a centralized system is implemented, some of security concerns have beed raised. Decentralized systems, like P2P, have no single server to control the system and play the main role in the whole system. So, by missing that, P2P became applications have beed changed from using simple data to more sensitive data to security threats [3].

Another important aspect is the duration of time that the peer should wait to get the data from the root [4]. In addition, for security purposes that time should not be long and the last nodes should get the session key as fast as the above nodes or so.

This paper proposes designing a B-tree based key distribution and management scheme for peer to peer networks. It will provide higher efficiency rate given the characteristics of B-tree data structure.

II. Related work

1) EKMD:

A research group, Liu, et. al. proposed a key distribution and management scheme in peer to peer live streaming network [5]. The major properties of given scheme are media-dependent and time-event-driven that the session keys are generated periodically and the re-keying messages are distributed with the media transmission track. The analysis and simulation results demonstrate its properties of security, scalability, reliability and efficiency. It achieves a high performance in security guarantee in p2p live media streaming applications, for which it is very suitable.

An interesting proposal that [5] had proposed an efficient media-dependent and time-event-driven key management and distribution scheme, named 'EKMD' for Peer-to-Peer (P2P) live streaming system. EKMD is Hierarchy Tree Scheme (HTS), centralized approach. It means the SK should be changed once a user joins or leaves the group. KDC only has to deliver a new SK securely to a small number of group users, which are its immediate neighbors. These neighbors forward the new SK securely to their own neighbor users.

The particular properties of the scheme include:

1) Media-Dependent: The key updating (re-keying) messages are embedded into the media content and then

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

delivered through the data transmission track in p2p streaming applications.
2) Time-Event-Driven: The session key updating process is carried out by the Key Distribution Center (KDC) periodically and irrespective of clients' join or leave behaviors.

One of the most important and challenging tasks in peer to peer network is maintaining consistent architecture as users join an leave the network:

- User Joins: When a user wants to join the p2p media streaming group, it should firstly contact the KDC to be authenticated. Then it can find its trust neighbors in the group, and get the future re-keying messages from them
- User Leaves When a user is going to leave the group, it should firstly notify all its neighbors. After that, the user contacts the KDC to logout.

Another research group has studied similarity formation of groups and key management in dynamic peer to peer e-commerce [6]. This research gave a clear outline of how peers form groups, select group leaders. Then, it addresses the key distribution among groups after selecting a leader for each group. This research also addresses how to establish trusts in peer to peer network.

[7] has presented a simple key distribution protocol, called VTKD (virtual token based key distribution) which was especially designed for collaborative applications to support closed, small dynamic peer group meetings. VTKD is a decentralized group key distribution protocol that is based on the Diffie-Hellman (DH) key exchange principle. There is no central group key authority. In contrast to the key exchange between two partners, in the distributed approach each group member calculates a secrete key with each partner using the Diffie-Hellmann principle. VTKD is a token based protocol. The group key is renewed whenever the group composition changes (join, leave, and failure of peers)

Another important issue we had to review the literature for is the performance of the join operation. The efficiency of the join operation can be measured by the join latency, which is defined by the time difference between the joining peer sending the join request to the server and the joining peer being inserted into the system. To give a quantitative analysis on the join latency, [8] use the number of hops the join request passes to estimate the join latency.

In general, there are two types of peer-to-peer network topologies; structured, and unstructured. [8] proposed a new approach to get a hybrid topology. The objective of this work is to design a hybrid peer-to-peer system for distributed data sharing which combines the advantages of both types of peer-to-peer networks and minimizes their disadvantages. In their article, [8] discusses two main things:

1) Leaving and joining the nodes, which we are interesting in.
2) Distributed and sharing data.

The authors separate the nodes into two main categories which are core and not core. The top nodes are connected in structured ring network. The bottom nodes are connected in nun-structured scheme. The core transit network, called t-network, is a structured peer-to-peer network which organizes peers into a ring similar to a chord ring. The basic idea behind the hybrid peer-to-peer system proposed by [8] is that the t-network is used to provide efficient and accurate service while the s-network is used to provide approximate best-effort service to accommodate flexibility.

In their research, [9] describe a height balanced tree structure which is Dissemination R-Tree. Each leaf node in the tree is an array of pointers to spatial objects. The joining and leaving nodes relays on some algorithms that's make the tree balanced. The hierarchy is getting changed by apply some strategies like correction of the cover, correction of the level and correction of the tree balance.

The research [9] also describe a height balanced tree structure which is Dissemination R-Tree. Each of the node can be the first node, so it can dynamically select the first node to eliminate the case of the first node's failure in a binary tree. We would like to highlight the following points in [9] proposal:

- DR-trees generalize P-trees which are the dynamic version of B+ trees.
- One of the future works that the authors were mentioned about is the time of node of the online: Loading capacity of nodes are influenced by online time. The model in order to consider it convenient setting the time-line of each node is a constant value.

Using balanced trees to optimize peer-to-peer network has a lot of benefits. A research group proposed a scheme called Skip B-Tree that implement a new algorithm to optimize the load balancing of the files among peers [1]. This research proposes a new implementation for a novel data structure called skip b-tree, which is a combination of skip graph and b-tree. The research propose implementing the skip b-tree data structure in peer-to-peer network. The proposed solution would increase the speed and the efficiency of the network.

The research proposed by [1] suggest implementing the skip b-tree in allocating resources to peers. However, it doesn't propose implementing the proposed data structure in distributing keys among peers.

According to [10] , the core design of B-trees has remained unchanged in 40 years: balanced trees, pages or other units of I/O as nodes, efficient root-to-leaf search, splitting and merging nodes, etc. On the other hand, an enormous amount

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

of research and development has improved every aspect of B- trees including data contents such as multi-dimensional data, access algorithms such as multi-dimensional queries, data organization within each node such as compression and cache optimization, concurrency control such as separation of latching and locking, recovery such as multi-level recovery, etc.

As suggested by [11], [10], [12], [1], [13], [14] The idea of optimizing the original design of B-tree for a specific purpose is not only a valid approach, but also an encouraged one. This actually support our approach in customizing the original B-tree data structure to make it suitable for distributing keys in peer-to-peer network architecture.

III. JOINING AND LEAVING NODES IN B-TREE

Joining and leaving peers in P2P usually happens by following some steps which have been explained in Kwon2007[15]. These steps illustrated there is no specific rules that control the joining node to determine the parent node based on balancing interesting. Consequently, the main goal of our scope is not presented her which is delivering the session key to the all nodes at the same time or so.

A. JOINING THE NETWORK

In B-tree architecture, joining nodes happens during two main steps which are searching about the value and split the child [11]. Although, these steps need more work to come up with a balanced B-tree, this additional work still important in terms of security. When node joins, it has to have the permission of joining a group and it has to go in place where keeps the tree balanced either it is leaf or not. Splitting the child means more expanded vertically which gives less number of raws which means that root node will be close to that nodes.

B. LEAVING THE NETWORK

Since there is different ways to implement B-tree, joining and leaving nodes goes through some steps in different strategies. One of these strategies is illustrated in Chang2009A [16] which implies that this node has to go in revers steps on joining nodes. Leaf node doesn't have to be prepared to any situation whereas the upper level nodes have to be prepared to rebuild the tree again.

IV. PROBLEM STATEMENT

Peer to peer network architecture increases networks efficiency and minimizes bandwidth consumption because it offers a highly decentralized architecture. This high level of decentralization in peer to peer networks increased its complexity and imposed security threats on peer to peer network architecture. Data encrypting techniques are implemented to provide security by increasing confidentiality, thus, eliminating the security threats. Encryption and decryption algorithms require having secret key shared between the sender and the receiver. Yet, those keys have to be send encrypted. These tasks are managed by a key distribution. The complexity of the scheme the key distribution center apply affect the efficiency of the peer to peer network significantly. Which would in turn affect the over all performance of the network by consuming more bandwidth.

We hypothesize that a B-tree based key distribution scheme can provide better performance in key distribution, which in turn, can lead to more efficient network services. We propose a B-tree based key distribution scheme. We intend to design and implement a key distribution and management scheme for peer to peer network based on B-Trees data structure. We will propose a novel version of B-tree algorithm that is customized to provide faster access time in peer to peer network architecture. We will perform experiments on the proposed scheme by simulating traffic in a control environment.

V. EXPECTED OUTCOMES

We are expecting by the end of this project to design and develop a novel key disruption and management scheme that would increase the efficiency of peer to peer network

The proposed scheme is also expected to implement a key distribution distribution algorithm, which will be developed using the blueprint of B-tree data structure.

The key distribution algorithm is expected to maintain the basic characteristics and functionalities of the B-tree data structure. However, it will be modified and customized to better serve it's purpose within the scope of this research.

The newly developed key distribution and management scheme will, then, be evaluated either by stress-testing it using a simulation program, or by developing the scheme program. The approach we are going to follow actually depends on the anticipated proposed scheme and it's complexity.

The newly developed key distribution scheme is expected to provide faster search, insert, delete, and update operations because it's going to capitalize on B- tree algorithm, which has already been established and proven to be one of the best in term of performance.

VI. APPLYING B-TREE CONCEPTS TO OPTIMIZE PEER TO PEER NETWORK

B-Tree supports any P2P network to be balanced which makes the key distribution process more complex. However, it affords a fully guarantee to deliver the session key to all nodes at very short time comparing with the distribution key through unbalanced tree. In this project, we went through

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

some assumptions to make the simulation goes perfectly. In following sections we will see some of these concepts or assumptions by some kind of details.

A. RANKING NODES AND LOOKUP TABLE

The first concept that we want to discuses is the value that the B-Tree will sort the nodes based on. The key value of our idea is calculation the nodes values based on the whole time that the node is being online in the P2P network. Based on this time, we give the nodes a sorting value which we named is as "Rank Value". The rank value is used as input value to the system and used by sorting algorithm to sort the B-Tree. Each node has to have a unique rank value, so we store the rank values in lookup table that the system uses to read them from.

One more important thing is, the online time is a cumulative value which means in case of leaving any node that time will be saved in the lookup table which will be stored in a server as database, we will discuss the idea of having this kind of server in section IV-C, and when the node joins the network the online time will be added to the old one. By doing that, we give the most trust ranking to the node who has the most online time value and so on.

B. JOINING/LEAVING NODES

The operation of joining/leaving nodes has been discussed in section III. In addition, there are two differences points that we would mention about:

1) REBALANCING THE TREE: There are two situations that any node could be in the P2P tree:

First situation, the node might be a leaf for a parent that has two leaves in the tree. So, with this case the system doesn't have to rebalance the tree because the leaf nodes don't make any changes on the distribution. However, if the parent only has one leaf, the tree needs to rebalanced again.

Second situation, the node might be a parent which means has children, so in this case when this node joins/leaves the tree, the system must rebalance the tree again.

2) REKEYING: In our system, the KDC generates the session key every time the system needs it in any situation. For security purposes, the system must regenerate the session key and distribute it between nodes. So, the process time of informing the root node about the joining/leaving any node will take the same time of delivering the session key to the level of this node.

C. CONTROLLING SERVER

The idea of having controlling server is that the KDC will not be connected directly with the root node because the system might have a different roots at any duration of time. So, we need a server that control this process which is request the rekeying from KDC and does the process of distributing and rebalancing the P2P tree. Also, this server works partly as a database to store an updated copy from the lookup table of the nodes.

VII. OUR SIMULATION

The main scope of our project is balancing the tree based on the online time of each node. Although we calculated the ranking value based on the B-Tree algorithm, we changed the values of nodes to give the concept of having parents that have more value than the children whereas the original B-Tree concept is that the highest value be the right child and lowest value be the left child.

In this section we will discuss the way that we have implemented our simulation by. The following sections discuss our work:

1) LOOKUP TABLE: We built the lookup table and give the simulator the ability to enter the number of nodes that the tree might have.This table has different values for each node as following:

- Online time: is generated randomly.
- User ID: based on number of nodes.
- Ranking value: we calculate it by giving the middle value for the node who has the highest online time.

2) Calculating the levels of the tree: by using the following equation, we calculated the levels of the tree:

$$O(log_d \quad n \quad) \tag{2}$$

Where:

- n: is the number of nodes.
- d: is number of children for the parent.

3) Implementation: by selecting the values of (n= 333, d=2) we got the following chart:

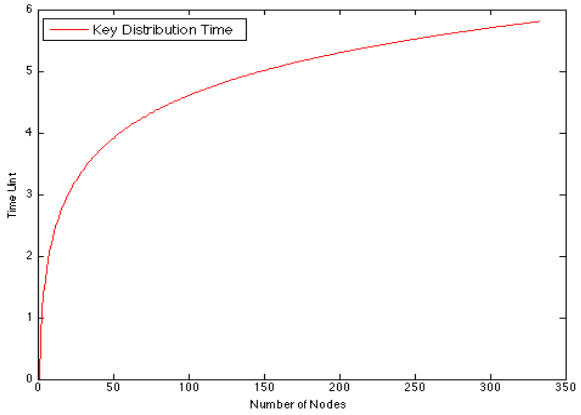


Figure 1. Number of nodes that every level could cover.

This chart illustrates the number of nodes for every unit time. Unit of time reflects the level number of the tree. By

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

reading the chart we find, in level one (time one) only the two children could be covered and get the session key. In time four, there will be around 50 nodes or so could be covered and get the session key. So, for all nodes we need only six time units to cover all 333 nodes.

VIII. RESULTS AND PERFORMANCE

From applying the different numbers of nodes, we got different results that reflected the high performance of having B-Tree to distribute the session key in P2P network. In any unbalanced P2P network some nodes like leaves nodes could get the session key after log time because this node location might be in the based of the tree or so.

The results give indications for the performance that we measured by doing the following. We calculated the performance of B-Tree which is calculated by equation number (2). Also, we added the performance of generating the session key by KDC and deliver it to the controlling server.

There two values are represented by a time unit and give the whole performance of the system which is optimizing key distribution in P2P network using B-Tree.

We have developed our simulation using Java programming language. As a result of that, we had to compromise having a high performance b-tree and settle with a data structure that applies the logic of b-tree on a list object. This because of the lack of pointers and memory address manipulation in Java. This, in fact, added some overhead to the proposed scheme. Such an overhead was successfully avoided in [9] by using an array of pointer to simulate their proposed distributed balanced tree, which is used to construct a peer-to-peer network optimized for selective dissemination of information.

Another issue this simulation has raised is the effort the b-tree based proposed solution would take to rebalance itself. This task would exhaust the system available resources more with higher number of nodes. To mitigate this issue, we can configure and tune the system to maintain reasonable balance rate that doesn't affect the overall performance. This implies that the tree structure in the proposed scheme wouldn't be completely balance all the time. However, this shouldn't reach an unacceptable rate.

IX. CONCLUSION

Peer-to-Peer networks need to be more secure because of absence of centralization of controlling the communication between peers. This weakness caused by different effects, one of these is the time of delivering the session key to all nodes in a very close time to avoid the chance of having the opponent eavesdropping to the communication.

This work concludes the high performance of using B-Tree to distribute the session key in Peer to Peer network by distributing the session key as less time as we can. For 333 nodes, we only need about 6 units time to deliver the key to all nodes. That makes the P2P more powerful and secure.

The security service that we offer to the network is confidentiality by allowing all nodes using the session key in a time where the opponent can't get it because of the very short distributing time. Also, by making the nodes get the same session key before joining/leaving more than one node, which means make all nodes using the same session key for the same session and keep the communication to be synchronous.

ACKNOWLEDGMENT

The authors would like to thank Professor. Wu, for his guidance throughout this research project. His constant remarks and constructive feedback were always valuable input for this works.

REFERENCES

[1] I. Abraham, J. Aspnes, and J. Yuan, "Skip b-trees," in *Principles of Distributed Systems; 9th International Conference, OPODIS 2005; Pisa, Italy; December 2005; Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 3974, Dec. 2005, pp. 366–380.

[2] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys (CSUR)*, vol. 35, no. 3, pp. 309–329, 2003.

[3] J. Arnedo-Moreno, K. Matsuo, L. Barolli, and F. Xhafa, "Secure communication setup for a p2p-based jxta-overlay platform," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 6, pp. 2086 –2096, june 2011.

[4] A. Ismail, M. Quafafou, G. Nachouki, and M. Hajjar, "A decision tree for queries routing in hierarchical peer-to-peer network," in *Informatics and Systems (INFOS), 2010 The 7th International Conference on*, march 2010, pp. 1 –8.

[5] X. Liu, H. Yin, C. Lin, and Y. Deng, "Efficient key management and distribution for peer-to-peer live streaming system," in *Intelligent Signal Processing and Communication Systems, 2007. ISPACS 2007. International Symposium on*, 28 2007-dec. 1 2007, pp. 638 –641.

[6] F. Musau and M. Abdullahi, "Similarity formation of groups and key management in dynamic peer to peer e-commerce," in *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, dec. 2010, pp. 1 –4.

[7] F. Liu and H. Koenig, "Secure and efficient key distribution for collaborative applications," in *Collaborative Computing: Networking, Applications and Worksharing, 2005 International Conference on*. IEEE, 2005, pp. 11–pp.

[8] M. Yang and Y. Yang, "An efficient hybrid peer-to-peer system for distributed data sharing," *Computers, IEEE Transactions on*, vol. 59, no. 9, pp. 1158 –1171, sept. 2010.

[9] S. Bianchi, P. Felber, and M. Gradinariu Potop-Butucaru, "Stabilizing distributed r-trees for peer-to-peer content routing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 21, no. 8, pp. 1175 –1187, aug. 2010.

[10] G. Graefe and H. Kuno, "Modern b-tree techniques," in *Data Engineering (ICDE), 2011 IEEE 27th International Conference on*, april 2011, pp. 1370 –1373.

[11] R. Beg, Q. Abbas, and R. Verma, "An approach for requirement prioritization using b-tree," in *Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on*, july 2008, pp. 1216 –1221.

[12] M. Beg, R. Verma, and A. Joshi, "Reduction in number of comparisons for requirement prioritization using b-tree," in *Advance Computing Conference, 2009. IACC 2009. IEEE International*, march 2009, pp. 340 –344.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[13] H. Pang, K.-L. Tan, and X. Zhou, "Steganographic schemes for file system and b-tree," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 16, no. 6, pp. 701 – 713, june 2004.
[14] R. Bayer, "Symmetric binary b-trees: Data structure and maintenance algorithms," *Acta informatica*, vol. 1, no. 4, pp. 290–306, 1972.
[15] H. Kwon, S. Kim, J. Nah, and J. Jang, "Public key management framework for two-tier super peer architecture," in *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*, june 2007, p. 72.
[16] Y.-K. Chang and Y.-C. Lin, "A fast and memory efficient dynamic ip lookup algorithm based on b-tree," in *Advanced Information Networking and Applications, 2009. AINA '09. International Conference on*, may 2009, pp. 278 –284.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A Distributed Deadlock-Free Quorum-Based Algorithm for Mutual Exclusion

Mohamed NAIMI
Department of Computer Science
University of Cergy Pontoise
33, Boulevard du port
95000 Cergy-Pontoise, France

Ousmane THIARE
Department of Computer Science
UFR S.A.T
University Gaston Berger
BP. 234 Saint-Louis, Senegal

Abstract— **Quorum-based mutual exclusion algorithms enjoy many advantages such as low message complexity and high failure resiliency. The use of quorums is a well-known approach to achieving mutual exclusion in distributed environments. Several distributed based quorum mutual exclusion was presented. The number of messages required by these algorithms require between $3\sqrt{n}$ and $5\sqrt{n}$, where n is the size of under- lying distributed system, and the deadlock can occur between requesting processes. In this paper, we present a quorum-based distributed mutual exclusion algorithm, free deadlock. Every group is organized as a logical ring of $\sqrt{n}$ processes. A requesting process sends its request to its successor on the logical ring. When a process receives its own request after one round, it enters in the critical section. The algorithm requires $2\sqrt{n}$-1 messages.**

Keywords-component; Distributed Mutual Exclusion, Quroum, Logical ring, free deadlock;

I. INTRODUCTION

Distributed system is a set of processes (computers) connected by communications links. To achieve collaborative tasks by a set of processes, many distributed algorithms have been proposed. The problem of mutual exclusion is one of fundamental problem in distributed systems, which is required to, for example, update of shared object consistently. By distributed mutual exclusion, it is guaranteed that the number of processes which updates the object is at most one at any time.

In distributed systems, different processes are running on different nodes of the network and they often need to access shared data and resource, or need to execute some common events. Their uses should be consistent and so any access to them should be mutually exclusive. The portion of an event or application, where any shared components or common events are needed to be used, is the Critical Section (CS). Mutual Exclusion (ME) algorithms ensure the consistent execution of CS. As the shared memory is absent in distributed systems the solutions of the ME problem is not straight forward. Due to the enormous importance of ME and the difficulty of its solution, this is an extensive research area since last three decades. The classic algorithms for mutual exclusion that have been proposed for fixed networks can be classified in two types: centralized and distributed approaches. In the centralized solutions, a node is designated as coordinator to deliver permission to the other nodes to access their critical section while in the distributed solutions, the permission is obtained from consensus among all network nodes.

On the distributed systems, distributed mutual exclusion algorithms are mainly classified in two categories: token based [1][2][11] and permission based [3][4][5][6][9]. Permission based mutual exclusion algorithms impose that a requesting node is required to receive permissions from other nodes (a set of nodes or all other nodes). In token-based mutual exclusion algorithms, a unique token is shared among the set of nodes. The node holding the token is allowed to enter its critical section. The basic idea of token-based algorithms is simple: a node must own the unique token (sometimes cited as privilege messages) before entering the CS. So, in the best case, no communication is necessary since the token may be available locally. Otherwise, a mechanism is needed to locate the token. In [2], a spanning tree of network for locating the token is used and it shows that the average number of messages exchanged in this protocol is *O(log n)*. But token-based algorithms suffer from poor failure resiliency. In particular, if the node holding the token fails, complex token regeneration protocols must be executed.

II. RELATED WORK

Ricart and Agrawala proposed the fair algorithm [3] that need 2(n-1) messages for a node to use the critical section. This algorithm is the first permission-based ME algorithm where a node need to collect permission from all other node for CS access. Though the algorithm is deadlock and starvation free, it is vulnerable to node and communication

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

failure and it is expensive in communication cost too.

There is elegant class of permission-based algorithms [6] that use concept of quorums to achieve mutually exclusive access of CS. A node needs to achieve permissions from all the nodes of a quorum to access CS. Quorum based algorithms are resilient to node and communication failures and often network partitioning and usually have lower communication cost. Communication cost of these algorithms is proportional to the quorum size. Therefore these algorithms try to achieve the two goals: small quorum size with high degree of fault tolerance. Its basic idea is to collect enough permission (votes) to guarantee the mutual exclusion. The majority quorum algorithm [8] can be considered as the first algorithm of this kind, where to attain mutual exclusion, a node must obtain permission from a majority of nodes in the network. Maekawa [4], proposed an ME algorithm by imposing a logical structure on the network. In this scheme, a set of nodes is associated with each node, and this set has a nonempty intersection with all other sets corresponding to the other nodes, which guarantee the ME. The size of each of these sets is n and so the algorithm cost n order.

Garcia-Molina and Barbara [8] have properly defined the concept of quorums with the notion of coterie. A coterie is a set of sets with the property that any two members of a coterie have a nonempty intersection and the minimality property. Combining the idea of logical structures and the notion of coteries, an efficient and fault tolerant quorum generation algorithm for ME is proposed by Agrawal and Abbadi [5]. Here, the nodes form a logical binary tree which is used to generate quorums. The quorum forming in this algorithm is recursive. It can be regarded as attempting to obtain permissions from nodes along a root-to-leaf path. If the root fails, then the obtaining permissions should follow two paths: one root-to-leaf path on the left subtree and one root-to-leaf path on the right subtree. The algorithm tolerates both node failures and network partitions while in the best case incurring logarithmic costs considering the size of the network. But the cost increases with the increase of node failures.

A. The distributed computational model

A distributed system consists of n sites (1,2,3,…i,…,n). A distributed system is *asynchronous*, i.e., there is no common global clock. Information exchanged between processes is done by asynchronous message passing. Each communication channel is FIFO and each message sent is delivered within finite time, but there is no upper bound on message delivery time. In this section, we present the computational model for the proposed algorithm and a review of Maekawa's algorithm.

1) Maekawa's algorithm: In Maekawa's algorithm, a site does not request permission from all the sites, but only from a subset of sites. The sites of the system is divided into groups called quorums (S_i, $1 \le i \le n$). The quorums are constructed such as to satisfy the following conditions :

1. $\forall i \forall j,\ Si \cap Sj \neq \emptyset, i \neq j, 1 \le i, j \le n$
2. $\forall i, node\ i \in S, 1 \le i \le n$
3. $\forall i, |Si| = k, 1 \le i \le n$
4. $\forall j, node\ j\ is\ with\ in\ k\ Si's\ 1 \le i, j \le n$

Condition 1 : is a necessary condition for the S_i's so that mutual exclusion requests can be resolved. Condition 2 : reduces the number of messages to be sent and received by a node. Condition 3 : means that each node needs to send and receive the same number of messages to obtain mutual exclusion (equal work).

Finally, condition 4 signifies that each node serves as an arbitrator for the same number of nodes. This ensures that each node is equally responsible for mutual exclusion (equal responsibility).

Maekawa established the following relationship between n and k defined as follows n = k(k-1)+1. Hence k can be found approximated to $\sqrt{n}$. The different types of messages used are *REQUEST, LOCKED, INQUIRY, FAILED, RELINQUISH* and *RELEASE*. Timestamps (TS) at any site *i* (where $1 \le i \le n$), Ts_i are ordered par (H_i,i), containing the Lamport's logical clock [10] value H_i and the site id i. Entry Section : Process i multicasts the *REQUEST* message to all the nodes in its S_i including itself. The intersection nodes can send the *REQUEST* messages to any one of the districts to which they belongs. When a process j receives the *REQUEST* message, it sends *LOCKED* message to site i if it has not yet sent it to any other site from the time it received *RELEASE* message. Or else it queues the *REQUEST*.

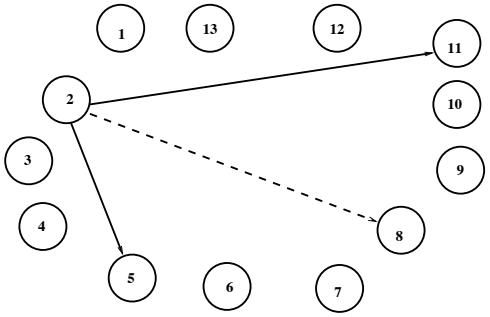
For any node i which intends to execute its CS, the algorithm works as follows :

CS Execution : Process i executes its CS after receiving *LOCKED* message from all the nodes of its S_i.

Exit Section : After executing its CS, site i sends *RELEASE* message to all nodes of its S_i which restores node's right to send *LOCKED* message to any other pending requests in the queue.

This basic algorithm is prone to deadlock which is handled as follows : Assume that a site j has *LOCKED* message to some site k and it later receives a *REQUEST* message from any other site i ($i \neq k$). Then, node j sends *FAILED* to site i if $TS_k < TS_i$, otherwise it sends *INQUIRY* message to site k. When such a process k receives *INQUIRY* message, it sends *RELINQUISH* message to site j if site k has received *FAILED* message from at least one site in S_k, and has not received new *LOCKED* message from it (after receipt of *FAILED* message).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

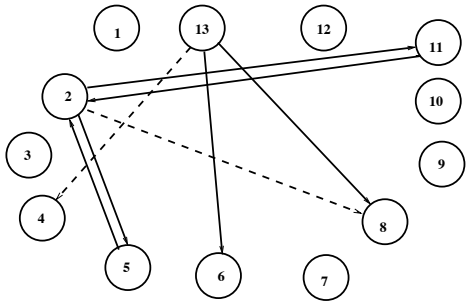


2 requests the critical section and sends requests to processes 5, 8 and 11

Fig. 1. Scenario 1

Example of execution: For Fig. 1, the sites are:

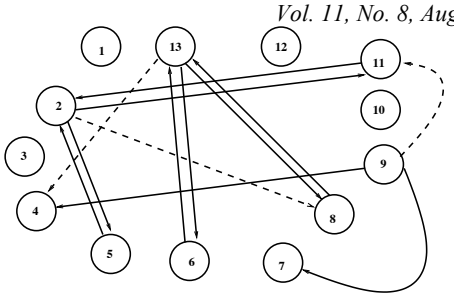
S_1={1,2,3,4}
S_2={2,5,8,11}
S_3={3,5,9,13}
S_4={4,5,10,12}
S_5={5,1,6,7}
S_6={6,2,9,12}
S_7={7,3,8,12}
S_8={8,1,9,10}
S_9={9,4,7,11}
S_{10}={10,2,7,13}
S_{11}={11,3,6,10}
S_{12}={12,1,11,13}
S_{13}={13,4,6,8}



5, 11 are locked for 2

13 requests the critical section and sends request to processes 4, 6 and 8.

Fig. 2. Scenario 2

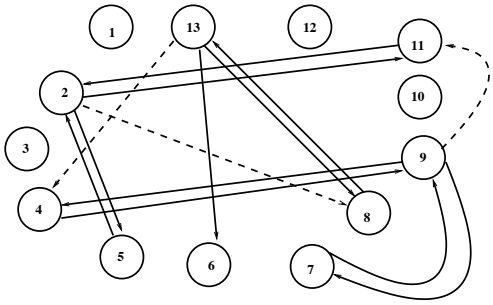


5, 11 are locked for 2

6 and 8 are locked for 13

9 requests the critical section and sends requests to processes 4, 7 and 11

Fig. 3. Scenario 3



5, 11 are locked for 2

6 and 8 are locked for 13

4 and 7 are locked for 9

The deadlock occurs: 2 waits 8, 9 waits 11, and 13 wait 4

Fig. 4. Scenario 4 in presence of deadlock

III. PRINCIPLE OF TH ALGORITHM

Each group is structured in circular ring oriented and arranged according to the identities of the process from smallest to largest.

n=3	n=7	n=13
S_1={1,2}	S_1={1,3,6}	S_1={1,4,5,7}
S_2={2,3}	S_2={2,6,7}	S_2={2,3,7,11}
S_3={3,1}	S_3={3,5,7}	S_3={3,4,10,13}
	S_4={4,2,3}	S_4={4,6,11,12}
	S_5={5,1,2}	S_5={5,8,11,13}
	S_6={6,4,5}	S_6={6,7,9,13}
	S_7={7,4,1}	S_7={7,8,10,12}
		S_8={8,1,3,6}
		S_9={9,2,4,8}
		S_{10}={10,2,5,6}
		S_{11}={11,1,9,10}
		S_{12}={12,3,9,5}
		S_{13}={13,1,2,12}

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

We consider the groups S_1={1,4,5,7}, S_9={9,2,4,8} and S_{13}={13,1,2,12}

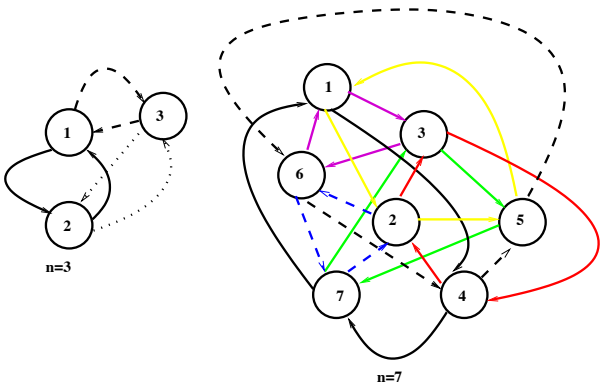


Fig. 5. Circular ordered lists

Local variable at node P_i :

The variables used in the algorithm for process P_i are listed below:

$Stat_i$: indicates whether a node P_i is in the **Wait**=requesting, **Ready**=in critical section or Passive=not requesting. Initially, ∀i, $Stat_i$ = **Passive** S_i : set of identities of processes of P_i's group.

F_i : local waiting queue of nodes P_i. Initially F_i=∅.

B_i: boolean that indicates whether a process P_i is blocked or not. In the algorithm, every process uses two messages:

Req: message sent by process P_i to request the critical section.

Rel: message sent by process P_i to release the critical section. This message is sent to every node in S_i.

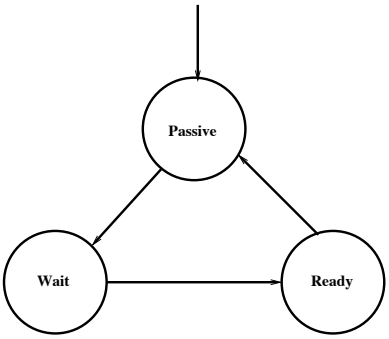


Fig. 6. States process

Principle of the algorithm without deadlock :

We assume that each process builds its circular list ordered L_i. Our algorithm do not use logical timestamps. When a node P_i requests the critical section, two cases are possibles: P_i is placed to the waiting queue F_i and there exists two cases:

case 1: $P_i = Min(L_i)$, then P_i is placed in its local queue F_i, if is the head of its waiting queue, then it sends a request Req(i) to its successor in L_i and waits an authorization to enter in the critical section.

case 2: $P_i = Max(L_i)$, then P_i sends the request message Req(i) to $P_j = Min(L_i)$, and waits for authorization to enter in the critical section. When process P_i release a resource, it broadcasts a message Rel(i) to all members of his group that is to say all the processes in its list L_i.

A. Pseudocode of the algorithm

When P_i requests the critical section

$Stat_i$ ←Wait

If (($P_i = Min(S_i)$) Then

Append(F_i, P_i)

If ($P_i = Head(F_i)$) Then

Send Req(P_i) To Succ(P_i)

B_i ←True EndIf

Else Send Req(P_i) To Min(S_i)

EndIf

When P_i receives Req(P)

If (P∉F_i) Then

Append(F_i , P)

EndIf

If (Head(F_i) = P_i) Then

State ← Ready

B_i ←True

Else

If (P = Head(F_i)) Then

Send Req(P) To Succ(P_i)

B_i ←True EndIf

EndIf

When P_i releases the critical section

∀P∈S_i send Rel(P_i) To P

Remove(F_i, Head(F_i)) $Stat_i$ ← Passive

If (F_i≠ [ ]) Then

Send Req(Head(F_i)) To Succ(F_i)

Else

B_i ←False

EndIf

When P_i receives Rel(P)

Remove(F_i,P)

B_i ←False

If (F_i≠ [ ]) Then

B_i ←True

If (P_i = Head(F_i))) Then

State ← Ready

Else

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Send Req(Head(F_i)) To Succ(Head(F_i))

EndIf

EndIf

B. Example of execution

We consider a network of 13 processes with the groups $S_1, S_2, \cdots, S_{13}$ constructedasinSection3.Weassumethat processes 2, 9 and 13 request to enter the critical section. Now we illustrate the algorithm by the following scenario:

T_1 : Process 2 comes in its queue and waiting to become head of the queue. Once he is the head of the waiting queue, it sends a request Req(2) to his successor in his group which is process 3.

T_2 : Process 9 comes in its queue, it sends a request Req(9) to the smallest of its group process that is process 2.

T_3 : Process 13 comes in its queue, it sends a request Req(13) to the smallest of its group process that is process 1.

T_4 : Process 3 receives the request Req(2) and puts 2 in tail in its queue, if 2 is the head, it sends the request Req(2) to process 7, otherwise 2 remains in the queue of process 3.

T_5 : Process 2 receives the request Req(9) and puts 9 in its queue.

T_6 : Process 7 receives the request Req(2) and puts 2 in its queue and sends Req(2) to process 11.

T_7 : Process 1 receives the request Req(13), puts 13 in his file and becomes blocked by requesting process, process 1 forwards the Req(13) to process 2.

T_8 : Process 11 receives request Req(2) and puts 2 in his queue and becomes blocked for 2, it sends Req(2) to process 2.

T_9 : Process 2 receives the request Req(13), puts 13 in his file.

T_{10} : Process 2 receives its own request Req(2) from process 11, it enters the critical section.

We have the following table :

Process	Waiting queue	State
1	(1,3)	blocked for 13
2	(2,9,13)	in critical section
3	(2)	blocked for 2
4	()	blocked for 9
5	()	blocked for 2
6	()	free
7	(2)	free
8	()	free
9	()	requester
10	()	free
11	(2)	free
12	()	free
13	()	requester

T_{11} :Process 2 releases the critical section, and broadcasts a message Rel(2) to all members in its group S_2 3,7,11. The process 2 sends the blocked request of process 9 to process 4.

T_{12} :Process 4 receives Req(9) from process 2, it puts it in its file, and forwards it to process 8.

T_{13} :Process 8 receives Req(9) from process 4, it puts it in its file and forwards it to process 9.

T_{14} : Process 9 receives its own request Req(9), enters its own queue. Process 9 is at the head of its file, it becomes blocked and enters in its critical section.

T_{15} : Process 9 releases the critical section and broadcasts the message Rel(9) to all members of his group, i.e the processes 2,4,8.

T_{16} : Process 2 receives the message Rel(9) from process 9, it removes the process 9 from its file, and sends the request of process 13 to process 12.

T_{17} : Process 12 receives the message Req(13) from 2, it puts the process 13 in its queue and sends Req(13) to 13.

T_{18} : Process 13 receives its own request Req(13), enters its own queue. Process 13 is at the head of its file, it becomes blocked and enters in its critical section.

We have the following table :

Process	Waiting queue	State
1	(13)	blocked for 13
2	(13)	blocked section
3	()	free
4	()	free
5	()	free
6	()	free
7	()	free
8	()	free
9	()	free
10	()	free
11	()	free
12	(13)	blocked for 13
13	(13)	in critical section

IV. PROOF AND CORRECTNESS

A. Mutual exclusion

Mutual exclusion is achieved when no pair of processes is ever simultaneously in its critical section. For any pair of processes, one must leave its critical section before the other may enter.

Theorem 4.1: The proposed algorithm ensures the mutual exclusion property.

Proof: Assume the contrary, that more than one node are

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

simultaneously in the critical section. Suppose that two application processes P_i and P_j ($i \neq j$) in different groups are in the critical section simultaneously. Let S_i and S_j be groups that P_i and P_j belong respectively. Because any two groups have non-empty intersection, we have $S_i \cap S_j \neq \emptyset$ and let P_k be a process in the intersection. Since P_k never grants permission for more that one group at a time, P_i and P_j cannot be granted by P_k simultaneously. This is a contradiction.

B. Deadlock and starvation freedom

1) Deadlock freedom: Maekawa's algorithm can deadlock because a process is exclusively locked by other processes and requests are not prioritized by their timestamps.

Proof: Deadlock handling in [4] requires three types of messages: failed, inquire and yield.

Deadlock could occur for a set of processes if they were each involved in a circular wait. A circular wait could occur if each of the processes P_i in the cycle is blocked at the waiting queue located at process P_j, and is yet to receive a request message from the successor process in the cycle and no there are no request in transit which are destined for any of these processes. Assume, by way of contradiction, that this is the case. Then each process in the circular wait has delayed sending a request message to its predecessor process in the cycle. A processes P_i will only defer sending a request to a process P_j. Thus, to achieve a deadlock, each process in the circular wait must be blocked by its predecessor process in its group, which is impossible. Therefore, the algorithm is deadlock-free.

2) Starvation freedom: Starvation occurs when a few processes repeatedly execute their critical section while other processes wait indefinitely . Assume, by way of contradiction, that process P_j has been repeatedly executing its critical section while process P_i has been waiting to enter in its critical section.

The groups of processes are organized as a logical ring of processes, and every process knows its successor on the ring. Every process uses a local waiting queue to store the pending requests.

Theorem 4.2: Every request process enter in the critical section during a bounded delay.

Proof: Every process receives, at most one, request from every process in its group. Every request is stored in its waiting queue for a bounded delay.

By examining the algorithm, when process releases its criticalsection, it sends a release message to all processes in its group.

when a process receives a release message, it removes the request placed at the head of its waiting queue. At most $\sqrt{n}$ request are placed in a waiting queu before any request. A request transits by $\sqrt{n}$ processes of its group.

C. Message complexity

The message complexity of a distributed mutual exclusion algorithm is the number of messages exchanged by a process per critical section.

Theorem 4.3: Message complexity of the proposed algorithm is $2\sqrt{n}$ in the best case and O(3|S|) in the worst case, where |S| is a quorum size that the algorithm adopts.

Proof: In the best case, two types of messages (Req, Rel) are exchanged between application process and each management process in a quorum. Thus, message complexity is 2|S| in the best case, where |S| is a quorum size that the algorithm adopts. Outline of the scenario of the worst case is as follows. A process P_i send a request message Req to P_j in the group S_i, but $P_i \neq \min(S_i)$ and $P_i \neq \max(S_i)$. In addition to the best case, additionally one (1) message is exchanged, we have the bound $|S| + 2|S| = O(3|S|)$.

V. CONCLUSION

Quorum-based mutual exclusion is an attractive approach for providing mutual exclusion in distributed systems due to its low message complexity and high resiliency. After the first quorum-based algorithm [4] was proposed by Maekawa more than a decade ago, many algorithms [3][4][5][6][9] have been proposed to construct different quorums to reduce the message complexity or increase the resiliency to site and communication failures. Some researchers also propose schemes for constructing delay-optimal quorums to reduce the average message delay. However, all these quorum-based algorithms depend on Maekawa's algorithm to ensure mutual exclusion and they all have high synchronization delay (2T).

We have presented a very simple free deadlock distributed mutual exclusion algorithm based on quorum principle. Every group is structured to ordering circular list, and every process is am smallest or the biggest of his group. The request message sends by a requesting process, visits all processes according to the order of its list. Every critical section execution, requires at least $2\sqrt{n}$ messages where n is the number of processes in the network.

REFERENCES

[1] S. Banerjee, and P. Chrysanthis, "A New Token Passing Distributed Mutual Exclusion Algorithm," Proceedings of the 16th ICDCS, pp. 717-724, 1996.

[2] M. Naimi, and M. Trehel, "How to detect a failure and regenerate the Token in the Log(n) distributed algorithm for mutual exclusion," LNCS 312, Amsterdam, 1987.

[3] G. Ricart, and A. K. Agrawala, "An Optimal Algorithm for Mutual Exclusion in Computer Networks," Communications of the ACM, Vol. 24, No. 1, pp. 9-17. 1981.

[4] M. Maekawa, "A $\sqrt{n}$ Algorithm for Mutual Exclusion in Decentralized Systems," ACM Trans. Computer Systems, vol. 3, No. 2, pp. 145-159, 1985.

[5] D. Agrawal, and A. El Abbadi, "An Efficient and Fault-Tolerant Solution for Distributed Mutual exclusion," ACM Trans. On Computer systems, Vol. 9, No. 1, pp. 1-20, 1991.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[6] C. Saxena, J. Rai, "A survey of permission-based distributed mutual exclusion algorithm," Elsevier Science Publisher B. V., Vol. 25, No. 2, pp. 159-181, 2003.

[7] R. H. Thomas, "A majority consensus approach to concurrency control," ACM Trans. On Database System, Vol. 4, No. 2, pp. 180-209, 1979.

[8] H. Garcia-Molina, and D. Barbara, "How to assign votes in a distributed system," Journal of the ACM, Vol. 32, No. 4, pp. 841-860, 1985.

