IJCSIS Vol. 13 No. 2, February 2015
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 BETA

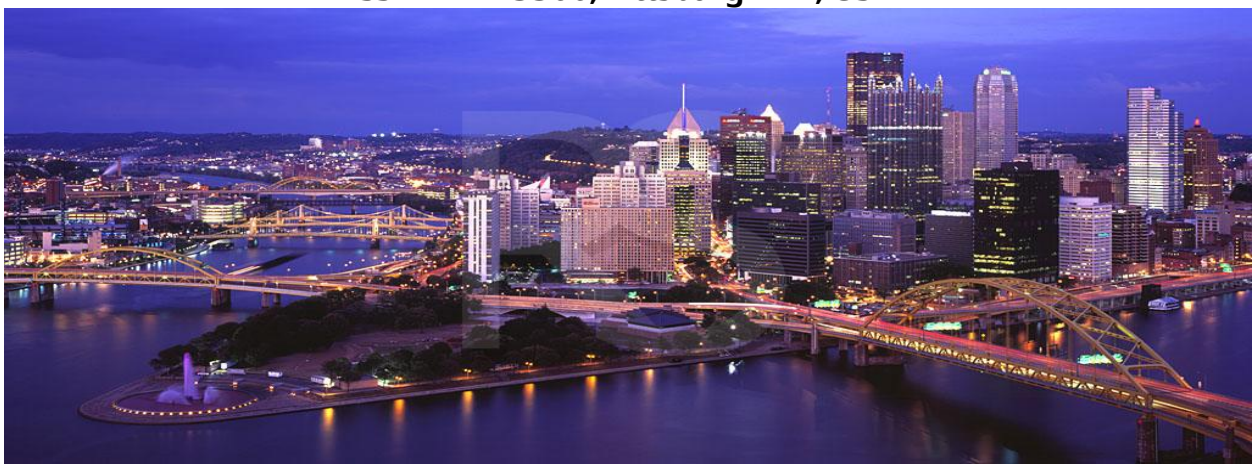
DOAJ DIRECTORY OF OPEN ACCESS JOURNALS

EBSCO HOST

ProQuest

IJCSIS April 2015 "SPECIAL ISSUE" CALL FOR PAPERS

International Journal of Computer Science and Information Security
ISSN 1947 5500, Pittsburgh PA, USA



The **International Journal of Computer Science and Information Security** (IJCSIS) seeks papers describing significant research contributions to the field of computer science, software engineering and network security. We invite submissions on a wide range of software technologies and network security research, including, but not limited to:

- Software Development, Data Modeling Techniques, Knowledge Engineering Methods and Practices, Software Design and Applications in Various Domain, Software Engineering: Demographics & Economics, Software Maintenance and Evaluation; Software Security; Software Reliability Engineering; Software Technologies and Platforms for Emerging Services.
- Communication Architecture, Algorithms, Modeling and Evaluation; Data Centers and Big Data Computing; Green Networks and Sustainable Computing; Grid, Cloud, Internet and Peer-to-peer Computing and Communication; Internet of Things (IoT); Mobile Ad Hoc and Sensor Systems, Multimedia Computing and Real-Time Networking; Security, Privacy, and Trust, Cloud Computing Security, Security Informatics, Network Security Attacks, Survivable Networks, Wireless Networks
- Data Mining and Knowledge Discovery; Geographical Information Systems; knowledge based systems; Semantic data Analysis; Business Data and Process Management; Data Warehousing; Database Security, Embedded Software and Systems, Innovative Computing Technology.

Prospective authors are invited to submit original technical papers by the deadline **31 March 2015** for publication in the IJCSIS April 2015 Proceedings. Submitted manuscripts must be formatted in standard IEEE camera-ready format (double-column, 10-pt font) and must be submitted to **ijcsiseditor@gmail.com**.

To submit papers to IJCSIS, first carefully read the following guidelines:
https://sites.google.com/site/ijcsis/authors-notes

Important Dates:

Paper submission Due: **31 March 2015**	Acceptance Notification: **22 April 2015**	Camera Ready and Registration Due: **30 April 2015**

Guest Editors (Biographies)

Dr. G. Krishna Mohan, is Associate Professor in the Department of Computer Science & Engineering, KL University. He obtained M.C.A degree from Acharya Nagarjuna University, M.Tech(CSE) from Jawaharlal Nehru Technological University, Kakinada, M.Phil from Madurai Kamaraj University and Ph.D(CSE) from Acharya Nagarjuna University. He qualified, AP State Level Eligibility Test. He is having 14 years of Teaching experience at various levels. His research interests lies in Data Mining and Software Engineering. He published 30 research papers in various National and International journals. Six scholars were pursuing their Ph.D under his guidance. He is an Editorial Board Member of Scholars Academic & Scientific Publishers, reviewer of Reviewer of Australasian Journal of Information Systems.

Dr Uttam Mande, is an Assistant Professor in GITAM UNIVERSITY. He has 11 years of teaching experience in Computer Science Department. He was awarded PhD in 2014 and with several journals including IEEE Conferences in the area of data miming for decreasing the road accidents, crime data analysis, rule-based data mining and automated profile generation research field.

Editorial
Message from Managing Editor

*The **International Journal of Computer Science and Information Security** (IJCSIS) promotes research publications which offer significant contribution to the computer science knowledge, and which are of high interest to a wide academic/research/practitioner audience. Coverage extends to several main-stream and state of the art branches of computer science, security and related information technology. As a scholarly open access peer-reviewed journal, IJCSIS mission is to provide an outlet for quality research & academic publications. It aims to promote universal access with equal opportunities for international scientific community; to scientific knowledge, and the creation, and dissemination of scientific and technical information.*

*IJCSIS archives all publications in major academic/scientific databases. 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. Moreover, Google Scholar reported increased in number cited papers published in IJCSIS **(No. of Cited Papers: 551, No. of Citations: 1248, Years: 6th)**. Abstracting/indexing/reviewing process, editorial board and other important information are available online on homepage. By supporting the Open Access policy of distribution of published manuscripts, this journal ensures "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, guarantees a rigorous peer-reviewing process. 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. 13, No. 2, February 2015 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

3. Paper 30011511: Technical Solutions to Resources Allocation for Distributed Virtual Machine Systems (pp. 18-23)

Ha Huy Cuong Nguyen, Departmentof InformationTechnology, Quangnam University, Quang Nam, Viet Nam
Van Thuan Dang, Departmentof InformationTechnology, Industrial University of HCM City, Quang Ngai, Viet Nam
Van Son Le, Departmentof InformationTechnology, Danang University of Education, The university of Danang, Da Nang, Viet Nam

Abstract — Virtual machine is built on group of real servers which are scattered globally and connect together through the telecommunications systems, it has an increasingly important role in the operation, providing the ability to exploit virtual resources. The latest technique helps to use computing resources more effectively and has many benefits, such as cost reduction of power, cooling and, hence, contributes to the Green Computing. To ensure the supply of these resources to demand processes correctly and promptly, avoiding any duplication or conflict, especially remote resources, it is necessary to study and propose a reliable solution appropriate to be the foundation for internal control systems in the cloud. In the scope of this paper, we find a way to produce efficient distributed resources which emphasizes solutions preventing deadlock and proposing methods to avoid resource shortage issue. With this approach, the outcome result is the checklist of resources state which has the possibility of deadlock and lack of resources, by sending messages to the servers, the server would know the situation and have corresponding reaction.

Keywords— Virtual machine, best-effort, lease, deadlock detection, distributed environments, virtual resources.

4. Paper 30011501: Comparative Analysis of Discrete Logarithm and RSA Algorithm in Data Cryptography (pp. 24-31)

Abari Ovye John (1), Simon Philip (2), and P. B Shola (3)
(1) Computer Science Department, Federal University Lokoja, Kogi State, Nigeria.
(2) Computer Science Department, Federal University Kashere, Gombe State, Nigeria.
(3) Computer Science Department, University of Ilorin, Kwara State, Nigeria

Abstract - Due to its speed, spread and ease of use, the internet has now become a popular means through which useful data and information are transported from one location to another. This shift in the way data and information is being transported then calls for a new or different approach to security issues to save data in-transit from hackers. Cryptography is one of the approaches that have been explored for data security on the internet. RSA and El-Gamal (based on concepts of discrete logarithm) cryptographic algorithms are mostly employed to handle data security on the internet. This research work present a fair comparison between RSA and Discrete Logarithm algorithms along this direction; efficiency (time and space) by running several encryption setting to process data of different sizes. The efficiency of these algorithms is considered based on key generation speed, encryption speed, decryption speed, and storage requirement of the cipher text. In this paper, simulation has been conducted using Java programming language. Texts of different sizes were encrypted and decrypted using RSA and El-Gamal during the testing. Based on the result of the simulation, El Gamal is faster than RSA in terms of key generation speed but consumes more memory space than RSA. RSA is faster than El-Gamal in terms of encryption and decryption speed.