[9] L. Lamport, "Time, clocks, and the ordering of events in a distributed system", Communications of the ACM, Vol. 21, No. 7, pp. 558-565, 1978.

[10] R. Atreya, and N. Mittal, "A quorum-based group mutual exclusion algorithm for a distributed system with dynamic group set", In IEEE Trans. On Parallel and Distributed Systems, Vol. 18, No. 10, 2007.

[11] I. Suzuki, and T. Kasami, "A distributed mutual exclusion algorithm," ACM Trans. On Computer Systems, Vol. 3, No. 4, pp. 344-349, 1985.

AUTHORS PROFILE

Mohamed Naimi. Received a PhD in computer science (Distributed systems) from the university of Franche-Comté Besancon, France. He is a Full Professor in the University of Cergy-Pontoise. He has been author and co-author of published papers in several journals and recognized international conferences and symposiums.

Ousmane Thiare. Received a PhD in computer science (Distributed systems) at 2007 from the university of Cergy Pontoise, France. He is an Associate Professor in Gaston Berger University of Saint-Louis Senegal. He has been author and co-author of published papers in several journals and recognized international conferences and symposiums.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Steganography in the Non-Edges of True Color Images

Ahmed Yaseen Kamel[(1)] Auf Abdul-Rahmaan Hasso[(2)] Shahd Abdul-Rhman Hasso[(3)]

(1) Assistant Lecturer in Directorate Nineveh Education
(2) B.Sc. in Electrical and Electronics Engineering
[(3)]Lecturer in Software Engineering Dept., College of Computer Sciences and Math., University of Mosul
Mosul, Iraq,

***Abstract*—This paper proposed a new technique for text hiding in the non-edges of a true color image. Text has been hidden as bytes by embedding it in the image (depending on its edges) and results showed high accuracy in the hiding subjectively and objectively and there is no evidence on the existence of hidden data in the true image in each color, any pixel is used for hiding 3 bytes of the text so it is possible using the proposed algorithm to hide text of any size, without the appearance of any effect on the resulting image.**

The results shows no change in the image size after embedding the text, and any increase or decrease in the text size does not represent a major factor in hiding, but whenever the size of the image is greater, the hiding will be secure.

Keywords- Steganography; Canny Edge Detection, True Color Image.

I. INTRODUCTION

Steganography is the method for secret communication. The word "Steganography" derives from Greek and it means "cover writing" . Steganography is method of invisible communication between two parties and it is opposite to cryptography. Its goal is to hide the content of a message [1]. Digital form of media as a cover-media being use in steganography are pictures, video clips, music and sounds. Text steganography have been moderate into the digital form whereas the steganography was also implemented in the digital text form. Text steganography is the most difficult kind of steganograph , due largely to the relative lack of redundant information in a text file as compared to picture or sound [2]. The following formula provides a very generic description of the pieces of the steganographic process.

stego_medium=stego_key+cover_medium+ hidden_data

In this context, the cover_medium is the file in which will behide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files. In this article, the image file will be focused and will therefore, refer to the cover_image and stego_image [2].

Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.

Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively [3].

The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640×480 pixel image using a palette of 256 colors would require a file about 307 KB in size (640 × 480 bytes), whereas a 1024×768 pixel true color 24-bit color image would result in a 2.36 MB file (1024 × 768 × 3 bytes).

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, the binary representation of the hidden_data will overwrite the LSB of each byte within the cover_image. If 24-bit color was used, the amount of change will be minimal and indiscernible to the human eye. But the LSB method has been in a worst case when the text file size is increased. Therefore, in this work, a new method for hiding is used that is hide the text in the 24 byte color pixel randomly depends on the non-edge map of the cover image, i.e., each pixel in the image could hide 3 bytes of text [4][5].

II. THE CANNY EDGE DETECTOR

The Canny edge detector is a standard edge detector applied to images. It is used to find the edges in an image and also convert it to a binary image. It defines edges as zero-crossings of second derivatives in the direction of the greatest first derivative.

The canny edge detector uses two different thresholds to detect the strong and weak edges, and it includes the weak edges in the object only if they are connected to the strong edges [6].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Some improvements can be gained using a dual threshold approach. Two thresholds are used one is significantly larger than the other. Application of these two different threshold will produce two binary edge images, denoted IT1 and IT2 respectively. Since IT1 is created using a lower threshold, it will contain more false hits than IT2. Points in IT2 are therefore considered to be parts of true edges. Connected points in IT2 are copied to the output edge image. When the end of an edge is found, some points in IT1 which could be a continuation of the edge. The process is continued until it connects with another IT2 edge point or no connected IT1 points are found [6].

III. RELATED WORK:

As long as people have been able to communicate with one another, there has been a desire to do so secretly. many researchers work on text steganography. In [7] Mehdi Hussain and M. Hussain (2011), proposed an information hiding method around the edge boundary of objects in image. The experimental results showed that the stego-image had identical edge boundaries as was in cover-image (using 'Sobel' and 'Canny' edge detection methods), so stego-image could directly used instead of cover-image for further image processing techniques.

In [8] Nuur Alifah Roslan et. al., (2011), presented new method Arabic text steganography in a sharp-edges method. The new method was hide the secret bits in the sharp-edges for each character in the Arabic text document. The main processes were identifying sharp-edges in the cover-text, secret message preparation to be hidden as a binary string and lastly, the bit hiding process. Their experiments showed that the capacity percentage used to hide the secret bit was increased up to 37.8%, resolving the capacity issue.

In [9] Nitin Jain et. al., (2012), search how the edges of the images could be used to hiding text message. It gave the depth view of image steganography and Edge detection Filter techniques for the gray image. They tried to find binary value of each character of text message and then in the next stage, tried to find dark places of gray image (black) by converting the original image to binary image for labeling each object of image by considering on 8 pixel connectivity. Steganalysis then used to evaluate the hiding process to ensure the data can be hidden in best possible way.

In [10] Sneha Arora and Sanyam Anand (2013), proposed a technique to hide the text data into the color images using edge detection method. The alteration in edges cannot be distinguished well so edges can hide more data without losing quality of an image. In their technique, Edges of an image were detected by scanning using 3×3 window and then text message was concealed in edges using first component alteration technique. Their proposed scheme achieved high embedding capacity and high quality of encoded image.

In [1] Sneha Arora and Sanyam Anand (2013), proposed a new technique for image steganography using edge detection for RGB images. In their study, edges of an RGB image was detected by scanning method using 3x3 window, and then text was embedded in to the edges of the color image. They achieve high embedding capacity and enhance the quality of the stego-image from the human vision system.

As been mentioned on the previous work, many researcher work on steganography and they used the image edges for hiding texts and embedding the text bit by bit in the cover image. In this work, we proposed a new method for hiding data in the non-edge in the true color images.

IV. THE NEW PROPOSED ALGORITHM

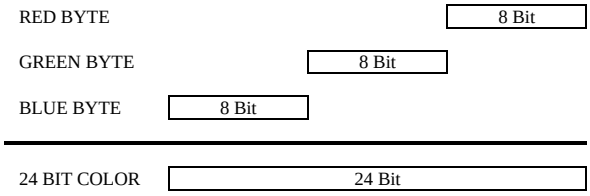
The presented work is divided into two levels; embedding level and retrieving level:

A. Hiding Level:

The hiding or embedding level is as follows:

1- Read the color image, the color image will be a three dimensional matrix. The first is the red content , second is the green and the third is the blue color content.

At this point, the image is converted into two dimensional 24 bit image as:



2- Apply the Canny edge detector on the image using thresholds (thr1, thr2). These threshold will be the private keys. The result of canny detector is binary image.
3- Find the non-edge pixels, i.e., the pixels that has a value (0) in the binary image because the edges will be of value (1).
4- Read the text file.
5- Find the coordinates of the non-edge pixels.
6- Embed the text file length in the first non- edge pixel.
7- Start hiding the text file in the non-edge pixel , starting from the middle, then going left and right respectively until the text is finished.
8- In a worst case, the text file length will be greater than the number of non-edge pixels. in this case embed the remainder text character after finding its coordinates and in the same arrangement (middle, left, right).
9- Finally send the cover image to the receiver. Figure (1) shows the flow chart of the embedding level of the proposed method.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

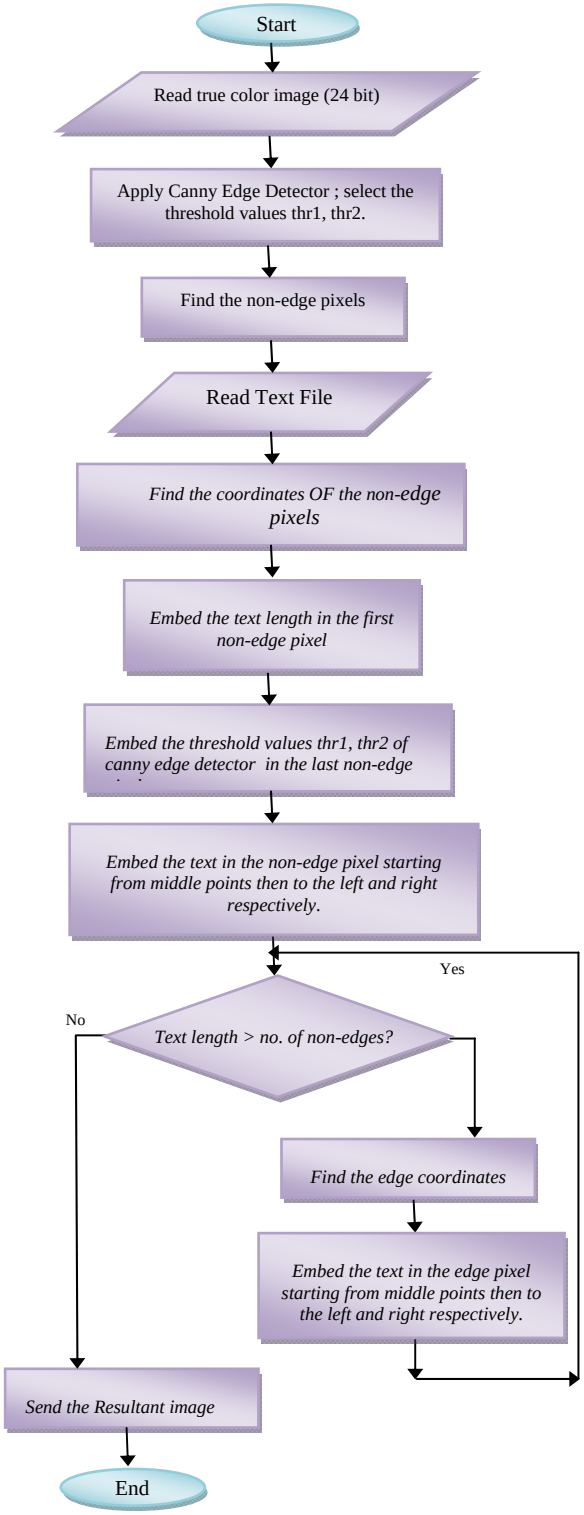


Figure (1); the Flow Chart of the hiding level in the proposed method

B. *Retrieving Level:*

The extracting or retrieving level is as follows:

1- Read the received image, the color image will be a three dimensional matrix. The first is the red content , second is the green and the third is the blue color content.

2- Apply the Canny edge detector on the image using thresholds (thr1, thr2). These threshold will be the private keys. The result of canny detector is binary image.

3- Find the non-edge pixels, i.e., the pixels that has a value (0) in the binary image because the edges will be of value (1).

4- Find the coordinates of the non-edge pixels.

5- Retrieve the text file length from the first non-edge pixel.

6- Start Retrieving the text file in the non-edge pixel , starting from the middle, then going left and right respectively until the text is finished.

7- If the text file length greater than the number of non-edge pixels. retrieve the text character after finding its coordinates and in the same arrangement (middle, left, right).

V. RESUALT AND DISCUSSION

The performance measures of the basic methods used to measure the progress of the algorithms used in the hiding that is a Peak Signal to Noise Ratio (*PSNR*) and the Signal to Noise Ratio (*SNR*) and the mean square error square error (*MSE*) are calculated by these equations:

$$SNR = 10\log 10\left[\frac{\sum\sum(input\_image)^2}{\sum\sum(Output\_image - input\_image)^2}\right] \quad .....(1)$$

$$MSE = \frac{1}{MN}\sum\sum(Output\_image - input\_image)^2 \quad .....(2)$$

$$PSNR = 10\log 10\left[\frac{\max value}{\frac{1}{MN}\sum\sum(Output\_image - input\_image)^2}\right] \quad .....(3)$$

Many type of images where applied on the proposed method and examine the performance measures of it. Table (1) shows the results of the performance measures for the proposed algorithm for text length (1416) bytes, Table (2) shows the results of the performance measures for the proposed algorithm for text length (2834) bytes, Table (3) shows the results of the performance measures for the proposed algorithm for text length (4920)bytes and Table (4) shows the results of the performance measures for the proposed algorithm for text length (7088) bytes . the tables show that the proposed algorithm efficient for concealment whatever increased the length of the text file and increase the image size the effect a very slight noticeable.

TABLE (1) THE PERFORMANCE MEASURES FOR THE PROPOSED ALGORITHM FOR TEXT OF (1416) BYTES

File Name	*Text file*	*SNR*	*MSE*	*PSNR*
Baby1	1776×1200	47.975	0.009	68.328
Baby3	1456×2592	48.765	0.007	69.615
Building2	600×800	33.932	0.00000	109.71
Building3	557×800	37.307	0.095	58.354
Cartoon1	1200×1600	43.875	0.023	64.573
Cartoon2	768×1024	44.876	0.034	62.861
Karekateer1	313×320	31.624	0.00003	93.367
Karekateer2	750×1000	39.354	0.081	59.069

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE (2) THE PERFORMANCE MEASURES FOR THE PROPOSED ALGORITHM FOR TEXT OF (2834) BYTES

File Name	Text file	SNR	MSE	PSNR
Baby1	1776×1200	42.811	0.013	67.077
Baby3	1456×2592	43.586	0.021	64.922
Building2	600×800	32.216	0.055	60.754
Building3	557×800	34.674	0.146	56.495
Cartoon1	1200×1600	39.381	0.053	60.893
Cartoon2	768×1024	38.327	0.105	57.925
Karekateer1	313×320	28.645	0.00003	93.367
Karekateer2	750×1000	35.320	0.161	56.068

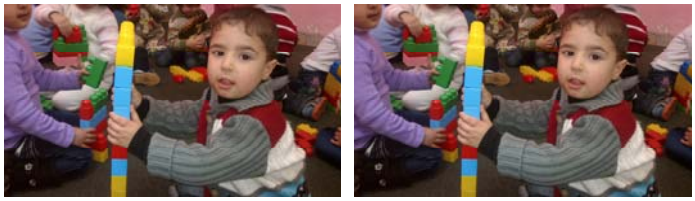
TABLE (3) THE PERFORMANCE MEASURES FOR THE PROPOSED ALGORITHM FOR TEXT OF (4920) BYTES

File Name	Text file	SNR	MSE	PSNR
Baby1	1776×1200	40.572	0.0217	64.776
Baby3	1456×2592	41.297	0.0381	62.326
Building2	600×800	29.673	0.0736	59.460
Building3	557×800	32.013	0.2623	53.943
Cartoon1	1200×1600	37.193	0.0835	58.916
Cartoon2	768×1024	35.266	0.180	55.573
Karekateer1	313×320	26.244	0.00003	93.367
Karekateer2	750×1000	33.451	0.279	53.673

TABLE (4) THE PERFORMANCE MEASURES FOR THE PROPOSED ALGORITHM FOR TEXT OF (7088) BYTES

File Name	Text file	SNR	MSE	PSNR
Baby1	1776×1200	38.852	0.036	62.562
Baby3	1456×2592	40.181	0.046	61.539
Building2	600×800	28.595	0.140	56.665
Building3	557×800	30.623	0.327	52.986
Cartoon1	1200×1600	36.307	0.099	58.166
Cartoon2	768×1024	33.998	0.261	53.959
Karekateer1	313×320	24.655	0.00003	93.367
Karekateer2	750×1000	31.619	0.402	52.089

Figure (2) shows the result of hiding 1416 bytes of data. Obviously not distinguish the existence of evidence within the cover image as well as the size of the cover image did not change after the hide data inside it, figure (3) represents the cover image resulting 2834 byte hiding, figure (4) represents the cover image for 4920 bytes of data and figure (5) represents the cover image for 7088 bytes of data.



Before hiding *After hiding*

Figure (2) A sample of baby image that hide (1416)byte text.

Before hiding *After hiding*

Figure (3) A sample of baby image that hide (2834)byte text.

Before hiding *After hiding*

Figure (4) A sample of baby image that hide (4920)byte text.

Before hiding *After hiding*

Figure (5) A sample of baby image that hide (7088)byte text.

IV. CONCLUSION

Through the application of the new proposed algorithm we conclude the following:

- ✓ The increase in the of the text file does not have a significant effect on the process of concealment and does not affect the evaluation of the resulting image.
- ✓ The efficiency of the algorithm that the text is hidden as a fully byte in the image and that each pixel possible to store 3 bytes of text and this is what enables the user to hide the text of any size (the largest size of the text is 2^{24} bytes) This is a size too big to hide.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- ✓ The efficiency of the algorithm is increase with the increase of cover image size as well as increase the dispersion of the colors and the emergence of the largest number of colors.

VI. REFERENCES

[1] Sneha Arora and Sanyam Anand, (2013), "A New Approach for Image Steganography using Edge Detection Method", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, May 2013

[2] Stallings William; (2011), "Cryptography and Network Security Principles and Practices" , 5th Edition, Pearson Education, Inc., Prentice Hall.

[3] González Rafael C. & Richard Eugene Woods, (2008), "Digital image processing", Pearson/Prentice Hall .

[4] Arjun Santosh, Atul Negi, Chaithanya Kranthi, Divya Keerthi; (2007): "An Approach to Adaptive Steganography Based on Matrix Embedding", IEEE 1-4244-1272-2/07/2007.

[5] Medeni, M.B.O.; Souidi, E.M.; (2010), "Steganographic Algorithm Based On Error-Correcting Codes For Gray Scale Images", I/V Communications and Mobile Network (ISVC), 5th International Symposium, pp: 1 – 4.

[6] Snyder Wesley E., Qi Hairong, (2004), "Machine Vision", Cambridge University Press

[7] Mehdi Hussain and M. Hussain, (2011), Information Hiding Using Edge Boundaries of Objects "", International Journal of Security and Its Applications Vol. 5 No. 3, July, 2011

[8] Nuur Alifah Roslan, Ramlan Mahmod and Nur Izura Udzir, (2011), "SHARP-EDGES METHOD IN ARABIC TEXT STEGANOGRAPHY", Journal of Theoretical and Applied Information Technology, 15th November 2011. Vol. 33 No.1

[9] Nitin Jain, Sachin Meshram, Shikha Dubey, (2012), "Image Steganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-3, July 2012 217

[10] Sneha Arora and Sanyam Anand "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 2, February 2013)

AUTHOR PROFILE

Mr. Ahmed Y. Kamel (M Sc.) is currently an assistant lecturer in Directorate Nineveh Education . learned in Mosul University/ College of Computer Science and Mathematics/ Computer Science Department. he received B.Sc. degree in Computer Science from University of Mosul in 2007 and M.Sc. degree from University of Mosul in 2010. His research interests and activity are in data security, network security, information hiding.

Mr. Auf A. R. Hasso (B Sc.) B.Sc. in Electrical and Electronics Engineering – University of Technology – Baghdad –1988. He is professional in English language (ILETS). He is Iraqi Engineering Syndicate Membership issued in 1988. He is Member in Iraqi federation of industries, Member in Baghdad chamber of commerce. His research interests and activity are in data security, network security, information hiding in addition to electrical engineering projects.

Mrs. Shahd A. R. Hasso (M Sc.) is currently a lecturer at Mosul University/ College of Computer Science and Mathematics/ Computer Science Department. She received B.Sc. degree in Computer Science from University of Mosul in 1998 and M.Sc. degree from University of Mosul in 2003. Her research interests and activity are in data security, data structures, network security, information hiding. Now, she teaches data security undergraduate students.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Image Integrity based on HMAC Structure

Shahd Abdul-Rhman Hasso
Lecturuer
Department of Software Engineering/
College of Computer Sciences and Math. / University of Mosul
Mosul, Iraq

***Abstract*— With the increasing of the online applications and aggravation of dealing with official papers via the Internet that is send by images. It has become very necessary to add ways to make sure of the reliability of the transmitted image. The presented work is a design of algorithm for the integration and authentication of the image by adding it' s hash message authentication code (HMAC) of the original image after encryption code using triple DES to it.**
The proposed algorithm depends on applying the HMAC-SHA-512 for finding the 512-bit HMAC code of an input (secured and must be integrated) image, then encrypt the resultant hash code by 3DES algorithm , forming it as an icon (small) image and send the resultant image icon attached.
The receiver will receive the original and icon image , he wants to insure that the original is integrated and authenticated, Therefore , the HMAC-SHA-512 will applied on the original , decrypt the icon image to obtain the hash code , then matching codes to check the integrity and make sure of the reliability of the transmitted image.
Results proved high precision and reliable images whatever the size of the image slight change the image pixel affect the output code which increases the reliability of the image.

Keywords-HMAC; 3DES; Image Authentication; Image Integrity.

I. INTRODUCTION

Digital images have been widely used in our community. Such massive amount digital images have been recently applied in forensic science, such as we can figure out features of suspects or characteristic marks of criminal vehicles. However, with proper computer software, we can modify or duplicate those image data easily. If those modification or duplication is unauthorized, it will make us doubtful when submitting digital images as evidence in court [1].

In cryptography, one of the techniques to produce a message authentication code is based on using hash functions. A hash function provides additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. Hash functions are widely used to protect password contents and interactive authentication in the internet. Even a single bit changed in the input message, though, will produce a different hash value [1].

.

The Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification.

In cryptography, a keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key [2][3].

An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, MD5 and SHA-1 operate on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of MD5 or SHA-1, respectively), although it can be truncated if desired. Table (1) shows the various types of associated with the HMAC-SHA algorithms [4][5].

TABLE(1); THE TYPES OF HMAC-SHA ALGORITHMS.

Algorithm ID	Block Size	Output Length	Trunc. Length	Key Length	Algorithm Type
HMAC-SHA-256-128	512	256	128	256	auth/integ
HMAC-SHA-384-192	1024	384	192	384	auth/integ
HMAC-SHA-512-256	1024	512	256	512	auth/integ

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. HASH CLASSIFICATION

The hash functions are classified based, based on further properties they provide and reflecting requirements of specific applications. There are two types of hash functions depending on its functional classification that are shown in figure (1) [6]:

1. Modification Detection Codes (MDCs)

Also known as manipulation detection codes, and less commonly as message integrity codes (MICs), the purpose of an MDC is (informally) to provide a representative image or hash of a message, satisfying additional properties as refined below. The end goal is to facilitate, in conjunction with additional mechanisms, data integrity assurances as required by specific applications. MDCs are a subclass of un-keyed hash functions, and themselves may be further classified:

(i) One-Way Hash Functions (OWHFs): for these, finding an input which hashes to a pre-specified hash-value is difficult;

(ii) Collision Resistant Hash Functions (CRHFs): for these, finding any two inputs having the same hash-value is difficult.

2. Message Authentication Codes (MACs)

The purpose of a MAC is (informally) to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity. MACs have two functionally distinct parameters, a message input and a secret key.

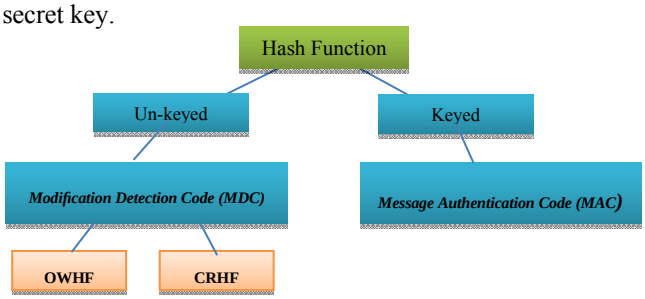


Figure (1): Simplified classification of cryptographic hash functions.

III. MAC PROPERTIES

MAC algorithm is a family of functions hk parameterized by a secret key k, with the following properties[2]:

1. ease of computation — for a known function h_k , given a value k and an input x, $h_k(x)$ is easy to compute. This result is called the MAC-value or MAC.

2. compression— h_k maps an input x of arbitrary finite bit length to an output $h_k(x)$ of fixed bit length n.

Furthermore, given a description of the function family *h*, for every fixed allowable value of *k* (unknown to an adversary), the following property holds:

3. computation-resistance— given zero or more text-MAC pairs$(x_i ; h_k(x_i))$, it is computationally infeasible to compute any text-MAC pair$(x; h_k(x))$for any new input $x \neq x_i$ (including possibly for $h_k(x) = h_k(x_i)$for some *i*).

If computation-resistance does not hold, a MAC algorithm is subject to MAC forgery. While computation-resistance implies the property of key non-recovery (it must be computationally infeasible to recover k, given one or more text-MAC pairs$(x_i; h_k(x_i))$for that *k*), key non-recovery does not imply computation-resistance (a key need not always actually be recovered to forge new MACs)[7].

Any message authentication or digital signature mechanism has two levels of functionality. At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as a primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

In recent years, there has been increased interest in developing a MAC derived from a cryptographic hash function. The motivations for this interest are :

1. Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES.

2. Library code for cryptographic hash functions is widely available.

With the development of AES and the more widespread availability of code for encryption algorithms, these considerations are less significant, but hash-based MACs continue to be widely used.

A hash function such as SHA was not designed for use as a MAC and cannot be used directly for that purpose, because it does not rely on a secret key. There have been a number of proposals for the incorporation of a secret key into an existing hash algorithm. The approach that has received the most support is HMAC. HMAC has been issued as RFC 2104, has been chosen as the mandatory-to-implement MAC for IP security, and is used in other Internet protocols,

such as SSL.HMAC has also been issued as a NIST standard.

IV. HMAC DESIGN OBJECTIVES

RFC 2104 lists the following design objectives for HMAC To use, without modifications, available hash functions. In particular [8]:

- To use hash functions that perform well in software and for which code is freely and widely available.
- To allow for easy replaceability of the embedded hash function in case faster or more secure hash functions are found or required.
- To preserve the original performance of the hash function without incurring a significant degradation.
- To use and handle keys in a simple way.
- To have a well understood cryptographic analysis of the strength of the authentication mechanism based on

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

reasonable assumptions about the embedded hash function.

The first two objectives are important to the acceptability of HMAC. HMAC treats the hash function as a "black box." This has two benefits. First, an existing implementation of a hash function can be used as a module in implementing HMAC. In this way, the bulk of the HMAC code is prepackaged and ready to use without modification. Second, if it is ever desired to replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module. This could be done if a faster hash function were desired. More important, if the security of the embedded hash function were compromised, the security of HMAC could be retained simply by replacing the embedded hash function with a more secure one (e.g., replacing SHA with SHA).

The last design objective in the preceding list is, in fact, the main advantage of HMAC over other proposed hash-based schemes. HMAC can be proven secure provided that the embedded hash function has some reasonable cryptographic strengths.

V. HMAC ALGORITHM

Figure (2) illustrates the overall operation of HMAC. Define the following terms.

H = embedded hash function (e.g., MD5, SHA-1, RIPEMD-160)
IV = initial value input to hash function
M = message input to HMAC (including the padding specified in the embedded
hash function)
Yi _ i th block of M, 0 _ i _ (L – 1)
L _ number of blocks in M
b _ number of bits in a block
n _ length of hash code produced by embedded hash function
K _ secret key; recommended length is n; if key length is greater than b,
the key is input to the hash function to produce an n-bit key

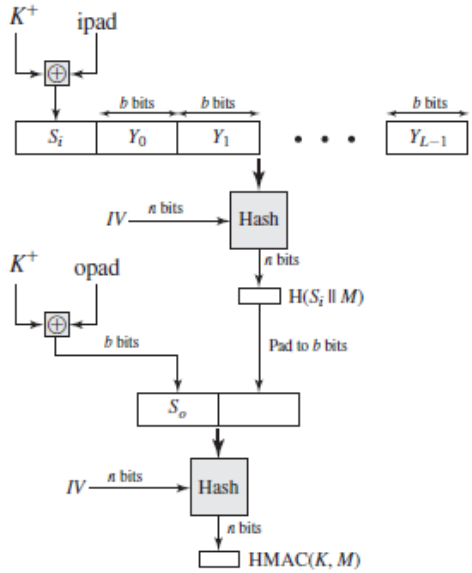


Figure (2) the HMAC structure.

K^+ _ K padded with zeros on the left so that the result is b bits in length
ipad _ 00110110 (36 in hexadecimal) repeated b/8 times
opad _ 01011100 (5C in hexadecimal) repeated b/8 times

Then HMAC can be expressed as the algorithm as follows [9].

1. Append zeros to the left end of K to create a b-bit string K^+ (for example, if K is of length 160 bits and b = 512, then K will be appended with 44 zero bytes 0x00).
2. XOR (bitwise exclusive OR) K^+ with *ipad* to produce the b-bit block S_i.
3. Append M to S_i.
4. Apply H to the stream generated in Step 3.
5. XOR K^+ with *opad* to produce the b-bit block S_o.
6. Append the hash result from Step 4 to S_o.
7. Apply H to the stream generated in Step 6 and output the result.

Note the XOR with *ipad* results in flipping one-half of the bits of K. Similarly, the XOR with *opad* results in flipping one-half of the bits of K, but a different set of bits. In effect, by passing S_i and S_o through the compression function of the hash algorithm, you have pseudo randomly generated two keys from K. HMAC should execute in approximately the same time as the embedded hash function for long messages. HMAC adds three executions of the hash compression function (for S_i , S_o, and the block produced from the inner hash).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

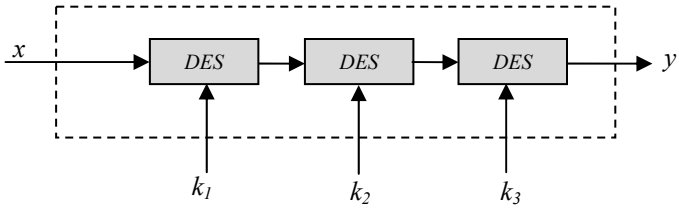
VI. TRIPLE DATA ENCRYPTION STANDARD (3DES)

Triple DES is a method to encrypt text using three 64bit keys, i. e, the total length of the key is 192bit key that is divided into three keys, each of which is composed of 64 bits. The encryption method in this algorithm is the same used in the regular DES algorithm but repeated three times where the data is encrypted with the first key, the second key and then the third as follows [2]:

$$y=DES_{k3}(DES_{k2}(DES_{k1}(x))) \quad \ldots\ldots\ldots(1)$$

where;
x: is the input text.
y: the encrypted text.
k_1 و k_2 و k_3 : *the three encryption keys.*

Figure (3) shows the implementation of the triple DES algorithm.



Figure(3); Triple Data Encryption Standard 3DES Algorithm .[2]

VII. THE PROPOSED ALGORITHM

The presented work is divided into two stages; sender stage and receiver stage:

A. *sender stage:*

the user at this stage perform the following steps:

step 1: read the image; the image may be colored or gray. If it is colored the steps (2-4) will repeated 3 times for red, green blue images respectively.
Step2: perform the HMAC algorithm to find the authentication code for the input image.
Step 3: perform the triple DES algorithm on the hash code.
Step 4: illustrate the encoded hash code as an icon image (small image).
Step 5: send the original and icon image.
Figure (4) shows the flow chart of the sender stage.

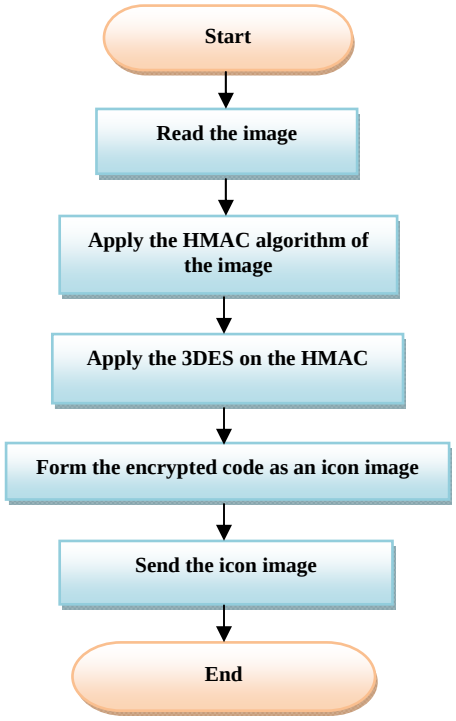


Figure (4)the flow chart of the sender stage.

B. *Receiver Stage*

To ensure the original image that is the correct one, the receiver must perform the following steps:

step 1: read the image; the image may be colored or gray. If it is colored the steps (2) will repeated 3 times for red, green blue images respectively.
Step2: perform the HMAC algorithm to find the authentication hash code for the input image.
Step 3: read the icon image.
Step 4: decrypt the icon image using triple DES algorithm.
Step 4: match the resultant code of step 2 and step 4.
Step 5: ; if match; then the input image is integrated; otherwise it is un authorized image.
Figure (5) shows the flow chart of the receiver stage.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

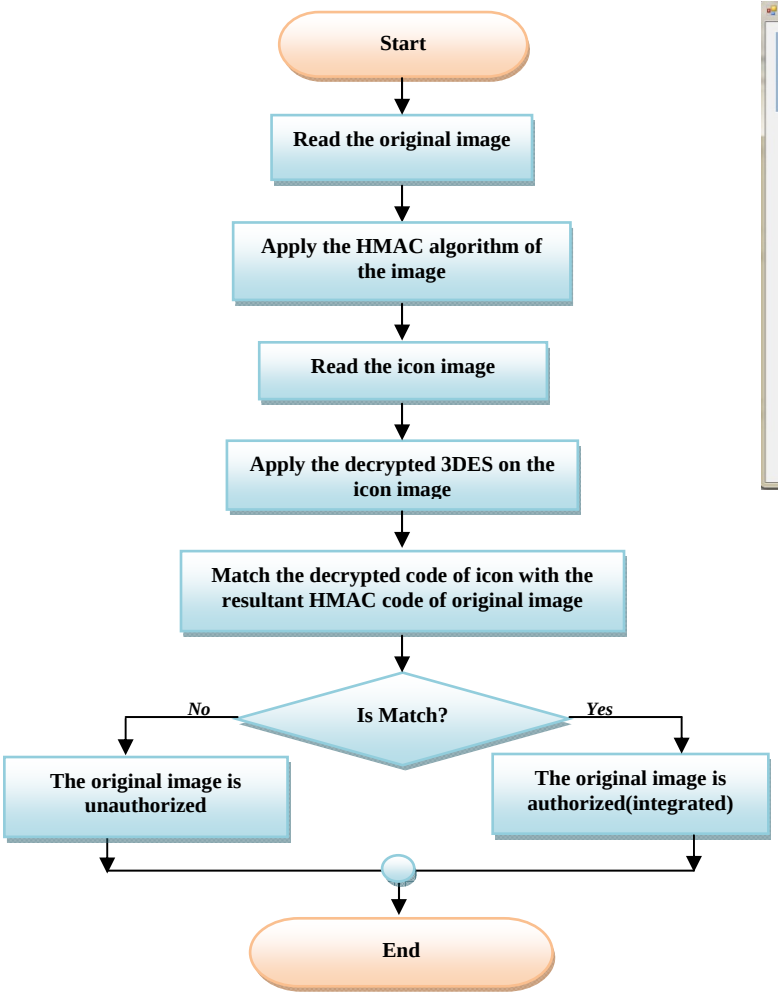


Figure (5)the flow chart of the receiver stage.

VIII. RESUALT AND CONCLUSION

1- Applying the proposed algorithm on any image result match hashing code as shown in the figure .

Figure (6)the Result of applying algorithm on an authenticated image

2- Applying the proposed algorithm is applied on a number of images with different types (biometrics, certifications, … , etc), a slight change on the input image is made a non-matching in the resulting code that means the image in unauthorized, as shown in the results listed below:

i. Figure (7-a) shows an original image of biometric - fingerprint, (7-b) shows the resultant image slight change, (7-c), shows the HMAC code of the two images (7-d) shows the icon image of the decrypted HMAC of the original image (a) and (b), as shown in the (7-e) the code is not match.

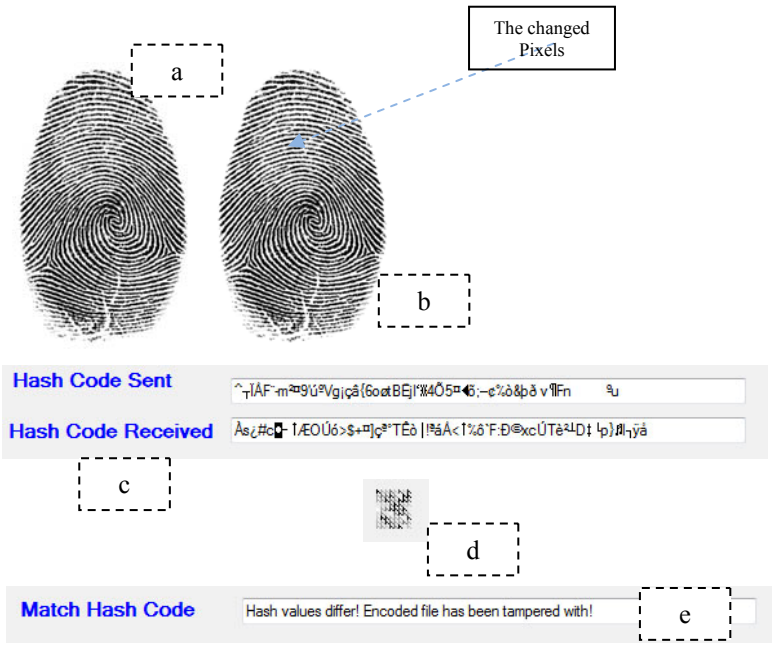


Figure (7-a) Original fingerprint image, (b) Image with slight change, (c), HMAC code for (a)&(b) (d) The icon image of the decrypted HMAC and (e) The code is not match.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

ii. Figure (8) shows the application of the proposed algorithm on a signature image, in the figure it appears the resultant image slight change, the HMAC code of the two images , the icon image of the decrypted HMAC of the two images and as shown in the figure the code is not match.

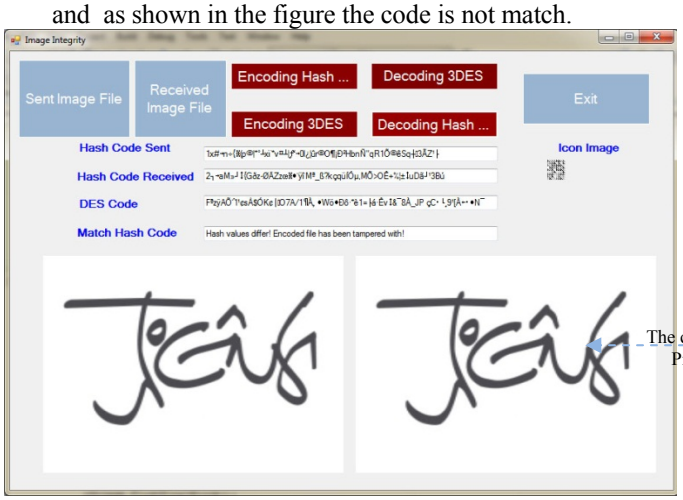


Figure (8)the proposed method application on a signature image sample.

iii. Figure (9) shows the application of the proposed algorithm on a certification image, in the figure it appears the resultant image slight change, the HMAC code of the two images , the icon image of the decrypted HMAC of the two images and as shown in the figure the code is not match.

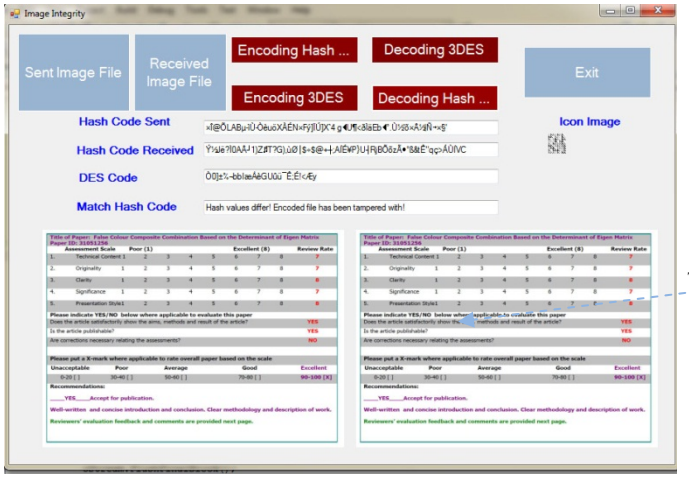


Figure (9)the proposed method application on a signature image sample.

IX. REFERENCES

[1] Che-Yen Wen,1,*Ph.D.;Kun-Ta Yang,1 M.S., 2006, "Image authentication for digital image evidence", Forensic Science Journal,Available online at:fsjournal.cpu.edu.tw.

[2] William Stallings, 2011, "CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE", FIFTH EDITION, , Prentice Hall.

[3] Thulasimani Lakshmanan1 and Madheswaran Muthusamy, 2012, "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[4] Avi Kak, 2013, "Hashing for Message Authentication Lecture Notes on "Computer and Network Security"", Lecture 15, Purdue University, April 28, 2013

[5] S. Kelly & S. Frankel , (2007),"Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec" , Network Working Group, The IETF Trust.

[6] A. Menezes, P. van Oorschot and S. Vanstone, 1996, "Handbook of Applied Cryptography", CRC Press ISBN: 0-8493-8523-7.

[7] P. D. Sheba Kezia Malarchelvi, 2013, "A Semi-Fragile Image Content Authentication Technique based on Secure Hash in Frequency Domain", International Journal of Network Security, Vol.15, No.1, Jan. 2013

[8] William Stallings, Lawrence Brown, 2012, "Computer Security: Principles and Practice" , 2nd Edition, Publisher: Prentice Hall.

[9] V.S.Bagad & I.A.Dhotre , 2008, "Cryptography And Network Security" , second revised edition, technical publication pune.

AUTHOR PROFILE

Mrs. Shahd A. R. Hasso (M Sc.) is currently a lecturer at Mosul University/ College of Computer Science and Mathematics/ Computer Science Department. She received B.Sc. degree in Computer Science from University of Mosul in 1998 and M.Sc. degree from University of Mosul in 2003. Her research interests and activity are in data security, data structures, network security, information hiding. Now, she teaches data security undergraduate students.

Security Issues on Cloud Computing

Harit Shah Sharma Shankar Anandane

Shrikanth

Abstract

The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection sphere of the data owner. Most of the discussions on these topics are mainly driven by arguments related to organisational means. This paper focuses on various security issues arising from the usage of Cloud services and especially by the rapid development of Cloud computing arena. It also discusses basic security model followed by various High Level Security threats in the industry.

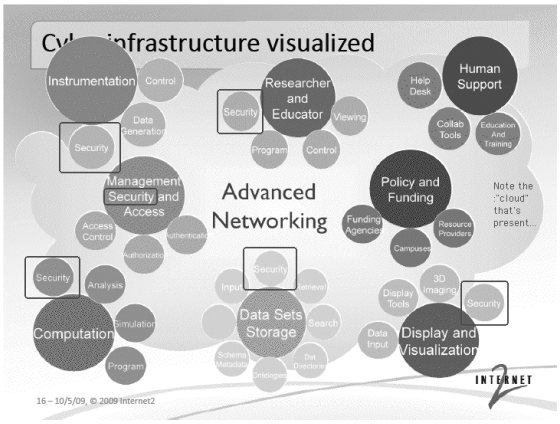
***Index Terms*—Cloud Computing, Security, Threats**

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing architecture, just like any other system, is categorized into two main sections: Front End and Back End. Front End can be end user or client or any application (i.e. web browser etc.) which is using cloud services. Back End is the network of servers with any computer program and data storage system. It is usually assumed that cloud contains infinite storage capacity for any software available in market. Cloud has different applications that are hosted on their own dedicated server farms. Cloud has centralized server administration system. Centralized server administers the system, balances client supply, adjusts demands, monitors traffic and avoids congestion. This server follows protocols, commonly known as middleware. Middleware controls the communication of cloud network among them. Cloud Architecture runs on a very important assumption, which is mostly true. The assumption is that the demand for resources is not always consistent from client to cloud. Because of this reason the servers of cloud are unable to run at their full capacity. To avoid this scenario, server virtualization technique is applied. In sever virtualization, all physical servers are virtualized and they run multiple servers with either same or different application. As one physical server acts as multiple physical servers, it curtails the need for more physical machines. As a matter of fact, data is the most important part of cloud computing; thus, data security is the top most priority in all the data operations of cloud. Here, all the data are backed up at multiple locations. This astoundingly increases the data storage to multiple times in cloud compared with a regular system. Redundancy of data is crucial, which is a must-have attribute of cloud computing.

Security of confidential data (e.g., SSN or Credit Card Numbers) is a very important area of concern as it can make way for very big problems if unauthorized users get access to it. Misuse of data can create big issues; hence, in cloud computing it is very important to be aware of data administrators and their extent of data access rights. Large organizations dealing with sensitive data often have well laid out regulatory compliance policies. However, these polices should be verified prior to engaging them in cloud computing. There is a possibility that in cloud computing network, sometimes the network utilizes resources from another country or they might not be fully protected; hence, the need arises for appropriate regulatory compliance policies. In cloud computing, it is very common to store data of multiple customers at one common location. Cloud computing should have proper techniques where data is segregated properly for data security and confidentiality. Care must be taken to ensure that one customer's data does not affect another customer's data. In addition, Cloud computing providers must be equipped with proper disaster recovery policies to deal with any unfortunate event.

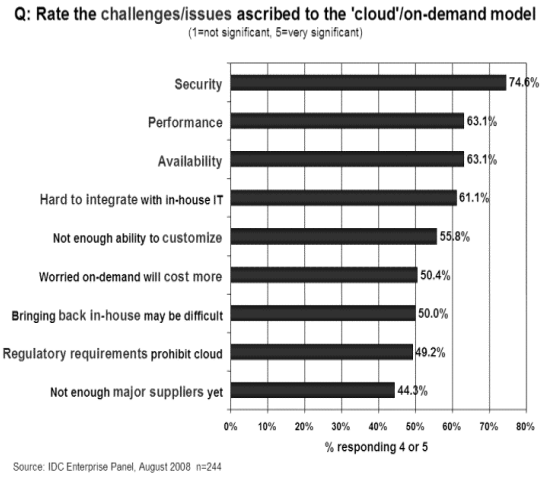
If we see architecture of the cloud computing that is used in many areas of current research and corporate world then it has Security as an important factor for selection of cloud configuration. Fig 1 shows the importance of security for various types of Clouds that are existing in current world.



[Fig. 1]

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

According to the survey carried by NIST [1], for most of the big companies security is biggest concern for migrating their product to cloud. Cloud computing has lucrative offers economically and on the technical part but they are still concerned about the security managed by cloud they will hire. Fig-2 shows the statistics of the survey.

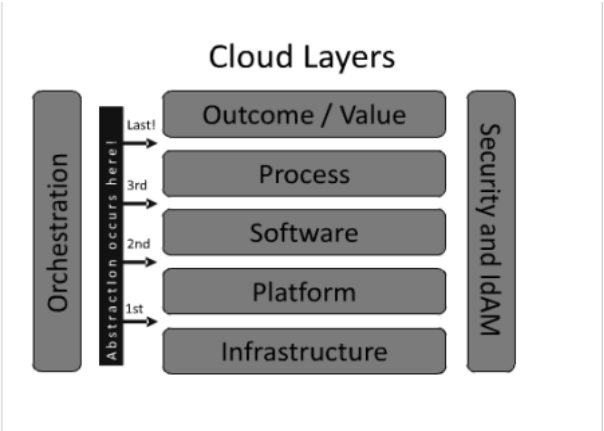


[Fig-2]

In this paper we will first discuss various aspects of security with security model that is been proposed by Jericho Forum[2], Followed by that we have discussed the CIA objectives of security related to cloud computing. In section 4 we have discussed major threats in current world by categorizing them in Computation Security, Storage Security and Network Security. Each sub-section discusses the priority, reasons for those threats, and repercussions of that threat and possible solutions that are currently accepted by the industry. In the end paper is concluding about the current severity on security issues in cloud computing.

II. Security Analysis

Basically Cloud model can be broken down in mainly three layers: 1. Infrastructure as a service (IaaS) 2. Platform as a Service (PaaS) and 3. Software as a Service (SaaS). Here security for each layer has different issues but still they can be closely combined in to one cardinal framework. Jericho Forum has proposed a model for cloud computing which integrates Security (and Identity Managers) inside the layers of the cloud computing. Fig-3 shows the pictorial view of the Cloud Computing model. For evaluating the security for any cloud there are mainly CIA objectives are to be taken in consideration. CIA analysis includes 1. Confidentiality 2. Integrity and 3. Availability. For anyone to select the cloud provider one must have to consider the CIA objectives. **Confidentiality** is one of the prime constraints for the growth of cloud computing paradigm. Users when select the Cloud provide they must be sure that the data that is given to the provider must be confidential. Provider must protect it from other users as well as must provide surety that even provider will also not peep into the data. Typically confidentiality is maintained by the encryption of the data that has been uploaded on the server of provider. But encryption has huge drawback in performance of the system.



[Fig. 3]

One other element within Confidentiality is the ability to destroy data. In a cloud, that we do not own, and on storage media that we do not control, there is high –probability that the same media be used for other purposes. These storage buckets are dynamic and the service /platform/ application provider might allocate them to other users. This sharing, and in many cases, repeated sharing, of storage media leads to the need for *assured destruction*. We must follow a strict regime that states how long is data to be kept, when and by whom destroyed, and how such destruction is verified. If we go in further detail the question of confidentiality become even more complicated. Also given problem is applicable to both storage and computation units of Cloud Computing. **Integrity** is important factor as well. Because for huge data user must be assured that whatever calculation is done by the cloud is done correctly without any minute errors. Also there should be some procedure that can assure the client that whatever data that will be stored on the file servers that will be stored without tempering any of the data. It will be in the same form and processed it without any assumption about the data. So Integrity requires two questions to be answered those are if data that is being computed is the original data and computation done on the data is error free and produces no harm effects on data or cloud models. **Availability** is most important concern for the users. They must be aware that what the availability ratio of the cloud provider is because availability of their product depends on the availability of the cloud. This is by far the most challenging issue for clouds. User has to be sure that how much of his data is available in case of corruption of existing data or what is the availability of the resources in cloud they are planning to buy. Because if it has no established recovery model or security threat solutions, then economic graph for that product will increase.

III. Computational Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. For many organizations, security of information is the most critical risk. This may be driven by a need to protect intellectual property, trade secrets, personally identifiable information, or other sensitive information. Making that sensitive information available on the Internet requires a significant investment in security

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

controls and monitoring of access to the content and the pathways to the information. The logging and auditing controls provided by some vendors are not yet as robust as the logging provided within enterprises and enterprise applications. The challenge here is to ensure that, post incident, the organization has visibility to anyone who had access to the document and what might have been done to the document (edit, download, change access, etc.). Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. While these concerns may not be absolute barriers to moving data storage and applications to the cloud environment, clearly they are significant obstacles that will require an enterprise to carefully examine its contractual obligations, risk profile, security infrastructure and oversight ability. An enterprise should be prepared to present the vendor with detailed security and legal requirements applicable to their business needs and the nature of the information being stored or transacted.

Some of the issues while processing information on the cloud are presented below.

A. Abuse and Nefarious use of Cloud Computing
B. Resource Exhaustion
C. Malicious Insider
D. Insecure Interfaces and APIs
E. Account or Service Hijacking

A. Abuse and Nefarious use of Cloud Computing

Cloud providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. The providers have traditionally suffered most from this kind of attacks; Future areas of concern include password and key cracking, DDOS[3], launching dynamic attack points, hosting malicious data, botnet command and control[4], building rainbow tables[5], and CAPTCHA solving farms[6].

Examples

Cloud providers have experienced attacks like the Zeus botnet[7], InfoStealer trojan horses and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used cloud servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of infected network addresses have been publicly blacklist.

Remediation

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

B. Resource Exhaustion

Resource Exhaustion happens when the cloud management does not properly restrict the size or amount of resources that are requested or influenced by an actor, which can be used to consume more resources than intended.

Limited resources include memory, file system storage, database connection pool entries, or CPU. If an attacker can trigger the allocation of these limited resources, but the number or size of the resources is not controlled, then the attacker could cause a denial of service that consumes all available resources. This would prevent valid users from accessing the software, and it could potentially have an impact on the surrounding environment. For example, a memory exhaustion attack against an application could slow down the application as well as its host operating system.

Resource exhaustion problems have at least two common causes:

1. Error conditions and other exceptional circumstances

2. Confusion over which part of the program is responsible for releasing the resource

Consequences

- The most common result of resource exhaustion is denial of service. The software may slow down, crash due to unhandled errors, or lock out legitimate users.
- In some cases it may be possible to force the software to "fail open" in the event of resource exhaustion. The state of the software – and possibly the security functionality - may then be compromised.

Detection Methods

Automated Static Analysis

Automated static analysis [8] typically has limited utility in recognizing resource exhaustion problems, except for program-independent system resources such as files, sockets, and processes. For system resources, automated static analysis may be able to detect circumstances in which resources are not released after they have expired. Automated analysis of configuration files may be able to detect settings that do not specify a maximum value.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Automated static analysis tools will not be appropriate for detecting exhaustion of custom resources, such as an intended security policy in which a bulletin board user is only allowed to make a limited number of posts per day.

Effectiveness: Limited

Automated Dynamic Analysis

Certain automated dynamic analysis techniques [8] may be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections. The technique may involve generating a large number of requests to the software within a short time frame.

Effectiveness: Moderate

Fuzzing

While fuzzing [9] is typically geared toward finding low-level implementation bugs, it can inadvertently find resource exhaustion problems. This can occur when the fuzzer generates a large number of test cases but does not restart the targeted software in between test cases. If an individual test case produces a crash, but it does not do so reliably, then an inability to handle resource exhaustion may be the cause.

Effectiveness: Opportunistic

Example

This code allocates a socket and forks each time it receives a new connection.

```
sock=socket(AF_INET, SOCK_STREAM, 0);
while (1)
{
newsock=accept(sock, ...);
printf("A connection has been accepted\n");
pid = fork();
}
```

The program does not track how many connections have been made, and it does not limit the number of connections. Because forking is a relatively expensive operation, an attacker would be able to cause the system to run out of CPU, processes, or memory by making a large number of connections. Alternatively, an attacker could consume all available connections, preventing others from accessing the system remotely.

C. Malicious Insider

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Impact

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider

D. Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third- parties in order to enable their agency.

Examples

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Impact

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

E. Account or Service Hijacking:

Account or service hijacking is not new. Attack methods such as phishing [10], fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Impact

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

IV. STORAGE SECURITY

Many experts in government and commerce still consider the greatest barrier to adoption of cloud services to be concerns about information security and privacy. While these risks exist across the entire cloud ecosystem, every cloud customer retains responsibility for assessing and understanding the value and sensitivity of the data they may choose to move to the cloud. As the owners of that information, cloud customers also remain accountable for decisions regarding the protection of that data wherever it may be stored. Organizations considering moving services to the cloud should keep these information security challenges in mind as they determine cloud adoption strategies:

- A growing interdependence amongst public and private sector entities and the people they serve continues to develop as government, industry, and commercial groups work to establish more widely accepted definitions of cloud computing. While those definitions and the associated standards continue to be created, one cloud requirement is clear—that platform services and hosted applications be secure and available.
- The cloud—however it is defined—is a dynamic hosting environment in which technologies and business models continue to evolve. This continuous change is a security challenge that cloud providers must address through an effective and dynamic security program.
- Sophisticated malicious attempts aimed at obtaining identities or blocking access to sensitive business data threaten to undermine the willingness of organizations to adopt cloud services. Cloud providers must prove that they have put into place and constantly evaluate the effectiveness of the technologies, controls, and processes used to mitigate such disruptions.
- In addition to these challenges, cloud providers must also address the myriad requirements related to delivering services globally online including those coming from governments, legal rulings, and industry standards.

In short, cloud service providers need to manage information security risks in a way that engenders trust with their customers—the government organizations or businesses that do provide such services to end users, as well as directly with end users.

Some of the issues while processing information on the cloud are presented below.

A. Shared Technology Issues
B. Data loss and Leakage
C. Insecure and Ineffective deletion of data

A. Shared Technology Issues:

Cloud vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor [11] mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Examples

- Joanna Rutkowska's Red [12] and Blue Pill [13] exploits
- Kortchinksy's CloudBurst presentations. [14]

Remediation

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Impact

Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were neverdesigned for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

B. Data Loss and Leakage:

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Examples

Insufficient authentication, authorization, and audit controls; inconsistent use of encryption and software keys; operational failures; persistence and remanence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.

Remediation

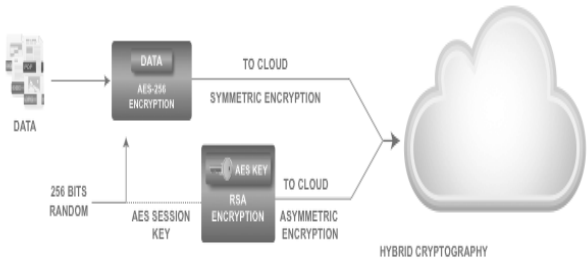
- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Impact

Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

Good Standard for Data Security

Open PGP [15] is considered as a better standard for data security. Open PGP combines symmetric and asymmetric encryption schemes to form a security model that not only protects the data but does so in a way that is practical and does not compromise the performance of the system. Symmetric encryption, where the same key is used to encrypt and decrypt, tends to be fast at encrypting lots of data. The Advanced Encryption Standard AES – 256 is a symmetric encryption scheme used by the U.S. government.



OpenPGP hybrid encryption to the cloud

The 256 indicates the size of the key in bits. Open PGP uses symmetric encryption like AES-256 to encrypt data and asymmetric encryption like RSA (Rivest-Shamir-Aldeman) to encrypt the keys used by AES-256. Asymmetric encryption simplifies key management, but is generally slower than symmetric encryption. This hybrid approach using the fast symmetric encryption to encrypt data and the slower asymmetric encryption only to encrypt the (comparatively small) keys allows data to be encrypted efficiently and a high level of granularity. Every data packet in the cloud can be protected separately with its own symmetric key and those keys can be managed together through their combined asymmetric key. This allows a practical level of control and granularity of keys and encrypted objects. The asymmetric keys can be maintained by the user in a key ring that becomes the single point of access control to the whole system.

C. Insecure or Ineffective deletion of data

Whenever a provider is changed, resources are scaled down, physical hardware is reallocated, etc, data may be available beyond the lifetime specified in the security policy. It may be impossible to carry out the procedures specified by the security policy, since full data deletion is only possible by destroying a disk, which also stores data from other clients. When a request to delete a cloud resource is made, this may not result in true wiping of the data (as with most operating systems). Where true data wiping is required, special procedures must be followed and this may not be supported by the standard API (or at all).

If effective encryption is used then the level of risk may be considered to be lower.

Remediation

Good encryption strategies
Good Timely deletion Strategies

Impact

Personal sensitive data and credentials are affected.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

V. NETWORK SECURITY

Since cloud computing uses the Internet as the communication media for providing different computing services like SaaS,PaaS, IaaS, it is vulnerable to various network security threats. This section explains various network security threats that could occur on the cloud and the possible ways of prevention/mitigation of those attacks.

The following are some of the network security threats that can cause damage on the cloud computing system.

A. Flooding attacks such as Dos and DDos
B. Data Interception attacks
C. Management Interface attacks
D. Cloud Malware attacks
E. Metadata spoofing attacks

A. *Flooding Attacks*

A major aspect of Cloud Computing consists in outsourcing basic operational tasks to a Cloud system provider [16]. Among these basic tasks, one of the most important ones is server hardware maintenance. Thus, instead of operating an own, internal data center, the paradigm of Cloud Computing enables companies (users) to *rent* server hardware on demand (IaaS). This approach provides valuable economic benefits when it comes to dynamics in server load, as for instance day-and-night cycles can be attenuated by having the data traffic of different time zones operated by the same servers. Thus, instead of buying sufficient server hardware for the high workload times, Cloud Computing enables a dynamic adaptation of hardware requirements to the actual workload occurring.
Technically, this achievement can be realized by using virtual machines deployed on arbitrary data center servers of the Cloud system. If a company's demand on computational power rises, it simply is provided with more instances of virtual machines for its services. Under security considerations, this architecture has a serious drawback. Though the feature of providing more computational power on demand is appreciated in the case of valid users, it poses severe troubles in the presence of an attacker. The corresponding threat is that of *flooding attacks*, which basically consist in an attacker sending a huge amount of nonsense requests to a certain service. As each of these requests has to be processed by the service implementation in order to determine its invalidity, this causes a certain amount of workload per attack request, which—in the case of a flood of requests—usually would cause a Denial of Service to the server hardware [16]. In the specific case of Cloud Computing systems, the impact of such a flooding attack is expected to be amplified drastically.

Direct Denial of Service

When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more VMs) more service instances...) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work *against* the attacker (by providing more computational power), but actually—to some extent—even *supports* the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all *n* servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [16].

Indirect Denial of Service Attacks

Depending on the computational power in control of the attacker, a side effect of the direct flooding attack on a Cloud service potentially consists in that other services provided on the same hardware servers may suffer from the workload caused by the flooding. Thus, if a service instance happens to run on the same server with another, flooded service instance, this may affect its own availability as well. Once the server's hardware
resources are completely exhausted by processing the flooding attack requests, obviously also the other service instances on the same hardware machine are no longer able to perform their intended tasks. Thus, the Denial of Service of the targeted service instances are likely to cause a Denial of Service on all other services deployed to the same server hardware as well.
Depending on the level of sophistication of the Cloud system, this side-effect may worsen if the Cloud system notices the lack of availability, and tries to "evacuate" the affected service instances to other servers. This results in additional workload for those other servers, and thus the flooding attack "jumps over" to another service type, and spreads throughout the whole computing Cloud. In the worst case, an adversary manages to utilize another (or the very same) Cloud Computing system for hosting his flooding attack application. In that case, the race in power would play both Cloud systems off against each other; each Cloud would provide more and more computational resources for creating, respectively fending, the flood, until one of them eventually reaches full loss of availability [16].
Examples

The following is one of the incidents of a Dos attack on Amazon cloud Posted in Enterprise Security, 5th October 2009 15:32 GMT

"DDoS attack rains down on Amazon cloud"

Web-based code hosting service Bitbucket experienced more than 19 hours of downtime over the weekend after an apparent DDoS attack (flooding of millions of UDP packets) on the sky-high compute infrastructure it rents from Amazon.com.

Remediation

- Usage of load balancers to mitigate the incoming aggregated traffic by routing the requests to different servers.
- Anycast networking concept wherein the same content is served from different physical and geographical servers.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Blackholing - Traffic to victim is redirected to a black hole(null interface, invalid server etc)
- Sinkholing using in-depth packet inspection

Remediation strategies used by Cloud Providers:-

Microsoft:-

- Microsoft applies several layers of security as appropriate to data center devices and network connections [17]
- Specialized hardware such as load balancers, firewalls, and intrusion prevention devices, is in place to manage volume-based denial of service (DoS) attacks [17].
- Through network hardware, Microsoft uses application gateway functions to perform deep packet inspection and take actions such as sending alerts based on—or blocking—suspicious network traffic[17].

Amazon:-

- Uses standard DDoS mitigation techniques such as sync cookies and connection limiting [18].
- Amazon maintains internal bandwidth which exceeds its provider-supplied Internet bandwidth.

B. *Cloud Malware Injection Attack*

A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of **Cloud malware** could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed [16].

Remediation

A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images. Thus, an attacker would be required to trick that hash value comparison in order to inject his malicious instances into the Cloud system [16]. Another approach to counter malware attack is to periodically scan the cloud systems for any suspected application such as worm/Trojan/malware etc.

Remediation strategies used by Cloud Providers:-

Amazon:-

Amazon uses HackAlert™ [20], a malware monitoring and detection software delivered as SaaS to protect the customer websites from cloud malware attack. HackAlert™ connects to the monitored website over a standard HTTP connection and captures all responses in deliberately unsecured "Honey Clients" located at Armorize data centers worldwide. All website responses are analyzed for the presence of both active malware content and suspicious links (to external sites not currently distributing malware). This distinction greatly reduces the amount of false positives.

Impact

Any malware attack could destroy the intellectual property of the cloud provider as well as the customers as their confidential data could be kept in the cloud system. Usually a malware attack attempts to retrieve the user credential information and use the same to retrieve critical information from the system. This type of attack could degrade the reputation and trust of the cloud provider.

Examples

"MALWARE ATTACK USES CHINA WORLD EXPO GUISE" [19]

Posted by Owen Fletcher March 25, 2010 06:12 AM ET

A malware attack dressed up as an e-mail from organizers of the upcoming Shanghai World Expo targeted at least three foreign journalists in China, in the latest sign of increasingly sophisticated cyber attacks from the country.
The e-mail appeared to be sent from the inbox of the Expo news office, but it was not sent by the Expo and may be targeting journalists who signed up to cover the event

C. *Data Interception Attack*

Cloud computing, being a distributed architecture, implies more data in transit than traditional infrastructures. For example, data must be transferred in order to synchronise multiple distributed machine images, images distributed across multiple physical machines, between cloud infrastructure and remote web clients, etc. Furthermore, most use of data-centre hosting is implemented using a secure VPN-like connection environment, a practice not always followed in the cloud context. Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources. Moreover, in some cases the Cloud Provider does not offer a confidentiality or non-disclosure clause or these clauses are not sufficient to guarantee respect for the protection of the customer's secret information and 'know-how' that will circulate in the 'cloud' [21].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Types of Data Interception Attacks

Sniffing
This attack involves sniffing and manipulating packets flowing through the cloud network or between web browser and the cloud system.

Spoofing
This kind of interception is done by sending illegitimate connection requests and messages from invalid sources. The scatter effect produced are utilized to produce further attacks on the cloud.

Man-In-The-Middle (MITM) attacks
This kind of attack involves interception of traffic by being in the middle of the traffic flowing between the cloud and the intended recipient. Spoofed data is sent to both the endpoints.

Side Channel Attack
This kind of attack involves using timing information, power consumption, electromagnetic leaks or even sound to break the system.

Possible Threat sources
AAA (Authentication, Authorization, Accounting) Vulnerability

A poor system for authentication, authorization and accounting, could facilitate unauthorized access to resources, privileges escalation, impossibility of tracking the misuse of resources and security incidents in general, etc, through:

- Insecure storage of cloud access credentials by customer
- Insufficient roles available
- Credentials stored on a transitory machine.

Furthermore, the cloud makes password based authentication attacks (trend of fraudster using a Trojan to steal corporate passwords) much more impactful since corporate applications are now exposed on the Internet. Therefore password-based authentication will become insufficient and a need for stronger or two-factor authentication for accessing cloud resources will be necessary [21].

Communication Encryption vulnerabilities
These vulnerabilities concern the possibility of reading data in transit via, for example, MITM attacks, poor authentication, acceptance of self-signed certificates, etc [21].

Weak Encryption of archives and data in Transit

Failure to encrypt data in transit, data held in archives and databases, un-mounted virtual machine images, forensic images and data, sensitive logs and other data at rest puts the data at risk. Of course the costs of implementing key management and processing costs must be taking account and set against the business risk introduced [21].

Remediation

The strategy to counter date interception attacks is to

- Have a strong AAA system which does not expose any vulnerability for unauthorized access/unclear role definitions.
- Have a strong encryption scheme for the data and control traffic between the cloud systems as well as between the customer and the cloud provider.

D. Management Interface Attack

The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities. This includes customer interfaces controlling a number of virtual machines and, most importantly, Cloud Provider interfaces controlling the operation of the overall cloud system. Of course, this risk may be mitigated by more investment in security by providers [21].

Threat Sources

One of the sources for the management interface attack is the AAA vulnerability. Lack of or inefficient challenge response system during the authentication through remote clients could cause attack on the management interfaces.
Another possible source of this attack could be misconfiguration of specific key parameters of the cloud system. This could be due to:

- Inadequate application of security baseline
- Invalid or incorrect implementation of hardening procedures
- Human error and untrained administrator

Misconfiguration or a known OS or System vulnerability could also cause a management interface attack. For example conflicting patching procedures used between the customer and the cloud provider could result in misconfiguration of the cloud system.

Remediation
Management interfaces should be exposed in the form of a secure channel. Instead of the password based authentication, it should use two-factor authentication. Periodic and efficient OS and hardware hardening procedures should be followed on the cloud system.

VI. CONCLUSION

Cloud computing is the next big wave in computing. It has many benefits, such as better hardware management, since all the computers are the same and run the same hardware. It also provides for better and easier management of data security, since all the data is located on a central server, so administrators can control who has and doesn't have access to the files. It is widely accepted today because of its economic benefits.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

There are some down sides as well to cloud computing. Out of those down falls one of the major factors is security. User will have to evaluate the security model that is been used by Cloud Provider makes lot of impact on taking the decision of the selecting the cloud provider. Also for Cloud Computing there is more number of threats than compare to security of single PC because clouds have many elements than single PC.

VII. REFERENCES

[1]http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt at slide 17.

[2]http://arielsilverstone.com/category/cloud-computing-security/

[3]Denail of Service, http://en.wikipedia.org/wiki/Denial-of-service_attack

[4] M. Bailey, J. Oberheide, J. Andersen, M. Mao, F. Jahanian, and J. Nazario. "Automated classification and analysis of internet malware", In Proceedings of Recent Advances in Intrusion Detection (RAID'07), 2007.

[5]Rainbow Tables, http://en.wikipedia.org/wiki/Rainbow_table

[6] A. Kolupaev and J. Ogijenko. "Captchas: Humans vs. bots." IEEE Security and Privacy, 6(1):68–70, 2008.

[7]Zeus Botnet, http://en.wikipedia.org/wiki/Zeus_(trojan_horse)

[8] M. D. Ernst. "Static and Dynamic Analysis: Synergy and Duality", In Proceedings of the Program Analysis for Software Tools and Engineering (PASTE 2004) Workshop, pp. 24–27, June 2004.

[9] Peter Oehlert. "Violating Assumptions with Fuzzing", IEEE Security & Privacy, pp. 58-62, March/April 2005.

[10] T. Moore and R. Clayton. "Examining the impact of website take-down on phishing", In Anti-Phishing Working Group eCrime Researcher's Summit (APWG eCrime), pp. 1–13, ACM Press, New York, 2007.

[11] Hypervisor, http://en.wikipedia.org/wiki/Hypervisor

[12] RedPill and its uses, http://en.wikipedia.org/wiki/Red_pill#Other_uses

[13] Blue Pill, http://en.wikipedia.org/wiki/Blue_Pill_(malware)

[14] Kostya Kortchinsky. "Cloud Burst :A VMware Guest to Host Escape Story". BlackHat USA, Las Vegas, 2009.

[15] OpenPGP, http://www.ietf.org/rfc/rfc2440.txt

[16] On Technical Security Issues in Cloud Computing By Meiko Jensen, J¨org Schwenk and Nils Gruschka, Luigi Lo Iacono

[17] Securing Microsoft's Cloud Infrastructure - http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf

[18] Amazon Web Services: Overview of Security Processes - http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf

[19] Malware Attack - http://www.computerworld.com/s/article/9174100/Malware_attack_uses_China_World_Expo_guise

[20]Amazon uses HackAlert™ - http://malware-info.com/mal_faq_hackalert.html

[21] Cloud Computing - Benefits, risks and recommendations for information security November 09 By ENISA

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Extraction of Pupil Region from Iris Image Using a Scheme Based On Gamma Transform and Contrast Stretching

Suhad A. Ali
Dept. of Computer Science
Babylon University
Babylon/ Iraq

Dr. Loay E. George
Dept. of Computer Science
Baghdad University
Baghdad/ Iraq

***Abstract*—Iris region extraction is almost the most challenging part in iris recognition system. The correctness of iris segment allocation is affected by the pupil localization accuracy. In this paper, a new method is developed for pupil region detection using a combination of gamma transform and contrast enhancement techniques. The proposed method is tested on 2639 iris images from CASIA v4.0 database (Interval class). The results prove the efficiency of the proposed method.**

Keywords-Gammas transform, Iris segmentation, Seed filling, Enhancement techniques.

i. INTRODUCTION

Among the physiological biometrics, iris is an important feature of human body due to its accuracy, reliability and speed. It is encircled by two concentric circles. The inner boundary is the junction of the iris and pupil, which is defined by the gray scale change and the border. The outer boundary is the junction between iris and sclera; which is characterized by smooth gray scale change and little vogue border [1]. Many algorithms was developed for both pupil and iris localization. The earliest one was proposed by Daugman [2] who become the inventor of most commercial iris systems. He made use of differential operator for locating the circular iris and pupil regions, along with removing the possible eyelid noises [3].Wildes [4] proposed an iris segmentation method through using edge detection followed by Hough transform to locate iris boundaries. Much of the subsequent work on iris localization was built on this basic approach. Wildes et al [5] have made use of parabolic Hough transform to detect the eyelid, approximating the upper and lower eyelid with parabolic arc. Hung et al [6] investigated the implementation of iris localization on downscale eye image to reduce search space. Yahya and Nordin [7] referred that iris boundaries are not exactly circles. They applied direct least square fitting of ellipse to detect the inner boundaries of iris, then, they used Hough transform to detect the outer boundaries of iris. Ling and Brito [8] proposed an algorithm to speed up the segmentation process and to have accurate result. Accurate pupil features detection is still a challenging problem. Most of the above methods are based on edge detection and finding the pupil and iris boundaries upon using circular edge detector or Hough transform, which involves two drawbacks. First, the quantity of data needed to calculate is very large resulting in low speed. Secondly, they require threshold values to be chosen for edge detection and this may cause critical edge points being removed, resulting in failure to detect circles [9]. Besides, most of these methods used static threshold which cannot handle several issues that founded and overlap with pupil region such as eyelash, specular highlights on pupil which, adds noise to input iris image. In this paper, a pupil localization technique is proposed using combinations of Gamma transform with some other image processing operations (i.e., intensity thresholding, image equalization, smoothing, and seed filling operations). The combination of gamma transform and contrast stretching techniques is used to locate the four pupil points (i.e., top, bottom, left, right), so it does not need to find all pupils' boundary points which made its localization is fast. The conducted experiments showed that the proposed method achieves very promising segmentation results (i.e., 0.988%) for the iris images of CASIA V4.0 databases.

ii. PROPOSED METHOD

The eye image will pass through many processing steps in order to localize the iris region. The block diagram of the introduced iris segmentation is shown in figure (1).

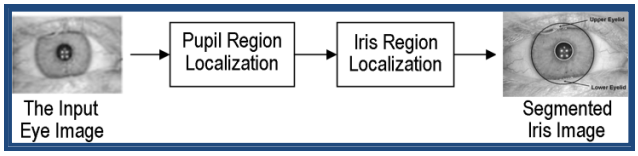


Figure 1. Block Diagram of Iris Localization

The pupil region localization is the first step in iris segmentation, which will be concerned in this paper.

A. Detection of Pupil Region

In order to detect the inner circle of iris, the image intensity behavior in both pupil/eye is taken into consideration. The overall intensity value in pupil area is relatively smaller

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

than its value in other regions of the whole eye image, beside to that pupil represents the largest connected and packed dark area will appear in the eye image. So, to get the benefit of these attributes the following steps were applied:

Step-1(Find a Seed Point): This stage consists of two steps

Step1-1(Image Integration): In order to remove the effect of eye image artifacts, smoothing the eye image is produced by applying 21x21 mean filter.

Step1-2(Select a Seed Point):A seed point in the pupil region (i.e., a pixel that shows lowest gray value) corresponds to the minimum pixel value of the image produced from previous step. Sometimes the eye image may contain dark, thick eyebrows, so to prevent the pixels belong to these regions from being detected as seed point the pixels belong the first 20% rows and the last 20% rows of eye image are excluded from seed point scanning domain. Also, the pixels belong to the first 20% columns and last 20% columns are excluded.

Step-2(Convert to Binary): In order to detect the pupil region, the eye image is converted to binary. The proposed method implies two steps to get the binary image:

Step2-1(Image Enhancement): Contrast stretching is applied again on the original eye image. The stretching is done by the applying following steps:

a. Compute the mean (m) and standard deviation (σ) of the eye image.

b. Determine the Low and High values according to the following equations:

$$\begin{aligned} Low &= m - \alpha \times \sigma \\ High &= m + \alpha \times \sigma \end{aligned} \qquad (1)$$

Where, α is the scaling factor whose value is within the range [1..3].

c. Then, the contrast stretching is done by applying the following mapping equation:

$$E(x,y) = \begin{cases} 0 & Img(x,y) \le Low \\ 255 \times \dfrac{Img(x,y) - Low}{High - Low} & \text{if } Low < Img(x,y) < High \\ 255 & Img(x,y) \ge High \end{cases} \qquad (2)$$

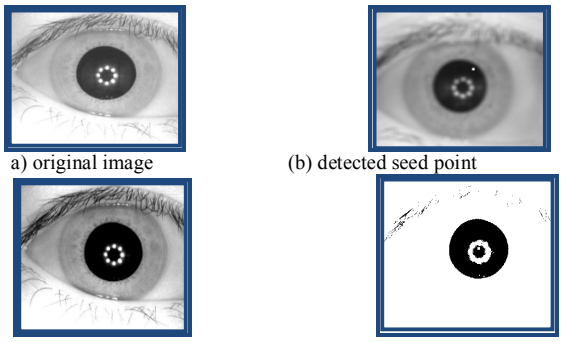
Where, E(x, y) is the enhanced image, Img(x, y) is the original image.

Setting the scaling factor (α) equal 2, for all images in databases, will made the pupil region more dark as shown in figure (2).

Step2-2(Gamma Transform): To guarantee accurate conversion of eye image a binary image; the gamma transform is applied on the enhanced image using the following:

$$G(x,y) = 255 \times \text{round}\left(\left(\frac{I(x,y)}{255} \right)^{\alpha} \right) \qquad (3)$$

Where, G(x,y) is gamma image, I(x,y) is input image, and α is gamma factor. The value of α determines the process type on the image. When α <1 the gamma image is darken the image, and for α >1 the gamma image is brighten the image. So, we have choose α =0.3 to convert all iris images in database to binary.



a) original image (b) detected seed point

c) histogram stretching with α =2 (d) binary image using gamma transform

Figure 2. Binary Iris Image

Step3 (Reflection Points Removing): As shown from figure (2-a) the pupil region of CASIA V4.0 contains approximately eight white points distributed in pupil region. In order to remove reflection gamma transform will used to detect the locations of these points by using gamma scaling factor α =100. The detected points will be converting to black color in binary image that obtain from figure (2-d).

Step4 (Collect the Whole Black Round Area): The pupil region represents the largest connected and packed dark area will appear in the eye image. So, the seed filling algorithm is applied using the selected seed point that found in step1-2. The first step in this algorithm is to save the seed point coordinates into temporary point array type, and then start checking its 4-neighboors, if any of the four tested points is found white then register it in the temporary array and convert the value of the detected white point to black.

Step5 (Compute Pupil Center): The pupil center (x_p, y_p) is computed by taking the average of points in pupil region in x-axis and y-axis directions according to the following equations:

$$xp = \frac{\sum_{i=1}^{n} x_i}{N} \qquad yp = \frac{\sum_{i=1}^{n} y_i}{N} \qquad (4)$$

Where N is the number of points in pupil regions.

Step6 (Compute Pupil Radius): From the point (x_p, y_p), we move in all four directions and find the first background pixel in each direction. Let x_l be the first background pixel to the left and x_r be the first background pixel to the right. Radius is compute in horizontal R_h as follow

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$R_h = \frac{1}{2}(x_l - x_r) \qquad (5)$$

Let xb, xt be the first background pixels to the bottom and top respectively. Radius is computed in vertical Rv as follow

$$R_v = \frac{1}{2}(x_t - x_b) \qquad (6)$$

Then, the pupil radius Rp is computed using the following formula

$$R_p = \frac{1}{2}(R_h + R_v) \qquad (7)$$

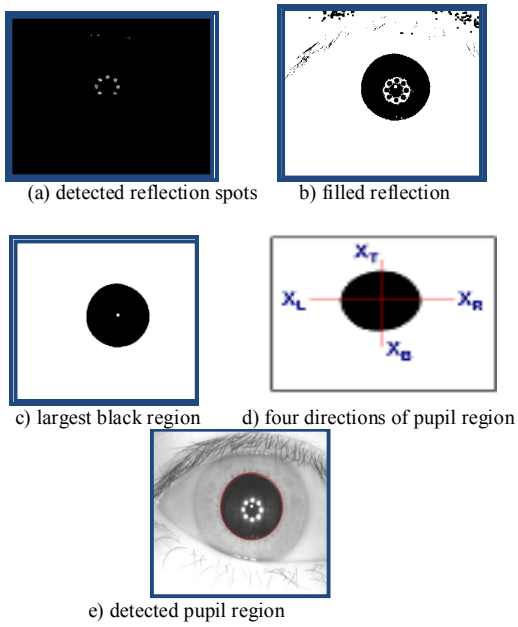


Figure 3. Pupil detection steps

iii. Experimental Result

The proposed system was evaluated on all iris images from CASIA V4.0 Interval class database [10]. In CASIA V4.0, there are 2,639 iris images belong to 359 different subjects. The size of the iris image is 320×280 pixels. Figure (4) shows the obtained results after applying the proposed method. In the first stage, a seed point is taken from the pupil region, this point detected (100%) correctly for all images. In the second stage, the iris image is converted to binary using equalization and gamma transform. The third stage which concerned by finding correct pupil parameters (yp, xp, Rp), the accuracy rate was 0.988%.

iv. Conclusion

A new method is developed for pupil region detection using a combination of gamma transform and contrast enhancement techniques. From the obtained results we conclude:

- As shown from figure(2-c) equalization process made pupil region more darkness and reflection points more brightness. This step will be very effective in detection process.
- Also, using combination of gamma transform and histogram enhancement techniques is very effective especially for images contain eyelash which represent one of the many noise problems found in eye image.
- Pupil region can be effectively detected by finding only four points (x_r, x_l, x_t, x_b) which make the detection process more faster.

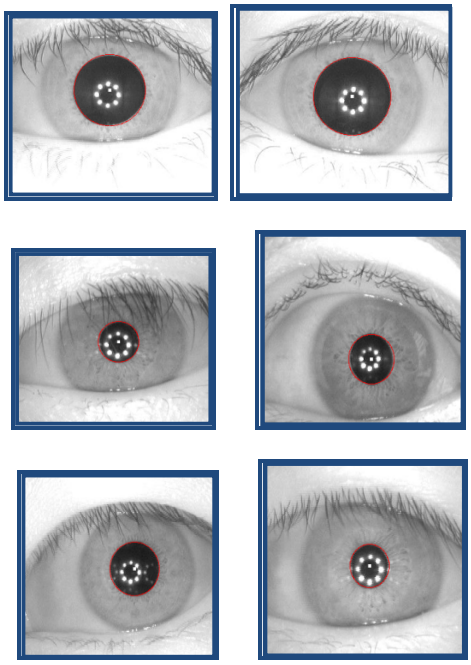


Figure 4. Pupil localization using proposed method

References

[1] Surjeet Singh, Kulbir Singh, "Segmentation Techniques for Iris Recognition System", International Journal of Scientific & Engineering Research Vol. 2, Issue 4, pp. 1-8, April-2011.

[2] J. Daugman, "High Confidence Visual Recognition of Person by a Test of Statistical Independence", IEEE Transaction on Pattern Analysis and Machine Intelligence, No 11, pp. 1148-1161, November- 1993.

[3] J. Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition", Pattern Recognition, Vol. 36, No. 2, pp. 279-291, 2003.

[4] R. Wildes, "Iris Recognition: An emerging Biometric Technology", Proceeding of the IEEE, Vol. 85, No. 9, pp. 1348-1363, September-1997.

[5] R. Wildes, J. Asmth, S. Hsu, R. Kolczynski, J. Matey, S. Mcbride, "Automated, Noninvasive Iris Recognition System and Method", Proceedings of the IEEE, Vol. 85, No. 9, pp. 1348-1363, September-1997.

[6] Y.P. Hung, S.W. Luo, and E.Y. Chen, "An Efficient Iris Recognition System", Machine Learning Conference and Cybernetics, Vol. 1, 2002.

[7] A.E. Yahya, M.J. Nordin, "A New Technique for Iris Localization", International Science Conference Computer Science, pp. 828-833, 2008.

[8] L.L. Ling, and D.F. Brito, "Fast and Efficient Iris Image Segmentation", Journal of Medical and Biological Engineering, Vol. 30, No. 6, pp. 381-392, September- 2010.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[9] G.J. Mohammed, B. Hong, A.A. Jarjes, "Accurate Pupil Features Extraction Based on New Projection Function", Vol. 29, pp.663-680, 2010.
[10] Center for Biometrics and Security Research, CASIA iris image database http://www.cbsr.ia.ac.cn/irisdatabase.

AUTHORS PROFILE

Suhad A. Ali has received his BS (Computer Science) degree from University of Babylon in 1998.Completed his Master Degree from computer science College, University of Babylon. She is PhD Research Scholar and working as Assistant Professor in Computer Science department of science college for woman, Babylon University, Babylon, Iraq. His areas of interests are Image Processing, Pattern Recognition.

Dr. Loay E. George received his PhD degree from Baghdad University , Iraq in 1997. Thesis title is "New Coding Methods For Compressing Remotely Sensed Images". He is a member of Arab Union of Physics and Mathematics, and the Iraqi Association for Computers. Now, he is the Head of Computer Science Department, Baghdad University.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Quadrate Design of Linear System for Color Image Encryption

Ashwaq T. Hashem
Computer Science Department
Babylon University
Hilla, Iraq

Dr. Loay E. George
Computer Science Department
Baghdad University
Baghdad, Iraq

***Abstract*— Nowadays the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. This paper attempts to design a simple and safer cryptographic algorithm. It is a new secret-key block cipher using type-3 Feistel network. The original image has been divided into 4×4 pixels blocks, which were rearranged into a permuted image using a linear system in quadrate design with mixing of operation from different algebraic group. The test results confirmed its security; which are shown in terms of statistical analysis using histograms, entropy and correlation. The test results showed that the correlation between image elements has been significantly decreased, and the entropy has been very close to the ideal value.**

Keywords-: Image encryption, Linear system, quadrate design, type-3 Feistal network.