Keywords: Cryptography, Algorithm, RSA, El-Gamal, Encryption, Decryption, Discrete Logarithm, Plain text, Cipher text.

5. Paper 30011509: Ensuring Consistent Patient Data Flow in a Low Bandwidth Environment with Mobile Agent (pp. 32-39)

Akomolafe, Oladeji Patrick, Department of Computer Science, University of Ibadan, Ibadan, Nigeria

Abstract - The present technological advancement in pervasive computing and the widespread of the internet and wireless networks and mobile communication systems can be harnessed by E-health to bring better monitoring of

patients to obtain a more efficient health care delivery, cost reduction and reduction in medical errors. Health care applications can take outstanding advantage of the intrinsic characteristics of multi-agent systems because of notable features that most health care applications share. This paper presents a patient monitoring system where context can be easily gathered from patient to caregivers. All the functionalities involved in transmitting data or contextual values from one end (patient) to another end (Doctor or Care givers) were abstracted into a middle ware using mobile agent technologies.

Keywords- Mobile data, Local Patient Information, Mobile Agents, Context Aware, Middleware

6. Paper 31051401: State of the Art: Vehicle-to-Vehicle Information Exchange (pp. 40-53)

Abdelsalam Obeidat, Software Engineering Dpt., College of Information Technology, World Islamic University for Science and Education, Jordan, Amman
Adnan Shaouot, The Electrical and Computer Engineering, The University of Michigan-Dearborn, Dearborn, MI 48128
Atef Nsour, Computer Engineerng Dpt., College of Engineeering, Yarmouk University ,Irbid, Jordan; World Islamic University for Science and Education, Jordan, Amman
Nidal Al-Omari, Software Engineering Dpt., College of Information Technology, World Islamic University for Science and Education, Jordan, Amman

Abstract - As with most 'new' ideas and technologies, there is not much 'new' involved in the basic concept but just with the implementation. The idea of vehicle-to-vehicle communication dates back to the widespread implementation of wireless communication devices and the need for passengers of one vehicle to communicate with those of another. The purpose of this paper is to explore the past, present and potential future application of technologies that enable occupants of two separate vehicles to exchange messages. Whether the intent is safety, courtesy or emergency notifications, there is opportunity to provide this message exchange over a distributed system via a low cost portable device.

Hybrid Intrusion Detection System Using Artificial Bee Colony Algorithm and Multi-Layer Perceptron

MAHMOD S. MAHMOD
College of science
University of Mosul, Mosul, Iraq

ZAKARIA A. HAMED ALNAISH
College of science
University of Mosul, Mosul, Iraq

ISMAIL AHMED A. AL-HADI
Amran University
Yemen

***Abstract*—Intrusion detection system (IDS) is a crucial instrument for monitoring the activities that take place in a computer networks. Recently, a large number of algorithms have been proposed which simulate the swarm intelligence which was used by a number of researchers. Intrusion detection system (IDS) is regarded as one of the applications that are based on Swarm Intelligence and the classification techniques such as the neural network. In this study, hybrid Artificial Bee Colony (ABC) algorithm and Multi-layer Perceptron (MLP) were proposed to build an efficient network IDS. The MLP was utilized as a classifier to distinguish the normal and abnormal packets in the network traffic. The structure of MLP has been created relying on the features of (NSL-KDD 99) dataset. In addition, ABC algorithm is employed for training MLP by optimizing the values of linkage weights and bias. Training and Testing were performed by means of using NSL-KDD Dataset, which is the improved version of KDD99 dataset. The experiments results showed that the proposed method provides a high detection accuracy which is about (87.54%) and with (0.124%) error rate.**

***Index Terms*—Intrusion detection system (IDS); Artificial Bee Colony (ABC) algorithm; multi-layer perceptron (MLP).**

I. Introduction

As the cost of information processing and Internet accessibility falls, organizations are becoming increasingly vulnerable to potential cyber threats such as network intrusions. So, there is an urgent need to provide secure and safe transactions by using firewalls, Intrusion Detection Systems (IDSs), encryption, authentication, and other hardware or software solutions. Many variants of IDSs are exist which allow security managers and engineers to detect the network attack packets primarily through the use of signature detection [1].

An Intrusion Detection System (IDS) is a mechanism which could be either Software or Hardware that monitors network or system actions for malicious activities and produces reports to a management station [2].IDSs have become a standard component in security infrastructures as they allow network administrators to detect policy violations.

These policy violations range from external attackers are trying to gain unauthorized access to insiders abusing their access [3]. IDS approaches can be divided into two main categories: misuse and anomaly detection [2]. The misuse detection approach assumes that an intrusion can be detected by matching the current activity with a set of intrusive patterns (generally defined by experts or “underground” web sites). Anomaly detection systems assume that an intrusion should deviate the system behavior from its normal pattern. There are many approaches to implement IDS by using statistical methods, neural networks, predictive pattern generation, association rules and others techniques. To build efficient and robust IDS, swarm intelligence techniques (e.g. Ant Colony Optimization, Artificial Bee Colony, and Particle Swarm Optimization) consider one of the new proposed methods to construct clustering and classification models to distinguish between normal behavior and abnormal behavior. In this study, hybrid new method proposed to construct IDS by utilizing Multi-Layer Perceptron (MLP) and Artificial Bee Colony (ABC) optimization algorithm. ABC algorithm is used to enhance the learning of MLP by optimizing its linkage weights. NSL-KDD dataset has been used to investigate the performance of proposed IDS to classify two classes (normal or attack). NSL-KDD dataset considers one of standard benchmark for intrusion detection evaluation [4]. The rest of this paper is organized as follow; related works are explained in section 2. Section 3 has shown a brief of MLP and ABC Algorithms. Section 4 depicts the Framework of the proposed system. The experimental results of the proposed system are indicated in Section 5. Finally, the conclusion of this study summarized in Section 6.

II. Related Work

In 2010, S. Lakhina *et al*. [5] proposed a new hybrid algorithm PCANNA (principal component analysis neural network algorithm) to reduce the number of computer resources, both memory and CPU time which are required to detect attack. The PCA (principal component analysis) is employed to reduce the number of the used features and the neural network is used to identify the kinds of new attacks.

Test and comparison have been done based on NSL-KDD dataset. The experiments demonstrated that the proposed model gives a better and robust representation of data which it was able to reduce features to get 80.4% data reduction.

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

As a result, approximately 40% reduction in training time and 70% reduction in testing time are achieved. S. Lakhina *et al*. [5] , are claimed that the proposed method not only reduces the number of the input features and time but also increases the classification accuracy.

In 2013, D. Y. Mahmood and M. A. Hussein [6] applied K-star algorithm with filtering analysis in order to build a network intrusion detection system. In the experimental analysis, they have used the benchmark NSL-KDD dataset, where 66.0% of the dataset are used for training and the rest are used for the testing. The proposed method was used to classify the dataset into two classes (Normal and Attack). WEKA which is consist of a collection of machine learning algorithms for Data mining tasks has been used in the training and testing processes.

In 2013, R. S. Naoum and Z. N. Al-Sultani [7] presented a hybrid intrusion detection system models, using Learning Vector Quantization and an enhanced resilient backpropagation artificial neural network. A Supervised Learning Vector Quantization (LVQ) represents the first stage of classification which was trained to detect intrusions; it consists of two layers with two different transfer functions, competitive and linear. A multilayer perceptron as the second stage of classification was trained using an enhanced resilient backpropagation training algorithm to classify the intrusions which are detected in the first stage. The evaluations were performed using the NSL-KDD99 dataset. The experimental results demonstrate that the proposed system (LVQ_ERBP) has a detection rate about 97.06% with a false negative rate of 2%.

In 2013, N. B. Ibraheem and H. M. Osman [8] aimed to design and implement a Network Intrusion Detection System (NIDS) based on genetic algorithm. In order to get rid of redundancy and in appropriate features principle component analysis (PCA) this is useful in features selecting process. The complete NSL-KDD dataset is used for training and testing data. A number of different experiments have been done. The experimental results shown that the proposed system based on GA and PCA (for selecting five features only) of NSL-KDD was able to speed up the process of intrusion detection, which effect on minimizing the CPU time cost and reducing the time of training and testing.

In 2013, Jha and L. Ragha [9] suggested novel IDS approach which includes two contributions. First, provides a review on current trends in intrusion detection using SVM together with a study on technologies implemented by some researchers in this research area. Second, it proposes a novel approach to select best feature for detecting intrusion. The proposed approach is based on hybrid approach which combines filter and wrapper models for selecting relevant features. This reduced the size of dataset which led to enhance the performance and detection accuracy of proposed detection model. Moreover the time of training and testing processes also reduced with reducing the features.