I. Introduction

All Currently, with the increasing growth of multimedia applications, information security is becoming more important in data storage and transmission. Different types of data demand different aspects, and so many different techniques should be used to protect confidential image data from unauthorized access. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

The security of digital images has become more significant with the rapid progress of the Internet. Numerous image encryption methods have been proposed to improve the security of the images. The image encryption algorithms can be classified into three major groups:

(i) Position permutation based algorithm: Position permutation means rearranging elements in the plain image. In 2001, Chin-Chen and et al. [1] proposed encryption method based on vector quantization, which is one of the popular image compression techniques. It has achieved the following two goals. One goal is to design a high security image cryptosystem. The other goal is to reduce computational complexity of the encryption and decryption algorithms. Mitra and et al. [2], in 2006, have used a random combinational of bit, pixel, and block permutations. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security.

(ii) Substitution (Value transformation) based algorithm: Substitution maps each element in the plain-image into another element. Yen and Guo [3], in 2000, proposed a chaotic key based algorithm (CKBA) to change the pixel values of the plain-image. This algorithm relies on a one-dimensional chaotic map for generating a pseudo random key sequence. The encryption procedure of CKBA is applied by selecting two bytes key_1 and key_2 (8 bits) and the initial condition of a one-dimensional chaotic system as the secret keys of the encryption system. Guan and et al [4], in 2005, presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher-image and the plain-image. The Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. Then the discrete output signal of the Chen's chaotic system has been preprocessed to be suitable for the grayscale image encryption, and the shuffled image is encrypted by the preprocessed signal pixel by pixel. Musheer and et al [5], in 2009, proposed a new image encryption algorithm based on three different chaotic maps. In the proposed algorithm, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

carried out using 2D Cat map. Further, the control parameters of shuffling are randomly generated by employing 2D Coupled Logistic map. After that the shuffled image is encrypted using chaotic sequence generated by one dimensional Logistic map.

(iii) visual transformation based algorithm: Kamali and et al [18], in 2010, proposed a new modified version of Advance Encryption Standard based algorithm for image encryption. In [18] a modification to the Advanced Encryption Standard (MAES) has been presented to provide a high level security and better image encryption. The mentioned result was higher than that of original AES encryption algorithm. These methods range from light encryption (degradation), to strong encryption algorithms.

Nowadays, there are so many algorithms available to protect image from unauthorized. Zeghid and et al [7], in 2007, analyzed the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance. Mohammad and Aman [8], in 2008, introduced a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Kumar and el al [9], in 2008, presented an image encryption technique using the Hill cipher. It generates self-invertible matrix for Hill Cipher algorithm. Using this key based matrix the gray scale as well as color images are encrypted. Their algorithm works well for all types of gray scale as well as color images except for the images with background of same gray level or same colur. Abdel fatah and Yahya [10], in 2008, proposed a new algorithm, called the Shuffle Encryption Algorithm (SEA), which applies nonlinear s-box byte substitution. Then, it performs shuffling operation that partially dependent on the input data and uses the given key. In 2011, Pallavi and Avadhani [11] proposed a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. In 2011, Rathod and el al [12] introduced a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image the binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm (HIEA)" algorithm. Nithin and el al [13], in 2013, proposed Fast Encryption Algorithm (FEAL) as an encryption/decryption strategy for gray scale images. FEAL works almost similar to Data Encryption Standard (DES) algorithm, but it is faster than DES. To encrypt the images, the input image is partitioned into 16x16 blocks of information. Encryption/ Decryption are carried out using 12 keys, each of length 16-bits. In 2013, Paree and el al [14] proposed an encryption algorithm for gray images using a secret key of 128-bits size. The visual quality of retrieved image is degraded by the mixing process. Resultant image is partitioned into key dependent dynamic blocks and, further, these blocks are passed through key dependent diffusion and substitution processes. Total sixteen rounds are used in the encryption algorithm.

II. The Proposed Algorithm Design

It is a new secret-key block cipher using type-3 Feistel network. In the encryption process of the proposed algorithm, the original image is divided into 4×4 pixels blocks, which were rearranged into a permuted image using a permutation process of linear system in quadrate design and combination of operations from different algebraic group. The proposed algorithm is designed to use a full menu of "strong operations" supported in modern computers to achieve better security properties, high speed, and implementation flexibility. The primitive operations that used in proposed algorithm are: add, multiply, and exclusive-OR, rotate right, and rotate left.

The way that ensures the key is long enough, to ensure a particular security level, is to design an algorithm with so many keys so that attacks that reduce the effective key length by several bits become irrelevant. The range of values, which a key will take, became large. A large key space is necessary to prevent exhaustive search for a key (i.e., solving the problem of finding the correct value for a key by testing possible values until the correct One is found) [15]. The proposed algorithm uses key with length 40 bytes (320 bits) (i.e. 24 bytes for Quadrate function, 6 bytes for E function and 8 bytes (40-bits) for Permutation function).

The block diagram of the proposed algorithm is shown figure (1).

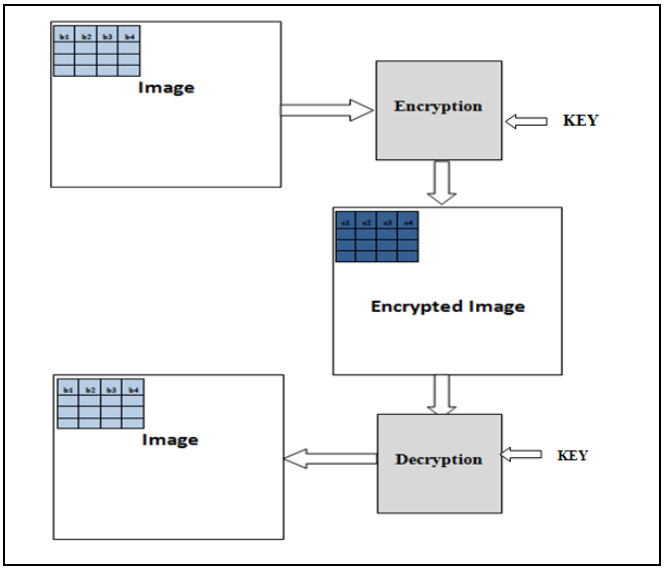


Figure 1. Block Diagram of Proposed Algorithm

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Image data have strong correlations among adjacent pixels; which in turn have formed intelligible information. By decreasing the correlation among the adjacent pixels the intelligible information among will reduced. The proposed encryption algorithm does this by modifying the pixel values of the image as well as reshuffling the pixels of the resultant image within itself. In figure (2), the functions used in the proposed algorithm are shown.

The encrypted image is divided into blocks starting from top to bottom. The first block is entered to the decryption function and the same encryption key is used or decryption. The process of decryption is continued with other blocks of the image from top to bottom**.**

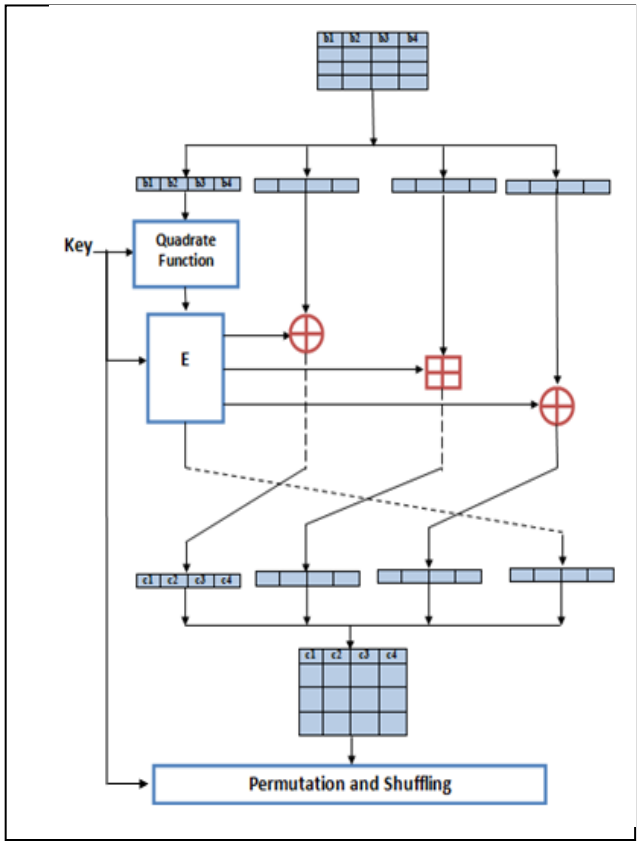


Fig.ure 2. The Proposed Algorithm

A. Quadrate Function

The core of the proposed cipher is quadrate function as shown in figure (3). For encryption, algorithm takes four successive pixels and construct 12 linear equations, 2 for each F_i function where i=1,..,6. The quadrate function steps are described below as follows:

Step1: The input is 4 pixels (i.e. b_1, b_2, b_3, b4) and a key of length 24 bytes (i.e., k_1, k_2,...., k_{24}).

Step2: The quadrate function consists of six F_i functions, where i=1,..6, and each of function has two inputs and two outputs, where: for each pair of pixels (b_1 and b_2) and four bytes sub-key (k_1, k_2, k_3 and k_4 calculate C_1 and C_2. The linear system, which is described in next section, such as following:

$$C_1 = (k_1 b_1 + k_2 b_2)\ mod\ 256\ ,.....(1)$$

$$C_2 = (k_3 b_3 + k_4 b_4)\ mod\ 256\ ,.....(2)$$

Step3: Fed the result for each Fi function to another two functions.

Step4: The output of Quadrate function is the set of encrypted pixels c_1, c_2, c_3, and c_4.

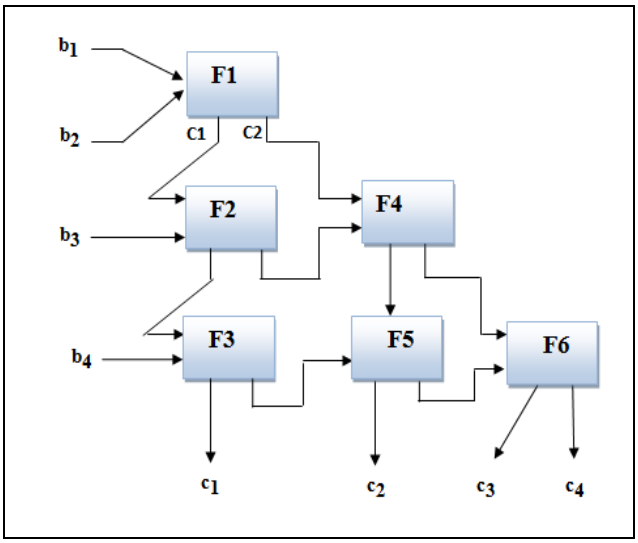


Figure 3. Proposed Quadrate Function

B. The Proposed Linear System

For a block of image data $\{V_j | j=1..q\}$, the i^{th} cipher value is computed using the following linear equation:

$$CV_i = \sum_{j=1}^{q} a_{ij} V_j \quad ,.....(3)$$

Where, CV_i is the i^{th} generated cipher value for the block $V()$, a_{ij} is the j^{th} key belong to the linear equation representing the i^{th} F function. So in case of collecting q cipher values (i.e., $\{CV_k | k=1...q\}$), then the inverse matrix of $A=\{a_{ij} | i,j=1...q\}$ could be used to retrieve the exact values of V(), that is:

$$\mathbf{V} = \mathbf{A}^{-1}\mathbf{Sh} \quad ,.....(4)$$

The proposed method work is divided into the cipher phase and the decipher phase. Details about the two phases of our proposed algorithm are described below.

Beside to utilization of linear equation the Modula algebra is used to overcome the size increase of the overall cipher size. So, instead of equation (1) the adopted share generation equation is:

$$S_i = \sum_{j=1}^{q} \left(a_{ij} V_j\right) mod 256 \quad ,.....(5)$$

Where, $i=1...n$ and $j=1..q$. According to equation (3), the range of cipher values S_i is [0..255]. The above equation could be rewritten as in the following form:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$\sum_{j=1}^{q} a_{ij} V_j = S_i + 256\, p_i \quad \text{.....(6)}$$

Where, p_i is an integer number its value will not registered as a part of cipher values, and during the retrieval stage their values will be compensated according to certain integer division based rules.

The decipher phase is the inverse coding process of the encryption phase. In this phase q cipher values, taken from the cipher image, are collected for decryption. These q cipher values are used to construct q simultaneous linear equations set and thereby the secret bytes $\{V_j | j=1,2,...q\}$ can be obtained by solving these linear equations set.

Since the proposed system uses Modula algebra with base 256 to reduce the range of the generated shares and keep them within the range [0, 255], so the algebra needed to recover of secret bytes $\{V()\}$ should take into consideration the imposed range restriction of the cipher value. The following steps have been adopted for the recovery process:

Step1: Take the consequence cipher values whose corresponding indexes are $\{n_1, n_2,..., n_q\}$; such that only one secret byte value is taken from any chosen cipher values(i.e., $\{S_{n_m} | m=1,2,...q\}$).

Step2: Construct the coefficients matrix, $A'()$, of the corresponding linear equations, that is

$$a'_{mk} = a_{n_m k} \quad \text{.....(7)}$$

Where, $a'_{mk} \in A'$, $a_{n_m k} \in A$, $m=1, 2,.., q$ and $k=1, 2, ..., q$.

Step3: Determine the determinant value of A (i.e., $D=det(A)$), and the corresponding complementary matrix C; such that for all values of j (i.e., $j \in [1,q]$) the following condition is satisfied:

$$\sum_{i=1}^{q} a_{ij} C_{ij} = \sum_{j=1}^{q} a_{ij} C_{ij} = D \quad \text{.....(8)}$$

Here, the matrix element C_{ij} is equal to the determinant of the reduced matrix C (whose i^{th} row and j^{th} column are removed) multiplied by the factor $(-1)^{i+j}$.

Step4: The values of the retrieved secret bytes $\{V'_j | j=1...q\}$ could be determined using:

$$V'_j = \frac{1}{D}\left\{\left(\sum_{i=1}^{q} C_{ij} S_{n_i}\right) + w_j\right\} \quad \text{.....(9)}$$

Where, w_j is an integer number its value is multiples of 256, such that:

$$w_j = 256 \sum_{i=1}^{q} C_{ij}\, p_i \quad \text{.....(10)}$$

According to the above equations for cipher values generation $\{S()\}$ and the secret bytes retrieval $\{V()\}$, the following two remarks are taken into consideration:

(a) The value of D should always kept non zero to ensure the applicability of equation (9); so, the generation process of all key matrix coefficients (i.e., $a_{ij} \in A | i=1..n, j=1..q$) should take into consideration that any combination (q**x**q) of a's coefficients should not lead to zero.

(b) Since the values of p's (see equation 6), will not registered as part of the share data, so the values of w's could not be determined directly from equation 10. To handle this problem the exhaustive test for the all possible values of w_j ($j \in [1,q]$), as multiples of 256, are tried. Here, the correct set of w_j values is selected when all values of the retrieved $\{V'_j | j=1...q\}$ are integer. In other words; the values of all numerators of equation (9) that are multiples of the denominator (i.e., D) value are considered during the test.

C. The Extended E Function

Diffusion requirement on cipher is that each plaintext bit should influence every ciphertext bit and each key bit should influence every ciphertext [16]. Diffusion is provided by the transformation called E function. The structure of E function is shown in figure (4). It has been transformed four bytes (pixels) data controlled by six more key bytes to produce three four output bytes.

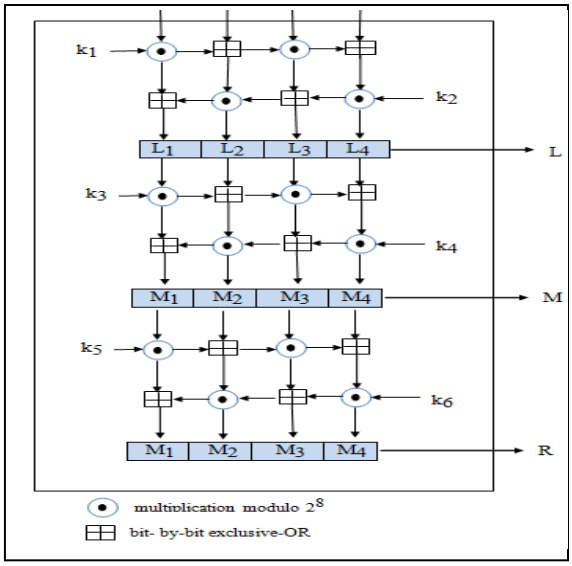


Figure. 4 Proposed Extended E Function

In this process, bitwise operations are performed on pixels of sub-blocks to change their properties. In this function three temporary four bytes has been used, denoted below by L, M and R (for left, middle and right).

D. Proposed Permutation and Shuffling Function

In the proposed algorithm more complicated reversible mixing permutation function is used. It has been required to

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

provide the necessary diffusion and confusion to the output block, where it's key dependent permutation such that additive differences have been destroyed as the key change as shown in figure (5). Proposed permutation function has 4×4 input block A and 4×4 input block output D. It Adopts "byte transposition" and the 40-bits subkey $(KP_1|\ KP_2)$ to control data rotations.

Let $KP_1=(m_1, m_2, m_3, m_4)$, and $KP_2=(n_1,n_2, n_3, n_4)$, where m_j and n_j are 5-bit subkeys, and each not equal to zero, j=1,…, 4. The function $D=P(A, KP_1|KP_2)$ is defined by following:

- Right rotation: Concatenation each row of input block to four long numbers (aj where j=1, ..., 4) then $b_j= a_j >>> m_j$, for j=1,…,4.
- Byte transposition: $c_{jl}=b_{lj}$, for j, l=1,...,4.
- Left rotation: Concatenation each row of the output block from byte transposition to four long numbers $d_j=c_j<<<n_j$, for j=1,…,4.

The proposed permutation function consists of a number of permutations using rotation and transposition operations. The generated group of rotation operations is isomorphic to cyclic group of order n. The number of permutations, which are generated by transposition, is equal to n! [2].

In the proposed shuffling function the elements (i.e., bytes) of the each output from proposed permutation function cipher block are stored in row order, from left to right, along each row representing one scan line of the image. This process is continued till the all plain image bytes are encrypted. Figure (6) illustrates the proposed byte shuffling method.

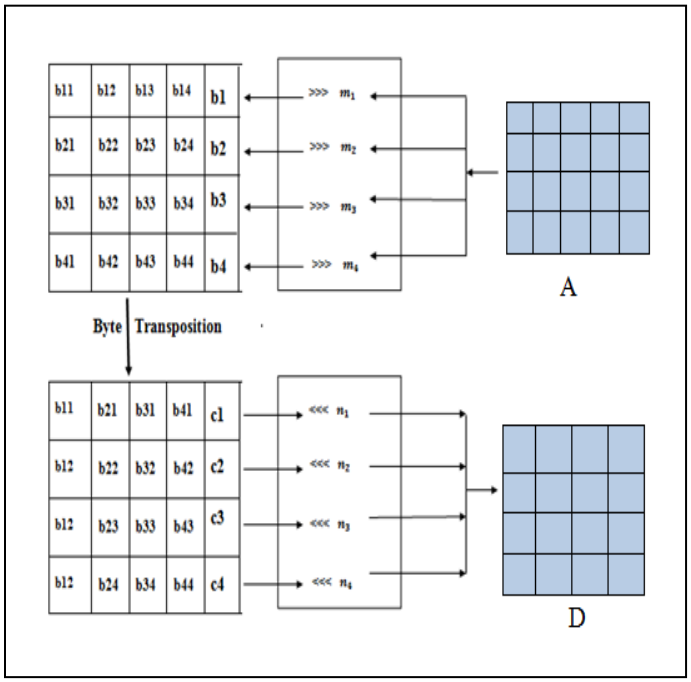


Figure. 5 Proposed Permutation Function

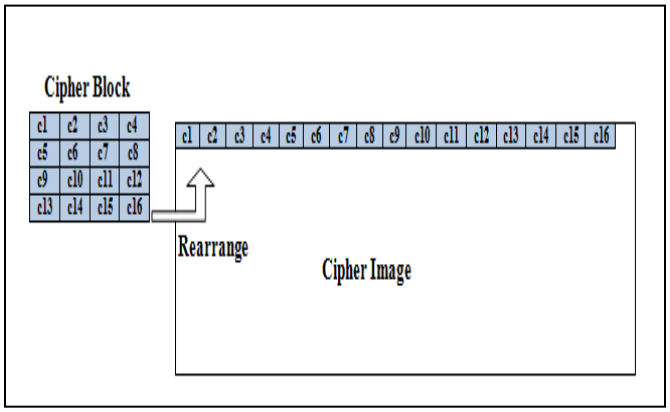


Fig.ure 6. Proposed Shuffling Function

III. Statistical Analysis

A Statistical analysis had performed to investigate the significant confusion and diffusion properties of the introduced system, the results indicate the system resistance against the statistical attacks. This is done by testing the statistical distribution of the pixels values of the ciphered images, the information entropy and the degree of correlation between the plain and cipher images.

A. Statistical Distribution of Image Pixels

In any image, the image pixels have statistical similarity, at different orders, with respect to color and intensity levels. A good encryption strategy should lead to secure encrypted image. Image histograms help in understanding the first order statistical behavior of the images. If there is no, or a negligible similarity, among the histograms of the original and cipher image, then the latter is considered secure from adversary attacks. Histograms of several cipher images and their corresponding plain images are shown in figure (7), they have widely different contents and different in their sizes.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

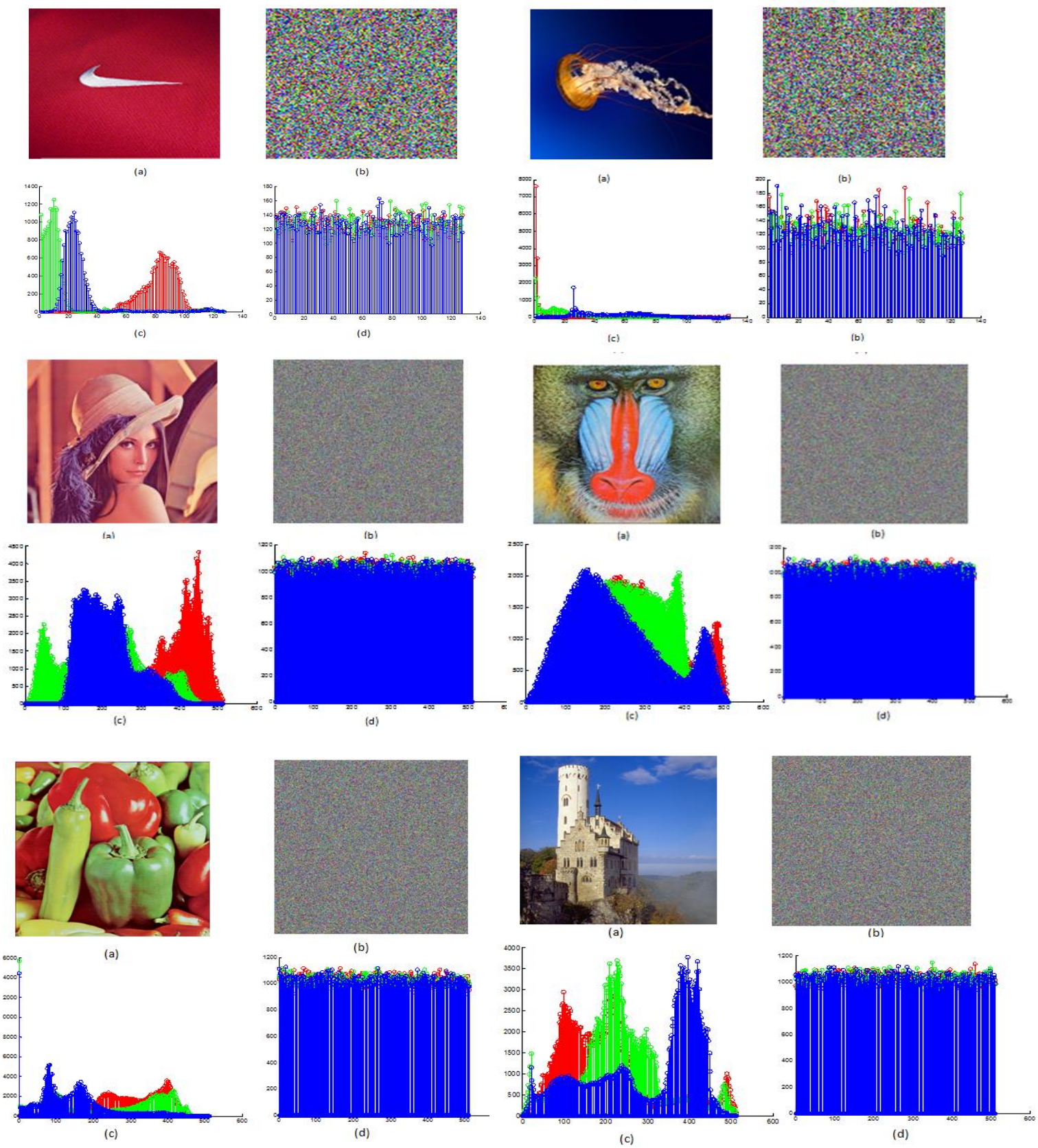


Figure 7. The encryption results, (a) Original image, (b) Encrypted image
(c) Histogram Original image, (d) Histogram of encrypted image

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. So, the encrypted image does not provide any clue to employ any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult.

B. Correlation between Plain and Cipher Images

Correlation is a measure of the relationship between two sets of variables; if the two variables are the original image and its cipher variant then they are uncorrelated. In case the encrypted image is similar to the original image (which is due to the encryption failure in hiding the details of the original image) then the correlation measure will show high values**.**

The cross correlation coefficient used in this research has following formulas [18]:

$$r=\frac{n\sum_i x_i y_i-\sum_i x_i \sum_i y_i}{\sqrt{\left(\sum_i x_i^2\right)-\left(\sum_i y_i^2\right)}} \qquad \text{.....(11)}$$

Where, r is the cross correlation coefficient, n is the number of image pixels, $\{x_i\}$ is the original image pixels values, $\{y_i\}$ is the cipher image pixels values.

The correlation coefficients (r) between many pairs of plain image and their corresponding cipher image have been calculated. The correlation coefficient (CR) for each of the RGB components of the plain images and corresponding cipher images have been calculated. Samples of the test results are shown in Table 1. The correlation coefficients shown in the Table 1 are very small (C≈0), indicates that the plain images and their corresponding cipher images are completely uncorrelated with each other.

TABLE 1. CR BETWEEN THE QRIGINAL IMAGES AND THEIR CORRESPONDING IMAGES

Image	Image Size	C_{RR}	C_{GG}	C_{BB}
JellyFish	128 ×128	-0.0016	0.0069	0.0019
Nike	128 ×128	-0.0078	-0.0077	0.0088
Lena	512 ×512	0.0019	-9.590e-004	-6.334e-004
Baboon	512 ×512	-4.6815e-004	9.184e-005	-9.324e-004
Peppers	512 ×512	3.7673e-005	-0.0019	0.0025
Lichtenstein	512 ×512	5.0069e-004	0.0022	-0.0023

C. Information Entropy

Illegibility and indeterminateness are the main goals of image encryption. This indeterminateness can be reflected by one of the most commonly used theoretical measure information entropy. Information entropy expresses the degree of uncertainties in the system and defines as follow [19]:

$$H=-\sum_{k=0}^{G-1} P(k)\ log_2\left(P(k)\right) \qquad \text{.....(12)}$$

Where, H is the entropy, G is the gray scale (=255), and $P(k)$ is the probability of the occurrence of symbol k.

The highest entropy is H =8, which corresponds to an ideal case. Practically, the information entropies of encrypted images are less compared to the ideal case. To design a good image encryption scheme, the entropy of cipher image should be as close as possible to the highest value. Information entropy values for some of the ciphered images are shown in Table 2 they are above 7.98 (which very close to the ideal value).

TABLE 2. THE ENTROPY VALUES FOR DIFFERENT CIPHERDIMAGES

Images	Plain Image	Cipher Image
JellyFish	5.0241	7.9841
Nike	7.2405	7.9875
Lena	7.7500	7.9920
Baboon	7.7324	7,9921
Peppers	7.6698	7.9919
Lichtenstein	7.7725	7.9917

D. Time Analysis

Table 3 shows the time comparison that required to encrypt and decrypt the original images "Jellyfish" of size 128 ×128×3 (49,152) and "Lena" of size 512×512×3 (786,432) from decrypted images using different range of secret keys (i.e. coefficients of linear system). Table 4 shows the time required to encrypt and decrypt using different keys.

TABLE 3. TIME COMPRESSION FOR DIFFERENT KEY VALUE RNAGES

Images	Size	Key Range	Time (in seconds)
JellyFish	128×128×3	10-39	0.015- 0.14
		40-69	0.24- 0.53
		70-99	0.70- 1.17
		100-129	1.45- 2.07
		130-159	2.35- 3.13
		160-189	3.61-4.60
		190-219	5.07-6.02
		220-255	6.83- 8.67
Lena	512×512×3	10-39	0.21- 2.27
		40-69	3.96- 8.51
		70-99	11.59- 18.39
		100-129	22.58- 32.52
		130-159	37.56-50.54
		160-189	56.84- 72.38
		190-219	80.16- 96.47
		220-255	106.88- 136.60

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE 4. TIME COMPRESSION FOR DIFFERENT KEYS

Image	Size	Key	Time in Sec.
JellyFish	128×128×3	ASEDRFTGYHUJIKLPKJHHHDFHCVDD FRASDREWQOFSERQFTY67I876JTY4E5 RFQFD	2.69
		012345678987654321234567898754301234 565786436523412502133432301	0.046
		abcdcbdesayhnjkiuewqfvghgffaaaszxdertgfvb nhyujikolpmngtfrdewqse	4.55
Lena	512×512×3	ASEDRFTGYHUJIKLPKJHHHDFHCVDD FRASDREWQOFSERQFTY67I876JTY4E5 RFQFD	42.39
		012345678987654321234567898754301234 565786436523412502133432301	0.71
		abcdcbdesayhnjkiuewqfvghgffaaaszxdertgfvb nhyujikolpmngtfrdewqse	71.32

IV. Conclusions

A secure, compact and simple block cipher algorithm is proposed. It offers good performance. During the design, implementation and test phase several notes have been recorded:

- The proposed algorithm is designed to be used in upgraded computer environments. It uses the full menu of "strong operations" supported in modern computers to achieve better security properties. This approach enables us to get better security per-instruction ratio for our implemented software than is possible for the existing ciphers. The design takes full advantage of the ability of today's computers to perform fast multiplications and data-dependent rotations.
- It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. So, the encrypted image does not provide any clue to employ any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult.
- By proposing encryption and decryption algorithm the entropy value of the encrypted images has been increased, as well as lower the correlation.
- The time requirement for encryption and decryption has been increased with the increase of key values.

References

[1] Chin-Chen Chang, Min-Shian Hwang and Tung-Shou Chen, "A New Encryption Algorithm for Image Crypto systems", The Journal of Systems and Software, Vol. 58, No. 2, pp. 83-91, 2001.

[2] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A New Image Encryption Approach Using Combinational Permutation Techniques," Journal of Computer Science, Vol. 1, No. 1, p. 127, 2006.

[3] J. C. Yen and J. I. Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Conference Circuits and Systems, Vol. 4, pp. 49-52, 2000.

[4] Zhi-Hong Guan, Fangjun Huang and Wenjie Guan, "Chaos-Based Image Encryption Algorithm", Physics Letter-A, Vol. 346, pp. 153-157, 2005.

[5] Musheer Ahmad and M. Shamsher Alam, "New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal on Computer Science and Engineering, Vol. 2, No.1, pp. 46-50, 2009.

[6] S.H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A new Modified Version of Advance Encryption Standard Based Algorithm for Image Encryption", Electronics and Information Engineering (ICEIE), Vol. 1, pp. 141-145, 2010 International Conference.

[7] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology, Vol. 3, pp. 526-531, 2007.

[8] Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03 Advance online.

[9] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[10] Abdelfatah A. Yahya and Ayman M. Abdalla, "A Shuffle Image-Encryption Algorithm", Journal of Computer Science, Vol. 4, No. 12, pp. 999-1002, 2008.

[11] S.P. Indrakanti, P.S. Avadhani, "Permutation Based Image Encryption Technique", International Journal of Computer Applications, Vol. 28, No.8, pp. 0975-8887, 2011.

[12] Hiral Rathod, Mahendra Singh Sisodia and Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by Using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol. 1, No. 3, 7-13, 2011.

[13] N. Nithin, M. A. Bongale, G. P. Hegde, "Image Encryption Based on FEAL algorithm", International Journal of Advances in Computer Science and Technology, Vol. 2, No.3, 2013.

[14] K. Narendra Paree, Vinod Patida and Krishan K. Sud, "Diffusion-substitution based gray image encryption scheme", Journal of Digital Signal Processing, Vol. 23, No. 3, pp. 894-901, 2013.

[15] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, Source, and Source Code in C", John Wiley and Sons, Inc., 1996.

[16] J. L. Massey, "An Introduction to Contemporary Cryptology", Proc. IEEE, Vol. 76, No. 5, pp. 533-549, 1988.

[17] Thilo Zieschang, "Combinatorial Properties of Basic Encryption Operations", Advances in Cryptology Eurocrypt'97, International Conference on the Theory And Application of Cryptographic Techniques Konstanz, Germany, May 11-15, 1997, Proceedings, Springer, 1997.

[18] M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 2nd ed., 1998.

[19] D. Feldman, "A Brief Introduction to Information Theory, Excess Entropy and Computational Mechanics," College of the Atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/

AUTHORS PROFILE

Ashwaq Talib Hashim is working as Assistant Professor, in System and Control Engenerring Department, University of Technology, Iraq. She obtained M.Sc. from University of Basrah in 2003. She published more than 12 papers in cryptography, steganography and VHDL.

Dr. Loay Edwar George received his Ph.D degree from Baghdad University , Iraq in 1997. Thesis title is "New Coding Methods For Compressing Remotely Sensed Images". He is a member of Arab Union of Physics and Mathematics, and the Iraqi Association for Computers. Now, he is the Head of Computer Science Department, Baghdad University.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Coin based Untraceable Incentive Mechanism for Multi-hop Cellular Networks

Vishnu Subramonian P
Department of Electronics and Communication Engg.
Nehru College of Engineering and Research Centre,
Pampady, Thiruvilawamala, Kerala, India .

Rahul M Nair
Department of Electronics and Communication Engg.,
Nehru College of Engineering and Research Centre,
Pampady, Thiruvilawamala, Kerala, India.

Parameshachari B D
Department of Electronics and Communication Engg.,
Nehru College of Engineering and Research Centre,
Pampady, Thiruvilawamala, Kerala, India
(Research Scholar, Dept. of ECE, Jain University,
Bangalore, Karnataka, India)

H S DivakaraMurthy
Department of Electronics and Communication Engg.,
Nehru College of Engineering and Research Centre,
Pampady, Thiruvilawamala, Kerala, India.

Abstract— **The multihop cellular network uses nodes to relay packets of data which helps in enhancing the network performance.Selfish node do not usually take part and this increases the load on cooperative nodes. This paper provides a fair charging policy which also includes hashing operations,public key cryptography, authentications to provide a secure and efficient communication.**

Keywords- **cryptography;fescim;hashing; selfishnodes;checks; networks;**

I. INTRODUCTION

Multihop cellular network has been undergoing changes in very fast pace. Nodes play an important role in communication with their commited bandwidth , memory battery power etc Nodes can reduce the energy consumption when data is transmitted over shorter distances. The presence of autonomous nodes hampers the communication. By proper security and identification of the selfish nodes can help in efficient communication. A routing algorithm in MCN introduces extra signalling overhead when broadcasting route information which adds extra interference. The effect of the interference is normally ignored in MANETs but cannot be neglected in cellular networks. This is mainly because the transmission power of nodes in MCNs can be several orders of magnitude higher than that of nodes in MANETs. In both MANETs and MCNs, the amount of signalling overhead mainly depends on the chosen routing algorithm. The routing algorithms can generally be classified into two categories: a) proactive routing and b) reactive routing. Proactive routing mechanisms discover and calculate routes all the time. Each node periodically exchanges its routing information with its neighbours by continuously broadcasting hello/topology messages, and thus, its signalling overhead depends on the broadcasting interval and the number of nodes in the network. In MCNs, the radio resources are centrally controlled, and thus, a mobile terminal has to establish a connection with the BS before data is transmitted. In such an environment, reactive routing offers several advantages over proactive routing.

II. RELATED WORK

A. *General fescim (fair efficient and secure cooperative incentive mechanism for MCN)*

First, In order to establish an end-to-end route, the source node broadcasts the Route Request Packet (RREQ) containing the identities of the source (IDS) and the destination (IDD) nodes, the route establishment time stamp (TS), and the payment-splitting ratio (Pr). The source node is charged the ratio of Pr of the total payment and the destination node is charged the ratio of 1-Pr. A network node appends its identity and broadcasts the packet if the time stamp is within a proper range. The RREQ packet is relayed by BSS to BSD (if the destination node resides in a different base station) that broadcasts it. Finally, the destination node sends back the Route Reply Packet (RREP) to establish the route. The source node initiates a new route discovery phase if the route is broken.”.

Mobile Information System, have began to address the limited bandwidth and QoS (Quality of Service) issue. An advantage of these networks is their low cost because no infrastructure is required, and, therefore, can be deployed immediately. However, these ad-hoc networks appear to be limited to specialized applications. such as battlefields and traveling groups, due to the vulnerability of paths through possibly many mobile stations. However, this vulnerability can

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

be significantly reduced if the number of wireless hops can be reduced and the station mobility is low. The throughput is analysed by modelling the packet departure process as a renewal process, in which the renewal point is defined as the time point when all stations in a sub-cell simultaneously sense that the channel is idle. Furthermore, mean hop count is analysed because it significantly influences the throughput of MCN, as confirmed by the numerical results. Analysis and simulation results for the throughput of SCN and MCN lead to three important observations. First, the throughput of MCN is superior to that of the corresponding SCN. Second, the throughput of MCN increases as the transmission range decreases.

The proposed mechanism for hybrid mode can be used for pure ad hoc mode figure 1, but the intermediate nodes have to submit the checks to the AC because the base stations are not involved in the communication. A check contains payment data for all the nodes in the route, but it is not secure to trust one node to submit the check because it may collude with the source and destination nodes so as not to submit the check to increase their welfare.

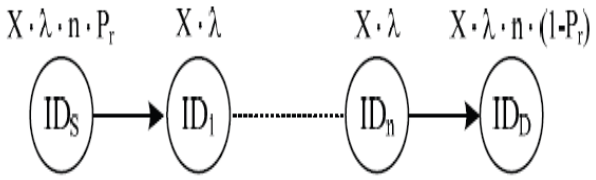


Figure 1 adhoc mode.

The charges and rewards for sending X messages in a route with n intermediate nodes. If the source and destination nodes collude with K intermediate nodes and the check is not submitted, the colluders can save X .λ (n-k) credits. Obviously, the colluders can achieve gains when K < n, and thus, the source and destination nodes can compensate the colluding intermediate nodes. On the other hand, it is not efficient to submit a check by each intermediate node due to significantly increasing the number of redundant checks. In this section, we propose two schemes for efficiently thwarting the collusion attacks against check submission.

B. Network and Communication Models

MCN includes an accounting centre, a set of base stations, and mobile nodes. The AC stores and manages the credit accounts of the nodes, and generates private/public key pair and certificate with unique identity for each node. Once the AC receives a check, it updates the accounts of the participating nodes. The base stations are connected with each other and with the AC by a backbone network that may be wired or wireless. FESCIM can be implemented on the top of any routing protocol, such as DSR and AODV ,to establish an end-to-end communication session provided that the full identities of the nodes in the route are known to the source and destination nodes. It is important to include these identities in the source and the destination node's signatures to compose valid checks. All communications are unicast and the nodes can communicate in one of two modes: pure ad hoc or hybrid. For pure ad hoc mode, the source and destination nodes communicate without involving base stations. The source node's messages may be relayed in several hops by the intermediate nodes to the destination node. For hybrid mode, at least one base station is involved in the communication. The source node transmits its messages to the source base station (BSS), if necessary in multiple hops. If the destination node resides in a different cell, the messages are forwarded to the destination base station(BSD) that transmits the messages to the destination node possibly in multiple hops. The nodes can contact the AC atleast once every few days. This connection can occur via the base stations or the wired networks such as the Internet. During this connection, the nodes submit checks, renew their certificates, and convert credits to real money and/or purchase credits with real money.

A fair charging policy is to support cost sharing between the source and destination nodes when both of them benefit from the communication. In order to make FESCIM flexible,the payment-splitting ratio is adjustable and service dependent, e.g., a DNS server should not pay for name resolution. For rewarding policy, some incentive mechanisms, such as, consider that a packet relaying reward is proportional to the incurred energy in relaying the packet. It is difficult to implement this rewarding policy in practice without involving complicated route discovery process and calculation of enroute individual payments. Any node that has ever tried to relay a packet should be rewarded no matter whether the packet eventually reaches its destination or not because relaying a packet consumes the node's resources. However, it is difficult to corroborate an intermediate forwarding action without involving too much overhead, e.g., all the intermediate nodes have to submit all the checks . Moreover, rewarding the nodes for relaying route establishment packets or packet retransmissions significantly increases the number of checks because a large number of nodes may relay route establishment packets and packet retransmission frequently happens in wireless networks. Therefore, the AC charges the source and destination nodes for every transmitted message even if the message does not reach the destination, but the AC rewards the intermediate nodes only for the delivered messages. For fair rewarding policy, the value is determined to compensate the nodes for relaying route establishment packets, packet retransmission, and undelivered packets. In will argue that our charging and rewarding policies can thwart rational attacks and encourage the nodes' cooperation. Similar to the VISA system and the incentive mechanisms in the nodes communicate first and pay later. The AC issues certificates to enable the nodes to transact by issuing digital checks without the need for direct verification from the AC to avoid frequently contacting the AC and thus creating a bottleneck at the AC. The nodes at the network border cannot earn as many credits as those at other locations because they are less frequently selected by the routing protocol. In order to communicate, they can purchase credits with real money. It is not considered as fairness problem because the philosophy behind incentive mechanisms is that packet relay is a service not an obligation. This service may not be requested from some nodes, i.e., the customers(source and destination nodes) request the packet-relay service from the best service providers (shortest route

Nehru College of Engineering and Research Centre, Pampady,
Thiruvilawamala, Kerala, India

nodes). If the traffic is directed through the border nodes, obviously, we sacrifice the network performance because the routes may be long. See figure 2 .Due to the node mobility, the border nodes can change their location and earn more credits as shown Moreover, the border nodes do not relay as many packets as others, and thus, it is fair to charge the border nodes real money to compensate the other nodes that relayed more packets.

In order to fairly and efficiently charge the source and destination nodes, the lightweight hashing operations are used to reduce the number of public-key-cryptography operations.

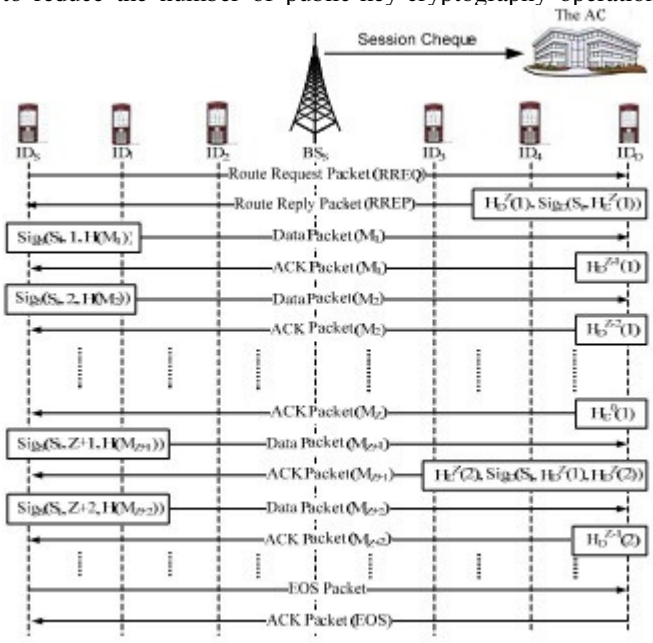


Figure 2.The exchanged security tags

Moreover, to reduce the overhead of the payment checks, one small-size check is generated per session instead of generating a check per message, and the Probabilistic-Check-Submission scheme has been proposed to reduce the number of submitted checks and protect against the collusion attack.

III. COIN BASED METHOD

In this method the incentives are termed as "coins" which are given to nodes in return of their service. These coins decide the priority of the node and thereby helps in elimination of selfish nodes or less cooperative node. Fig 2 shows the secured request packets after coins are given. The enhancement of this paper is that an additional access point is given to the fescim which is mainly used to provide communication between cluster heads in a controlled manner. AP enables communication or updating between the nodes in a systematic manner. More over each node is designed in such a manner that it has to check all the nodes and also the key which is generated before the transmission. Each message is divided into hash for this has signature is given so the no. of checks is reduced.

ID_S: $\langle ID_S, ID_D, T_S, Sig_S(ID_S, ID_D, T_S), Cert_S \rangle$

ID_1: $\langle ID_S, ID_D, T_S, ID_1, Sig_1(Sig_S(ID_S, ID_D, T_S)), Cert_S, Cert_1 \rangle$

ID_2: $\langle ID_S, ID_D, T_S, ID_1, ID_2, Sig_2(Sig_1(Sig_S(ID_S, ID_D, T_S))), Cert_S, Cert_1, Cert_2 \rangle$

ID_D: $\langle ID_S, ID_D, T_S, ID_1, ID_2, Sig_2(Sig_1(Sig_S(ID_S, ID_D, T_S))), Cert_S, Cert_1, Cert_2 \rangle$

Figure 3. Secured route request packets

This signature is encrypted with public key cryptography which reduces the overhead also. Instead of generating two signatures per packet (one from the source and the other from the destination), we have replaced the destination node's signature with hashing operations to reduce the number of public-key-cryptography operations nearly by half. The source node attaches a signature in each data packet to ensure the payment nonrepudiation and to verify the message integrity at each intermediate node to thwart Free- Riding attacks. Here, we will focus on reducing the number of public-key-cryptography operations due to the source node's signatures. Although the payment non-repudiation can be achieved using a hash chain at the source node side, we will study how to efficiently verify the message integrity at each intermediate node. In addition, similar to the existing incentive mechanisms, FESCIM can thwart selfishness attacks, but it cannot identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets to launch .This method helps in identifying irrational nodes by means of providing each node a particular id while a data is transported ,the nodes without the transmitting id will be discarded because the chance of that node being a selfish node is more.

Extensive analysis and simulations have demonstrated that our incentive mechanism can secure the payment and significantly reduce the overhead of storing, submitting, and processing the checks

IV. SIMULATION SETUP

In this section, we evaluate the checks overhead in terms of the check size and the number of generated checks. We also evaluate the overhead of the signed and hash-chain-based ACKs in terms of energy consumption and end-to-end packet delay.

NS2 is the main simulation used here. All possibilities that is NAM,GNU simulations are used. In order to estimate the computational processing times for the signing, verifying, and hashing operations, we have implemented 1,024-bit RSA and SHA-1 using the Crypto++ library. The mobile node is a laptop with an Intel processor at 1.6 GHZ and 1 GB Ram, and the operating system of the mobile node is Windows XP. The results given in indicate that the RSA signature generation is computationally intensive but the signature verification is much faster. The energy consumption of the RSA and SHA-1 operations is measured in and the results are given in. The resources of a real mobile node may be less than a laptop, scaled by the factor of 5 in our simulations to estimate a limited-resource node. Some results are shown below.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

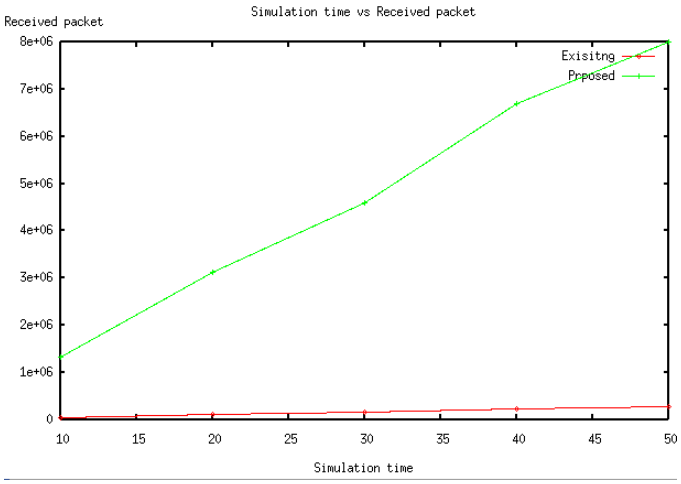


Figure 4. Simulation time vs received packets

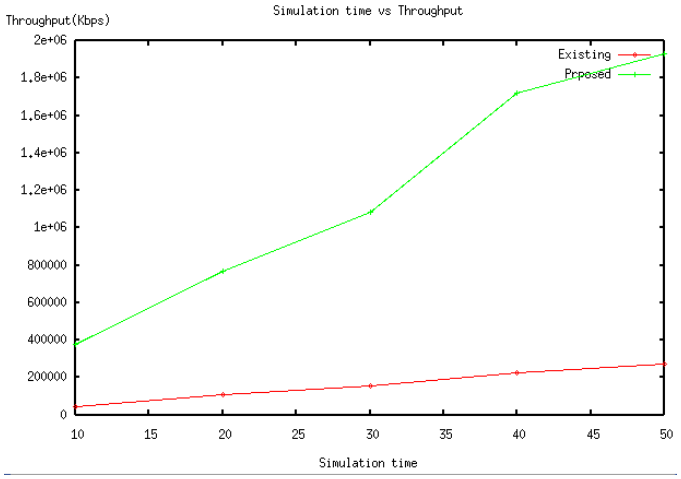


Figure 5 .Simulation Time vs Throughput

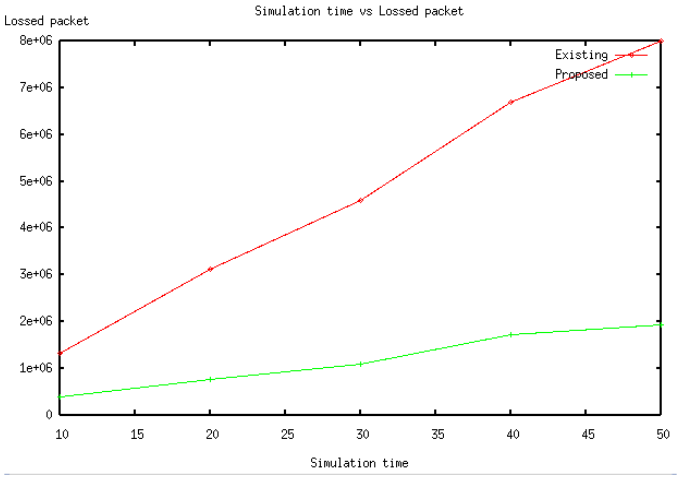


Figure 6. Simulation time vs lossed packets

V. Conclusion And Future Work

A fair efficient and secure mechanism for proper transmission of data between the nodes .The number of checks and public key cryptography is reduced as hashing operations were widely used. The overhead was reduced considerably and more secure transmission is made possible .In future more reduction in the cryptography reduces overhead and also the efficiency of the communication.

Acknowledgement

The work described in this paper is supported by Adv.Dr.P.Krishnadas,Managing Trustee&Dr.P Krishnakumar, CEO & Secretary, Nehru Group of Institutions, Tamil Nadu, Kerala-India. Authors are grateful to Prof. Dr. P.N. Ramachandran, Principal and Dr.N K Shakthivel, Vice-Principal, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, for providing us the opportunity to undertake this project.

References

[1] M.E.A. Mahmoud, Member, IEEE and Xuemin (Sherman) , Shen , Fellow, IEEE"FESCIM " *IEEE* transactions on mobile computing vol 11 no 5. may 2012

[2] Y. Lin and Y. Hsu, "Multihop Cellular: A New Architecture for Wireless Communications," Proc. IEEE INFOCOM, vol. 3, pp. 1273-1282, Mar. 2000.

[3] X. Li, B. Seet, and P. Chong, "Multihop Cellular Networks: Technology and Economics," Computer Networks, vol. 52, no. 9, pp. 1825-1837, June 2008.

[4] C. Gomes and J. Galtier, "Optimal and Fair Transmission Rate Allocation Problem in Multi-Hop Cellular Networks," Proc. Int'l Conf. Ad-Hoc, Mobile and Wireless Networks, pp. 327-340, Aug. 2009.

[5] H. Wu, C. Qios, S. De, and O. Tonguz, "Integrated Cellular and Ad Hoc Relaying Systems: iCAR," IEEE J. Selected Areas in Comm., vol. 19, no. 10, pp. 2105-2115, Oct. 2001.

[6] G. Shen, J. Liu, D.Wang, J.Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[7] R. Schoenen, R. Halfmann, and B. Walke, "MAC Performance of a 3GPP-LTE Multihop Cellular Network," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4819-4824, May 2008.

[8] 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, "Opportunity Driven Multiple Access," G Technical Report 25.924, Version 1.0.0, Dec. 1999.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, Aug. 2000.

[10] P. Michiardi and R. Molva, "Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks," Proc. European Wireless Conf., Feb. 2002.

[11] J. Hu, "Cooperation in Mobile Ad Hoc Networks," Technical Report TR-050111, Computer Science Dept., Florida State Univ., Jan. 2005.

[12] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas,
"Cooperation Enforcement Schemes for MANETs: A Survey,"
J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332

Authors Profile:

Vishnu Subramonian P studying M.tech degree course in applied electronics and communication systems at Nehru College of engineering and research centre thrissur, under University of Calicut. I have successfully completed B.tech degree in Electronics and Communication Engineering from Baselios Mathews II college of engineering ,sasthamcotta, kollam, under the University of Kerala in 2011.

Rahul M Nair working as a Assistant Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre,kerala,India Completed B.tech from Ilahia College of Engineering Kothamangalam under MG university.Completed M.Tech from Viswajyoti College of Engineering.

Parameshachari B D working as a Associate Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut. Worked as a Senior Lecturer and inchage HOD in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He worked at JSSATE, Mauritius for Three years and also worked as a Lecturer at Kalpatharu Institute of Technology, Tiptur for Seven years. He obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore, affiliated to Visveswaraiah Technological University, Belgaum. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India under the guidance of Dr. K M Sunjiv Soyjaudah, Professor, University of Mauritius, Reduit, Republic of Mauritius and Co-guidance of Dr. Sumithra Devi K A, Professor and Director, Department of MCA, R V College of Engineering, Bangalore. Parameshachari area of interest and research include image processing, cryptography and Communication. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

Muruganantham.C working as a Assistant Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre,kerala,India. Worked as Assistant Professor-II in SEEE of SASTRA University. Worked as Lecturer in Electrical & Computer Engg Department of Ethiopian Universities. Published papers in national/international conferences. He is member of ISTE. His area of interest are VLSI, Signal Processing.

Divakara Murthy H S has multi faceted experience in Research, Industry and Academic fields, He is working as a Dean and HOD in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut and also served as a Principal at JSS Academy of Technical Education, Mauritius for two years. Involved in Administrative & Academic activities in development of infrastructure facilities marketing, mounting new courses and strategic planning. He worked at RGV telecom Ltd Bangalore as Deputy Vice president,for providing optical communication for Indian Railways for nearly two years and also worked nearly 27 years in Telecom in Industry at senior level in various capacities in Telecom Projects and Planning, Production and Marketing. During my intial career involved in Design and development of Instrumentation at NAL Bangalore. He obtained his B.E in Electronics and Communication Engineering from Siddaganga Institute of Technology, Tumkur from University of Mysore and MSc(Engg)in communication system from PSG Institute of technology, Coimbatore , from University of Madras. Divakara Murthy area of interest and research include Micro and Pico Satellite communication, Optical Communication and Wireless communication, GSM and WiMAX technology. He is a Member of ISTE, IETE

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Multidimensional Analysis applied to WSN Case study: routing Protocol

Ziyati Elhoussaine, Rachid Haboub, Mohammed Ouzzif, and Khadija Bami
RITM laboratory, Computer science and Networks team
ENSEM - ESTC - UH2C,
Casablanca, Morocco

***Abstract*—Mobile Ad-hoc Network is a kind of wireless ad-hoc network where nodes are connected wirelessly and the network is self configuring [1]. This paper shows the use of data warehouse as an alternative for managing data collected by Wireless Sensor Networks. In general Wireless Sensor Network is used to produce a large amount of data that need to be analyzed and normalized, so as to help researchers and other people interested in the information. These data managed and compared with information from other sources and systems could contribute in technical decision processes. This paper proposes a model to extract, transform and normalize data collected by Wireless Sensor Networks by implementing a multidimensional warehouse for comparing many aspects in WSN such as (routing protocol[4], sensor, sensor mobility, cluster ….). Hence, data warehouse applied to the context above is detached as a useful alternative that helps specialists to obtain information for decision processes and navigate from one aspect to another.**

Keywords-WSN, Data Warehouse, multidimentional design, OLAP, Routing Protocol

I. INTRODUCTION

MANET is autonomous collection of mobile nodes that communicate over limited bandwidth and energy constraints [6]. These mobile nodes are in motion so the topology of the entire network changes rapidly and unpredictably over time. All network is managed by the network nodes themselves, as there is no special device or router involved, every nodes itself work as a router to forward the traffic.

Energy conservation in ad-hoc networks is very important due to the limited energy availability in each wireless node [2]. Since the communication between two wireless nodes consumes more energy, it is pertinent to minimize the cost of energy required for communication by exercising an energy aware routing strategy. Such routing procedures/policies potentially increase the lifetime of the network. In this paper, the energy metrics of AODV and DSDV [3] are compared by simulating with increasing the density of nodes and using DW technologies to depicts and control some WSN's behavior over time.

A. Routing protocol

Routing protocols [8] is a standard that controls how nodes decide to route the packets between the source and the destination node. Each node learns about nodes nearby and how to reach them.

Each node is maintaining one or more tables that containing routing information about every other node in the network. Examples for table driven protocols are:

1) *AODV* : This protocol performs Route Discovery using control messages route request (RREQ)[12] and route reply(RREP) whenever a node wishes to send packets to destination. To control network wide broadcasts of RREQs, the source node uses an expanding ring search technique. The forward path sets up an intermediate node in its route table with a lifetime association RREP.

2) *DSDV:* Destination Sequenced Distance Vector protocol belongs to the class of proactive routing protocols. Based on the classical Bellman-Ford routing algorithm [4]. DSDV also has the feature of the distance-vector protocol [1] in that each node will maintain a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded [5]. Each entry in the routing table is marked with a sequence number that is assigned by the destination node; the sequence numbering system will avoid the formation of loops.

II. RELATED WORKS

Energy consumption, since nodes are powered by batteries, depending on the use, energy can last from days to weeks [5]. With the help of WSN, it is possible to monitor various characteristics of the environments, but these data alone or simply collected over time are difficult to be interpreted by users. In this section, we outline the context of our work on WSN. In [6][8] The energy metrics of AODV and DSDV are compared by simulating with increasing the density of nodes using trace file generated NS2 simulator.

For the monitored data to be recovered in a productive way by the parties, it must be organized in a repository or database, and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

have an interface with easy access, through which the user can view consolidated information and be able to make analysis.

The description above refers to Data Warehouse (DW) that means a set of technologies for decision support used by people interested in making decisions quickly and easily. A major contribution of this paper is an alternative to manage data collected by WSN based on a model to extract, transform and normalize this data and load it in a DW. The results showed that the crossing of tabulated data with others sources, such as technical reports could improve data accuracy and help to create better data warehouse views. Data in sensor database -trace file- is transformed, loaded in warehouse and then displayed. In figure 1 represents all sources supported by the architecture proposed.

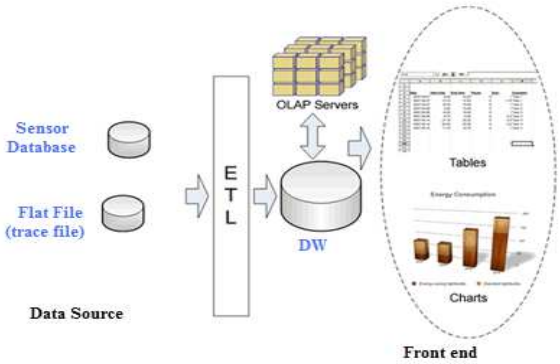


Figure 1. Data Warehouse Architecture.

The remainder of this paper is organized as follows. Section 3 reviews the technologies and terminologies used in the whole paper, presenting products used in the prototype developed. Section 4, modeling the proposed warehouse and data extraction-analyze and highlights the small amount of research in this area of knowledge that deal with data warehouse to manage data collected by WSN. Section 5 presents the architecture proposed focusing on the process of acquiring and delivering data from WSN to DW. Section 6 shows the results obtained using collected by WSN. Section 6 concludes this paper and outlines our future plans, abstracting it and focuses on data from WSN and extract-transform-load operation into a DW.

The main purpose of this research was to monitor some measures behaviors in situations, such as energy [6]. To analyze data from WSN, [9] introduces an approach based on tasking sensor networks through declarative queries. Given a user query, a manager creates a plan for this statement execution. A leader node is necessary to consolidate data from other nodes.

III. DATA WAREHOUSE AND OLAP

OLAP consists objects that are a part of dimensional model. The dimensional data model (include: dimensions, attributes, levels, hierarchies, measures and cubes) is highly structured and implies rules that govern the relationships among the data and control how the data can be queried. The fact table is referred to a cube, and the columns (in table) are referred to measures. The cube has edges, which are referred to dimensions. The fact table include measures that are linked to a dimension [9]. Each dimension is a grouping of related columns from one or more tables. Analysts know which business measures they are interested in examining.

In viewing data, analysts use dimension hierarchies [10] to recognize trends at one level, drill down to lower levels to identify reasons for these trends, and roll up to higher levels to see what affect these trends have on a larger sector of the business.
An attribute provides additional information about the data. Some attributes are used for display. You might also have attributes like protocol, descriptive attributes.

Online Analytical Processing (OLAP) allows navigation of the data in a DW, having a suitable structure for both research and for presenting of information. In the navigation tools, OLAP can navigate between different granularities of a cube [11]. Through a process called Drill, the User can increase (Drill down) or decrease (Drill up) the level of detail of the data. For example location dimension figure, a report may be consolidated by the country. With the Drill down, the data will be submitted by region, state and so on until the lowest level possible figure 2. The opposite process, Drill up, causes data to be consolidated at higher levels. Note that Data provided by sensors are reorganized in multidimensional warehouse, (real time processing will be crucial in term of energy, resources and time) and require more high technology to enhance this process.

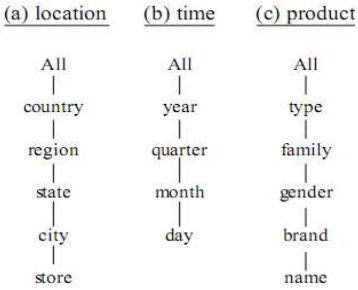


Figure 2. Dimensions hierarchies

IV. PROPOSED ARCHITECTURE

After extracting and transforming data -flat file-, it is necessary to load this information into a DW that modeled in dimensional modeling. According to [11], dimensional modeling (DM) is the name of a logical design technique often used for data warehouses. It is different from, and contrasts with, entity-relation modeling (ER) [9].
Figure 3 depicts the proposed multidimensional model; the prototype contains energy, temperatures measures and three dimensions DSensor, DPaquet and DTime presented with hierarchies mentioned to ensure navigation between levels.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

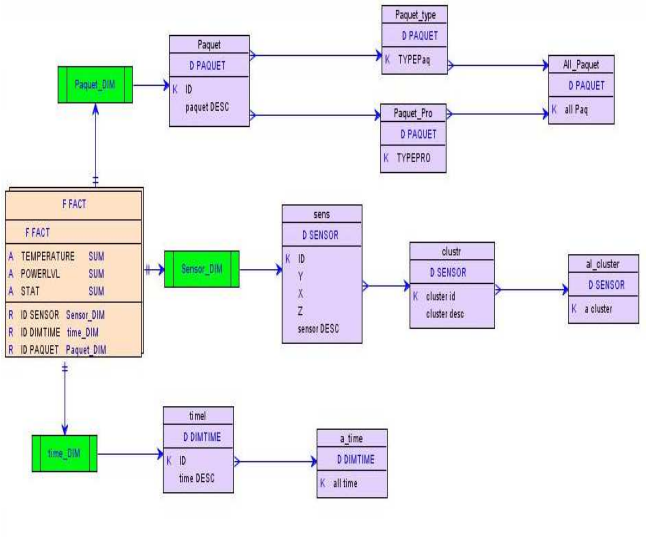


Figure 3. Multidimensional Model.

Other possibility is to present the warehouse in relational model, by defining table instead of dimension by rearrange columns and rows figure [4].

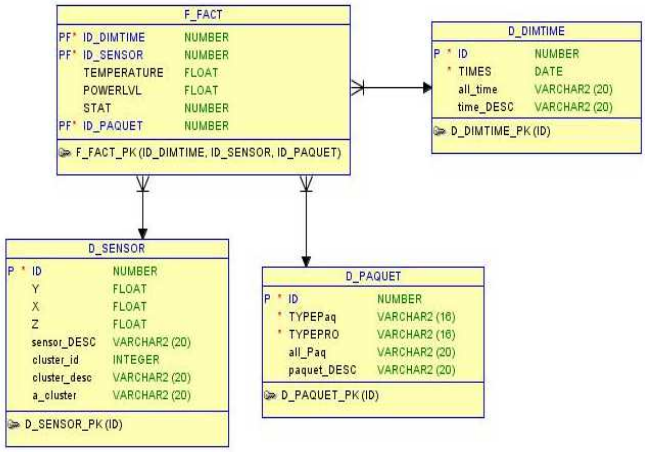


Figure 1 : Warehouse relational star schema.

Normally data is collected at different times and transformation process is accounts for consolidating this data in the same time zone and granularity, this action will be critical because of the huge quantity of data.

V. RESULTS

In this section we show the usefulness and some technical report extracted from the proposed warehouse, implemented in Oracle tools: Oracle Analytic Workspace Manager (AWM), Oracle SQL Developer Data Modeler and other package in order to fill the data warehouse by mapping source to target DW. It allows both logical and physical design of the warehouse.

Collected data [6] is loaded in DW; using AWM [13] can present data –Energy behavior -in tabular or graphically form figure 5.

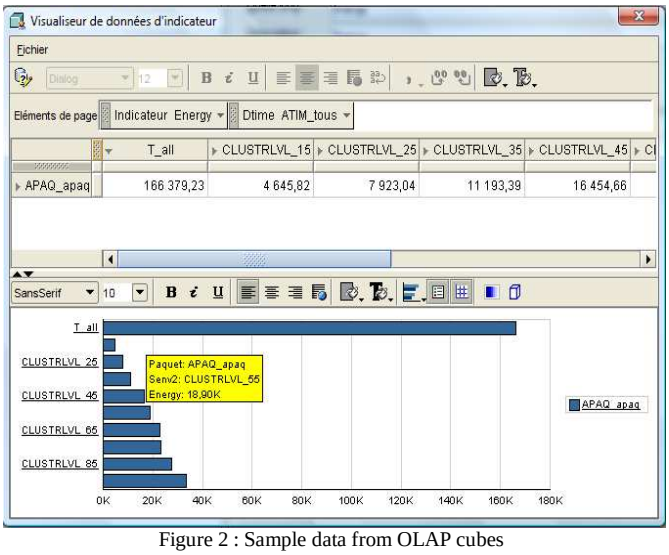


Figure 2 : Sample data from OLAP cubes

Hence, data warehouse applied to the context above shows to be a useful alternative that helps specialists to obtain information for the whole process, which could generates energy and observation of many measures.

The analysts can manipulate cube objects with use of drag and drop methods. They may also limit the scope of the presented data using filters that limit data on individual dimensions, hierarchies and levels. They can also drill down or drill up using level figure drill down to specify protocol type in order to evaluate energy figure 6.

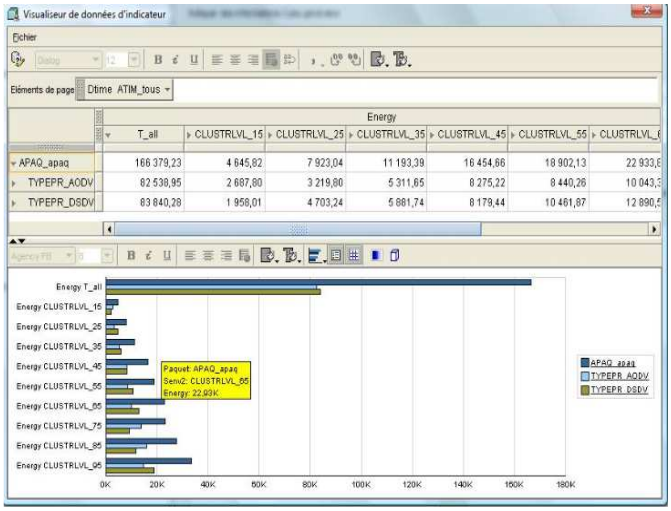


Figure 3 : node cluster level Vs consumed energy

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSION AND FUTUR WORKS

The association of WSN and DW is little explored a research area. However, the benefits of using DW to manage data collected by WSN are shown here. Among the things that stand out is the possibility to help technical decision-making.

In this paper, we have presented a simulation tool/prototype which can give a set of graphs and interactive interface in order to compare many aspect and measures of a WSN such as energy, and navigate across dimensions and levels to crossover and have a global view.

As our future works, we would like perform more analysis in WSN especially exchange traffic and QoS using DW environment.

REFERENCES

[1] Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010, ISSN: 2010-0248.

[2] Aravind B Mohanoor, Sridhar Radha Krishnan, Venkatesh Sarangan, "Online energy aware routing in wireless networks" , September 2007.

[3] M.Z Aslam, A. Rashid. Comparison of Random Waypoint & Random Walk Mobility Model under DSR, AODV & DSDV MANET Routing Protocols. International Journal of Advanced Research in Computer Science (IJARCS) Volume 2 Issue1 Jan-Feb 2011 Page 381-386

[4] Bhabani Sankar Gouda "A Comparative Analysis of Energy Preservation Performance Metric for ERAODV, RAODV, AODV and DSDV Routing Protocols in MANET" International Journal of Computer Science & Engineering Technology (IJCSET),Volume 3,Issue No. 10, pp. 516-524,Oct 2012.

[5] V. Kanakaris, D. Ndzi and D. Azzi, "Ad-hoc Networks Energy Consumption: A review of the Ad-Hoc Routing Protocols", Journal of Engineering Science and Technology Review 3 (1) (2010), pp.162-167.

[6] Vijayalakshmi P, V.Saravanan ,P. Ranjit J.T, Abraham D.J. Energy-Aware Performance Metric for AODV and DSDV Routing Protocols in Mobile Ad-Hoc Networks. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814.

[7] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks" in ACM SIGMOD Record, vol. 31, New York, NY, USA, 2002.

[8] S.A. Gupta and R. K. Saket, "Performance Metric Comparison of AODV and DSDV Routing Protocols in MANETs using NS-2", June 2011, Volume 7, Number 3, pp: 339-350.

[9] S. Chaudhuri and U. Dayal, "An overview of data warehousing and OLAP technology," ACM SIGMOD Record, vol. 26, no. 1, pp. 65-74, Março 1997.

[10] Mazon, ´ J.-N. and Trujillo, J. (2006). Enriching Data Warehouse Dimension Hierarchies by Using Semantic Relations. In XXIIIrd British National Conference on Databases (BNCOD 2006), Belfast, Northern Ireland, volume 4042 of LNCS.

[11] R. Kimball, "A Dimensional Modeling Manifesto," in DBMS and Internet Systems, San Francisco, 1997, pp. 58-70.

[12] Rachid Haboub & Mohammed Ouzzif, "Secure & reliable routing in MANET" in IJCSES Vol.3, No.1, February 2012.

[13] Oracle OLAP - User's Guide 11g. Release 1 (11.1). B28124-03.

AUTHORS PROFILE

Dr Ziyati Elhoussaine received PHD degree in Computer Science from Mohammed V. University in 2010, Presently, he is a Professor in Computer Engineering department in ESTC Institute of Technology, Casablanca, morocco In Intelligence, Networking and Data warehousing.

Rachid Haboub is a Ph.D student. He received the Master degree in computer science, from Hassan II University, Ben M'sik faculty of Morocco in 2009. His research spans wireless communication..

Dr. Mohammed Ouzzif is a professor in the computer science department of the higher school of technology of Casablanca - Hassan II university of Morocco.

Khadija Bami is a PHD student working in Data warehousing in ESTC, RTIM lab, university Hassan II, Casablanca

"People Are the Answer to Security":
Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization

Oyelami Julius Olusegun
Department of Information systems
University Technology Malaysia
Faculty of Computing
Skudai, Johor Bahru 81310

Norafida Binti Ithnin
Department of Information systems
University Technology Malaysia
Faculty of Computing
Skudai, Johor Bahru 81310

ABSTRACT

Educating the users on the essential of information security is very vital and important to the mission of establishing a sustainable information security in any organization and institute. At the University Technology Malaysia (UTM), we have recognized the fact that, it is about time information security should no longer be a lacking factor in productivity, both information security and productivity must work together in closed proximity. We have recently implemented a broad campus information security awareness program to educate faculty member, staff, students and non-academic staff on this essential topic of information security. The program consists of training based on web, personal or individual training with a specific monthly topic, campus campaigns, guest speakers and direct presentations to specialized groups. The goal and the objective are to educate the users on the challenges that are specific to information security and to create total awareness that will change the perceptions of people thinking and ultimately their reactions when it comes to information security. In this paper, we explain how we created and implemented our information security awareness training (ISAT) program and discuss the impediment we encountered along the process. We explore different methods of deliveries such as target audiences, and probably the contents as we believe might be vital to a successful information security program. Finally, we discuss the importance and the flexibility of establishing a sustainable information security training program that could be adopted to meet current and future needs and demands while still relevant to our current users.

CATEGORIES AND SUBJECT DESCRIPTORS

[Computer and Education]: *Computer and Information Security Education*
[Management of Computing and Information Systems]: *Security and Protection*
General Terms: *Information Security, Human Factors, Management and Education*

Keywords: *Information Security, Awareness, End-User, Education and Training*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

I. INTRODUCTION

The essentiality and the role of information security awareness training (ISAT) should not be underestimated. ISAT program and the Information Assurance and Security Research Group of University Technology Malaysia (IASRG-UTM) with the School of Professional and Continue Education of the University Technology Malaysia (UTM-SPACE), has established and implemented a comprehensive and coherent information security awareness program to educate our users about the importance of information security (ISec). This paper will explore the creation and the establishment of the information security program, the identification of different audiences and methods of information delivery and how to define what content is vital to a successful information security program. It will also discuss how to successfully maintain a relevant and sustainable long term information security awareness program.

II AIM AND OBJECTIVE

The goals and objectives of the ISAT program are to:

1. Change the perceptions of people's thinking and reactions when it comes to information security issues,
2. Develop a metrics as a yardstick to measure the level of knowledge of target audiences and the success of the ISAT program, and
3. To continually address the viability and importance of information security on the university premises.

III. METHODOLOGY

UTM developed an information security awareness program for students, faculty and staff member. The program aims is to educate users and change their behavior via two main avenues as follows: (1) information security awareness training and (2) monthly activities. The methodology or planning process in achieving this will focus and consist of determining vital contents, defining audiences and choosing the correct methods of delivery.

A. Determining the Content

In order to determine the content, the first thing we did is to evaluate the security related challenges and problems that UTM dealt with on a daily basis. We did this, based on tangible statistics, such as reports from our system users, as well as problems perceived. While having a dialogue to people about what they perceived to be our biggest security challenges and problems, we realized that some factors will always be problems and those factors will only be a problem or challenges at a specific time, and as a result of that, a new problems or challenges will always emerge. Based on these factors, we decided to incorporate flexibility with our content so we could be able to inculcate new problems or concerns as they arose. In order to accommodate this needs and the avoidance of constant revising of our material, we decided that the training component of our information security awareness training (ISAT) program would consist of topics that are static and will be evaluated on a annual basis, while the ongoing monthly activity components of our ISAT program would consist and focus of topics that were relevant at the time. Since the monthly activities focus on what is important at the time, the initial focus was to establish the list of necessary topics for the ISAT program.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

After we felt it strongly that we have gotten a good idea of what should be inculcated in the ISAT program, we seek and solicited for opinions from academic managers within the UTM premises, this include our IT and desktop support team, help desk support team, server support, networking team and training managers. During this solicitation for opinions from this array of staff, we suspected and concluded that, most of the academic and non academic staff was in support and agreement with us as far as what topics should be incorporated and covered. However, some of the technical staff (Non academic) felt it strongly that we had not included enough specialized information security content to keep it more interesting. Based on this feedback, we re-evaluated the ISAT program content. In doing this, we discovered what we admitted and considered to be a more appropriate in maintaining balance between non-technical and technical information. At this juncture, our list of topics for the ISAT consisted of safety of password and security, security of workstation, emails and security of internet and physical security and protection of academic records and health data according to Buckly, (1974) and United state congress report, (1996).

In our view, we also felt it strongly that, the ISAT curriculum was a good beginning and it covered the majority of the challenges and problems UTM deals with on a daily basis, but along the process, we decided to advance further by consulting and evaluating what the information security industry would says is vital for end-user education by seeking their opinion, this become an eyes opener to another two concepts we had not considered previously that is the, social engineering which consist the integration of culture, believes and norms of the people and the principle of low or least privilege. This where not initially perceived as a major problem at MU, we now decided we would like to inculcate social engineering and the principle of least privilege to educate our users before they become a problems, although the addition of these two topics to the ISAT program for the monthly activities, we first came up with an initial list of topics with the idea and the believe that they could be adapted to meet our needs at the time. This initial list consisted of requirements for new password and digital millennium copyright according to (digital millennium copyright act) DMCA, identity theft and the university's acceptable use of information security policy.

B. Defining the Target Audiences

We initially bear in mind that we would have two different audiences that is the students and the faculty/staff. While we are nurturing this idea, we quickly realized that it's not as simple as we thought as we actually have multiple or more than one audiences within the two groups and it is likely we would have more than what we have recognized so far.

C. Students

The broad array of categories of students includes on-campus students living in residence halls within the university premises and off-campus students living in a self rented apartment outside the university premises. To consider these two subsets of the student population in different location will require different methods of deliveries, which will be discussed later in this paper

D. Staff and Faculty Member

While most staff and faculty can be integrated into a general category for the purpose of our information security awareness program, we do recognized earlier on

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that many of the our faculty and staff members in administrative positions, such as deans of faculty (DOF) and head of department (HOD) belong in a category of their own. The people in these positions do not have enough time to devote in attending an enormous hours of training class or reading a long article, so we intend or have to consider their needs in a separate manners . In getting the upper level of administrators involved in the security awareness program was vital. With their signing in, we adduced that we would be more likely to obtained co-operation from the rest of their department.

IV. METHODOLOGY FOR ISAT DELIVERY

In this particular portion of the planning process or phase was very fundamental to the success of our ISAT program. We had to consider not only the topics or the content of the program and the appropriate and adequate ways to deliver those topics, but we also need to take into consideration our different audience factions.

A. Based On Students

In selecting our method of delivery, we have decided on a few methods of delivery that would work for all students by focusing on mass e-mail, our monthly technology newsletter articles, advertisement in the student newspaper and groups or clubs presentations. Additional methods we also planned to put in-place to reach on-campus students specifically included posters in residential and dining halls, mail-box stuffers and table-tents in all dining halls. For off-campus students, we engaged campaigns posters in the student unions, classroom buildings and frequently visited places such as the university library or computing sites, however, we had to bear in mind that exposure is not fully guaranteed as it is in the residence halls and dining places. In our observation, there are some factors that distinguish or differentiated students from faculty or staff. For instance, we can reach out to faculty and staff with in-person or personal training than their department coordinates. With students, it is much more cumbersome to coordinate training face-to-face so, we decided to concentrate and strengthen our focus on web-based training for them.

B. Based On Faculty and Staff

For faculty and staff members, we planned and decided to use in-person and online training, campaigns poster, the monthly technology newsletter articles, payroll stuffers and targeted mass e-mails. Additionally, we also decided to make use of a concise high-level overview of the information security training to fulfill requests from administrators and people who are seeking to fix us into a preliminary scheduled meeting.

V. IMPLEMENTATION

In the next phase, UTM began implementation on the ideas that where formulated during the planning process or phases. A comprehensive information security awareness training (ISAT) program was created that has two components: topic specific monthly activities and the general information security awareness training (ISAT) program.

A. Our Monthly Activities

In our monthly activities UTM chooses one “hot and interesting topic” per month on which we spotlight the efforts of our information security education. The goal and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

objective of the monthly topic and the activities is to enhance the user's knowledge and the awareness of a particular information security challenges. Also, we hope and believed that we can get security-related information out to the campus premises in an organized manners and consistent fashion.

B. Monthly Topic for January (Example)

The theme for January information security training (ISAT) program was "Security and Password Safety". This topic was affiliated and tied to a compulsory campus wide-range password reset campaign that was initiated. The topic was also covered in our article for information security connections newsletter ("What's the need and why change of Passwords?"). We created and mounted a poster that included instructions on passwords changing and listed password best practices to follow. We hung this poster in strategic areas where most students can observe and read, such as the computing sites, dining and residential halls. We also made it available to all departmental computer personnel support for distribution in their buildings. Furthermore, we forwarded a mass e-mail to all faculty, academic and non academic staff and students with information on the password reset campaign and general password best practices code.

C. Monthly Topic for March (Example)

The theme for information security training program for March topic was "Cyber-Security". We invited a guest speaker from the Cybernetic Malaysia, a cyber crime task force to speak about their various on-going, current and future cyber-security efforts. We tailored and fashioned a presentation to all business and information technology (IT) classes at graduate and postgraduate level that covered issues in general security and information auditing. Finally, we created an information security awareness website that included links to and descriptions of various security sites of interest to our UTM premises and other academic milieu.

D. Security Awareness Training

The second component of the information security awareness training (ISAT) program is our security awareness training course itself. The materials used in this course are compiled during the planning stage and process of the program. This first of this training was implemented in early January 2013.

E. In-Person Training

The key factor of our information security awareness training (ISAT) program is currently based a one-hour, in-person training tutorial class. This class covers a wide and variety of topics, including safety of password and security, physical security and workstation and security of internet and e-mail to name a few. The ISAT is delivered without a charge to departments and students. The availability of this program was initially advertised to our computer support departmental personnel and community, who then contacted ISAG-UTM when they deem it fit to schedule their training. The course instructors are from SPACE-UTM and they do meet with each departmental support personnel prior to delivering the training program to review and preview all material and note any special circumstances or error that might exist within a particular department. It is then training would be delivered to the department. Some departments agreed to make the ISAT program mandatory while others decided to have it as an optional. This decision was left to the discretion of the department. Some group of student has also opted to take

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

advantage of the ISAT program. These groups of students have a contact and representative of SPASE-UTM to set up the time and location for the program and classes respectively. Up to date, it has been noted and recorded that almost 900 faculty, staff and students have attended and benefited from the Information Security Awareness Training (ISAT) program.

F. Our Online Based Training

Another ISAT training option that we deep fit is currently under development is an online training course created by using Web-CT that would be ready to commence in the fall of 2013 precisely. This Web-CT course entails the same information that is embedded in the in-person training however; this method of delivery will allow us to expand and reach out to those users who do not have the opportunity to be served by our traditional training method. For example, we have students studying abroad, residing outside the campus, part-time students and faculty and staff members at outreach sites across the country. The online training course will allow these users to receive our information security awareness training (ISAT).

VI. FINDINGS

We realized that our ISAT program does not address all the need require by the users, which means there is a need to adjust the program to meet their need. When adapting our ISAT program to meet our current needs, we were pleased that from the starting point we had already built in flexibility. This flexibility allowed us to make an adjustment or amends where necessary without the integrity of our ISAT program had been compromised. By being flexible and maintain the flexibility with our delivery methodology, we were able to reach out to quite a number of people, in this regard, we realized that the campus community is generally receptive to the ISAT program and they are happy to be given the opportunity to learn more about our information security awareness training.

VII. OUR PLANS FOR IMPROVEMENT

Currently, we are hoping to work with specific academic professors especially, those who have taught computer intensive courses in all ramifications to make the Web-CT tutorial course mandatory for all students that have been enrolled or admitted into the university will also entails hypertext entry that will enable student or participant to actively add questions, comments, examples, arguments, further resource and other contribution to the text, by this all participant will be able to read and respond to the hypertext entries and create a discussion related to the lecture text. We also hope to make in-person and the online training compulsory for all staff and faculty members. In addition, we also planned to develop and enhance policies and procedures that would enable us to adequately address new information security threats or issues without having to design another information security program each time. We hope to continually identifying new delivery methods, such as working with complexes of local apartment that accommodate students to distribute fliers and mailbox stuffers. We are also looking ahead into using pre-defined communities (such as new students groups, student's residential hall, learning centers and communities) as an information dissemination avenue. Since our ISAT program is still new, the metrics to determine the level of improvement are cumbersome for us to define at the moment. For instance, we have seen an increase in reports regarding threats to information assets and computer viruses on daily bases, but we are unable to link this trend of reports to a specific cause. Are more computer viruses being circulated on the internet everyday or has our ISAT program led to the increased of report on virus infections? Acquiring

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

statistics in this regard will allow us to measure our success of ISAT program more accurately. Finally, we also plan to continually revise the current information security awareness program to address new issues or topics, with the intention of adjusting and keeping the program relevant to our users and to the academic community as a whole.