In 2013, R. A. Sadek *et al*. [10] produced a new hybrid approach called NNIV-RS (Neural Network with Indicator Variable using Rough Set). The proposed approach aimed to reduce the amount of computer resources which are required to run the detection process such as memory and CPU time. Rough Set Theory is used to select important features. Indicator Variable is used to represent dataset in more efficient way. Neural network is used for network traffic packet classification. Tests and comparison were done on NSL-KDD dataset. The experimental results showed that the proposed algorithm gives better and robust representation of data as it was able to select features resulting in 80.4% data reduction, select significant attributes from the selected features and achieve detection accuracy about 96.7% with a false alarm rate of 3%.

III. Artificial Bee Colony Algorithm

The Artificial Bee Colony (ABC) algorithm is an optimization algorithm proposed by Karaboga in 2005 [12] based on the principles of the foraging process in swarm intelligence. In the ABC algorithm the performance depends on food sources and the tasks of the bees which are employees, onlookers and scouts bees. Each food source represents one solution for the problem [13,14]. For every food source, there is only one employed bee. In other words, the number of employed bees is equal to the number of food sources [15]. The nectar amount for each food source represents the fitness value of each possible solution. After all employed bees complete the search process; they share the information about their food sources with onlooker bees. An onlooker bee evaluates the nectar information taken from all employed bees and chooses a food source with a probability related to its nectar amount [16]. The employed bee becomes a scout bee when one of the solutions cannot be enhanced further through a predetermined number of cycles which is called *limit* parameter as a result that food source is assigned as an abandoned source [16]. In the ABC algorithm, the main parameters are population size (colony size) which is divided equally between employees and onlookers [14], the number of the variables that will be optimized (dimensions), maximum iteration and the value of the limit parameter. The main steps of the algorithm are given bellow:

1. Initialize the population of solutions x_{ij} by using equation (1)
$$x_{ij}= x_{min,j}+ rand(0, 1)(x_{max,j}-x_{min,j}) \qquad (1)$$
Where x_{ij} the values of the food source, i=1,...,CS/2, CS is the colony size, j=1... D, D is the number of the variable that would be optimized.
2. Evaluate the population using a predefined function.
3. Repeat the following steps until reach the maximum iteration.
4. Produce new solutions (food source positions) v_{ij} in the neighborhood of x_{ij} for the employed bees using equation (2) and evaluate them.
$$v_{ij}= x_{ij}+ \phi_{ij}(x_{ij} - x_{kj}) \qquad (2)$$

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

Where ϕ_{ij} is a random number within the interval [-1,1].

5. Apply the greedy selection process between x_i and v_i.
6. Calculate the fitness values of solutions as shown below:

$$fit_i = \begin{cases} \frac{1}{1+f_i}, & fi \geq 0 \\ 1 + |f_i|, & fi < 0 \end{cases}$$

Where, f_i represents the object value of solutions which is calculated by a predefined objective function. Then calculate the probability values p_i for the solutions x_i using equation (3) and normalize p_i within the interval [0,1].

$$p_i = \frac{f_i}{\sum_{i=1}^{SN} fit_i} \qquad (3)$$

7. Produce the new solutions (new positions) v_i for the onlookers from the solutions x_i selected depending on p_i and evaluate them.
8. Apply the greedy selection process between x_i and v_i for the onlookers bees.
9. If there is abandoned solution x_i (scout bee), replace it with new solution which will produce randomly using equation (1).
10. Memorize the best food source position (optimal solution) achieved so far. The flowchart of the basic algorithm is shown in Figure (1) explaining the simplicity of the algorithm.

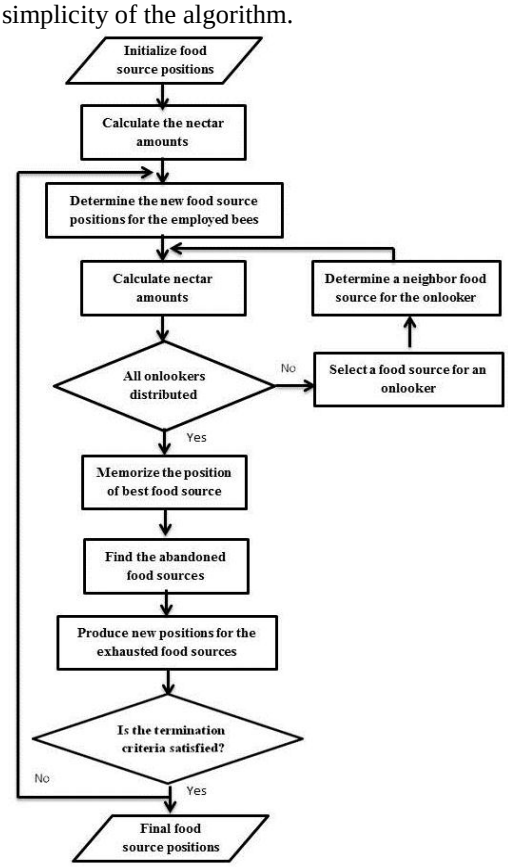


Figure (1) The flow chart of the ABC algorithm [11]

IV. Artificial Neural Networks

Artificial neural network (ANN) [29] is a branch of artificial intelligence. It is a computational system inspired by central nervous systems. The most common applications of ANN are machine learning, classification, pattern recognition as well as prediction [17]. Usually, ANN structure consists of at least three layers which are input, hidden and output layers. Each layer includes a number of nodes which is determined based on the problem which is wanted to be solved. Figure (2) shows a general structure of ANN.

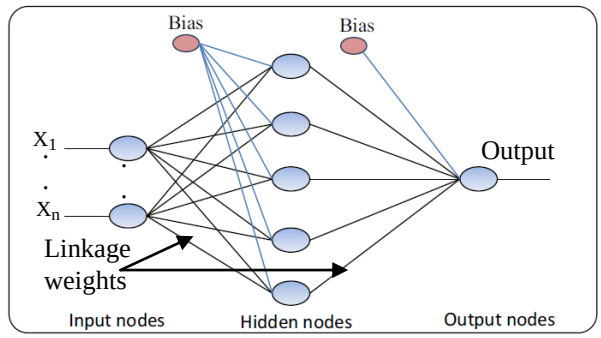


Figure (2) MLPANN [18]

As shown in figure (2), each node connects to all nodes in the next layer through the linkage weights. In addition, there are node in each layer called bias node also are connected to all node on the particular layer by the bias weights [18]. The training process includes update the values of the linkage weights and biases weights between the layers of ANN structure by one of the optimization algorithm. Moreover, there are two types of training process which are supervised and unsupervised learning. In supervised learning, input and desired output must be available but in unsupervised learning only input data is available [19]. Furthermore, the output for each node in each layer is based on the weighted inputs of the node and the used activation function. The sigmoid function considers one of the most common used as an activation function [20, 11] which is used in this study for a node (x) as shown in Equations (4) and (5).

$$f(x) = \frac{1}{1+e^{-net(x)}} \qquad (4)$$

$$net(x) = \sum_{i=1}^{n} W_i I_i + \theta_x \qquad (5)$$

Where W_i represents the (i)th linkage weight of node (x), I_i indicates the (i)th input value of node (x) and θ_x is the bias of node (x).

Consequently, the linkage weights and biases are changed until getting the minimum error of the output which is calculated as shown in Equation (6) [17].

$$\text{Error} = \frac{1}{2}\sum\sum(T-O)^2 \qquad (6)$$

Where, (T) represents the desired output and (O) represents the actual output (O).

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

V. HYBRID ARTIFICIAL BEE COLONY AND MULTILAYER PERCEPTRON (ABC-MLP)

In this study, ABC is utilized to optimize the learning in ANN by tuning the weights and biases of ANN as an intrusion detection system (IDS). Basically, the structure of implementation ABC algorithm on ANN includes two procedures for (NSL-KDD 99) dataset. The first procedure involves constructing the structure of the ANN for the dataset. The second procedure includes obtaining the optimum weights and biases with minimum error rate and highest classification accuracy rate by applying ABC algorithm on the ANN structure for (NSL-KDD 99) dataset. The mechanism of learning ANN using ABC includes two important steps. The first step is encoding the problem for food source of ABC-ANN. Actually, there are three encoding strategies [22] which are vector encoding, matrix encoding and binary encoding. In this study, the matrix encoding has been selected for encoding process. The second step is selecting the fitness function to find the fitness value for each food source (solution). The mean square error (MSE) is used as fitness function to measure the nectar amounts (fitness value) of the food sources (solution) for the ABC-ANN model, as shown in Equation (7).

$$\text{MSE}= \frac{1}{2}\sum_{i=1}^{m}(T_{i-}\ O_i)^2 \qquad (7)$$

Where, T_i indicates the i*th* actual output value, O_i indicates the i*th* estimated output value of ANN and *m* represents the total number of the input instances. Thus, the dimensions (*d*) (no. of variable to be optimized) for each food source equal to the number of all the linkage weights and biases (wb) in ANN which are represented by the columns of array (1) and the rows of array (1) represents the number of food sources (*n*)(solutions).

$$\text{Bee swarm}=\begin{bmatrix} wb11 & wb12 & \cdots wb1d \\ wb21 & wb22 & \cdots wb2d \\ \vdots & \vdots & \vdots \\ wbn1 & wbn2 & \ldots\ wbnd \end{bmatrix} \qquad (1)$$

Therefore, the dimension of the ANN in this study calculated using Equation (8)[18].

$$\text{Dimension} = (\text{Input} \times \text{Hidden}) + (\text{Hidden} \times \text{Output}) + \text{Hidden} + \text{Output} \qquad (8)$$

Where input, hidden and output represents the numbers of ANN nodes in input layer, hidden layer and output layer, respectively. The number of nodes in hidden layer calculated based on Kolmogorov Theorem [23, 18] using Equation (9).

$$\text{Hidden nodes} = 2 \times \text{Input nodes} + 1 \qquad (9)$$

Generally, Figure (3) indicates the general flowchart of the proposed model (ABC-ANN).