VIII. CONCLUSION

Information security awareness training program is required by all organization either large or small medium. Organization who see the need of protecting there valuable asset should educating the user. The users play an enormous role in information security believing and bearing in mind that, people are the key and the answers to information security that mean, people can breach information security and they can also secure it, if they lack or have the adequate and relevant information security awareness training. As many organization are envisaging new threats and challenges in information security, the information security awareness training (ISAT) program should be flexible and adjustable to meet the current challenges and that of the future by that, a sustainable information security awareness training program (ISAT) would have been established to meet the future need without jeopardizing the current. The ISAT program will also accord the users to get abreast with the knowledge of sensitive and personal data, knowledge of the organization security goal and security policies and the skills needed towards information security administration and management and to change there perceptions and reasoning when come to information security issues and also where sharing information and data exchange are required. Our flexibilities in this program, the delivery methods and the general receptiveness towards the ISAT program and the wiliness to learn more about our information security awareness training by the campus community at large has given us the impetus to further improved on the ISAT program, maintaining flexibilities and be able to reach out to more people.

REFERENCES

[1] Buckly James L, . Family educational rights and privacy act of 1974 (FERPA)

[2] United State congress. Health insurance portability and accountability act of 1996(HIPAA).

AUTHORS PROFILE

Oyelami Julius Olusegun Is a graduate of electrical engineering technology with electrical power option from college of science and technology Ghana in collaboration with French institute of technology in 1996. Having served in engineering industry for over 10 years, in the quest for computer knowledge, he enrolled into Kursk state technical university, Russia where he obtained a B.Sc. in computer system and network engineering in 2009 and several professional certificates in IT with over ten years industrial experience in engineering. Currently is a postgraduate research student in department of information system, faculty of computing, University Technology Malaysia (UTM), and a member of information assurance and security research group (IASRG-UTM), His research interest are in information security management, social networking and information sharing and Information System. He is a professional member, association for computing machinery (ACM) and an academic member, association for information systems (AIS). He has recently extended his research interest into ICT, cloud and grid computing.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Norafida Binti Ithnin is currently a senior lecturer and head of department in Universiti Teknologi Malaysia (UTM), faculty of computing. She received her B.Sc degree in Computer Science (Computer Systems) form Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia in 1995 and her M.Sc degree in Information Technology (Computer Science) from Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia in 1998. She bagged her PhD degree in Computation from UMIST, Manchester, United Kingdom in 2004. Currently, her main research interests are security management and graphical password.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Enhancing the Conventional Information Security Management Maturity Model (ISM^3) in Resolving Human Factors in Organization Information Sharing

Oyelami Julius Olusegun
University Technology Malaysia
Faculty of Computing
Department Information systems
Skudai, Johor Bahru 81310

Norafida Binti Ithnin
University Technology Malaysia
Faculty of Computing
Department of Information system
Skudai, Johor Bahru 81310

ABSTRACT

Information sharing in organization has been considered as an important approach in increasing organizational efficiency, performance and decision making. With the present and advances in information and communication technology, sharing information and exchanging of data across organizations has become more feasible in organization. However, information sharing has been a complex task over the years and identifying factors that influence information sharing across organization has becomes crucial and critical. Researchers have taken several methods and approaches to resolve problems in information sharing at all levels without a lasting solution, as sharing is best understood as a practice that reflects behavior, social, economic, legal and technological influences. Due to the limitation of the conventional ISM3 standards to address culture, social, legislation and human behavior, the findings in this paper suggest that, a centralized information structure without human practice, distribution of information and coordination is not effective. This paper reviews the previous information sharing research, outlines the factors affecting information sharing and the different practices needed to improve the management of information security by recommending several combinations of information security and coordination mechanism for reducing uncertainty during sharing of information .This thesis proposes information security management protocol (ISMP) as an enhancement towards ISM3 to resolve the above problems. This protocol provides a means for practitioners to identify key factors involved in successful information sharing. The first one is the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

identification of all stakeholders to be incorporated into information flow. The second is the integration of the existing information sharing legal frameworks, information sharing protocols, information security standards from the ISO/IEC 27001 and management standard ISO9001 with the existing information security management model (ISM^3). An experiment was conducted to evaluate the performance of the proposed protocol. The results revealed that interoperability, culture and behavior towards information sharing improved by an average of 10 percent.

Categories and Subject Descriptors

[Information Systems]: Information Security, Data and Information Sharing
[Information Security Management]: Security and Protection
General Terms: Information Security, Human Factors and Management

Keywords: Information Security Management, Information Sharing and Human Factors.

I. INTRODUCTION

Most recently, the report from the national government for information sharing strategies, (2009), Meyer. (2009) and Rodgers, (2010) has observed moral hazard, poor leadership, inadequate information management practices, a non-sharing culture, the negative behaviors of people towards information as well as confidentiality of information share and the privacy and accountability have been noted as a major factors against information sharing today. In another submissions by Sung Jun Jo and Back-Kyoo Joo (2011) observed that culture, psychological commitment and behavior are antecedents of information sharing, it was noted that the intention of employees to share or not have a role to play in effective information sharing, either negatively or positively. From the strand of information sharing research, researchers above have indicated factors that influence information sharing within an organization and its boundaries and as a result, information and data leakages, information insecurity, lack of compliance and management, loses of confidentiality on information shared have increase tremendously, while interoperability among employee and the system have decreased significantly. To keep up with the recent trend in information security management, organization must build a strengthened and formidable information security management system ISMS for it information sharing Kwon et al. (2007). Information behavior seems to evolve as a result of the interplay between elements in cultural contexts. Information behavior, cultural and behavioral difference of indigenous people proved to be the underlying factor that determines the outcome of information sharing across cultural boundaries. The differences in information behavior of literate and indigenous people can influence the extent to which information is shared across cultural boundaries and can undermine it's successfully accomplishment. Taking into account that cultural contexts as well as information products and services play a significant roles in people's information behavior. It seems obvious that information behavior, organization behavior, culture, confidentiality and trust as becomes a factor to be reckoned with when information sharing is planned across organization.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. AIMS AND OBJECTIVES

In this paper, we aimed at developing an information security management protocol (ISMP) as a compliment to the existing and conventional information security management maturity model (ISM^3) as an alternative tool that could be helpful to control, understudy human behavior and resolve human factors by building trust among employee's and compliance towards information security policies, rules, laws and regulations for effective information sharing. It also aims at addressing the impact of information sharing failure within an organization and the perceptions organization hold as regard to the management of information security. The question is, (1) How organization would evaluate it current state of information security towards information sharing? (2) What are the factors to consider while creating an information security management towards information sharing? In order to achieve the aim in this paper, we stated the following objectives:

1. To formulate information security management process that could be used to standardized information sharing.
2. To integrate laws and legislation in information sharing, information sharing protocols and relevant ISO27001 and 9001 standard with the existing ISM3 and
3. To develop and propose information security management protocol towards the enhancement of the existing ISM3 as a complement for rendering effective information sharing within organization and its partners.

III. METHODOLOGY

Our method in achieving this stated objective was divided into phases; the first phase is to acquire data. The data acquisition was done by interview, questionnaire and e-mail correspondence. The central focus in this data acquisition is the departments of human resources, operational and management department. The goal of this first phase is to identify the type of data the organization shared on daily bases.

The second phase is to establishing information security awareness training program (ISAT) as a contributing factor to formulate information security management process that could be use to standardized information sharing as stated in objective 1. The goal of establishing ISAT is to enable us to (1) Indentified all stakeholders to be incorporated into the information flow, (2) design policy and governance for information sharing, (3) develop rules for information and data elements for sharing and(4) determine a common operation system for information sharing as a contributing factors in achieving objective 1.

In the third phase, we intend to evaluate the existing standards, frameworks and legislation. Theses existing standards are: ISO27001 and ISO9001 respectively, while the existing information security frameworks like ISM3 would be consider and finally, the legislation (laws and regulation). This legislation comprises of Data Protection Act (DPA) of 1987, Computer Misuse Act (CMA) of 1990, Privacy Act (PA) of 1985, Human Right Act (HRA) of 1998, Common Law Duty of Confidentiality (CLC), Access to Information Act (AIA) of 1985 and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Freedom of Information Act (FOIA) of 2000 and information sharing protocol (ISP) that consist a set of good practices to follow when sharing information. The goal of the third phase is to identify the strength, the impact and the weakness of the existing standards, framework and legislation for the selection purposes and this will serve as an input in achieving objective 2 in this paper.

In the fourth phase, we would integrate and justify the reasons why those components and clauses where selected form the laws and legislation in addition to information sharing protocols and relevant clauses from ISO27001 and ISO9001 standard with the existing ISM3. The selection and integration process would be made easy after indentified the strengths, the impact and weakness of this standards, frameworks and legislation from the third phase. The justification process would also be carefully outlined according to each selected items. The goal of this phase is to identify the right components, clauses and sets of good standards of practices when sharing information is concern.

The fifth phase is the development and enhancement process, in this phase we intend to enhance the conventional information security management maturity model (ISM3) into information security management protocol (ISMP) as a compliment for rendering effective information sharing within organization and its partners as stated in objective 3. To achieve this, a careful recommendation would be outline based on phase 1 (data source), phase 2 (establishing information security awareness training program), phase 3 (Evaluating the Existing Standards, Frameworks and legislation) and Phase 4 (integration and justification process), the goal of this fifth phase is to enhance the existing and conventional ISM3 from the careful and selected recommendations towards the development and enhancement of ISM^3 and to propose information security management protocol, so as to achieve the third objective in this paper.

A. Case study: the organization of YHLI

YHLI is one of the leading manufacturing companies with around 2,500 employees in the formal capital of Malaysia (Kuala Lumpur) with over 500 employees in Saber and Sarawak. The company has more than 5 locations around Malaysia. This study focuses on one divisions of the organization on how they share information and what are the challenges they faced as they are trying to create a balance information sharing system. As one of the leading manufacturing company in the south-east of Asia, the organization manufactures chemicals such as the industrial chemicals, food chemicals and agro-allied chemical, paints etc. The company serves a wide range of industries, such as food chemical, pharmaceutical, biotechnology and many more. The company has following different departments: Finance, accounting, marketing, information technology, production, purchase, customer service and the human resources department that take cares of employees data. Such data involve personal, non-personal, sensitive and non-sensitive data. The organization shared information with external party such as the Malaysian Health Department that provides medical services to the organization, Insurance firm that insured the legal property and its employees, banks (financial institution) that relate to the employees loans etc and the stakeholders. The stakeholders are people who have direct or indirect

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

interest and shares within the organization and they need to share information with the organization regarding there annual dividend and other capital or investment benefits.

In addition, the information technology (IT) Department of YHLI Company has more than 20 employees serving around 100 users. Apart from employees, there are 4 consultants working on SAP implementation. The company has successfully implemented SAP in 2008 for all major business functions and is currently using it as their ERP system.

This organization was chosen as a subject of analysis due to its geographical location and the enrichment in terms of multi-cultural and devise ethics group and to serve as the specific in-depth case study for the investigation on how human factors that could influence the sharing of information and what factors to be consider when planning and implementing information security management for effective information sharing and data exchange across the organization.

IV. DATA ANALYSIS

In this session, there is a need to analyzed and interpret the dataset from the data entry. The data entry was done on a Microsoft Excel after correlating the entire questions attempted from all respondent. It should be noted that, the questionnaires were distributed at random to the employees of YHLI. From the survey identity, the total numbers of respondent is 35 and there are 37 questions in the questionnaire, question 1 to 25 focuses on culture and behavioral questions, information security questions, education, training and awareness questions, experimental validation questions respectively while, questions 26 to 37 is an interview question. In details, question 1-8 based on the culture and behavior of employees. This question is tag dataset A, table 1 below shows the frequency table of responses to the questions as dataset A.

Table 1: Culture and behavioral questions (dataset A)

Response	Frequency								
No	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Total
Yes	32	12	16	10	22	17	11	10	130
No	3	14	10	16	9	5	15	5	77
Blank	0	9	9	9	4	13	9	20	69

Key: Q means question

From table 1, out of the total number of the questionnaire, this frequency table tag (dataset A) comprises only questions (Q) 1 to 8. It should also be noted that, the blank dataset will be considered as a missing values; hence, it will not be relevant in this thesis. Question 1(Q1) one indicate there believe in culture and out of 35 responses to question one, 32 says yes, 3 says no. This indicates that almost all employees believe in culture as a way of life. Question two is know if culture and there individual believes influence there behavior towards others, in response, 12 says no, while 14 says yes, indicating that the particular respondent to Q2 do not influence others with his/her culture and behavior , the other 12 influenced other with there culture and behavior . Observing Q3, this is to figure out if the employees share information among same culture, the dataset A

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

indicates that, 16 responded with yes while 10 says no which means that some employee shared information based on same culture and believes, it also means that, they are more open-up to other employees with same culture. In Q4 the responses are 10 for yes and 16 for no, this also indicate that, most of the employees are easily going among other cultures, believes and ethnic groups while the other 10 are not. In Q5, Twenty-two (22) have been influenced by other culture and believes while 9 responses negatively, this means that, they are not influence by other culture. Looking at Q6 subset of Q5, 17 responded that the impact affect there sharing behaviors towards others while 5 says no. In Q7, eleven (11) says they have been able to influence others with their own culture, while 15 says No, and in question 8 (Q8) 10 responded that those influence by them developed negative information sharing behavior toward others and 5 remain negative towards the question. Figure 1 show the bar chat that further illustrate dataset A.

From figure 1, the total response to yes in dataset A is 130. In dataset A analysis, yes means that, the organization lack culture and behavior towards information sharing and also there is a general indication regarding culture and behavior show that, culture and behavior plays important roles in information sharing. The organization must initiate a common ground for culture and behavior among employees as it could strengthen information sharing therefore, there is a need to improve on culture and the behavior of employees. To summarize dataset A, the word yes means, the organization need to improve on culture and behavior towards information sharing as the organization is a multicultural environment.

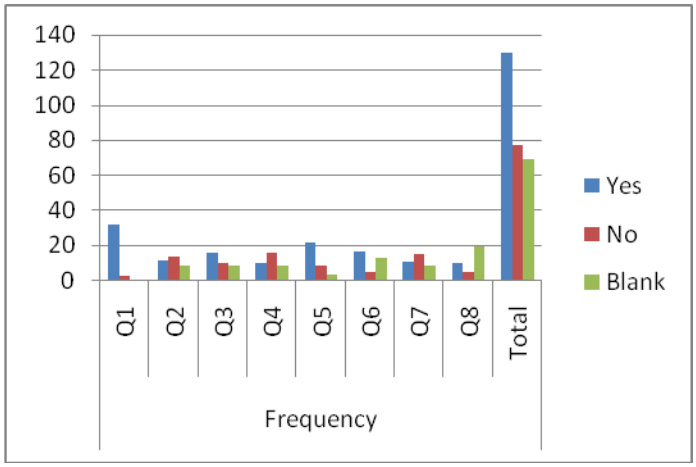


Figure 1: Bar chart of dataset A

V EXPERIMENTAL VALIDATION

Under this session, there are needs to further explain experimental validation and its significances in this research. Experimental validation could be the extent of which the finding is genuine and due to the independent variable been manipulated, sometimes, it is hard to interprets the information that where obtained from the interviews and questionnaire due to social desirability bias, this is the tendency to provide socially desirable rather than honest answers during the interviews and on the questionnaires another challenges in experimental validation is the complex interactional process and self-fulfilling prophecy. This self-fulfillment prophecy might be seen as a tendency for someone expectation about another person to lead to the fulfillment of those expectation, that means depending on another person to fulfill a task. These three factors may have influence on our data collection, to avoid this, we perform an

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

experimental validation to determine the genuineness of the data we collected. Table 1.2 shows the frequency of the response of the employees who attempted the questionnaires, this dataset will be tagged datasets D. It is to note that 35 employees responded to this experimental validation questions. Table 2 below shows the frequency in the responses to the experimental validation question.

Table 2: Experimental Validation questions (dataset D)

Response	Frequency					
No of Qs	**Q21**	**Q22**	**Q23**	**Q24**	**Q25**	**Total**
Yes	**5**	**1**	**28**	**29**	**5**	**68**
No	**25**	**27**	**0**	**0**	**23**	**75**
Blank	**5**	**7**	**7**	**6**	**7**	**32**

From the table 2, the experimental validation question carries only 5 questions, Q21 to Q25; these questions are structured towards the sincerity and confidence of employees who contributed in answering the questionnaire. This would enable the researcher to study the variables and to judge the experiment has been done without prejudice, fear and social desirability bias. This frequency table for this dataset D revealed that, only 5 employees responded positively to Q21, 25 employees say No and 5 is blank (missing values). In Q22, 27 says No, 7 blank, while only 1 employees responded positively meaning that, only 1 employee would not entertain fear even when been observed. In Q23, almost all the employees responded positively with 28 showing that, they are honest enough during the filing of the questionnaire, while in Q24 employees yes frequency 29 , this also indicate that, they have answer the questions to the best of there knowledge. Observing the last question in the table 2, 23 employees where negative with response of 23 revealing that, they are not afraid that there commitment towards transparency might affect there job while 5 say yes and 7 blank. From this dataset, it will be concluded that, employees where honest enough during this data collection and the answers given to the best of there knowledge. The bar chart in figure 2 will further illustrates on the overall result of dataset D.

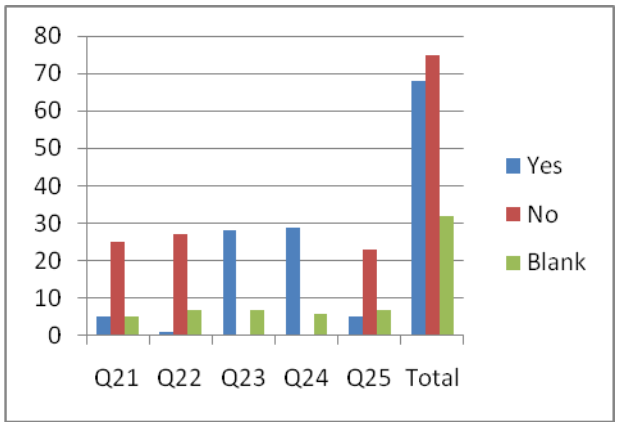


Figure 2: Bar Chart for Datasets D

Observing this figure 2, No is the highest, this shows that an average employees responded without been influenced by the demand characteristic of the situation, even they have been observed, it does not influence there behavior towards answering the questionnaire, they have been honest enough during the filing of the questionnaire, they have been able to answer the questions to the best of there knowledge and they where not afraid that the commitment made towards transparency might affect there job.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. FINDINGS

It is observed from the data analysis that, information sharing does not take place adequately due to lack of leadership, information management practices that restrict sharing of information, privacy and accountability concern, absence of clear value proposition, culture that probably resistant to sharing information and inadequate security education, training and awareness and as a result, this have brought negative impart to the organization in respect to loses of interoperability, the ability of systems and employees working together if there is no good culture and behavior towards information sharing, loses of confidentiality, information leakages, information insecurity, financial and data loses would be inevitable to the organization information assets.

VII. IMPLEMENTATION

In achieving the first objectives, what we did was to first evaluate the current information security practices of the organization and we compared and contract it with the data we collected for analysis, from the analysis, we discover that, their are lapses in the organization information security system, although data analysis revealed that, the organization have some considerable information security policies and framework but could not resolve the human error that where observed. This Human error is contributed by negative culture and behaviors towards information sharing, lack of trust, confidentiality, improper management responsibility towards information sharing, privacy and accountability, lack of leadership roles in information sharing coordination etc. that might result into fraud (Illegal alteration of information for selfish interest) and corruption (wilfully revealing information to unauthorized person for selfish interest) and Incompetence as a result of insufficient information and security education. We then indentify all the stakeholders to be incorporated into information flow of the organization, develop rules and data elements for sharing and the exchange of information to determine a common operating system. The identified stakeholders are: the banking and insurance institution, health ministry, education ministry, external distributors and the customers. With this, we are able to establishing a common trust by improving (1) the employee's act of collaboration and (2) build trust and interoperability.

In achieving the second objective, what we did is to integrate the carefully selected clauses from the ISO27001 and 9001 standards, legal framework and a set of good practices from the information sharing protocol to enhance the conventional ISM3 model to address the human error in information sharing. Then we developed a culture that will rewards information sharing behaviours. This was achieved by promoting mechanisms for sharing information; This mechanism requires the development and execution of the information sharing strategic implementation plan (ISSIP). This implementation planning and execution will occur at all levels. The success of sharing will be a unified and coordinated set of initiatives will span from department leadership to system owners, operators and other entities that share information with the organization. With this, we are able to remove obstacles and welcome better tools that help the organization to succeed in sharing information.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The third objective was achieved with a careful recommendation. These recommendations were noted during the process in achieving the stated objective. Those recommended clauses; standards and frameworks are used in the enhancement process. It is believe that, the recommendations will guide the organization towards effective information sharing within the organization and its external partners. It should also be noted that the recommendations were also induced after careful studies and analysis of the datasets, close-ended interview and the existing information security of the organization. With the recommendations, we are able to propose an information security management protocol (ISMP).

A. The Proposed Framework

This proposed information security management protocols (ISMP) consist of the selected information security standards from the ISO27001 and quality management system from the ISO9001, these are the two basic standards for information security and effective management respectively while the information agreement and protocol are sets of procedures to follow when considering sharing information within and across the organization. Looking at information sharing legal frameworks served as a legal requirements when sharing information that relate to personal and sensitive data, this also serve in protecting the interest of those who involves in the sharing of information while culture and trust will assist the organization in the establishment of a common trust among employees and developed culture that will reward information sharing within the organization. Indemnity serves as a measures towards punishment to any party that breach the agreement made before and after sharing information, while consent is a kind of documents sign and agreed to by both party who intend to share information or who involves in the sharing of information, in this regards policies and governance in the sharing of information will be clearly stated and the identification and development of rules and data element for sharing will also spelled out clearly. The confidentiality agreement and statement is to indicate to any party sharing the information that, the information been shared is accurate and there is no loss in value of those information. Education, training and awareness is to set the pace for information and security education, this enable the employees to understand why some information are sensitive and also to distinguished all data elements from one another, it will also enable employees to handle information accurately.

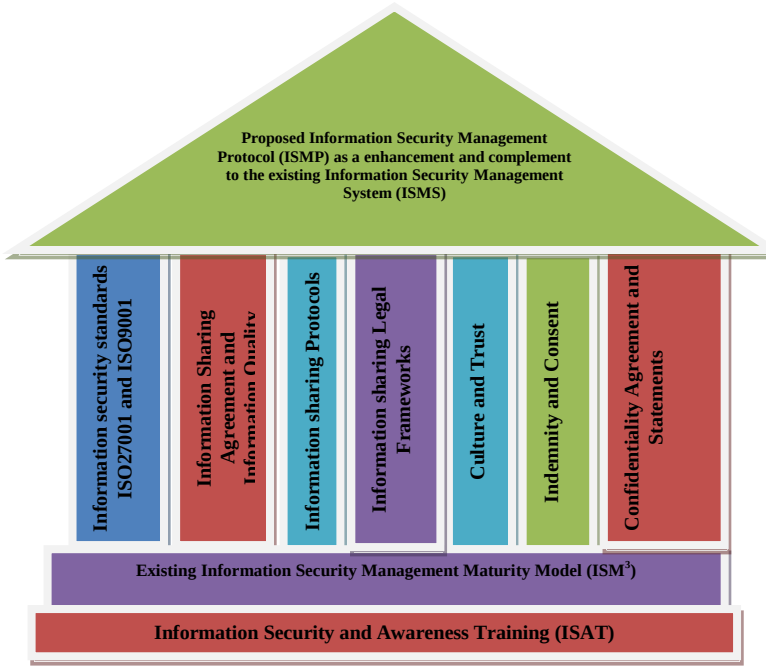


Figure 3: The propose ISMP

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VIII. FUTURE WORK

The first step in this direction would be a survey to all certificate users of the ISM3 framework focusing on the use of the ISM3 tool, the perceived efficiency, and reliability etc, a study like this, in cooperation with IT organization in its designing phase and interview with information sharing experts will stir up a new research area. Another idea that has grown stronger during this study is to interview acknowledged experts on the management of information security in organizations, and to analyze these interviews in line with the ideas of grounded theory of information sharing, communication and technology (ISCT) to search for themes and patterns in their views on the issue at hand. In the case study of organization, most of the materials presented in this paper are general, in the sense that, it does not directly tackle the chaotic reality in which organizations have to try to resolve their information sharing problems. In the practical situation, therefore, it would be very valuable to study various organizations in their efforts to manage information security towards information sharing.

IX. CONCLUSION

Further, this paper reviews the historical and academic contribution on information sharing over the last 30 years. We started with the review of articles in information sharing and the attempt and effort to define information sharing as related to organization and some existing models, frameworks and standards that are related to information security management in the quest to develop an enhancement protocol for information sharing. This paper also highlights the various legislations that have been passed into law to moderate information during sharing and after.

It introduced the concept of information security management protocol (ISMP) as a techniques based on the existing information security model, standards and information sharing legislation (the laws that governs information in the sharing context. Some information sharing expert and researchers like Hepworth, (2007), Williams et al. (2008), Sung Jun Jo and Back-Kyoo Joo (2011), Gary Rodgers, (2010) and many others have seen the need to secure and improve information sharing in organization through positive behaviour, good culture and management practices, while some other researchers like Constant et al. (1994), Brown and Duguid, (2000), Fulk et al., (1995) believe that information sharing is base on social, norms, believe , culture and behaviours, it is also noted from the trend of literature that challenges confronting information sharing is basically on human and researchers like Albert and Barabasi, (2002), Newman, (2003), Kelle and Abrials, (2007), Razavi, (2006), Rafaeli and Raban, (2005). indicated that, information sharing challenges is not to be solely addressed by technology but through a non technical aspect based on human practices, sharing behaviour, culture that encourage sharing of information with the help of leadership and compliance.

REFERENCE

[1] Albert R. and Barabasi A (2002). Statistical mechanics of complex networks. Review Modern Physics, 74, 47-79.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[2] Brown J.S. and Duguid P. (2000). The Social Life of Information, Boston, MA: Harvard Business School Press.vol 4.

[3] Constant D., Kiesler S. and Sproull L. (1994). 'What's mine is ours, or is it? A study of attitudes about information sharing', Information Systems Research, Vol. 5, No. 4, pp.400–421.

[4] Data Protection Act (1998). Part II (Rights of data subjects and others), Section 10, Office of Public Sector Information and accessed 6 September 2007

[5] Data Protection Act (1998). Part III (Notification by Data Controllers), Section 21, Office of Public Sector Information.

[6] Data Protection Act (1998). Part VI (Miscellaneous and General), Section 55, Office of Public Sector Information, accessed 14 September 2007 Directorate Access to Information and Privacy, (2009).

[7] Fulk J., Flanagin A.J., Kalman M.E., Monge P.R. and Ryan T. (1996). 'Connective and communal public goods in interactive communication systems', Communication Theory, Vol. 6, No. 1, pp.60–87.

[8] Kwon S., Jang S, Lee J and Sangkyun K. (2007). Common Defects in Information Security Management System of Korean Companies. Journal of Systems and Software. 80(10), 1631-1638.

[9] Kelle Juris and Abrials Diana, (2007). Overcoming Information Sharing Obstacles and Complexity.pg 200.

[10] Meyer, H.W.J. (2009). "The influence of information behavior on information sharing across cultural boundaries in development contexts" *Information Research*, **14**(1) paper .

[11] National Government Information Sharing Strategy,(2009). Unlocking Government information assets to benefit the broader community, ISBN: 978-1-921600-44-9, Copyright of all Australian Governments.

[12] Newman M. E. J. (2003). The structure and function of complex networks. SIAM Review, Vol. 45, No. 2, pages 167-256.

[13] Rafaeli, S. and Raban, D.R. (2005) 'Information sharing online: a research challenge Int. J. Knowledge and Learning, Vol. 1, Nos. 1/2, pp.62–79.

[14] Rodgers G., (2010). Hint print intelligent, Government Information Workflow: Managing Information effectively, gary.rodgers@hp.com

[15] Razavi Maryam N and Iverson Lee, (2006). A Grounded Theory of Information Sharing Behavior in a Personal Learning Space. November 4–8, 2006, Banff, Alberta, Canada.Copyright ACM 1-59593-249-6/06/0011.

[16[Sung Jun Jo and Back-Kyoo Joo, (2011). Journal of Leadership and Organization studies August 1, 2011 18: 353-364.

[17] Williams Heyford, Rose Ginman and Gunilla Mariam, (2008)An introduction to information Sharing System for Small Organization. 3rd edition, pg 221.

ABOUT THE AUTHORS

Oyelami Julius Olusegun Is a graduate of electrical engineering technology with electrical power option from college of science and technology Ghana in collaboration with French institute of technology in 1996. Having served in engineering industry for over 10 years, in the quest for computer knowledge, he enrolled into kursk state

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

technical university, Russia where he obtained a B.Sc. in computer system and network engineering in 2009 and several professional certificates in IT with over ten years industrial experience in engineering. Currently is a postgraduate research student in department of information system, faculty of computing, University Technology Malaysia (UTM), and a member of information assurance and security research group (IASRG-UTM), His research interest are in information security management, social networking and information sharing and Information System. He is a professional member, association for computing machinery (ACM) and an academic member, association for information systems (AIS). He has recently extended his research interest into ICT, cloud and grid computing.

Norafida Binti Ithnin is currently a senior lecturer and head of department in Universiti Teknologi Malaysia (UTM), faculty of computing. She received her B.Sc degree in Computer Science (Computer Systems) form Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia in 1995 and her M.Sc degree in Information Technology (Computer Science) from Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia in 1998. She bagged her PhD degree in Computation from UMIST, Manchester, United Kingdom in 2004. Currently, her main research interests are security management and graphical password.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Robinson Edge Detector Based On FPGA

Farah Saad Al-Mukhtar
M. Sc. Student in Computer Science Dept. /College of Computer Sciences and Mathematics/University of Mosul. Mosul, Iraq

Dr. Maha Abdul-Rahman Hasso
Computer Science Dept. /College of Computer Sciences and Mathematics/University of Mosul.
Mosul, Iraq

Abstract— **Edge detection is one of image enhancement techniques that are used to extract important features from the edges of an image (e.g., corners, lines, curves). The aim of image enhancement is to improve the interpretability of information in images for human viewers, or to provide "better" input for other automated image processing techniques.**

The proposed work presents Programmable Gate Array (FPGA) based architecture for Edge Detection using Robinson edge detection operator in respect of both time and space complexity.

The algorithm are implemented using MATLAB 2010 language code as well as the VHDL language to deal with use of FPGA device, which was of a kind (Xilinx XC3S500E Spartan-3E), and it implemented on 8 bit grayscale image data, Robinson edge detection algorithm is produced using the pixel windows (3×3 windows) to calculate its output, make a comparison between the resultant image in MATLAB and VHDL by calculate the Peak Signal-to-Noise Ratio (PNSR), Root Mean Square error (RMSE) and the correlation between resultant images from MATLAB and VHDL.
cument. *(Abstract)*

Keywords-component; FPGA; Robinson Edge Detectot, VHDL, Windowing.

I. INTRODUCTION

Edges are places in the image with strong intensity contrast. Since edges often occur at image locations representing object boundaries, edge detection is extensively used in image segmentation when we want to divide the image into areas corresponding to different objects. Representing an image by its edges has the further advantage that the amount of data is reduced significantly while retaining most of the image information [1].

Edge detection operators are based on the idea that edge information in an image is found by looking at the relationship between pixel and neighbors, If a pixel's gray-level value is similar to those around it, there is probably not an edge at that point, If a pixel's has neighbors with widely varying gray levels, it may present an edge point, examples of edge detectors are Canny, Laplacian, Prewitt, Roberts, Sobel, kirsch, and Robinson filters [2][3].

This paper presents implementation of Robinson edge detector on FPGA using MATLAB and VHDL.

II. FPGA and VHDL

Field Programmable Gate Arrays (FPGAs) are part of current reconfigurable computing technology, which in some ways represent an ideal alternative for image and video processing [4]. FPGAs generally consist of a system of logic blocks, such as look up tables, gates, or flip flops, just to mention a few, and some amount of memory, all wired together using a vast array of interconnects. All of the logic in an FPGA can be rewired, or reconfigured, with a different design, according to the designer needs. FPGAs generally consist of a system of logic blocks (usually look up tables and flip-flops) and some amount of Random Access Memory (RAM), all wired together using a vast array of interconnects [5].

Usually engineers use a hardware language such as VHDL which is a hardware description language. It describes the behavior of an electronic circuit or system, from which the physical circuit or system can then be implemented.[6][7]. VHDL stands for VHSIC Hardware Description Language. VHSIC is itself an abbreviation for Very High Speed Integrated Circuits, an initiative funded by the United States Department of Defense in the 1980s that led to the creation of VHDL [7].

VHDL is designed to fill a number of needs in the design process. Firstly, it allows description of the structure of a design that is how it is decomposed into sub-designs, and how those sub-designs are interconnected. Secondly, it allows the specification of the function of designs using familiar programming language forms. Thirdly, as a result, it allows a design to be simulated before being manufactured, so that designers can quickly compare alternatives and test for correctness without the delay and expense of hardware prototyping [8].

III. DESIGN FLOW FOR THE PROJECT

The design flow for this project is represented in Figure (1). It shows the interaction between the VHDL design environment and the FPGA-specific tools.

- In the first stage, a design is created on VHDL, read the image from a file created using MATLAB or from FPGA's RAM.
- The code's syntax is verified and the design is synthesized, or compiled, into a library.
- The design is next simulated to check its functionality. Stimulating the signals in the design and viewing the output waveforms in the VHDL simulator allows the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

designer to determine proper functionality of the design.

- ❖ The outputs are saved in a file; this file is converted to image using MATLAB to see the output image after processing.
- ❖ Finally the design is processed with vendor-specific place-and-route tools and mapped onto a specific FPGA in software. This allows the designer to view a hierarchical view of the design, which can help in verifying a proper mapping procedure.

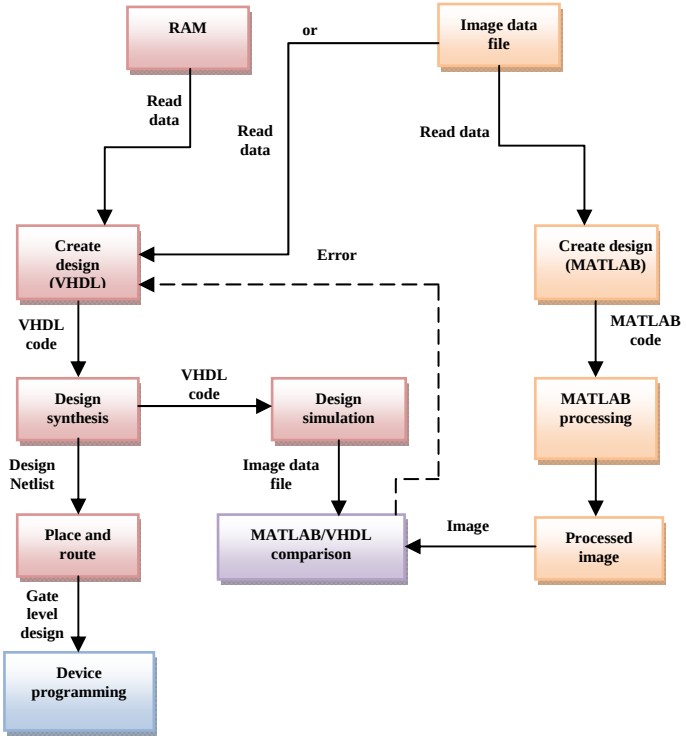


Figure 1; Flow design of the project

IV. ROBINSON EDGE DETECTOR

Robinson edge detection masks are called compass masks because they are defined by taking a single mask, and rotating it to eight major compass directions North, Northwest, West, Southwest, South, Southeast, East, and Northeast, Robinson masks are easy to implement because they rely only on coefficients of 0, 1 and 2 and are Symmetrical about their directional axis- the axis with zeros. Only need to compute the result on four of the masks. The results of the other four can be obtained by negating the first four results, Robinson masks is shown in equation [9]:

$$r_0 = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad r_1 = \begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & 1 \\ -2 & -1 & 0 \end{bmatrix} \quad r_2 = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \quad r_3 = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & -2 \end{bmatrix}$$

$$r_4 = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \quad r_5 = \begin{bmatrix} 0 & -1 & -2 \\ 1 & 0 & -1 \\ 2 & 1 & 0 \end{bmatrix} \quad r_6 = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \quad r_7 = \begin{bmatrix} -2 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

The edge magnitude is defined as the maximum value found by the convolution of each of the masks with the image. Notice that r0 and r6 are the same as the Sobel masks.

The Robinson edge detection algorithm can be found in the following manner:

1. Read the image.
2. Convolve the image with eight Robinson masks.
3. At each pixel location results eight numbers from the eight major compass orientations.
4. Use these numbers to compute the edge magnitude.

The first step in Robinson edge detector using MATLB is to convolve the image with eight masks, find the magnitude which represents the maximum value found by the convolution of each of the masks with the image and then compare the magnitude with threshold.

The algorithm on MATLAB can be represented by the following pseudo-code:

Define the masks window of the eight directions
For loop x –> number of rows
For loop y –> number of columns
window_vector = vector consisting of current window pixels
*mult = multiply (window_vector * x-direction mask)*
sum = summation of the mult
define threshold and compare the result of sum with it
end
end.
For loop x –> number of rows
For loop y –> number of columns
window_vector = vector consisting of current window pixels
*mult = multiply (window_vector * Y-direction mask)*
sum = summation of the mult
define threshold and compare the result of sum with it
end
end.
Repeat the previous steps for all directions
For loop u –> number of rows
For loop v –> number of columns
mod(u,v) –> the maximum value found by the convolution of each of the masks with the image

The design of the Robinson edge detector algorithm on VHDL is take the same steps as it was in MATLAB.

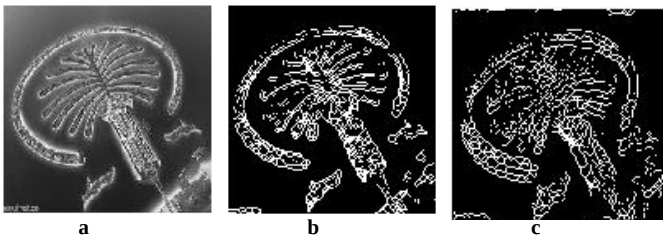
Figure (2) (*see the last page*) shows a graphic representation of the mathematics of the hardware Robinson edge detector.

As shown in figure (2), the image is read then stores the value of image in register (r) move the content of (r) to another register (w) which represents windows value, m represent a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

multiplexer (mx) where window values is multiplied by the kernel (k_x), then the results is added by adder (a_{xx}) then the result is divided by the no. of pixel in the window using shifting method, finally the result compared with threshold value if it is less than the threshold then the output is set to zero else the output is set to 255.

Figure (3) shows the image after applying Robinson edge detection in MATLAB and in VHDL.



a b c

Figure 3; (a) original natural image, (b) image after Sobel edge detector in MATLAB,
(c) Image after Sobel edge detector in VHDL

Figure (4) show the comparisons of the VHDL and MATLAB algorithm's results of Sobel edge detector implementation, also shown the histogram of the two images and the histogram of the different between two images.

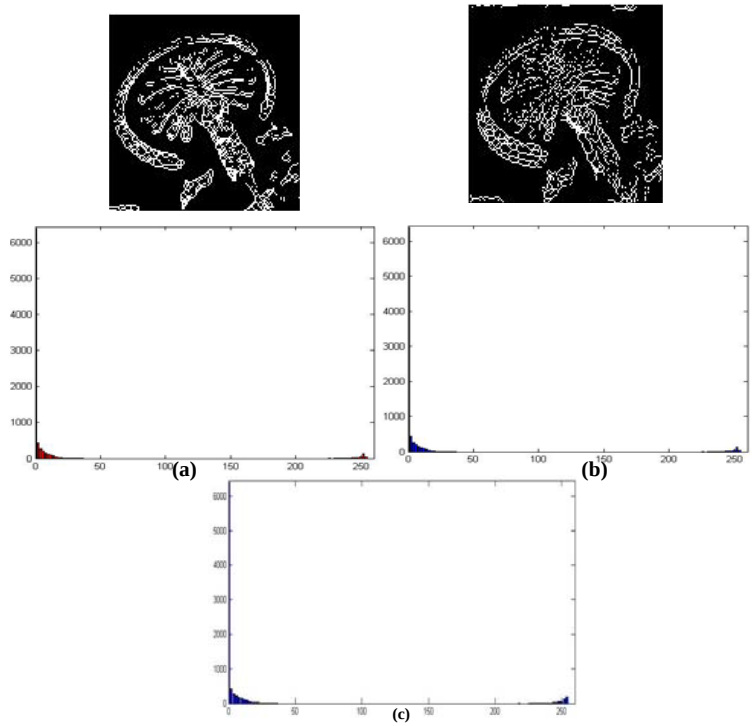


Figure 4; (a) image and its histogram after Sobel edge detector on MATLAB, (b) Image and its histogram after Sobel edge detector on VHDL, (c) Histogram of the different between two images.

V. DOWNLOADING ROBINSON EDGE DETECTOR DESIGN TO THE FPGA DEVICE

- Creating VHDL source
- Check the syntax of the design
- Creating design simulation

Figure (5) shows the simulation of Robinson edge detector

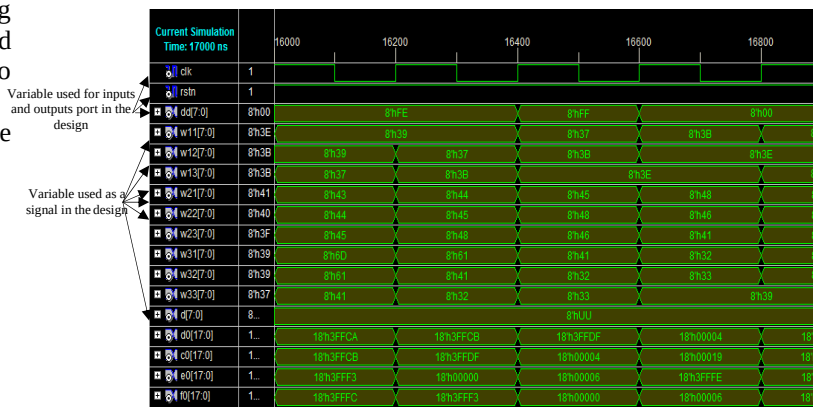


Figure 5; Simulation of Robinson edge detector

- Assign package pin

Figure (6) shows Assigning package pin for median filter

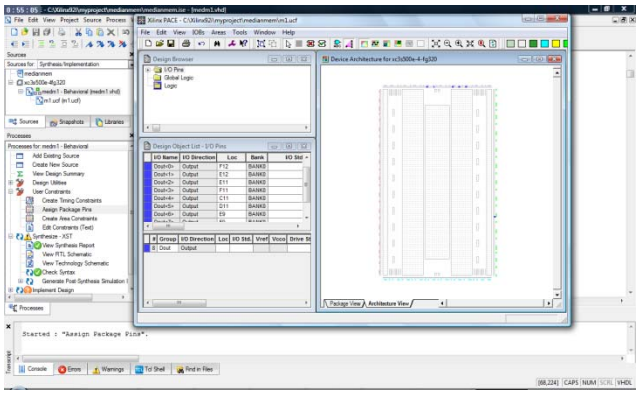


Figure 6; assigning package pin for median filter

- Downloading Robinson edge detector design to Spartan-3E

Figure (7) shows the device utilization summary of Robinson edge detector

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	513	9,312	5%	
Number of 4 input LUTs	1,105	9,312	11%	
Logic Distribution				
Number of occupied Slices	2,337	4,656	50%	
Number of Slices containing only related logic	2,337	2,337	100%	
Number of Slices containing unrelated logic	0	2,337	0%	
Total Number of 4 input LUTs	4,411	9,312	47%	
Number used as logic	1,105			
Number used as a route-thru	98			
Number used for Dual Port RAMs	3,120			
Number used as Shift registers	88			
Number of bonded IOBs	10	232	4%	
IOB Flip Flops	1			
Number of Block RAMs	1	20	5%	
Number of GCLKs	1	24	4%	
Total equivalent gate count for design	285,115			
Additional JTAG gate count for IOBs	480			

Figure 7; device utilization summary of Robinson edge detector

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSION AND RESULT DISCUSSION:

This work presents the implementation of Robinson edge detection operator on FPGA Xilinx XC3S500E Spartan-3E using VHDL by using windowing operators that are use a window to calculate the outputs.

The resulted image gets from VHDL are compared with the results get from MATLAB and found the RMSE, PSNR, MSE, and Correlation between the images, and the results show that the two images are almost the same.

TABLE 1; THE DIFFERENCE VALUE BETWEEN IMAGES THAT FILTERED BY MATLAB & VHDL USING ROBINSON EDGE DETECTOR

Images	PSNR	RMSE	Correlation
$Image_1$	59.0921	0.2831	0.8323
$Image_2$	63.6156	0.1682	0.9398
$Image_3$	56.6091	0.3768	0.7064
$Image_4$	57.4458	0.3422	0.7580
$Image_5$	57.4567	0.3417	0.7580
$Image_6$	58.3009	0.3101	0.7987
$Image_7$	61.7769	0.2078	0.9084
$Image_8$	61.8131	0.2070	0.9092
$Image_9$	58.5762	0.3004	0.8116
$Image_{10}$	58.4799	0.3038	0.8071
$Image_{11}$	59.2805	0.2770	0.8412
$Image_{12}$	57.9005	0.3247	0.7831

As shown in table (1), the Peak signal-to-noise ratio (PSNR) is high it generally indicates that the reconstruction is of higher quality, the mean square error (MSE) is small between two images that's mean the best explaining the variability in the observations, and the correlation value is closest to one that's mean there are little different between the images, and it is clear from that the better application result is on face images that is result the maximum value of PSNR , the minimum RMSE and maximum correlation value.

Many point could be concluded from the proposed work that is:

1. The hardware implementation gives the application higher efficiency and lower time, the Clock period in MATLAB was 1.9500 second but in VHDL was 7.838 nano second;
2. For high-speed, windowing algorithms are desired, the FPGA technology is ideally suited to the task. In fact, with the aid of the window generator, a whole series of image processing techniques is available to the designer, many of which can be synthesized for high-speed applications.
3. Using the pointer to reach the positions in RAM instead of using the first in first out implementation (FIFO) reduce the complexity of the algorithms implementation, also it reduce the size of the algorithms.

REFERENCES

[1]. J. Clerk Maxwell Huiyu Zhou, Jiahua Wu and Jianguo Zhang, (2010);" Digital Image Processing Part I", © by Huiyu Zhou, Jiahua Wu and Jianguo Zhang & Ventus Publishing ApS, ISNB 978-87-7681-541-7.

[2]. R. Gonzalez and R. Woods,(2008); " Digital Image Processing" , Addison-Wesley Publishing Company, p 191.

[3]. Ehsan Nadernejad, Sara Sharifzadeh, and Hamid Hassanpour, (2008); "Edge Detection Techniques: Evaluations and Comparisons". Applied Mathematical Sciences, Vol. 2, 2008, no. 31, 1507 – 1520.

[4]. Bruce A. Draper, J. Ross Beveridge, A.P. Willem Bohm, Charles Ross, Monica Chawathe, (2003); "Accelerated Image Processing on FPGAs". IEEE Transactions on Image Processing, Vol. 12, No. 12. Pp. 1543-1551.

[5]. Juan Manuel Ramirez, Emmanuel Morales Flores, Jorge Martinez Carballido, Rogerio Enriquez, Vicente Alarcon-Aquino, David Baez-Lopez, (2010); " An FPGA-based Architecture for Linear and Morphological Image Filtering". © IEEE 978-1-4244-5353-5.

[6]. Mohd Fauzi Bin Othman, Norarmalina Abdullah , Nur Aizudin Bin Ahmad Rusli, (2010); " An Overview Of Mri Brain Classification Using FPGA Implementation". IEEE Symposium on Industrial Electronics and Applications (ISIEA 2010), October 3-5, 2010, Penang, Malaysia, 978-1-4244-7647-3.

[7]. Volnei A. Pedroni, (2004); "Circuit Design with VHDL". MIT Press Cambridge, Massachusetts London, England ISBN 0-262-16224-5.

[8]. Peter J. Ashenden, (1990); "The VHDL Cookbook First Edition".

[9]. Scott E Umbaugh, (1998); "computer vision and image processing". © by Prentic Hall PTR , chapter 2,page 64-72.

AUTHORS PROFILE

Miss Farah Saad Al-Mukhtar (M. Sc. Student) is currently a master of science student at Mosul University/ College of Computer Science and Mathematics/ Computer Science Department. She received B.Sc. degree in Computer Science from University of Mosul in 2002. Her master research is on image enhancement techniques based on FPGA. One of these techniques is the edge detectors. She work hardly on her reseach and get good results.

Dr. Maha A. R. Hasso (the supervisor) is currently the supervisor of Miss Farah, she is an Assistant Professor at Mosul University/ College of Computer Science and Mathematics/ Computer Science Department. She received B.Sc. degree in Computer Science from University of Mosul in 1991, M.Sc. degree from University of Mosul in 1998 and Ph. D. degree from University of Mosul. Her research interests and activity are in image processing, computer vision, pattern recognition, remote sensing applications and biometrics. Now, she teaches digital image processing, pattern recognition and visual programming for postgraduate and undergraduate students.

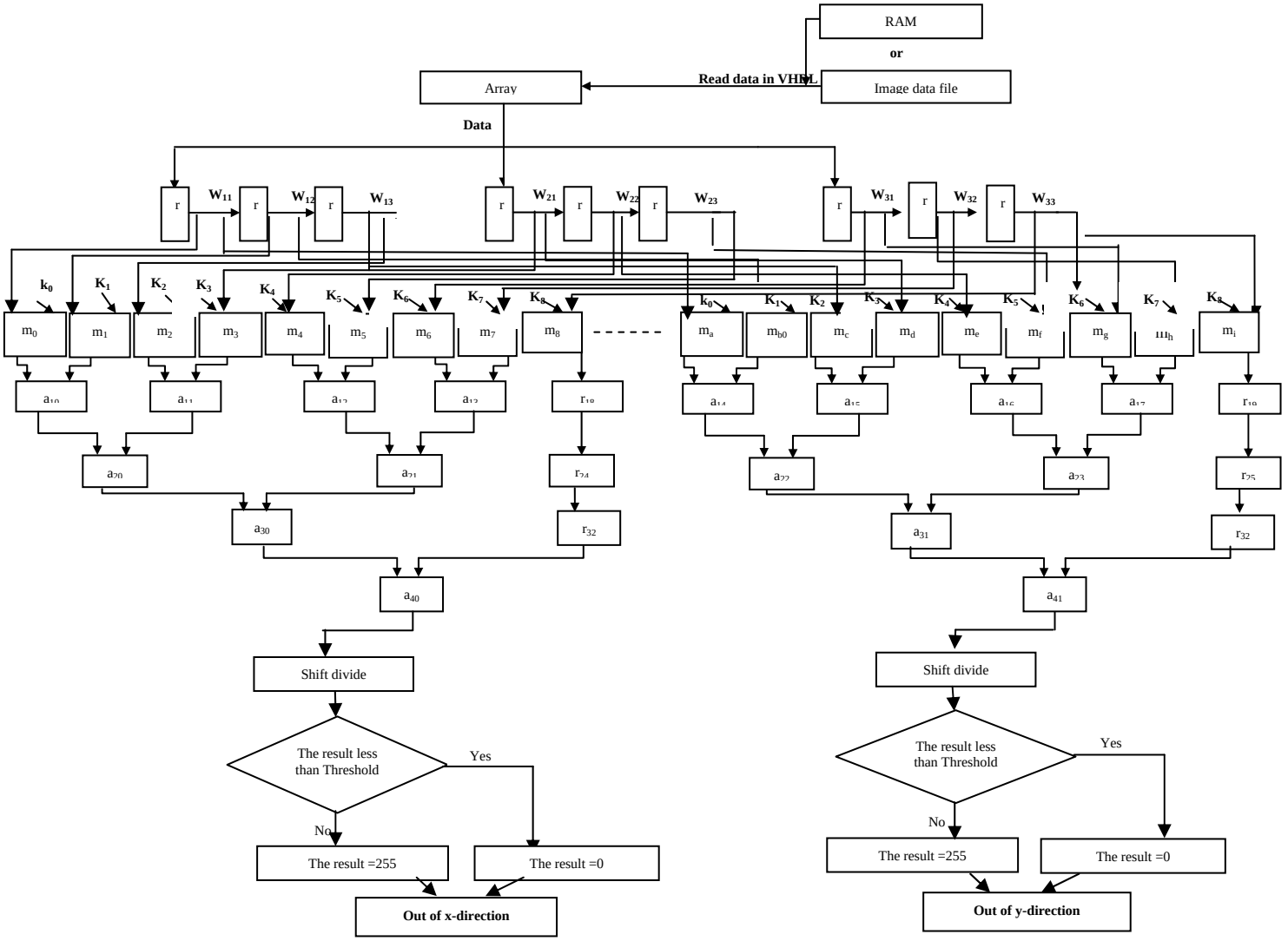


Figure 2; Graphic representation of the eight masks Robinson edge detector on VHDL

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Profile Cloning in Online Social Networks

Fatemeh Salehi Rizi
Department of Computer and IT
Sheikh Bahaei University of Isfahan,
Isfahan, Iran

Mohammad Reza Khayyambashi
Department of Computer, Faculty of Engineering,
University of Isfahan, Isfahan, Iran

***Abstract*—Today, Online Social Networks (OSNs) are becoming important due to the recent explosive growth in online interactions. They allow their users to express their personality and to meet people with similar interests. Meanwhile, there are also many potential privacy threats posed by these websites, such as identity theft and the revealing of personal information. However, many users have not yet been made aware of these threats, and the privacy setting that is provided by OSNs'service providers is not flexible enough to preserve users' data. Furthermore, users do not have control over what others share about them. One of the recently emerging attacks is the impersonation of a real user, instead of creating a fake account for a non-existing user, which is called Identity Theft Attack (ICA) or profile cloning. The purpose of cloned profiles is to try to steal real users' identities by making contact with their friends in order to financially abuse them or misuse their reputation. In this paper profile cloning attacks and some possible ways of detecting them are discussed. Then, based on the recent techniques and attack strategies further directions in research are proposed.**

Keywords-Profile Cloning, Online Social Networks, Security

I. Introduction

Advances in information technology cause many changes in the natures of communication and socialization. In recent years, blogs, forums, instant messaging services, and podcasts have evolved on the internet. Nowadays, all of these media outlets have been integrated in online social networking sites. A social network is a website which provides a virtual community for people who are interested in similar subjects or who just want to spend time together [1]. The rapid growth in the number of users on social networking sites in recent years indicates that they are the mainstream of communication technology for many people. People who use OSNs regard them as being fun and leisure. Through OSNs, users can contact family members and friends, especially people with whom they do not meet on a regular basis, find new friends, make contact with a friend of their friends or even with people they have never met in the real world. By extending social circles, users have the chance to contact people with common interests to exchange their knowledge and experiences. However, the reputation of these OSNs has been sullied by a number of events in new media such as the massive worldwide spamming campaign on *Quechup* [2] *sexual predators, stalkers, child molesters* [3] and users of OSNs have founded some strong reasons to worry about their privacy. Privacy threats on OSNs are divided into three categories [4]:

- *Security risks* (identity theft, phishing…)
- *Reputation and credibility risks* (for example, doing background checks on prospective employees or the case where Canadian border guards posted inappropriate and unprofessional materials on Facebook)
- *Profile risks* (spamming, unsolicited collection of users' data)

Although OSNs provide some mechanisms (privacy setting, user blocking …) to protect users against these risks, they are not effective [4]. In this paper, one of the security risks on OSNs which is called an identity theft attack is addressed and the paper is organized as follows: first, the concept of identity theft is discussed in section 2. Next, profile cloning attacks and existing solutions for detecting them that have been suggested so far are studied in section 3 and section4, respectively. Finally, concluding remarks and future research directions are given in section 5.

II. Identity theft

Identity theft, through which criminals use the identity and other related information of a person in an

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

unauthorized manner, is becoming important and a growing problem in many countries. One of the main reasons behind the sudden increase in identity thefts is the explosive growth of the internet applications and the widespread use of identity information in these applications, which has made them a main target for adversaries. Though identity theft has become a significant concern in the age of information, its more dangerous aspect is how terrorists could use it to penetrate national security systems. An identity thief is a person or an organization that tries to illegally seize people's personal identities and use them for financial abuse and other malicious objectives. The wrongdoer could be a terrorist or a fraud. Although it is deemed by people that identity thief occurs by strangers, statistics show that criminals already know victims and that may be one of their relatives, close friends or colleagues. Identity thieves always do their tricks in two steps: First, stealing the victim's information and building his fake identity and next, using fake identity to illegally access the victim's services or to do other malicious activities, among their classic tactics are dumpster driving to retrieve people's information from discarded credit cards, stealing bills, abducting personal mails from home inbocies, robbing personal bags, bribing employees to access customers' information and stealing confidential files from computer hard drives. Online identity thieves attack databases by spoofing (sending a message to a computer from a source who claims it is a valid and trustworthy IP address) and phishing (sending email messages to a target person, asking him to open the fake website that is very similar to the real one and to enter personal information. Next, these websites disclose all personal information of the user) [5]. Online social interactions create too much data on the network. Such data consist of people's private and sensitive information; hence they are the main sources for felons who try to obtain users' identities through attacking data on social networks [6]. One of the major and most serious of such attacks is called Identity Clone Attack (ICA) or profile cloning that is describe in the next section.

III. Identity clone attack or profile cloning in OSNs

OSNs simplify communication among friends and in order to fulfill this goal service providers try to preserve users' privacy against unauthorized accesses. All of main OSNs allow users' friends to access all of their personal information in which the user uploaded on his/her profile by default, while they blocked others. However, the concept of friend in OSNs is a social link that two users compromise to establish, with disregard to real offline relationship. This difference in the concept of friend provides a potential channel to hijack personal information through making friends by users [7]. Even the simplest forms of these attacks are successful [8].Bilge et al. In [9] presented two attacks consisting of automated identity theft from real users' profiles. In the first attack an already existing profile in OSN is cloned and friend requests are sent to victim's friends.Therefore it is able to steal victims' contacts by forging his identity and making second identification profile in the same network. Having access to victim's contacts means that the sensitive information which is gathered by theses contacts is accessible. Experimental results show that a typical user tends to confirm a friend request from a forged identity which as a matter of fact is an already confirmed contact in that friend's list. In the second attack, it is shown that to launch a cross-site profile cloning is both effective and feasible.In this attack, users who are registered on an OSN but have not yet registered on other OSNs are identified, automatically. Then, the victims' identities are cloned on the website they are registered and forged on those they are not yet. After successfully creating a forged identity, attempts will be made to automatically build the victim's friend network again, using his/her friends who are registered on the both OSNs. Experimental results show that this kind of attack is very effective, because profiles only exist on the OSN that is the target for attack. As a result, the sent friend requests seem completely legitimate and do not cause any doubt on the part of users for whom they have been sent.Two types of attacks are shown in Figure 1. In [10] a model is proposed that applies an array of attack techniques to build a persistence automated identity cloning of real users on a number of OSNs which is able to gain personal information and other private data in an extended period of time. A system is presented that works through different OSNs. In this model the existing identity cloning attack is extended by adding components which simulate online behavior automatically to continue for obtaining more private information.

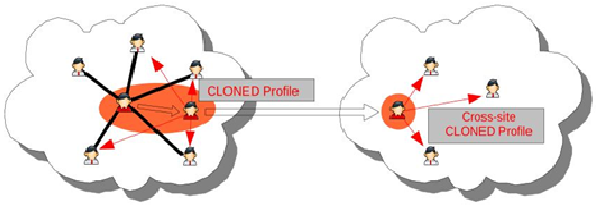


Figure 1.Profile cloning and Cross-site profile cloning in social networks

IV. Solutions for detecting profile cloning attacks

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Identity theft attacks in OSNs are not only a privacy attack for victims but also may cause potential loss and affect trust that victims built on OSNs [9]. Most users may trust their friend's activities on OSNs more than their activity in other websites. The main reason is that OSNs are built based on friendship and sharing information together. Such trust makes it easy for adversaries to obtain victim's information and then to make clone identities. Hence, creating some mechanisms for detecting ICA and locating them on OSNs is essential. In order to combat against ICAs, most solutions are focused on training users to control distributing personal information and digital identities. FightID Theft [11] and Facebook Identity Theft [12] focus on providing detailed suggestions to help users to define their privacy policies. For instance well-designed OSNs allow their users to customize privacy policies. For example Facebook has a privacy page that allows users to assign which parts of their profiles each user can see. However, privacy settings on OSNs are complicated and time-consuming tasks, to the extent that most users become confused and eventually skip it. Unfortunately, users prefer usability over security when they build a profile. There are some third party applications presented on OSNs that are implemented to defend users against ICAs, for example in Facebook, *Identity Badge* [13] and *mysafeFriend* [14]. Although these applications may help users to validate who they are and protect their identity, they are passive mechanisms and are only used to identify users themselves and cannot defend them against targeting ICAs [15]. Fake identities are still available on OSNs and adversariesdeceive more victims by using them without any restriction. In [15] Jin et al. it is proposed an active identification framework to detect fake profiles on OSNs. A cleverly crafted fake identity not only forges victim's attributes but also may add victim's friends on his/her network. Two approaches are presented to calculate profile similarity between two identities based on attribute similarity and friend network similarity. Based on profile similarity, a framework for detecting a fake identity on OSNs is suggested that includes three steps: first, searching and filtering identities in the set of profiles where input is a profile.And the second step, detecting a list of suspicious profiles related to input profile, using profile similarity schemes and third deleting fake identities. In the detection process, a set of parameters are used which can be adjusted for discovering a victim from its clones and might result in an accurate detection on different OSNs where faked identities may have different behaviors.

In this model, attribute similarity measure computes similarity between two profile attributes built on similar attribute values on two profiles.

Definition 1. Let P_c be the public profile of a candidate identity c and P_v be the public profile of a victim v. Let SA_{cv} donate the number of attribute for which P_c and P_v have similar values. The attribute similarity of two profiles is defined as S_{att} ,:

$$S_{att}(P_c, P_v) = \frac{SA_{cv}}{\sqrt{|A_c| \times |A_v|}}$$

Where $|A_c|$ and $|A_c|$ represents the number of attributes in P_c and P_v, respectively.

The next important component is finding friend network similarity, which calculates similarities between the two identities' friend network. It is done with regard to three types of users' friends.

Friend list: It is obtained from user's profile.

Recommended friend list: It is usually offered dynamically by the OSN system.

Excluded friend list: They are people who user does not tend to add them in his profile like neighbors, colleagues.

In order to calculate friend network similarity between a candidate identity and a victim identity, at first similarities are defined in relation to Friend list, Recommended friend list and Excluded friend list.

Definition 2. Let P_c be the public profile of a candidate identity c and P_v be a the public profile of a victim v. The similarity between the FLs in two identities as S_{ff} , similarity between FL of P_c and RFL of P_v as S_{frf} and similarity between FL of P_c and RFL of P_v as S_{fef} are defined :

$$S_{ff}(P_c, P_v) = \frac{|MFF_{cv}|}{\sqrt{|F_c| \times |F_v|}}$$

$$S_{frf}(P_c, P_v) = \frac{|MFRF_{cv}|}{\sqrt{|F_c| \times |RF_v|}}$$

$$S_{fef}(P_c, P_v) = \frac{|MFEF_{cv}|}{\sqrt{|F_c| \times |EF_v|}}$$

Where

- MFF_{cv} denotes the set of mutual friends common in the FLs of P_c and P_v

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- $MFRF_{cv}$ denotes the set of mutual friends common in the FLs of P_c and RFL of P_v
- $MFEF_{cv}$ denotes the set of mutual friends common in the FLs of P_c and EFL of P_v
- |X| represents the number of elements in the set X.

Definition 3. Given a public profile P_c be the of a candidate identity c and a public profile P_v be a of a victim identity v. The friend network similarity of these two identities for BPS is defined as S_{bfn} :

$$S_{bfn}(P_c, P_v) = (\alpha S_{ff} + \beta S_{frf} + \gamma S_{fef}), \alpha + \beta + \gamma = 1$$

Where α, β and γ are parameters that are used to balance the weights of similarities related to FL, RFL and EFL for the overall similarity of the friend networks in two identities.

Definition 4. Given a public profile P_c of a candidate identity c and a public profile P_v of a victim v. The Basic profile similarity of these two identities as S_{BPS} is defined:

$$S_{BPS}(P_c, P_v) = \frac{\sqrt{(\kappa S_{att})^2 + (\chi S_{bfn})^2}}{\sqrt{\kappa^2 + \chi^2}}$$

Where κ and χ are the parameters to balance the effect of attributes similarity and friend networks similarity on the BPS.

At the end, by calculating the schemes and adjusting the parameters clone profiles are detected.

Kontaxis et al. [16] presented a tool which searches and identifies clone profiles on OSNs automatically. The key concept behind its logic is that it employs user-specific data which is gathered from users' original network profiles for finding similar profiles through OSNs. Eventually, a list of possible clone profiles and the similarity score for each profile is presented to user. The process of detecting clones profiles consist of three components, as follows:

Information Distiller: This component is responsible for extracting information from legitimate OSN profiles. After analyzing users' profiles a piece of information on users' profiles that is user specific is extracted and used to build test queries in search engines of OSN services.

Profile Hunter: This component uses the extracted information in previous step to locate OSNs profiles that might belong to users. The profiles are gathered by search mechanisms on OSNs.

Profile Verifier: This component processes users' records and extract their information. Each profile is tested according to the amount of similarity to the real profile. Similarity score is computed based on common values of information field and at the end a list of profiles with their similarity scores are presented to users. The diagram of system can be observed in Figure 2.

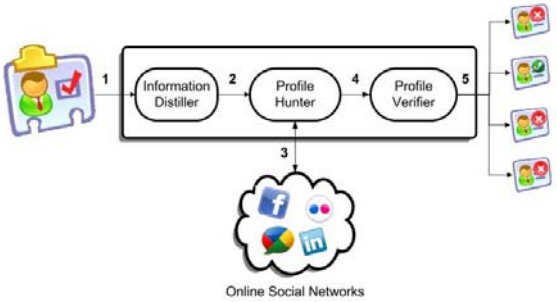


Figure 2. Diagram of detection system architecture

The efficiency of proposed method is evaluated on LinkedIn social network and it is showed that it is able to identify duplicate profiles.

V. Conclusion and future work

Privacy on OSNs is almost a new field and it has an immense potential for future research because of numerous recent users registered on them. OSNs are significant application drivers with many users from all over the world that put their trust in them, keep their contacts and share information with others on them. This huge number of users needs to adjust to a correct security measure that helps to protect users'privacy. In this paper one of the threats that is called identity theft attack, has been studied. Adversaries use OSNs as the rich sources of personal information in order to do their malicious activities. They make friends with users and steal their personal information by creating clone profiles on OSNs. After introducing the attack, the solutions suggested so far have been studied. Putting things in future perspective, clone profiles can be detected accurately by creating new mechanisms which have the possibility of comparing profile images and finding profile relations from common pages or similar shared information, as well as identifying cross-site profile cloning attacks that are found difficult to detect, by presenting new practical approaches.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

References

[1] D. Boyd and N. Ellison, "Social network sites: Definition, history, and scholarship," Computer mediated communication. J, vol. 13, pp. 210–230, November 2008.

[2] C. Lake. Quechup launches worldwide spam campaign eConsultancy 2007 [cited18.08.2008]; Available from: http://www.econsultancy.com/news-blog/364182/social-network-launches worldwidespam-campaign.html.

[2] CBCNews. Concordia bans Facebook access on campus computers 2008 [cited 28-09-2008]; Available from: http://www.cbc.ca/consumer/story/2008/09/17/mtlconcordiafacebook0917.html.

[4] W. Wang, D. Univ, Y. Yuan N. Archer and, "Privacy protection Issues in Social Networking Sites", Digests IEEE/ACS Conf. Computer System and Applications Morocco, pp. 271-278, 2009.

[5] A. Ho, A. Maiga and E. Aimeur, "A Contextual Framework for Combating Identity Theft", IEEE Security and privacy. J, vol.4, pp. 30-38, April 2006.

[6] P. Joshi, C. C. J. Kuo, "Security and privacy in Online Social Networks: A Survey", Digests IEEE International Conf. Multimedia and Expo (ICME) Spain, pp. 1-6, 2011.

[7] H. Gao , Jun Hu ,T. Huang , J. Wang and Y. Chen, "Security issue in online social networks", IEEE Internet Computing. J, vol. 16, pp. 56-62, April 2011.

[8] K. Jump, "A New Kind of Fame," Columbia Missourian, 1 Sept. 2005 (updated 21July 2008), www.columbiamissourian.com/stories/2005/09/01/a-new-kind-of-fame.

[9] L. Bilge, T. Strufe, D. Balzarotti and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks," Digests 18th ACM International Conf. World Wide Web USA, pp. 551-560, 2009.

[10] Bhume Bhumiratana, "A Model for Automating Persistent Identity Clone in Online Social Network", Digests IEEE 10th International Conf. Trust, Security and Privacy in Computing and Communications China, pp. 681-686, 2011.

[11] FightIDTheft [Online]. http://www.facebook.com/FightIDTheft

[12] Facebook Identity Theft - Don't be a Victim! [Online], http://www.facebook.com/group.php?gid=7086517815

[13] Identity Badge [Online]. http://apps.facebook.com/identity_badge

[14] MysafeFriend [Online]. http://apps.facebook.com/mysafefriend

[15] L. Jin, H. Takabi and J. Joshi, " Towards Active Detection of Identity Clone Attacks on Online Social Networks", Digests first ACM Conf. Data and application security and privacy USA, pp. 27-38, 2011.

[16] G. Kontaxis, I. Polakis, S. Ioannidis and E. P. Markatos ," Detecting Social Network Profile Cloning" Digest IEEE International Conf. Pervasive Computing and Communications USA, pp.295-300, 2011.

Software Cost Estimation using Fuzzy-swarm Intelligence

Mustafa shakir mahmood Al-Sabaway
M.Sc. Student Software Engineering Dept.
University of Mosul
Mosul, Iraq
pro.mustafa833@Gmail.com

Dr.Jamal Salahaldeen Majeed Al-Neamy
Assistant professor, Software Engineering Dept.
University of Mosul
Mosul, Iraq
jamal_alneamy@yahoo.com

Abstract— Estimation is the most challenging and emerging field in software engineering development life cycle. Software cost estimation is a part of it. In this paper, Software cost estimation techniques were used to estimate cost of software development, the proposed system was built from four phases, Fuzzification, Fuzzy Inference, Parameter Tuning (using PSO) & Defuzzification, compute Cost

Index Terms— Lines of Code, Fuzzy Logic System, Particle Swarm Optimization, Software cost Estimation.

1. INTRODUCTION

Software cost and effort estimation will never be an exact science. Too many variables like human, technical, environmental, political, can affect the ultimate cost of software and effort applied to develop it. However, software project estimation can be transformed from a black art to a series of systematic steps that provide estimates with acceptable risk. To achieve reliable cost and effort estimates, a number of options arise:

1. The delay in the process of estimates late during the development of the project.
2 Adoption of the estimates on previous projects have already been completed.
3. Use one or more empirical models for software cost and effort estimation [1].

The estimated cost means an estimate of the final total cost of execution of a construction project. This definition requires two important issues, namely

a) The estimate is an approximate calculation.
b) Estimate contains uncertainties.

Main purpose of estimating costs is to provide a size reference for cost control, to verify that the resources consumed during the execution of the project are kept in the costs assessed in feasibility phase of the project. Deviations from these issues can endanger the profitability of the project and a successful project can turn into a disaster. Accuracy of estimates of cost depends on existing information to reflect and their calculation [2].

When the cost for a project is a function of many parameters. Foremost amongst them in size of project in order to reduce the skeptism at the input level, i.e. size, triangular membership function is used, this process is known as fuzzification. The parameters of the cost model equation are tuned by using PSO algorithm [3]. By applying fuzzy inference, the suitable equation for cost estimation is obtained; finally, defuzzification is done through weighted average method, which actually translates fuzzy values into output [4].

2. RELATED WORKS AND OUR CONTRIBUTION

2.1 Related Works

Many researches and methods were presented in the field of Software Cost Estimation

On 2011 Srinivasa Rao.T, Prasad Reddy P.V.G.D, Hari Ch.V.M.K proposed a thesis Fuzzy Based PSO technique is applied for Software Effort Estimation[].

On 2012 A.BalaKrishna, T.K.Rama Krishna proposed a thesis Fuzzy Based PSO technique is applied for Software Effort Estimation[]

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

2.2 Our Contributions

Our proposed Fuzzy Based PSO technique is applied for Software cost Estimation

3.TECHNICAL APPROACH

3.1 Fuzzy logic:

In 1965, Zadeh first introduced the concept of fuzzy set for modeling the vagueness type of uncertainty [5].A fuzzy set is a set with a smooth boundary. Fuzzy set Theory generalizes classical set theory to allow partial Membership [5,6]. The best way to introduce fuzzy sets is to start with a limitation of classical sets. A set in classical set theory always has a sharp boundary because membership in a set is a black-and-white concept, i.e. an object either completely belongs to the set or does not belongs to the set at all. The degree of membership in a set is expressed by a number between 0 and 1; 0 means entirely not in the set, 1 means completely in the set, and a number in between means partially in the set [7].

3.2 Swarm intelligence & PSO

Swarm intelligence (SI) as defined by Bonabeau, Dorigo and Theraulaz is "any attempt to design algorithms or distributed problem-solving devices inspired by the collective behavior of social insect colonies , Particle swarm optimization (PSO) and other animal societies" .So every time swarms inspire something – it is swarm intelligence.[8]

Particle swarm optimization (PSO), inspired by the social behavior of birds flocking or fish in schools, is a population-based stochastic optimization technique developed by Kennedy and Eberhart (1995). The main strength of PSO is its fast convergence, which compares with many global optimization algorithms like GAs, simulated annealing, and other global optimization algorithms [9]. PSO is a robust stochastic optimization technique based on the movement of intelligent swarms. PSO applies the concept of social interaction to problem solving. It uses a number of agents(particles) that constitutes a swarm moving around in the search space looking for the best solution. Each particle is treated as a point in an N- dimensional space which adjusts its flying according to its own flying experience (Pbest-personal best) as well as flying experience of other particles (Gbest –global best) . The basic concept of PSO lies in accelerating each particle towards its Pbest and Gbest locations with a random weighted acceleration at each time. The modifications of the particles positions can be mathematically modeled according to the following equations:

$$V^{k+1} = V_i^k + C_1 * rand()_1 * (Pbest - S_i^k) + C_2 * rand()_2 * (Gbest - S_i^k) \quad (1)$$

$$S_i^{k+1} = S_i^k + V^{k+1} \quad (2)$$

Where,

S_i^k is current search point, S_i^{k+1} is modified search point.

V_i^k is the current velocity, V^{k+1} is the modified velocity,

V_{Pbest} is the velocity based on Pbest, V_{Gbest}

Is velocity based on Gbest, C_j is the weighting factors. rand() are uniformly distributed random numbers between 0 and 1. [10]

4. The Proposed method

The proposed work to improve the process of estimate cost consists of four phases. This process is start with takes the inputs such as size of the software project, measured effort, and methodology and generates optimized parameters, effort, and calculate cost from estimated effort.

Step 1: Fuzzification, The input size is fuzzified by using triangular membership Function shown in Figure 1. The triangular membership function is defined as (α, m, β), where α, β left and right side of boundaries and m are is the model value. It is defined in this figure.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$Y = Triangle(x,\alpha,m,\beta) = \begin{cases} 0, & x \le \alpha \\ \frac{x-\alpha}{m-\alpha}, & \alpha \le x \le \beta \\ \frac{\beta - x}{\beta - m}, & m \le x \le \beta \\ 0, & \beta \le x \end{cases}$$

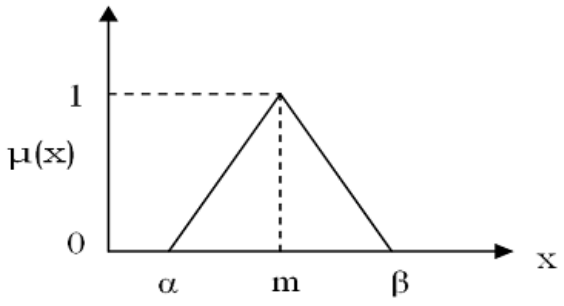


Figure 1: Triangular Member Function

Step 2: Fuzzy Inference, Then Fuzzy inference is applied to determine the Effort equation to be considered for parameter tuning. The rules are

1. If input is only size then apply the equation

$$\text{Effort} = a*(\text{size})^b \quad (3)$$

2. If input in size and methodology (me) then

$$\text{Effort} = a*(\text{size})^b + c*(\text{ME}) \quad (4)$$

Step 3: Parameter Tuning & Defuzzification ,
In this step we integrate defuzzification process (using weighted average method) with PSO that tuning the parameters "a, b, c", and finally fuzzy values are translates into actual output that represent estimated effort.

The defuzzification formulas for cost estimation and parameters obtained by using PSO with inertia methodology are

Case 1: size only.

$$E = w_1 *(a*\alpha^b) + w_2 *(a*m^b) + w_3*(a*\beta^b)/w_1 + w_2 + w_3 \quad (5)$$

Where a, b from pso, and α= 3.2, β= 0.795.

Case 2: size and Methodology

$$E = \{w_1 *[(a*\alpha^b)+c*(ME)] + w_2 *[(a*m^b) + c*(ME)] + w_3*[(a*\beta^b)+ c*(ME)]\}/w_1 + w_2 + w_3 \quad (6)$$

Where a, b, c from pso, and α= 3.2, β= 0.795.

Step 4: Now we convert effort to cost in Dollar.

By review of historical data indicates that the organizational average productivity for systems and Based on a burdened labor rate, we will obtain the cost per line of code. Then we multiply the cost per line of code by effort estimated, and then we will obtain the estimated cost.

5. Experimental Results

One of the objectives of the present work is to employ Particle Swarm Optimization for tuning the cost parameters, fuzzy logic for reducing uncertainty in input and test its suitability for software cost estimation. This methodology is then tested using NASA dataset provided by Boehm.

SL.NO	SIZE	MEASURED EFFORT	METHODOLOGY
1	2.1	5	28
2	3.1	7	26
3	4.2	9	19
4	12.5	23.9	27
5	46.5	79	19
6	54.5	90.8	20
7	67.5	98.4	29
8	78.6	98.7	35
9	90.2	115.8	30
10	100.8	138.3	34

Fig. 2. NASA dataset

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

S.NO	SIZE	PRO. EFF.	ME	ESTIMATED COST OF OUR MODEL Case1	Case2
1	2.1	5	28	4.6175	3.1390
2	3.1	7	26	6.7324	6.8222
3	4.2	9	19	8.9012	14.0637
4	12.5	23.9	27	22.8538	23.5271
5	46.5	79	19	67.1727	76.9745
6	54.5	90.8	20	76.3711	86.2054
7	67.5	98.4	29	90.7539	95.4333
8	78.6	98.7	35	102.5863	104.0077
9	90.2	155.8	30	114.5904	120.4676
10	100.8	138.3	34	125.2846	129.2132

Table 1 .Estimated cost of Proposed Model.

Figure1: show case1: where only size of projects (ten projects from NASA)

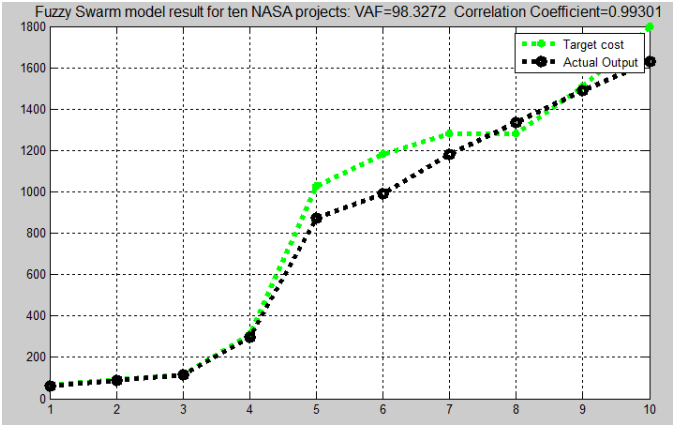


Fig. 3. variance and correlation metrics

Performance Measures

Two criterions were considered and they are outlined below:

1. Variance Accounted For (VAF)

VAF=

$$\left[1-\frac{\text{var (Measured Effort - Estimated Effort)}}{\text{var (measured effort)}}\right] \text{x } 100 \qquad (7)$$

2. Correlation:

$$\text{correlation} = \frac{\sum (X-\bar{X}) \bullet (Y-\bar{Y})}{\sqrt{\sum (X-\bar{X})^2 \bullet \sum (Y-\bar{Y})^2}} \qquad (8)$$

Figure2: show case2: where size and methodology of projects (ten projects from NASA)

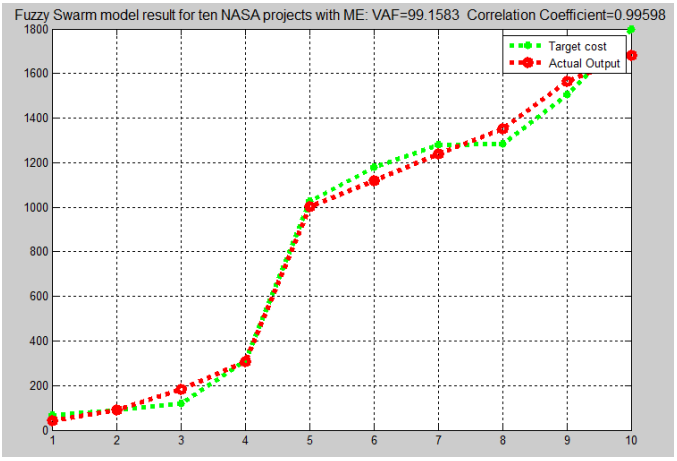


Fig. 4. variance and correlation metrics

CONCLUSION

Accurate software development cost estimation is very important in the budgeting, project planning and control, trade off and rink analysis of effective project management. This chapter investigated to reduce the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

uncertainty in the input sizes by using fuzzy logic and by lining the parameters of the cost model using PSO with inertia weight in order to generate an optimal result. The model was tested in NASA software project and proved to be efficient on the basis of VAF and Correlation.

References

1- Roger S. Pressman, "Software Engineering A Practitioner's Approach, seven Edition", 7th , McGraw-Hill Company, 2001

2- Asachi Gheorghe, " Appreciation of the role of reconstruction in life Cycle", Universitatea Tehnică , 2010.

3- Behrouz Fathi-Vajargah, Akram Heidary- Harzavily ,"Sketching the Graph of Fuzzy Riemann Integral Based on alpha-Level Sets", Advances in Information Technology and Management (AITM), 2012.

4- ABU WAHID Md Masud Parvez," A Managed Approach to Interact between Agile Scrum and Software Configuration Management System", Advances in Information Technology and Management (AITM), 2012.

5- Hao Ying, " The Takagi-Sugeno fuzzy controllers using the simplified linear control rules are nonlinear variable gain controllers, ELSEVIER: Automatica, 1998.

6- Magne Jrgensen, "Evidence-Based Guidelines for Assessment of Software Development Cost Uncertainty", IEEE,2005.

7- Xishi Huang, Danny Ho, Jing Ren, Luiz F. Capretz, , "Improving the COCOMO model using a neuro-fuzzy approach",Elsevier, 2005.

8- Pfeil Jonas, "Swarm Intelligence", Communication and Operating Systems Group Berlin University of Technology, 2011.

9- Bardsiri Vahid Khatibi, Abang Jawawi Dayang Norhayati, Hashim Siti Zaiton Mohd, Khatibi Elham, "A PSO-based model to increase the accuracy of software development effort estimation", 2012.

10- Reddy Prasad, CH.V.M.K. Hari, Rao T Srinivasa.,"Multi Objective Particle Swarm Optimization for Software Cost Estimation", International Journal of Computer Applications, 2011.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

An Operating System-based Model for Mobile Agent Deployment

Oyatokun, B.O.
Department of Mathematical Sciences
Redeemer's University,
Mowe Ogun State, Nigeria

Osofisan, A. O.
Department of Computer Science
University of Ibadan,
Ibadan, Nigeria

Aderounmu, G.A
Obafemi Awolowo University,
Ile-Ife
Osun State Nigeria

***Abstract*— Mobile agent technology has grown in acceptance over the years for distributed applications, but it is yet to be adopted as ubiquitous solution technique. This is due to its complexity and lack of interoperability. Mobile agent executes on mobile agent platform, these platforms from different vendors are design, and language specific, and are thus non interoperable. In other words mobile agent built on one platform cannot interact with or execute on any other platform. There is a need to provide a common base on which agents from different vendors can interact and interoperate. This work presents a framework for mobile agent interoperability by providing an Embedded Mobile Agent (EMA) system into the Windows Operating System kernel so that it can run as a service; this was done to eliminate the overheads associated with the agent platforms and enhance mobile agents' interoperability. The targeted OS were Windows XP, Windows Vista and Windows7.**

Index Terms— embedded mobile agent, mobile agent platform, interoperability, operating system service.

I. Introduction

Mobile agent paradigm has been recognized as a viable tool and a promising approach for building distributed applications and a lot of research has been done, nevertheless, it is still a promising area of research, because, a lot of its many potentials are yet to be exploited. Agents solve complex software problems in distributed environments where protocols, operating systems, hardware and runtime environments are heterogeneous. Mobile agents are autonomous software capable of performing computational tasks on behalf of another software or human user [1, 2]. Mobile agent is defined as a computer entity capable of reasoning, use the network infrastructure to run in another remote site, search and gather the results, cooperate with other sites and return to its home site after completing the assigned tasks [3]. Mobile agents paradigm provides infrastructure for executing automous agents and also migrate them between computers connected by a network. Mobile agent paradigm is made up of two prominent components, the mobile agent itself and the mobile agent middleware system called the mobile agent platform or Mobile Agent System (MAS). The mobile agent platform provides the run time execution needed by the mobile agents that travel from one host to another host through the network to perform its tasks. Mobile agent platforms is the execution environment for agents, and provides functionalities that support migration of agents, communication between agents, various programming languages and various forms of security [4].