The methodology and the learning process for the proposed model (ABC-ANN) are illustrated in the following steps:

1) Initialize randomly the values of each food source (solution) in ABC-ANN model depending on the structure of the ANN for (NSL-KDD 99) dataset with in the interval [-1, 1].
2) Cycle =1
3) Calculate the fitness value for each food source (solution) based on the structure of ANN which is represents the error value by using Equation (7).
4) Optimize the weights and biases of ANN utilizing (ABC) algorithm.
5) Keep the best weights and biases (food source) which have minimum error.
6) Cycle = Cycle+1.
7) Repeat the steps (3-6) until Cycle = maximum iteration.

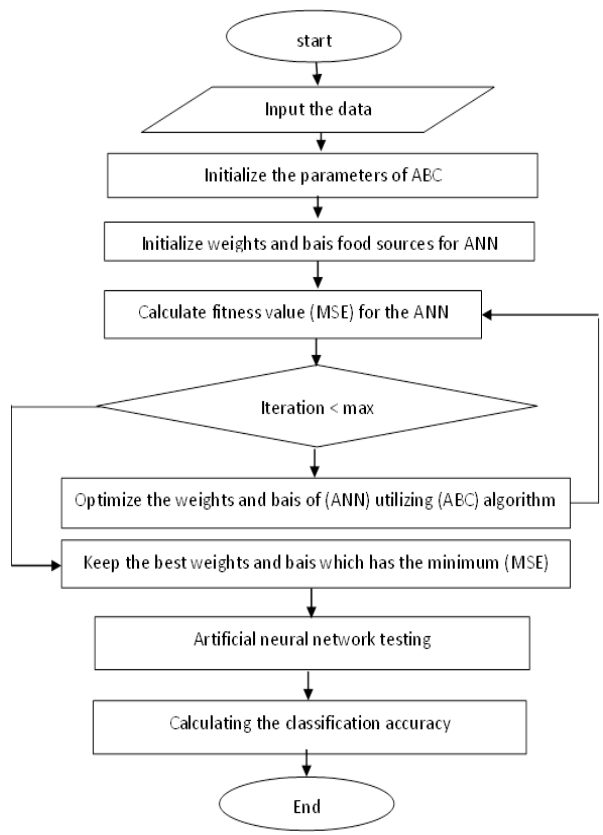


Figure (3) general flowchart of the proposed model (ABC-ANN)

VI. NSL-KDD DATASET

NSL-KDD is a data set suggested to solve some of the inherent problems of the KDD'99 data set which are mentioned in [24]. Although this new version of the KDD dataset still suffers from some of the problems discussed by McHugh [25] and may not be a perfect representative of

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

existing real networks because of the lack of public data sets for network-based IDSs, it still can be applied as an effective benchmark data set to help researchers to compare different intrusion detection methods [27,28]. Furthermore, the number of records in the NSL-KDD training and testing sets are reasonable. This advantage makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of different research work will be consistent and comparable.

The NSL-KDD data set has the following advantages over the original KDD data set. Firstly, It does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records.Secondly, there is no duplicate records in the proposed test sets; therefore, the performance of the learners are not biased by the methods which have better detection rates on the frequent records.Thirdly, the number of selected records from each difficulty level group is inversely proportional to the percentage of records in the original KDD data set. As a result, the classification rates of distinct machine learning methods vary in a wider range, which makes it more efficient to have an accurate evaluation of different learning techniques. NSL-KDD contains 125973 records of training samples and 22544 records of test samples with 42 features in each record.

VII. Normalization Process

Normalization Process is applied on NSL-KDD 99 to become the values of the features in the [0,1] range because features of the NSL-KDD 99 data set have either discrete or continuous values, which made it incomparable. In this study, min-max normalization [26] process is applied as shown in Equation (10).

$$\text{Normalized (x)} = \frac{x-\min(X)}{\max(X)-\min(X)} \qquad (10)$$

Where (x) represents the current value of attribute (X).

VIII. Experiments and Results

To evaluate the performance of the proposed IDS (ABC-MLP), three various experiments were applied with different parameters values as shown in the table (1).

Table (1) parameters values for three various experiments

Name of parameter in ABC-MLP	First experiment	Second experiment	Third experiment
Number of food source	10	20	30
Colony size (CS)	20	40	60
Dimension (linkage weights and biases)	3656	3656	3656
Maximum iteration	100	100	100
Limit	20	10	10

NSL-KDD 99 dataset is used in all the experiments, where 125973 patterns are used for training and 22544 patterns are used for testing in each experiment based on the resource of the data. Also, the number of nodes in input layer, hidden layer and output layer are 41, 81 and 1, respectively.

The detection accuracy rate and the false alarm rate were calculated according to equations (11) (12), respectively.

$$\text{Accuracy rate} = (1\text{-error rate})*100 \qquad (11)$$

$$\text{Error rate} = \frac{1}{2}\sum\sum(T-O)^2 \qquad (12)$$

Where (T) represents the desired output and (O) represents the actual output (O).

The experiments are executed on a system with a 2.3GHZ core i5 processor and 6GB of RAM running windows 8. All the processing is done using MATLAB® 2010b.

In the training phase, figure (3) shows the comparison between the obtained accuracy rates of the three experiments. The first and the third experiments produce the best accuracy which is equal to (87.55 %); whereas, the second experiment achieved the worst accuracy rate over (87.51%).

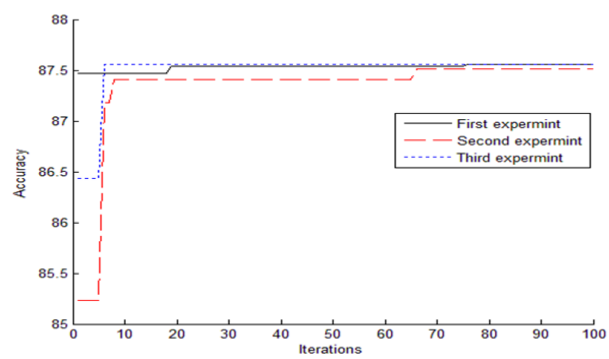


Figure (4) comparison between the obtained accuracy rates of the three experiments

In addition, Figure (5) shows the comparison between the obtained error rates of the three experiments. The all experiments produce the minimum error rate which is equal to (0.12%).

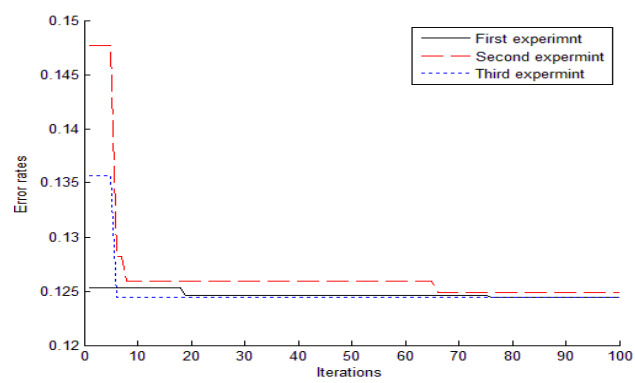


Figure (5) comparison between the obtained error rates of the three experiments

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

Moreover, in the terms of accuracy rate, in the first experiment, the convergence ratio was very low based on Standard division (Std). While, the second and third experiments have higher convergence ratio; although, the first experiment produced the highest accuracy (87.55%) as shown in the table (2).

Table (2) experimental results of training ABC-MLP

Parameters	First experiment		Second experiment		Third experiment	
	Accuracy (%)	Error (%)	Accuracy (%)	Error (%)	Accuracy (%)	Error (%)
maximum	87.55	0.125	87.51	0.147	87.55	0.135
minimum	87.46	0.124	85.23	0.124	86.43	0.124
Mean	87.53	0.124	87.33	0.126	87.49	0.125
Standard division (Std)	0.032	3.1977e -004	0.487	0.0049	0.2448	0.0024

In the testing phase, the second experiment has realized the best performance in terms of accuracy and error rates which were (87.54%) and (0.124%), respectively with duration time five seconds only, as shown in table (3) and figure (6) and figure (7).