II. Existing Mobile Agent Systems

Over the years, several mobile agent platforms have been developed to support mobile agent applications [4, 5, 6]; these platforms operate independent of one another which hinders the interoperability of mobile agents. The platforms are different in design, goals, language and vendor, thus they are not interoperable. In other words an agent designed on one platform cannot execute on another platform, neither can it interact with an agent from other platforms. Most agent platforms either offer enormous flexibility at the cost of usability or extended built-in functionality at the expense of interoperability [7].

We examine some of the existing agent platforms briefly in this section

- JADE: written in java and uses Message Transport protocols (HTTP, IIOP, HTTPS) for communication and migration.[8,9].

- TACOMA: Tromso And Cornell Moving Agent developed by university of Tromso, Norway & Cornell University, NY, written in TCL (Tool Command Language) but can carry scripts in other languages [4].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Aglet: is a combination of Agent and Applet, written in Java programming language and uses HTTP for communication [10].

- Agent TCL (D'Agent): created at Dartmouth College, the platform is written in C and the agent in TCL, it uses proprietary protocol over TCP/IP and PGP [11].

- Telescript/odyssey: Telescript is an object oriented scripting language for implementing mobile agents, it implements strong migration (**agent go** to **place**) [12]. Telescript was later implemented in java and was called odyssey.

- Voyager: is java-based and agent-enhanced Object Request Broker (ORB). Voyager communicates through RMI (Remote Method Invocation) using proxies, uses TCP/IP for migration; it is commercial product with free license allowing non-commercial use of its core technology [4].

- Grasshopper: complies with MASIF and FIPA standards, it is implemented in java and supports TCP/IP, RMI/JRMP and CORBA/IIOP [13].

- Mole: developed in java, uses RMI for communication[4]

The development of these agent platforms is motivated by different goals which include support for specific agent models, programming environments, mobility and security [5].

III. MOBILE AGENT INTEROPERABILITY

Agents need to communicate with one another in the process of working together to achieve a common goal; agent paradigm of software development believes that communities of agents are much more powerful than any single agent, which necessitates interoperation of agent systems. Interoperability in mobile agent community focuses on the execution environment and standardization of certain aspects and features of agents while in the non-mobile agent context the focus is on communication, i.e. effective exchange of information and knowledge content of agents. Interoperability has been defined by [14] as follows:

> two mobile agent systems are interoperable if a mobile agent of one system can migrate to the second system, the agent can interact and communicate with other agents (local or even remote agents), the agent can leave this system, and it can resume its execution on the next interoperable system [14].

A lot of research work is presently going on in the area of mobile agents interoperability [14,15,16] several solutions have been proposed but they lack the necessary flexibility to provide adequate degree of interoperability among the available MASs. Interoperability is paramount to the global acceptance of mobile agent system (MAS) in heterogeneous and open distributed environments where agents must interact with other agents to fulfil their tasks and visit different agent platforms to access remote resources [16].When mobile agents migrate to a new host, the platform on the host provides execution environment, the mobile agent might execute code, make remote procedure calls to access resources on the host, collect data or initiate another migration process. Problems arise from the fact that not all platforms for mobile agents are the same and thus, cannot provide necessary services for non-compliant mobile agents[4]. Interoperability is directed at making an agent system accept and support the running of agents from another agent system and vendor, support the transfer of agent to other agent systems and find other agents and agent systems. To achieve these, mobile agent paradigm must clearly define some features such as agent management, agent transfer, agent and agent system name, agent system types, authority and location syntax. Efforts have been made by Foundation for Intelligent Physical Agent (FIPA) and Mobile Agent System Interoperability Facility (MASIF) to define sets of standards for mobile agents and agents' platform. FIPA addresses the interoperability among agents, attempt to standardize certain aspects of mobile agent and defines features of agents such as communication, agent management and the agent abstract architecture [8]. MASIF addresses the interoperability between agents' platforms, attempts to standardize some aspects of the execution environment to provide for mobile agents to interoperate and it focuses on agent management, agent transfer and name for agents and agent platform [8, 17]. These efforts are yet to be effective at providing the necessary interoperability among agents and agent systems [14].

MASIF consists of a collection of definitions and interfaces that provides interoperability among mobile agent systems, it provides two interfaces; the MAFAgentSystem for agent transfer and MAFFinder for naming and locating [17].

Interoperability Application Programming Interface (IAPI) that supports registration, lookup, messaging, launching and migration of agent across different platforms was proposed in [15]. The system provides three layers to the GMAS layer, the Foreign2GMAS translator, GMAS2Native translator and common communication and discovery service. The system only enabled agent migration among diverse agent platforms but the agents may fail to execute due to difference in the level of the java API. The additional software layers constitute a significant overhead, at the same time, the performance of the system was also slow, the additional layers on the platforms being the major factor.

A java-based framework for interoperability among java-based mobile agent systems was proposed by [18]. The framework permits interoperability of execution, migration and interaction of java-based mobile agent systems. The framework consists of three software layers, the Interoperable Mobile Agent Layer (IMAL), the Adaptation Layer (AL) and the Platform-dependent Mobile Agent Layer (PMAL) which

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

constitute a considerable overhead. At the same time, a Mobile Agent Bridge must be developed for each agent platform to be able to migrate; this constitutes an additional overhead on the system.

Secure and Open Mobile Agent (SOMA) [19] is another attempt at achieving interoperability; it was developed in compliance with both CORBA (Common Object Request Broker Architecture) and MASIF. SOMA uses a CORBABridge which consists of CORBA client/server which simplifies the design of SOMA entities as CORBA client /server and MASIFBridge which implements the MASIF functionality. The security and fault tolerance of the system is important for interoperability to be fully attained, SOMA achieves security but it is not fault tolerant. Moreover, the MASIFBridge introduced a considerable overhead and the model has a close connection with CORBA which limits its application.

Agent operating system (AOS) designed by [5], provides common primitives required by most agent platforms so they can interoperate, AOS was portable and language-neutral middleware that resides between the agent platform and the operating system. AOS facilitates interoperability between agent platforms and between different implementations of AOS itself. The AOS provides a common interface for different agent platforms to execute in order to achieve interoperability, in other words it provides a meeting point for the agent platforms and does not attempt to eliminate agent platforms. The AOS contribute another overhead to the system.

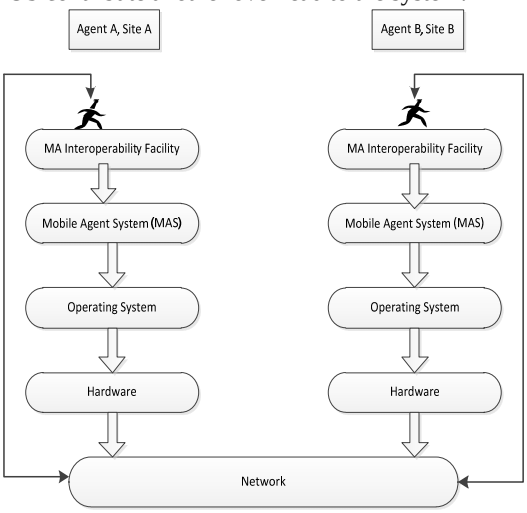


Figure 1: the conceptual model of existing platform-based mobile agent system

The shortcomings of the above interoperability models led to our attempt to find a common platform on which agents from different platforms and vendors with different design and architecture can communicate, execute and interact effectively and efficiently without fear of risk or vulnerability to failure and other attacks. Several mobile agent platforms have been developed by different groups, although these agent platforms differ in their goals, designs, motivations and implementations, they all provide common functionalities that support: agents' migration, agents' communication, various programming and interpreted language and various forms of security [4]. This work is an attempt to provide such stage on which agents from different vendors can interoperate without necessarily going through the agent platform.

IV. ARCHITECTURE OF THE PROPOSED SYSTEM

The proposed system consists of a lightweight static agent embedded into the kernel of the windows operating system in the form of a service as a Terminate and Stay Resident (TSR) program. The static agent is installed as part of the executive services in the kernel mode of the Windows operating system. Windows (XP and higher versions) operating system provides a mechanism to make certain user programs run in its kernel mode giving an impression of programming the operating system. In the actual sense of it, the services of the operating system are being extended.

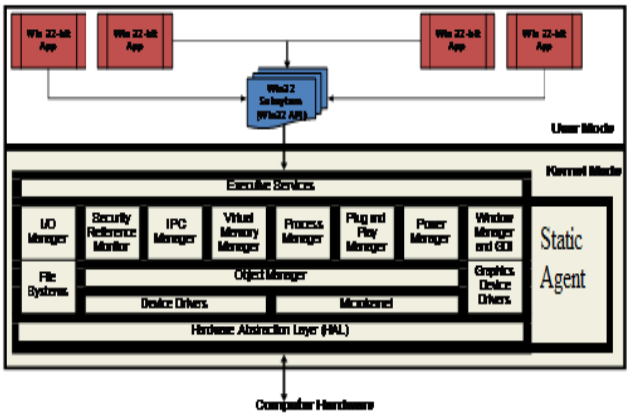


Figure 2: structure of Windows XP with static agent embedded (adapted from [20])

Mobile agent from remote host interacts with the static agent in the kernel mode of the visited host operating system, giving an impression of directly interacting with the operating system.

V. THE CONCEPT OF THE PROPOSED SYSTEM

The static agent executes on the host where it begins execution performs a number of functions related to information storage and retrieval.

- It is responsible for listening to the port for incoming agent.
- It negotiates passage to the destination host and ensures that the mobile agent is successfully transferred. If the mobile agent is rejected, it restarts the agent to allow it choose another destination.
- It validates and authenticates the incoming agent

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- It launches received mobile agents and provides runtime execution for the mobile agent according to the level of trust given to the agent. The runtime execution environment will depend on the access level granted to the mobile agent and the functions it wishes to perform.
- It provides a registration to register mobile agents and hosts on the network with the available resources on them.

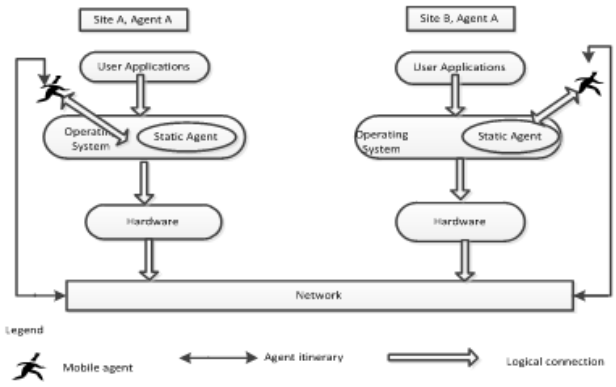


Figure 3: the concept of the proposed system

VI. SYSTEM OPERATION

The static agent on the remote host authenticates and receives in coming mobile agent, searches its local files for the relevant information, and then downloads the information and forwards it to the mobile agent to add it as part of its bag. The mobile agent moves to the next host in its itinerary. On reaching a new host in its itinerary, the mobile repeats the same process and moves to the next host until the last node in its itinerary. It then returns home with the results in its bag and forward the result to the static agent who displays the result to the user.

- Incoming Mobile Agent seeks permission to perform its tasks. The static agent receives and authenticates the incoming agent.
- The static agent after receiving the requests interprets the requests and searches the local database for available relevant documents, it queries the database using keywords
- The static agent adds the downloaded documents to the mobile agent as part of its bag.

The mobile agent saves its current state, signs off the visited node, exit and continue in its itinerary, and if it's the last node in its list, returns to the origin, delivers the result and disposes itself.

VII. CONCLUSION

This work presents a proposal for implementing and deploying mobile agent as an operating system service to make mobile agent interact directly with the operating system. This mode of design and deployment eliminates the use of agent platform which for a long time has been the limiting factor for mobile agents' interoperability. This work is similar but different from other proposals made in the past for mobile agents' interoperability. The main focus of [21] is the standardization issues for agent interoperability; it integrates two standards (MASIF and FIPA-ACL) to propose an architectural model for mobile agent system interoperability. The focus of [22] is on agent architecture, it separates all platform specific code from platform independent main procedure of an agent, so that the agent can migrate to an incompatible platform. The agents however, cannot use all the features of the underlying platform. An Interoperability Application Programming Interface (IAPI) built on top of the agent platform serving as a translator between agents and the platforms was proposed [15]. Secure and Open Mobile Agent, SOMA [18] focuses on standardization for achieving agents' interoperability, SOMA was developed to comply with both CORBA and MASIF. The Agent Operating System (AOS) focuses on interaction between agent platforms and provides a set of primitives that are common to agent platform [5]. The AOS was designed as a portable middleware layer between the mobile agent platform and the operating system and facilitate interoperability between agent platforms. Our approach to interoperability however, focuses on the mode of deployment of mobile agent. A light weight static agent is embedded into the kernel of the operating system as an operating system service and provides runtime execution for mobile agents thereby, eliminating the need for an agent platform. The framework has been implemented in java programming language and tested on the Windows XP, Windows vista and Windows 7. Work is ongoing in implementing the framework on other operating systems, specifically Unix and any of its flavour, as well as provision of adequate security for the system. In addition, the implementation of mobile agents from other vendors and platforms is a continuation of this work.

REFERENCES

[1] Lange D. B. 1998. Mobile objects and mobile agents: the future of distributed computing? Proceedings of the European Conference on Object-Oriented Programming (ECOOP'98), 1998.

[2] Biermann E. 2004. A Framework for the Protection of Mobile Agents Against Malicious Hosts. Unpublished Ph.D thesis, University of South Africa, South Africa.

[3] Outtagarts Abdelkader (2009). "Mobile Agent-Based Applications: A Survey." *International Journal of Computer Science and Network Security, 331 - 339.*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[4] Syed A., John D. and Pavana Y. (2000). A survey of mobile agent systems.

[5] van 't Noordende, G.J., Overeinder, B.J., Timmer, R.J., Brazier, F.M.T. and Tanenbaum, A.S. (2009). Constructing secure mobile agent systems using the agent operating system', *International Journal of Intelligent Information and Database Systems*, Vol. 3, No. 4, pp.363–381.

[6] Stoian G. and Claudiu I. P. (2010). A Proposal for an Enhanced Mobile Agent Architecture (EMA). *Annals of the University of Craiova, Mathematics and Computer Science Series, 37(1): 71 – 79.*

[7] Tudor M., Bogdan D., Mihaela D., Ioan S.mie (2004). A Framework of Reusable Structures for Mobile agent Development. *Proceedings of the 8th IEEE international Conference on Intelligent Engineering Systems (INES '04), Cluj-Napoca, 2004.*

[8] Bellifemine, F.L, Greenwood D and Caire G (2007). Developing Multi-agent systems with JADE. John Wiley & Sons Ltd, England.

[9] Giovanni C. 2009. JADE Programming for Beginners. TILAB, S.P.A.

[10] Venners B. 1997. Under the hood: The architecture of aglets. Java-World, January 1997.

[11] Robert S. G. (1997). Agent Tcl: a flexible and secure mobile-agent system. Unpublished PhD thesis in Computer Science at Dartmouth College, Hanover, New Hampshire.

[12] General Magic. 1995. Telescript language Reference.

October,1995

[13] Gupta R. and Kansal G. 2011. A survey on comparative study of mobile agent platforms. *International journal of engineering, science and technology* (IJEST), 3(3): 1943 - 1948.

[14] Pinsdorf U and Roth V. (2000). Mobile Agent Interoperability Patterns and Practice. Available at http://jade.tilab.com/papers/EXP/pinsdorf.pdf.

[15] Grimstrup A., Gray R., Kotz D., Breedy M., Carvalho M., Cowin T., Chacon D., Barton J., Garrett C. and Hofmann M. 2002. Toward interoperability of mobile agent system. *Proceedings of the sixth IEEE international Conference on Mobile Agent, Bercelona, Spain, 106-120.*

[16] Labrou Y, Fini T and Peng Y. 1999. The Interoperability problem: Bringing together mobile agents and agent communication languages. Proceedings of the Hawaii International Conference on System Sciences, copyright 1999 IEEE.

[17] Milojicic D., Breugst M., Busse I., Campbell J., Covaci S., Friedman B., Kosaka K., Lange D., Ono K., Oshima M., Tham C.. Virdhagriswaran S. and While J. MASIF: The OMG Mobile agent System Interoperability Facility, personal technologies, 2(3), 117-129, December, 1999.

[18] Bellavista P., Corradi A. and Stefanelli C. (2001). Mobile agent middleware for mobile computing. IEEE Computer Society, Washington DC, USA, 73-81.

[19] Fortino G. and Russo W. 2003. High-level interoperability between java-based mobile agent systems. A report of the project ' Giovane Ricercatore 2003', University of Calabria.

[20] WIN133. 2009. The big picture….which makes more sense now. Retrieved on 20 *September*, 2012.

[21] Zeghache L., Badache N., and Elmaouhab A. (2004). An Architectural Model for a Mobile Agents System Interoperability.

[22] Pauli M., and Kimmo R. (2000). Agent Migration between incompatible agent Platforms. p*roceedings of the 20th IEEE International Conference on Distributed Computing Systems (ICDCS'00,), : 4.*

AUTHORS PROFILE

Oyatokun, B. O holds a B.Tech (Hons) degree in Computer Engineering from LAUTECH, Ogbomosho, Nigeria, in 2000. She obtained her M.Sc in Computer Science from the University of Ibadan where she is currently doing her Ph.D. She is currently teaches at the Redeemer's University, Nigeria. Her research interests are in the areas of computer communication and deployment of mobile agent software management of management of heterogeneous computer network.

Osofisan, A. O. obtained a B.Sc (Hons) degree in Computer Science from the Obafemi Awolowo University, Ile Ife, M.Sc from Georgia Tech. and Ph.D from Obafemi Awolowo University. She is currently a Professor and the director of Business School, The University of Ibadan where she also lectures in the department of Computer science. Her areas of specializations are data communications, data warehousing and data mining. She has many articles in these areas at both local and international level to her credit.

Aderounmu G. A. obtained a B.Sc. (Hons) degree in Computer Engineering from the Obafemi Awolowo University, Ile-Ife, Nigeria, in 1991. He obtained his M.Sc and Ph.D in Computer Science from the same University in 1997 and 2001 respectively. He lectures in the department of Computer Science and Engineering; he is presently a professor and the director of the Information Technology and Communication Unit (INTECU) of the same University. His areas of specializations are design, analysis, and simulation of ATM networks with respect to switching, protocol, and buffer management and mobile agent software development. He has many articles at both local and international level to his credit.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Pre-SOA Models

First step to SOA

Safa Talal Hasan Al-Ramadani
Software engineering. Mosul University
Mosul University, uomosul
Mosul, Iraq

***Abstract*— In this paper I propose a number of steps as a starting point to any SOA project. First we talk about SOA and its importance in nowadays, then listing other researches opinions in the first step to SOA. After that I'll lists my proposed practical approach to start the way toward any SOA system, and enforce that by a practical case study for a technical institution system.**

Keywords-component; formatting; SOA : Service Oriented Architecture, Pre-SOA Model.

I. INTRODUCTION

Organizations tend to use SOA to achieve their strategic goals such as agility, productivity, and interoperability. SOA is a way or architectures used to build systems, these systems were build as a set of independent, loose coupled, and interoperable services. Each service is as simple as a distinct function, (or can be obtain multiple capabilities) which can works independent from others. These services can be reused to building new enterprise by using a correct recomposing architecture. The use of SOA might increase the alignment between organization's business and IT, resulting in more agility, well organization performance, and increased Return On Investment (ROI) [6][10].

II. FIRST STEP TO SOA

Many papers and books talk about first step to SOA. Many of them have the same opinion, others have a different look with different proposing way. Such as listing a service set [2], determine the scope and direction of SOA project*, view business as a collection of independent services, identifying critical business problems and challenges, start as a small project then increase toward business and technology metrics [3], messaging backbone or ESB [5][7], and other opinions as proposed by many of researchers.

Any person new to SOA see any of these suggested starting point is not enforced by a practical and explanation approach. We can consider these point of views just as a theoretical opinions. The question coming into account is how to put correct step in the SOA road with any of them?

In this paper I try to produce a practical point to start with any SOA weather legacy or new system, and enforce my proposed perspective with a practical case study, to produce a workable opinion.

III. PRE-SOA MODELS

When we tend to start a new enterprise by using SOA, the first question came into mind is how and when will we start? Is the start point from classical software engineering? Or from business patterns? Or any other ways? In this paper I'll give answer about this question.

I'll suggest to start from enterprise-Business side toward technology side.

1- Dimensions : As an organization, we first take into account the importance organization's dimensions. These dimensions are: Business (which can be considered as the basic of an organization), Tier, and department dimension. Then analyze each dimension to its major components (the tier is known that it contribute data, process, and front-end tier) those the organization and the system to be developed were interested in.
We can add another dimension called Entity, which can be used to build additional tables by contribute with the main dimensions metioned above. This new dimension can give us a different perspective, we can see the degree of relationship of dimensions those related to the same entity. (in this paper we use only the three main listed dimensions).

2- Build Tables : Second step is to build a number of two dimension tables, each of which take two of the earlier dimensions mentioned in the above step. First dimension components represent the column's address of the table, and the other represents the rows. (a detailed case study listed in the next section). After building tables schema we can start analyzing the intended system.

3- Services Analysis: The analysis phase can take place either after or as a parallel with requirements gathering process. In this phase we decompose the intended system (according to each table's column-row relation) into a small parts called services , each service is capable of doing a distinct function. And put the resulted services in the corresponding

* *http://msdn.microsoft.com/en-us/library/bb833022.aspx*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

column-row intersection. This analysis is done for each tabular according to its dimensions relation, and can be done incrementally as system requirement changed.

4- Service Filtering : the next step after models filling completed, we start an assessment process. Assessment process can be considered as service filtering process. We examined every model for new service(s) (which is not exists in an organization inventories), and reused services.
When we have complete a filtering of services we get a two lists of services, one for reusable (exist within one of inventories) and the other for new services (need to be developed).

After these steps we can work with new service list and implement it as it is an agnostic or non-agnostic services and according to service oriented architectures and patterns .

IV. CASE STUDY : BUILDING A SYSTEM FOR TECHNICAL INSTITUTION:

We work to build a SOA system for the Mosul technical institution which provide deferent systems and services as the next requirement list explained:

System name	function	Output
Salary	Money transaction, compute salary	reports
Absence	Compute absence	Hunt, report
Technical development	Learning, training	Reports, certified
Library	Borrowing	Report, bill, alarm
Store	Inbound, outbound, compute existing items	Report, alarm
Student	Student information	Report,
Employee	Employee information	Report
Exam committee	Degree, subjects, certified	Report, degree bill

First step we begin with analysis of dimensions to their major components.

- Tier dimension components are kwon : Data, Process, and Front-End.
- The business major components those resulted from the analyzing phase are : Finance, Technical Development, and Security.
- Departments contain : Salary , Absence, Store, Exam committee, Technical Development.

Now we can building the following tables :

1- Business – Tier table.
2- Business – Department table.
3- Department - Tier table.

The next step is the analysis of system and fitting it to tables dimensions. By applying this step we get the following tables :

1- Business – Tier mapping Model :

	Data	Process	Front End
Technical Development	Update Data Subject material	Train Learn	Reports Certification Course
Finance	Data hardware store Data analyst & Modeler cost	Processing environment cost Executer Cost Compute Salary	
Security	Access rights		Accounts

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

2- Department- Tier Model

	Data	Process	Front End
Salary	Get employee information Checked delivering field	Compute salary Transform money Compute service duration	C/S report
Absence	Modify	Compute Absence	Send alarm
Store	Delete Insert	Compute items quantity Books restoration Check available book Books Borrow system	Create/ delete borrowed bill
Technical development		Create clearance for training or learning	Send start date alarm
Exam Committee		Compute sum of degree Sort students Compute average	C/S students degree report C/S &Archiving students report

3- Business – Department Model :

	Finance	Technical Development	Security
Salary	Transfer money	addition experience salary Work hours	Safety money transfer Authorize access
Absence	Discount ratio per hour/day	Hunting system	
Technical development	Training cost Awards cost Fellowship	Training courses learning	
Exam Committee		Class, course, student, and degree system	
Store	Buying of items	Books borrow system Thesis classifying system Item availability	Secure inbound and outbound system

From above tables we can recognize some services were repeated in many tables, these repetitions giving us a wider insight of a service capabilities, which can be a useful thing when we deals with SOA patterns and when IT implementation taken place.

ACKNOWLEDGMENT

I would to thanks Dr. Abdul Sattar M. Khidir for his support.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1] A. Rotem-Gal-Oz, SOA patterns, 1st ed. Shelter Island, NY 11964, 2012.

[2] BEA, VMware, SOA and Virtualization: How Do They Fit Together?, white paper, 2007, pp. 3.

[3] C. Abrams, R. W. Schulte , Service-Oriented Architecture Overview and Guide to SOA Research, Gartner, ID Number: G00154463, 2008, pp.5.

[4] G. Lewis, Getting Started with Service- Oriented Architecture (SOA) Terminology, Software engineering institute, white paper, 2010.

[5] IBM Corporation, Providing a messaging backbone for SOA connectivity, White paper, 2007, pp. 4.

[6] J. Hurwitz, R. Bloor, M. Kaufman, and F. Halper, *Service Oriented Architecture for Dummies*, 2nd ed. USA, 2009.

[7] L.I. Terlouw, A. Albani, Identifying Services in SOA, ICRIS White Paper , 2009, pp. 3.

[8] S. M. Glen, J. Andexer, A practical application of SOA *Combine the technology and business perspectives of SOA implementation, IBM, 2007.*

[9] T. Erl, *SOA Design Patterns,1*st ed. USA, 2009.

[10] T. Erl, SOA : Principles of Service design, USA, 2008.

AUTHORS PROFILE

Safa T. Al-Ramadani : received the B.S. degree in software egineering from Mosul University, Mosul, Iraq, She is currently pursuing the M.S. degree in software engineering at Mosul University.

Performance Analysis of Call Admission Control Schemes in WCDMA Network

Syed Foysol Islam
Faculty of Engineering
University of Development Alternative (UODA)
Dhaka, Bangladesh
.

Mohammad Shahinur Islam
Faculty of Engineering
University of Development Alternative (UODA)
Dhaka, Bangladesh
.

Abstract— The main objective of this research is to derive a numerical model of call admission control in WCDMA network and examines its performance. Three important call admission algorithms: wideband power based (WPB), throughput based (TB) and adaptive call admission control (ACAC) algorithms are investigated along with their performance analyzed throughout this paper and a little comparison between them is presented.

Key Words: Wide Band Code Division Multiple Access (WCDMA), Wideband power based (WPB), Throughput based (TB) and Adaptive call admission control (ACAC)

I. INTRODUCTION

When a new call arrives in the system, it needs to check whether to accept the call or not. At first the system has to examine whether the new call is going to degrade the quality of the ongoing calls or the planned coverage area. If it attempts to make degradation in the system, then the system should block the call. In order to maintain the required quality of service of the new incoming call, there are three parameters that have to be checked: required SIR, inter cellular interference, intracellular interference. Based on these parameters the system admits the call in a selective way that does not affect the ongoing calls. This decision making part of the UMTS network is called the call admission control (CAC). In this research we will deeply study three call admission schemes and their performance.

Calculation of SIR:

$$SIR = \frac{Signal\ Power}{Total\ Interface\ Power} \qquad (1)$$

Equatiion (I) can be simplified as

$$SIR = SF.\frac{P_j}{I_{total}} = SF.\frac{P_j}{I_{inter} + I_{intra} + P_n} \qquad (2)$$

Where,

P_j = Received signal power of the user at Node B,

$$I_{total} = I_{inter} + I_{intra} + P_n \qquad (3)$$

I_{inter} = Interference caused by the Intercellular communications, I_{intra}= Interference caused by the Intra cellular communications, P_n= Thermal Noise which is assumed to be -99dBm in the downlink and -103 dBm in the uplink

SF= Spreading Factor

$$\text{Spreading Factor} = \frac{Carrier\ Bandwidth}{Information\ Rate} = \frac{Chip\ Rate}{Data\ Rate} = \frac{W}{R} \qquad (4)$$

II. CALL ADMISSION CONTROL SCHEMES

We have reviewed a lot of papers on this issue. Each method takes different parameter to make the decision criteria. Intercell interference and intracell interference are taken into account to measure the wideband received power based (WPB) admission control and the system throughput based (TB) admission control, service specific admission control, an heuristic method for making the decision of admission control, call admission control depends on the available bandwidth and capacity of the system presented in [1] [7] [5] [6] respectly. An adaptive method for call admission control (ACAC) focused in [4]. In this paper we have investigated on two main call admission control algorithm WPB and TB. A brief discussion on these methods is presented in this paper. A new promising method adaptive call admission control (ACAC) also compared with the previous two methods.

A. WPB Admission Control

Interference caused by the mobile stations within the own cell and also by the neighboring cells taken into account in this method The system maintains a threshold value both for uplink and downlink for accepting a new call.

UP Link: A new call is accepted only when the new total interference ($I_{total}+\Delta I$) caused by the new call is less than the threshold value (I_{th}) set by radio network planning. If the new resulting total interference that caused by the new call exceeds the threshold value it should be blocked. The mathematical representation of this formula is given by the equation (5)

$$\underbrace{I_{total\_old} + \Delta I}_{Total\ Interference} < I_{th} \qquad (5)$$

Where,

I_{total}= The interference before admitting the new call

ΔI = The estimated interference caused by the new call,

Figure 1 shows the explanation of this method. Let us assume that in a power controlled system the load of the system at any

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

instant is L_{old} and that creates the interference I_{old}. Now consider a new call coming to the Node B for getting admission then the RNC estimates the interference it would create as ΔI which is marked as I_{new}. The admission control algorithm checks whether this total interference (I_{old}+ ΔI) would exceed the predefined threshold value I_{th}. If the total interference exceeds the threshold value I_{th} then that call must be blocked.

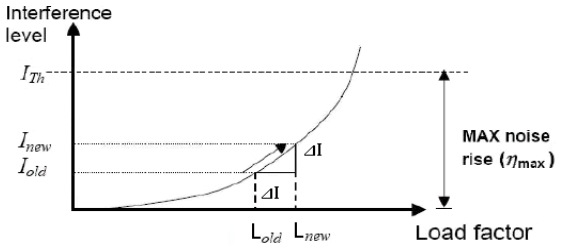


Figure 1: Interference level as a function of Load factor. [1]

As we have seen from the equation *(4)* that the estimated value of interference need to calculated. There are two methods for the calculation of increase interference or power, the derivative method and the integration method. Both take into account the load curve and are based on the derivative of uplink interference with respect to the uplink load factor i.e.

$$\frac{dI_{total}}{d\eta} \qquad (6)$$

We Know Noise rise is given by [1],

$$Noise\ rise = \frac{The\ interference\ before\ admitting\ new\ call}{Thermal\ Noise}$$

$$\approx \quad \frac{I_{total}}{P_n} \approx \frac{1}{1-\eta}$$

$$\therefore I_{total} \approx \frac{P_n}{1-\eta}$$

$$So,\ \frac{dI_{total}}{d\eta} \approx \frac{P_n}{(1-\eta)^2} \qquad (7)$$

The change in the uplink interference can be obtained by the following equations

$$\frac{\Delta I}{\Delta L} \approx \frac{dI_{total}}{d\eta}$$

$$\therefore \Delta I \approx \frac{dI_{total}}{d\eta}\Delta L \qquad (8)$$

Now using equation (7),

$$\therefore \Delta I \approx \frac{P_n}{(1-\eta)^2}\Delta L \qquad (9)$$

Substituting by the value of P_n, equation (8) can be simplified as

$$\Delta I \approx \frac{I_{total}}{1-\eta}\Delta L \qquad (10)$$

The second uplink interference increase estimation based on the integration method in which the differentiation of uplink interference with respect to the load factor is integrated from the old value of load factor ($L_{old} \approx \eta$) to the new value ($L_{new} \approx \eta + \Delta L$) i.e.

$$\Delta I \approx \int_{\eta}^{\eta+\Delta L} dI_{total} \qquad (11)$$

$$\approx \int_{\eta}^{\eta+\Delta L} \frac{P_n}{(1-\eta)^2}\Delta L$$

$$\approx \frac{P_n}{1-\eta-\Delta L} - \frac{P_n}{1-\eta}$$

$$\approx \frac{P_n(1-\eta-1+\eta+\Delta L)}{(1-\eta-\Delta L)(1-\eta)}$$

$$\approx \frac{\Delta L}{(1-\eta-\Delta L)} \cdot \frac{P_n}{(1-\eta)} \qquad (12)$$

Simplified by equation (6)

$$\Delta I \approx \frac{I_{total}}{1-\eta-\Delta L}\Delta L \qquad (13)$$

The value of load ΔL is given by

$$\Delta L \approx \frac{1}{1+\frac{W}{(E_b/N_0)vR}} \qquad (14)$$

Where, E_b/N_0 denotes signal to noise ratio, W is the chip rate, v is the activity factor and R data rate of traffic.

Downlink: In the downlink the same strategies is used but in this case the considering parameter is transmission power. If the new total downlink transmission power does not exceed the threshold power value, then the call is admitted.

$$\underbrace{P_{total\_old}}_{Total\ Powe}\ \underbrace{+\ \Delta P}_{r} \ \langle\ P_{th} \qquad (15)$$

P_{total_old}: The transmission power before admitting the new call, ΔP*:* Estimated transmission power required for the new call, P_{th}*:* Threshold value set by radio network planning, *Total Power*: Total estimated transmission power,The power increase ΔP_{total} is estimated by the initial power.

B. Throughput Based Admission Control

Unlike wide band power based admission control, throughput based admission control takes into account the load. Two different threshold values one for uplink threshold and downlink threshold are used for taking decision.

Uplink:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The new user is not admitted in the system if the new total load exceeds the predefined uplink threshold set by the radio network planning.

$$\underbrace{\eta_{ul} + \Delta L}_{Total\ Load} \rangle\ \eta_{ul\_Th} \qquad (16)$$

Where, η_{ul}: The load before admitting new user L_{old}, ΔL : Estimated load for the new user or call, η_{ul_Th}: Threshold value for the uplink load factor, *Total Power:* Total estimated load for the new user

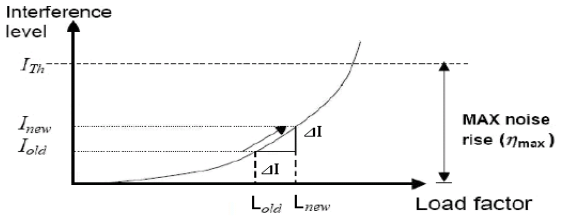


Figure 2: Load Curve

Down Link: The new call is not admitted in the system if the total resulting load exceeds the downlink threshold value.

$$\eta_{DL} + \Delta L\ \rangle\ \eta_{DL\_Th} \qquad (17)$$

Where η_{DL} can be calculated as

$$\eta_{DL} \approx \frac{\sum_{j\approx 1}^{N} R_j}{R_{\max}} \qquad (18)$$

N is the total no of connections in the system, R_j is the bit rate of user j and R_{max} is the maximum allowed throughput of the cell [1].

C. Adaptive Call Admission Control

ACAC scheme, the base station updates the total no of users to the RNC in regular intervals (τ). This small interval may call an epoch. With this information the RNC should decide which scheme (WPB or TB) it needs to switch to, by calculating the number of each type of user presented in the system at the end of a previous epoch. If there are more voice users, the ACAC switches to WPB and if there are more data users, it switches to the TB scheme. This prediction depends on α, which is the parameter used to predict the number of calls in the coming epoch and β, keeps the information of total number of calls that have originated in the system since start-up. The values of α and β varies between 0 and 1 and are calculated adaptively through simulations [4], [8]. The predicted no of calls that arrive in the system determined by the following equations

$$\hat{V}_{n+1} = \alpha V_n + (1-\alpha)\hat{V} + \beta V_{total} \qquad (19)$$

$$\hat{D}_{n+1} = \alpha D_n + (1-\alpha)\hat{D} + \beta D_{total} \qquad (20)$$

Where, $\hat{V}_{n+1}$ *:* voice calls arrival in the coming epoch, $\hat{D}_{n+1}$ *:* data calls arrival in the coming epoch, $\hat{V}_n$ *:* voice calls in the previous epoch, $\hat{D}_n$ *:*data calls in the previous epoch, V_n *:* Originated number of voice calls in the previous epoch, D_n *:* Originated number of data calls in the previous epoch.

In a system where (m-k) channels are busy is defined by the following equation

$$\beta(m,k) = \frac{\beta(m-1,k-1)}{1+\frac{1}{m}\sum_{r=0}^{R-1} A_r b_r \beta(m-1,b_r-1)} \qquad (21)$$

Here, *R:* The number of traffic classes (*0 – R –1*), b_r*:* Required data rate, *m:* No of servers in the system and *k >0*

$$A \approx \frac{\lambda_r}{\mu_r}$$

$$\approx \frac{Poisson\ \ distributed\ \ call\ \ arrival\ \ rate\ \ of\ \ class\ \ r}{Exponential\ \ distributed\ \ call\ \ arrival\ \ rate\ \ of\ \ class\ \ r}$$

The initial values of β measured by the following equations

$$\beta(m,0) = \frac{\frac{1}{m}\sum_{r=0}^{R-1} A_r b_r \beta(m-1,b_r-1)}{1+\frac{1}{m}\sum_{r=0}^{R-1} A_r b_r \beta(m-1,b_r-1)} \qquad (22)$$

III. COMPARATIVE RESULT

Contrast between WPB and TB schemes is shown by the figure 3. It has been observed from the graph that more interference will add from the neighboring cells with the increasing value of *i*. The other cell to own cell interference ratio *i* with value 0 means no interference from the neighbor.

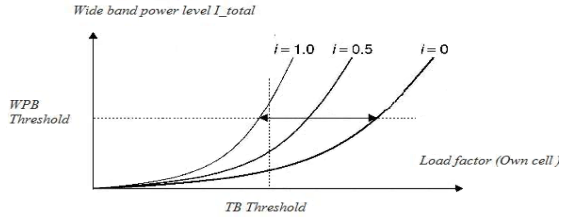


Figure 3: WPB and TB admission criteria

WPB takes the interference from adjacent frequency bands. This could be originated from the other operator's mobile station, which is closer to a base station. So that it could perform an overestimate of the wide band received power. TB does not take inference from the neighboring cells. Rather it concern about the loading of the neighboring cells through the RNC.

Adaptive call admission control (ACAC) combines the WPB and TB schemes. Depending on the total no of voice *(19)* and data users *(20)* it switches between WPB and TB scheme. If there is more voice user in the system ACAC switches to WPB mode and if there is more data users than the voice users the ACAC follow the TB mode. The limitations of WPB and TB overcome by the ACAC scheme. The call blocking probability in ACAC is tends to be zero comparing other two methods. Figure 4 and 5 compares the performance of these

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

three methods by call blocking probability call dropping probability.

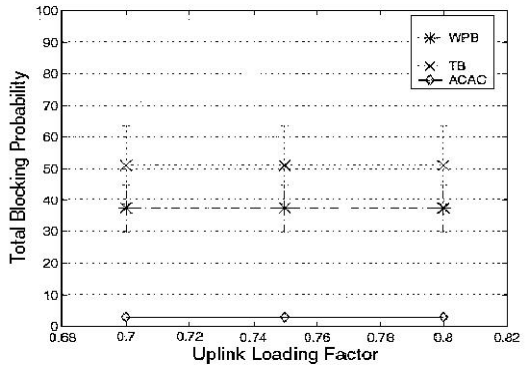


Figure 4: Call blocking probability of WPB, TB and ACAC scheme

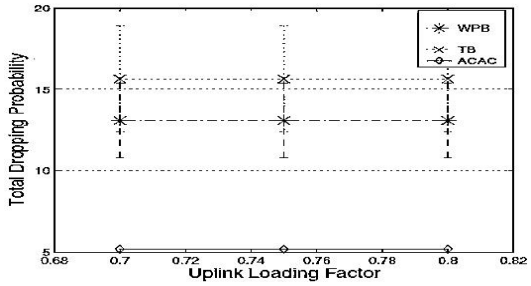


Figure 5: Call dropping probability of WPB, TB and ACAC Scheme

Figure 4 and figure 5 help us to observe that the call blocking probability in ACAC is less than the WPB and TB. The call dropping probability in ACAC is less than the WPB and TB schemes. So we can say that the ACAC is best algorithm.

IV. CONCLUSION

Call admission control plays the primary role in radio resource management. As it is used in wireless networks to optimize the system performance and guarantee the QoS. By using a perfect admission control algorithm congestion and over load of the network can be eliminated. Two major admission control algorithms WPB and TB are studied in this paper. One of the latest algorithms ACAC is also studied in this paper. We have observed that Adaptive CAC's which is the combination of the above two methods could be a better option for a system design. We have limited our work only within the WCDMA FDD mode.

REFERENCES

[1] Harri Holma and Anti Toskala ,"WCDMA for UMTS radio access for third generation mobile communications", *John wiley and sons ltd.*

[2] Il-Min Kim, Byung-Cheol Shin, and Dong-Jun Lee," SIR-based call admission control by intercell interference prediction for DS-CDMA systems", *IEEE COMMUNICATIONS LETTERS, VOL. 4, NO. 1, JANUARY 2000.*

[3] Technical Specification of 3rd Generation Partnership Project on Radio Resource Management "3G TR 25.922 V3.0.0".

[4] Kamala Subramaniam, Arne A. Nilsson,"An analytical model for adaptive call admission control scheme in a heterogeneous UMTS-WCDMA system", *2005 IEEE.*

[5] Jun Ye, Xuemin (Sherman) Shen and Jon W. Mark ," Call admission control in Wideband CDMA cellular Networks by using fuzzy logic", *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 4, NO. 2, MARCH/APRIL 2005.*

[6] Songsong Sun and Witold **A.** Krzymien, "Call admission policies and capacity analysis of a multi-service CDMA personal communication system with continuous and discontinuous transmission", *1998 **I**EEE.*

[7] Chae Y. Lee and Jun Jo, "Service specific call admission control in WCDMA system".

[8] Kamala Subramaniam, Arne A. Nilsson, "Tier-based analytical model for adaptive call admission control scheme in a UMTS-WCDMA system".

[9] William Stallings, "Wireless communication and Networks", Pearson Education.

AUTHORS PROFILES

Syed Foysol Islam
MSc Engg in Electrical Engineering (BTH, Sweden)
BSc, MSc in Computer Science (Rajshahi University, Bangladesh)
Assistant Professor, Department of ETE
University of Development Alternative (UODA)

Mohammad Shahinur Islam
BSc in Electronic and Telecommunication Engg (UODA, Bangladesh)
Junior Lecturer, Department of ETE
University of Development Alternative (UODA)

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs 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
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. 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. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2013
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, Embeded 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 .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/