Table (3) experimental results of testing ABC-MLP

The experiment	Accuracy (%)	Error rate (%)	Duration time
1	87.15	0.128	4.95 second
2	87.54	0.124	5 second
3	87.12	0.128	4.96 second
Average	87.27	0.126	4.97 second

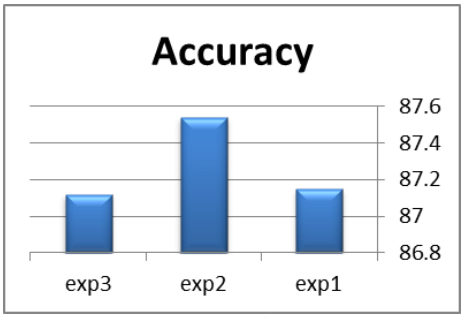


Figure (6) Accuracy rate of testing ABC-MLP

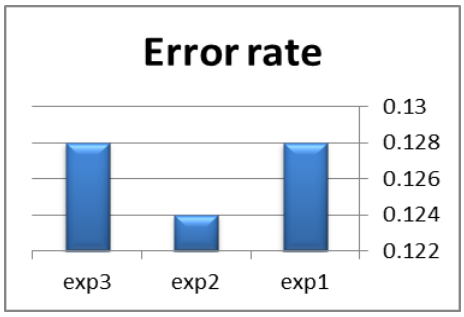


Figure (7) Error rate of testing ABC-MLP

Furthermore, to investigate the performance of the proposed IDS (ABC-MLP), the performance is compared with the performance of recently proposed methods from the literature, as revealed in table (4).

Table (4) comparative results of testing phase

Methods name	No. of patterns	No. of features	Accuracy rate (%)	Error rate (%)	Time (second)
Multinomial Naïve Bayes + N2B [27]	22544	41	38.39 %	/	/
SOM [28]	22544	41	75.49%	5.77 %	0.55
Discriminative Multinomial Naïve Bayes+PCA	/	/	94.84%	/	/
Discriminative Multinomial Naïve Bayes+RP	/	/	81.47%	/	/
Discriminative Multinomial Naïve Bayes+N2B	/	/	96.5%	/	/
Proposed method (ABC-MLP)	22544	41	87.27%	0.126	4.97

As depicts in table (4), the performance of the proposed method is comparable with other methods in literature. Despite some methods have higher performance than proposed method, the proposed method considers an efficient IDS because it has been tested based on all features of NSL-KDD which simulates a real network features.

IX. Conclusion

Recently, network attacks have increased through the computer network. Intrusion detection system (IDS) considers a primary tool to secure the network; therefore, enhancing the performance of IDS gets the attention of many researchers.

Artificial neural network (ANN) plays an important role in classification process. Multilayer Perceptron (MLP) is one of the efficient types of ANN. Thus, it is used to classify between normal and abnormal manners. Due to the good performance of artificial bee colony (ABC) in solving optimization problems, it is used in this study to enhance the learning of MLP. Also, NSL-KDD 99 dataset is used to evaluate the performance of the proposed approach (ABC-MLP). The experiments results conducted that the proposed approach has superior performance in terms of accuracy and error rates. As a future work, another optimization algorithm and another type of ANN could be applied to develop a new IDS system which could be detect and classify attacks in computer network environment.

References

[1] V. M. Boncheva, "A Short Survey of Intrusion Detection Systems," Institute of Information Technologies, BULGARIAN ACADEMY OF SCIENCES, Sofia, vol. 58, 2007.

[2] W. Lee, S.J. Stolfo and K.W. Mok, “A data mining framework for building intrusion detection models,” in: Proceedings of IEEE Symposium on Security and Privacy, 1999, pp. 120–132.

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

[3] A. S. Subaira and P. Anitha, "An Efficient Classification Mechanism For Network Intrusion Detection System Based on Data Mining Techniques: A Survey, " vol. 6, no. 1, October 2013.

[4] C. Gu and X. Zhang, "A Rough Set and SVM Based Intrusion Detection Classifier," Second International Workshop on Computer Science and Engineering, 2009.

[5] S. lakhina, S. Joseph and B. verma, "Feature Reduction using Principal Component Analysis for Effective Anomaly– Based Intrusion Detection on NSL-KDD," International Journal of Engineering Science and Technology, vol. 2, no. 6, pp.1790-1799, 2010.

[6] D. Y. Mahmood and M. A. Hussein, " Intrusion Detection System Based on K-Star Classifier and Feature Set Reduction," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 15, no. 5, PP. 107-112, Nov. - Dec. 2013.

[7] R. S. Naoum and Z. N. Al-Sultani, "Hybrid System of Learning Vector Quantization and Enhanced Resilient Backpropagation Artificial Neural Network For Intrusion Classification," Ijrras, vol. 14, no. 2, February 2013.

[8] N. B. Ibraheem and H. M. Osman, "Principle Components Analysis in network Intrusion Detection System using NSl-KDD,"Raf. J. of Comp. & Math's. , Fifth Scientific Conference Information Technology, vol. 10, no. 1, Dec. 2013,

[9] J. Jha and L. Ragha,"Intrusion Detection System using Support Vector Machine," International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA, 2013.

[10] R. A. Sadek, M. S. Soliman and H. S. Elsayed, "Effective Anomaly Intrusion Detection System based on Neural Network with Indicator Variable and Rough set Reduction," IJCSI International Journal of Computer Science Issues, vol. 10, issue 6, no. 2, November 2013 .

[11] N. Karaboga and M. B. Cetinkaya, "A novel and efficient algorithm for adaptive filtering: Artificial bee colony algorithm," Turk J ElecEng and Comp Sci, vol.19, no.1, pp. 175 – 190, 2011.

[12] D. Karaboga, "An Idea Based on Honey Bee Swarm for Numerical Optimization," Technical Report-TR06, Computer Engineering Department, Engineering Faculty, Erciyes University, Kayseri, 2005.

[13] D. Karaboga and B. Basturk, "A Powerful and Efficient Algorithm for Numerical Function Optimization: Artificial Bee Colony (ABC) Algorithm," Journal of Global Optimization, Vol. 39, pp. 459-471, 2007.

[14] E. Gerhardt and H. M. Gomes, "Artificial Bee Colony (ABC) Algorithm for Engineering Optimization Problems,"EngOpt2012-3rd International Conference on Engineering Optimization, Rio de Janeiro, Brazil, July 2012.

[15] D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm," Applied Soft Computing, vol. 8, no. 1, pp. 687-697, 2008.

[16] D. Karaboga and C. Ozturk, "Fuzzy clustering with artificial bee colony algorithm," Scientific Research and Essays, vol. 5, no. 14, pp. 1899-1902, July 2010.

[17] Y. Cakir, M. Kirci and E.O. Gunes, "Yield prediction of wheat in south-east region of Turkey by using artificial neural networks," Third International Conference on Agro-geoinformatics, 2014, pp.1-4.

[18] I.A.A. AL-Hadi, S.Z.M. Hashim and S.M.H. Shamsuddin, "Bacterial Foraging Optimization Algorithmfor neural network learning enhancement," 11th International Conference on Hybrid Intelligent Systems (HIS), 2011, pp. 200-205.

[19] J. C. Hua, "Study of Particle Swarm Optimization Fitness Functions for Multilayer Perceptron Network In Classification Problems," M.Sc. Thesis, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia, 2009.

[20] L. M. Fu, "Neural Networks in Computer Intelligence," New York: McGraw Hill, 1994.

[21] S.A. Mirjalili, S. Z. M. Hashim and H. M. Sardroudi, "Training feedforward neural networks using hybrid particle swarm optimization and gravitational search algorithm," Applied Mathematics and Computation, vol. 218, pp. 11125–11137, 2012.

[22] J.-R Zhang, J. Zhang, T.-M Lok., M. R.Lyu, "A hybrid particle swarm optimization back propagation algorithm for feedforward neural network training," Applied Mathematics and Computation, vol. 185, no. 2, pp. 1026 -1037, 2007.

[23] M. H. Hassoun, "Fundamentals of Artificial Neural Networks", PHI Learning Private Limited New Delhi-110001. Book-Page 46, 2008.

[24] M. Tavallaee, E. Bagheri, W. Lu and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[25] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262–294, 2000.

[26] M. S. Mahmood, "Using ant and self-organization maps algorithms to detect and classify intrusion in computer networks," MSc. Thesis, University of Mosul, 2011.

[27] M. Panda, A. Abraham and M.R. Patra, "Discriminative multinomial Naïve Bayes for network intrusion detection," Sixth International Conference on Information Assurance and Security (IAS), vol. 5, no. 10, pp. 23-25, Aug. 2010.

[28] L. M. Ibrahim, D. T. Basheer, M. S. Mahmod, "A Comparison Study for Intrusion Database (Kdd99, NSL-Kdd) Based On Self Organization Map (Som) Artificial Neural Network," Journal of Engineering Science And Technology, vol. 8, no. 1, pp. 107 – 119, 2013.

[29] X. Yao, "A review of evolutionary artificial neural networks". International Journal of Intelligent Systems, pp. 203-222, 1993.

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

New Secure Communication Design for Digital Forensics in Cloud Computing

Mahmoud M. Nasreldin
Ain Shams University
Cairo, Egypt

Magdy El-Hennawy
Shorouk Academy
Cairo, Egypt

Heba K. Aslan
Electronics Research Institute
Cairo, Egypt

Adel El-Hennawy
Ain Shams University
Cairo, Egypt

Abstract— **Digital forensics experts are facing new challenges in collecting evidences in cloud computing environment. Eevidences are often located in data centers that are geographically separated. Digital forensics experts cannot bear travelling burden to acquire evidences. Moreover, the volume of hosted data is so big and the data is so complex. For the evidence to be admitted in court, evidence collecting process must guarantee evidence integrity, authenticity, non-repudiation, and confidentiality. To achieve a secure cloud forensics process, researchers have proposed many solutions in literature with major drawbacks in security, high communication, and computation overheads. Furthermore, received packets should be analyzed without assuming the availability of the entire original packet stream. Recently, Sign-Encrypt-Sign and Encrypt-Sign-Encrypt techniques were used to provide evidence confidentiality, authenticity, non-repudiation, and integrity. In this paper, we propose an identity-based signcryption protocol to reduce the computation, communication, and implementation overheads in evidence colleting in cloud forensics. Signcryption protocols have the advantage of achieving the basic goals of encryption and signature protocols in more efficient way than Sign-Encrypt-Sign and Encrypt-Sign-Encrypt techniques. Also, a validation of the proposed protocol using BAN logic is illustrated.**

Keywords- Digital Forensics, Cloud Computing, Evidence Collecting, Authentication, Confidentiality, Signcryption, Identity-Based Cryptography, BAN Logic.

I. INTRODUCTION

Cloud computing environment brings attractable services to users and organizations through efficient digital solutions with low cost. On the other hand, digital forensics has an arising need in digital solutions. Digital forensics in cloud computing (cloud forensics) is a multi-disciplinary research area that has technical and legal millstones, such as, chain of custody, acquisition of remote data, big and distributed data, ownership, and trust. For evidence to be admitted to court, it has to be authentic with no malleability. Sometimes, evidence confidentiality is required. Cloud computing is the future of Information Technology (IT) to supply organizations' need and reduce the life cycle cost of services/equipment. At the same time, cloud computing environment raises security concerns and demands modifications to current security solutions that do not consider cloud in their designs. Cloud computing makes use of the Internet to provide users and organizations with new services. NIST describes cloud computing as a set of computing means such as servers, networks, services and applications that deliver accessibility, flexibility and extra performance on demand network-access that comprises of five essential characteristics, three service models and four deployment models. Cloud computing brings consistent admission to distributed resources and it reorganizes the IT domain due to its availability, scalability, less maintenance cost, data and service availability assurance, and services provision infrastructure [1-2]. In cloud computing, there are no fears regarding over estimation of services that do not comply with forecasts. Thus, there is no expensive misuse of resources, or underestimate for one that becomes widespread on large scale. Cloud computing reduces the possibility of losing customers and reducing revenue. Moreover, large batch-oriented tasks can get fast results to comply with programs scalability. Cloud computing new model consists of facilities that are provided similarly to utilities, such as gas, water, electricity, and telephony services. In this model, customers do not care to identify how the services are provided or where they are hosted. In cloud computing, the infrastructure is a "Cloud" from which clients can access applications from anywhere using on demand methods. Main software industry players have admitted the importance of cloud computing. Worldwide definition of cloud computing did not known yet. But, literature defines the basic principles. Several authors believes that cloud computing is an extended cluster computing environment, or more precisely Cloud Computing = Cluster Computing + Software as a Service [3]. What is relatively clear is; cloud computing is based on five key characteristics, three delivery models, and four deployment models.

Cloud computing denotes both the delivered applications as services over the Internet and the hardware and systems software in the data centers. The data center hardware and software form the cloud. The Cloud Computing Service Model is based on three primary tenants: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In the SaaS, the application is hosted and delivered online through a web browser. In Paas, the cloud provides the software platform for systems. Iaas is a set of

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

virtualized computing resources. All IT roles, such as security, storage, applications, networking, and software work in harmony to provide users with a service based on the client-server model. There are four deployment models for cloud services specific requirements [4]:

- Public Cloud: The cloud infrastructure is available to public or a large industry group. The owner is an establishment that sells cloud services (e.g. Amazon EC2).
- Private Cloud: The cloud infrastructure is operated exclusively for a single establishment and might be managed by the same establishment or a third party (on-premises or off-premises.)
- Community Cloud: The cloud infrastructure is shared by some establishments and supports a specific community with common interest (e.g., security requirements, mission, policy, or compliance considerations) and might be managed by the same establishment or a third party (on-premises or off-premises) (e.g. academic clouds.)
- Hybrid Cloud: The cloud infrastructure is an alignment of two or more clouds (private, community, or public.) It allows data and application portability (e.g., cloud bursting for load-balancing between clouds) (e.g. Amazon VPC).

Cloud computing interact with challenges that might define the degree of utilization (i.e. data and applications interoperability, security, data exchange and transfer, business continuity and service availability, data and applications interoperability, performance unpredictability, storage scalability, bugs in large scale distributed systems, scaling quickly, and software licensing). These five essential characteristics of cloud computing are on-demand self-service, ubiquitous network access, rapid elasticity, Location independent resource pooling and measured service (pay-per-use). Cloud computing accomplishes efficient utilization of resources. However, cloud computing protocols do not provide any mechanisms for providing confidentiality or authenticity of the received messages. The cloud computing authentication is a serious problem. Authenticity means that the recipient could verify the identity of the sender and ensures that the received message comes from the supposed originator. For cloud computing communication, authentication is a challenging problem, since it requires the verification of big data. Cloud computing authentication protocols must have the following characteristics: it must have low computation and communication overheads. Researchers have proposed many solutions in literature. The major drawback of some of these solutions was the high communication and computation overheads. Others suffer from security pitfalls. Due to the rapid development in cloud computing, numerous challenges in cybercrime investigations appear. This brings the need for digital forensics professionals to encompass their expertise in the cloud computing and digital forensics domains in order to reduce the risks of cloud security breach. Apart from that, some characteristics of cloud computing such as lack of well-defined physical characteristics, different service models, and different deployment models have created a new setting for cloud forensics dimensions. Through this paper, we will refer to digital forensic in non-cloud environment as traditional digital forensics, the traditional digital forensics require a specific description to the evidence that will be acquired. This description should include the physical descriptions which are size, media type, the evidence interfaces, and file system format that will be acquired. Digital forensics (computer forensics) is the use of scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources to enable successful prosecution. The objective of digital forensics is to enhance and acquire legal evidence that is found in digital media. The current NIST definition of digital forensics is the scientific procedures used to recognize and classify, collect, evaluate, and analyze the data while maintaining the level of integrity of the information throughout the forensics process. The purposes of digital forensics are including forensic computing, forensic calculations and computer forensics. Being called into judicial proceedings is one of the digital forensics risks. Thus it must have a correct procedure in conducting the forensic investigation and doing the inspection setup where this procedure or methodology must basically base on the scientific principles [5].

Distributed big data cannot use disk cloning to collect evidence in the cloud. Moreover, shared hosts comprise both suspicious data that is related to the cybercrime and sensitive non-related data. To enhance the cybercrime investigation and protect data confidentiality/privacy of irrelevant users in cloud forensic, Hou *et al.* [6-8] and Nasreldin *et al.* [9] proposed several solutions to protect the authenticity and integrity of the collected evidence. It is essential to have a well-thought-out way of proper handling of evidence in order to minimize errors in investigations. This well-thought-out way is known as the digital forensic process. Moreover, for the trustworthiness of evidence, the digital forensic investigators are typically requested to clarify the process they used in gathering evidence in a court of law. This means that the digital forensic investigator should always know the digital forensic process and the suitable toolsets used in a digital forensic investigation [10-11]. The digital forensic process can be classified into four phases namely acquisition, examination, analysis and reporting. This process is well known in mobile and network forensics fields. The acquisition phase defines how data will be acquired from different types of digital information sources. Data has to be acquired in a way that maintains its integrity and authenticity. The acquired data has to experience forensic duplication or sector level duplication. A write blocker should be used in building duplicates. The write blocker guarantees that nothing is written to the original evidence. Software imaging tools can also be used. Imaging could be a physical image (bit-for-bit image) that is created of the entire physical device or a logical image that is created from active directories and files available to the operating system. Hash function is used to verify the integrity of acquired data. Digital hash conducts a mathematical algorithm

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

to provide a fingerprint that authenticates that the data has not been tampered with or altered. This fingerprint is maintained within the case file. Several studies that focus on technical issues, challenges and the opportunities have been done, but more research is needed to find effective methods to evaluate the uncertainty of the evidence or any forensic findings in the cloud forensics processes. Forensic investigators need to update themselves in multiple disciplines of knowledge in order to investigate the digital evidence in a cloud environment. In particular, they need to acquire high level of knowledge in specific areas such as mobile, hard disk, registry and others that can be considered as legal evidence in court. In order to enhance the digital forensics process in cloud computing, basic framework and architecture are needed [12-14].

Cryptography offers effective techniques to ensure users' security and privacy in an efficient way. To protect the cloud computing environment from intruders/attackers and transmit evidence over an insecure channel, encryption and digital signature algorithms could be used within different designs to provide secure networks and security solutions in order to protect users' information and their data from being attacked. In a previous work [9], we presented a security mitigation to fix the scheme proposed by Hou *et al.* to verify data authenticity and integrity in server-aided confidential forensic investigation [8]. In this paper, we deploy the signcryption technique that solves the problem of communication, computation, implementation overheads. The proposed protocol makes use of identity-based cryptography to overcome the Public Key Infrastructure (PKI) problems. The deployment of PKIs has many disadvantages such as high storage cost, large bandwidth requirement, non-transparency to users, and the need for certificate revocation lists (CRLs). Finally, a verification of our proposed protocol using BAN logic is performed. The remainder of this paper is organized as follows. In the next section, we briefly review the fundamental and technical background of cloud forensics, signcryption, and identity-based cryptography. In section 3, we elaborate on the computational number theory problems related to the security of the proposed protocol. Then, a detailed description of the proposed identity-based signcryption protocol is given in Section 4. The security analysis of the proposed protocol is included in Section 5. The verification of the proposed protocol is discussed in Section 6. Finally, we conclude in Section 7.

II. RELATED WORK

A. Cloud Forensics

Cloud computing allows establishments to make use of high scalable infrastructure resources, pay-per-use service, and low-cost on-demand computing. Clouds attract various establishments. However, the security and trustworthiness of cloud infrastructure has become a growing concern. Clouds can be a destination of attacks or a source to launch attacks. Malicious individuals can simply abuse the power of cloud computing and manipulate attacks from nodes/hosts inside the cloud. Most of these attacks are original and exclusive to clouds. Many characteristics of cloud computing make the cloud forensics process complex. In cloud computing, the storage system is not local [15]. Moreover, law enforcement agents cannot seize the suspect's computer/digital device in order to get access to the digital evidence, even with summon to appear. In the cloud, each server/host encompasses files from many users. Therefore, it is not easy to confiscate servers/hosts from a data center without violating the privacy of other users. Furthermore, when identifying data that belongs to a particular suspect, it is difficult to separate it from other users' data. There is no standard way, other than the cloud provider's word, to link given evidence to a particular suspect. So, the credibility of the evidence is also doubtful [16].

In traditional digital forensics, investigators have physical access and full control over the evidence (e.g., process logs, router logs, and hard disks). Unfortunately, in cloud digital forensics case, the control over data diverges in different service models. There are different levels of control of customers' data for the three different service models (i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)). Cloud users have highest control in IaaS and least control in SaaS. Thus, lack of physical access of the evidence and absence of control over the system make evidence acquisition a challenging task in the cloud environment. In the cloud computing environment, the source of the evidence is ubiquitously and the connection to the source is complicated. Furthermore, the investigators have to hire others (inside/outside the country.) Unlike copying a file from one folder to another folder, the processes of retrieving the evidence in cloud storage is complex. Usually, it costs a lot of time and money in parallel to the investigation time. Investigators have to determine the computational structure, attribution of data, and the integrity of the data. Also, investigators have to keep the stability of evidence and present/visualize it [17-18].

There are two different ways to include digital forensic investigation in could computing. In the first way, considers the cloud as a tool of the crime. In the second one, the cloud hosts a service as a target of the crime. In this section, we elaborate on the inspection of a targeted system of the forensics investigation exists in the cloud. There are many technical ways to conduct a forensic examination in cloud environment. These ways are similar to traditional examination. In the cloud environment, there are three aspects to be considered. First, the nature of crime determines the type of the system (alive or dead) which the forensics process will be performed on. Second, to determine what took place in the cloud. Third, the availability of secure channel to collect evidences over the cloud (i.e. installed collecting client on the cloud nodes/hosts must deploy digital signature and encryption algorithms to communicate with imager device.) Traditional digital forensics has two scenarios of evidence acquisitions (i.e. live-system/powered-on-system acquisition,

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

dead-system/powered-off- system acquisition.) In the dead system, investigators only analyze hard disk images (stored data without power.) Alive systems have the capability to analyze more evidences to be acquired than dead systems. For the same case, more evidences (e.g., running processes) can be acquired in alive system than the dead system. One advantage of digital forensics in cloud environment over traditional digital forensics is that digital forensics in cloud environment is considered alive system. The cloud has valuable information and there is a possibility to be partially up, in the case of compromise. This gives the investigator more files, connections, and services to be acquired and investigated. The cloud is totally dead when shutting down the entire cloud. This possibility is almost impossible and contradicts the basic idea of cloud environment [19-21]. Trust in the cloud environment is very important issue. For example, assume that a computer has been manipulated to plan a murder and if law enforcement removes the hard drive for imaging. In this case, law enforcement must trust their hard drive hardware to correctly read the disk. On the other hand, if law enforcement run forensic tool on alive computer, they must trust the integrity of the host operating system in addition to the hardware. Let us assume that the compromised system is hosted in the cloud, new layers of trust are introduced. As a risk mitigation strategy, the forensic investigator should examine evidence as multiple items, as mentioned before in the seven acquiring steps. This allows the investigator to check for inconsistency and to correlate evidence [22-23].

In [8], Hou *et al.* proposed an "encryption-then-blind signature with designated verifier" scheme to prove the authenticity and integrity of the evidence in cloud environment. Hou et al. aim to improve the investigation efficiency and protect the privacy of irrelevant users, one strategy is to let the server administrator search, retrieve and hand only the relevant data to the investigator, where the administrator is supposed to be responsible for managing the data in a secure manner. Due to some special crimes, the investigator may not want the administrator to know what he is looking for. In short, it is indispensable to consider how to protect both confidentiality of investigation and privacy of irrelevant users in such forensic investigation. For simplicity of description, Hou *et al.* refer to this problem as "server-aided confidential forensic investigation". When the above-mentioned relevant data is presented as evidence during a trial, Hou *et al*. aim to realize that the administrator (or the third party the administrator trusts) can verify whether the presented evidence is the data that comes from the server and whether the evidence is altered or not.

B. Signcryption

The common approach to achieve both evidence confidentiality and authenticity is to sign the evidence and encrypt it with its signature. The sender would sign the evidence using a digital signature scheme and then encrypt it with an appropriate encryption algorithm. The signature would use a private key encryption algorithm, under a randomly chosen message encryption key. The random evidence encryption key would then be encrypted using the recipient's public key. These are "sign-then-encrypt" or "encrypt-then-sign" techniques. Encrypt-then-sign is subject to the plaintext-subsection and text stealing attacks. The composition of the sign-then-encrypt approach suffers from a forwarding attack [24-25].

To mitigate these security breaches, Sign-Encrypt-Sign and Encrypt-Sign-Encrypt techniques is used [9, 26-33]. Sign-Encrypt-Sign and Encrypt-Sign-Encrypt suffers from computation, implementation, and communication overheads. The term signcryption was originally introduced and studied by Zheng in [34] with the primary goal of reaching greater efficiency than can be accomplished when performing the signature and encryption operations separately. In spite of proposing some security arguments, most of the work on signcryption [34-50] missed formal definitions and analysis. The signcryption scheme requires one computation for "encryption" and one inverse computation for "authentication", which is of great practical significance in directly performing long messages, since the major bottleneck for many public encryption schemes is the excessive computational overhead of performing these two operations [26]. Moreover, signcryption schemes must achieve non-repudiation, which guarantees that the sender of a message cannot later repudiate that she has sent the message. Namely, the recipient of a message can convince a third party that the sender indeed sent the message. It is worth noting that typical signature schemes provide non-repudiation, since anyone, who knows only the sender's public key, can verify the signature. This is not the case for signcryption, because the confidentiality property entails that only the recipient can comprehend the contents of a signcrypted message sent to him. Nevertheless, it is feasible to accomplish non-repudiation by other means. Instead of using encryption/signing process, signcryption can be applied in place of separate encryption and signing to reduce both communication bandwidth and computational time overheads. Any authentication scheme for big data streams should verify the received packets without assuming the availability of the entire original stream.

C. Identity-Based Cryptography

Public Key Infrastructures (PKIs) [51] bind public keys to their corresponding digital certificates. This is a mandatory requirement to provide the authenticity of public keys that users can trust in order to perform encryption and signing operations. Unfortunately, the deployment of PKIs has many disadvantages such as high storage cost, large bandwidth requirement, non-transparency to users, and the need for certificate revocation lists (CRLs). In order to bypass the trust problems encountered in conventional PKIs, in 1984, Shamir [52] introduced the concept of identity based cryptography and constructed an id-based signature scheme. Identity-based cryptography is a type of public-key cryptography in which the public key of a user is some unique information about the identity of the user (e.g., an e-mail

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

address, an IP address, or a social security number.) Identity-based cryptosystems simplify key management and remove the need of public key certificates as much as possible. This is due to the fact that the public key is the identity of its owner, and hence, there is no need to bind users and their public keys by digital certificates. The only keys that still need to be certified are the public keys of the trusted authorities (called the Private Key Generators (PKGs)) that have to generate private keys associated with users' identities. Several practical solutions for Identity-based Signatures (IBS) rapidly appeared after Shamir's original paper, but, despite several attempts [53-57], finding a practical Identity-based Encryption (IBE) scheme remained an open challenge until 2001. The latter proposals either require tamper-proof hardware, expensive private key generation operations for PKGs or end users who are assumed not to collude in order to expose the authority's master key. The first practical construction came in 2001 when Boneh and Franklin [58] proposed to use bilinear pairing to construct an elegant identity based encryption algorithm. Another IBE scheme was also suggested by Cocks [59]. This second method relies on simpler mathematics but is much less practical because of the large expansion in the size of its ciphertext. Many other identity based signature and key agreement schemes based on pairings were later proposed [60-64].

III. PRELIMNARY

In this section, computational number theory problems related to the security of the proposed protocol are discussed. The reader is referred to [58, 65, 66] for further details regarding the definitions below.

A. Elliptic Curve Discrete Logarithm (ECDL)

Let q be a prime power and let F_q denote the finite field of order q. Let $E(F_q)$ denote a set of points on the elliptic curve E over a field F_q, and let $E(F_q)$ denote the order of the group $E(F_q)$. Let $P \in E(F_q)$ be a point of order $p|\#E(F_q)$. The Elliptic Curve Discrete Logarithm (ECDL) problem is defined as follows:

Elliptic Curve Discrete Logarithm (ECDL) problem: Given a point P on the elliptic curve, along with the curve coefficients, and a point $Q = xP$, find the integer x, $0 \le x \le p - 1$, such that $Q = xP$.

B. Diffie-Hellman Problems

An abstract understanding of bilinear mapping requires knowledge of Gap Diffie-Hellman groups and bilinear groups. Gap Diffie-Hellman groups are created from disjointing computational and decisional Diffie-Hellman problems. Bilinear groups are based on the existence of a bilinear map. Let G be an additive cyclic group of prime order p, and P is its generator. In this group, the well-known Diffie-Hellman problems carry on as follows [67-69].

Computational Diffie-Hellman (CDH): Given $P, aP, Q \in G$, compute $aQ \in G$. An algorithm that solves the computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine,that on input P, aP, Q, outputs aQ with non-negligible probability. The Computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. This assumption is believed to be true for many cyclic groups, such as the prime subgroup of the multiplicative group of finite fields [70].

Decisional Diffie-Hellman (DDH): Given $P, aP, Q, bQ \in G$, decide whether a equals b. Quadruples of this form (P, aP, Q, bQ) are named Diffie-Hellman quadruples.

Gap Diffie-Hellman Groups (GDH): GDH are examples of gap problems presented in [71]. There are many subgroups of group Z^*_q that have prime orders, and both the CDH and DDH assumptions are believed to be held over these groups. The subgroup G with the prime order p is one of these. However, on certain elliptic-curve groups, the DDH problem is easy to solve, whereas CDH is believed to be hard [68]. Such groups are named Gap Diffie-Hellman (GDH) groups. Hence, if G belongs to these specific elliptic-curve groups, we call it a Gap Diffie-Hellman group.

C. Bilinear Maps

Bilinear groups. Until now, there is no known implementable example of GDH groups except bilinear maps. A bilinear group is any group that possesses such a map e, and on which CDH is hard.

Bilinear maps. Assume that G is an additive group and G_T is a multiplicative group such that $|G| = |G_T| = |p|$, where p is a prime number. P is the generator of G.

Then, the map $e : G \times G \rightarrow G_T$ is a computable bilinear map if it satisfies:

1) Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G$.
2) Bilinearity: for all $P, Q \in G$ and $a, b \in Z$, we have $e(aP, bQ) = e(P, Q)^{ab}$.
3) Non-Degeneracy: $e(P, P) \neq 1$. In other words, if P is a generator of G, then $e(P, P)$ generates G_T.

Bilinear Diffie-Hellman Problem. The group G is a subgroup of the additive group of points of an elliptic curve $E(F_q)$. The group G_T is a subgroup of the multiplicative group of finite field F^*_q and $|G| = |G_T| = |p|$, where p is a prime number.

Let $e : G \times G \rightarrow G_T$ be a bilinear pairing on (G, G_T). The bilinear Diffie-Hellman problem (BDHP) is the following: Given P, aP, bP, cP, compute $e(P, P)^{abc}$.

Typically, the mapping $e : G \times G \rightarrow G_T$ will be derived from either the Weil or the Tate pairing on an elliptic curve over a finite field. More comprehensive details on GDH groups, bilinear pairings, and other parameters are defined in [42-46].

IV. PROPOSED IDENTITY-BASED SIGNCRYPTION PROTOCOL

Signcryption techniques are intended to simultaneously accomplish confidentiality, authentication and non-repudiation to reduce communication and computation overheads. In this section, we propose an identity-based signcryption protocol to reduce the computation, communication, and implementation overheads in evidence colleting in cloud forensics. The

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

proposed protocol is more efficient than all the previously presented protocol. It allows the recipient (verifier) to restore the message blocks upon receiving their corresponding signature blocks. The proposed protocol is perfect for some application requirements and it fits packet switched networks. In the proposed protocol, we construct two stages of verification to ensure that the message has been recovered efficiently and correctly. The first verification step is to ensure the integrity and authenticity of the message (e.g., no modification or substation in the ciphertext r_i). The second verification step is to ensure that the message M_i is reconstructed successfully. This stage is useful for public verification in the case of a dispute takes place. It guarantees that the proposed protocol satisfies the non-repudiation property. In order to perform the proposed protocol, the following parameters must be set.

Setup: The Private Key Generation center (PKG) chooses a *Gap Diffie-Hellman* group G_1 of prime order q, a multiplicative group G_2 of the same order, and a bilinear map $e : G_1 \times G_1 \rightarrow G_2$, together with an arbitrary generator $P \in G_1$. Then it chooses a random value $s \in Z_q^*$ as the master secret key and computes the corresponding public key $P_{pub} = sP$. H_1 and H_2 are two secure cryptographic hash functions, such that $H_1 : 0, 1^* \rightarrow G_1$ and $H_2 : 0, 1^* \rightarrow Z_q^*$. The system parameters (G_1, G_2, P, P_{pub}, H_1, H_2, e, q) and the master secret key is s.

KeyExtract: Given identity ID, PKG computes $S_{ID} = sH_1(ID)$ and sends it to the user with identity ID. We define Q_{ID} as the public key of the user with identity ID. We assume that the sender is A with identity ID_A. The sender A has public key $Q_A = H_1 (ID_A)$ and secret key $S_A = sQ_A$. The recipient, B, has identity ID_A. The recipient B has public key $Q_B = H_1 (ID_B)$ and secret key $S_B = sQ_B$.

When a sender A wants to send a message M to the recipient B, it divides the stream into blocks, M_i, where $M_i \in Z_q^*$.

SignCrypt: The sender A, with secret key S_A and public key Q_A, uses the following steps before sending the signcrypted message. The sender A chooses a random number $k \in Z_q^*$ and lets $r_0 = 0$. Then, A calculates:

(1) $r_i = M_i \cdot H_2 (r_{i-1} \oplus e (P, Q_B)^k)$, for $i = 1, 2, 3, \ldots, n$

(2) $\alpha = H_2 (r_1, \ldots , r_n , e (P, Q_B)^k)$

(3) $\beta = H_2 (M_1, \ldots , M_n , \alpha, e (P, P)^k)$

(4) $\gamma = \beta \cdot P$

(5) $\theta = \beta \cdot Q_B$

(6) $S = \beta^{-1} \cdot k \cdot P - \beta^{-1} \cdot S_A$

The sender, A, sends (S, α, γ, θ, r_1, … , r_n) to B over a non-secure channel.

Un-SignCrypt: The recipient, B:

(1) Verifies: $\alpha \stackrel{?}{=} H_2 (r_1, \ldots , r_n , e (S, \theta) \cdot e (S_B, Q_A))$

(2) Recovers M:

$$M_i = r_i \cdot [H_2 \ (r_{i-1} \oplus [e (S, \theta) \cdot e (S_B, Q_A)])]^{(-1)}$$

(3) Checks :

(3) $\gamma \stackrel{?}{=} H_2\big(M_1, \ldots, M_n, \ \alpha, \ e (S, \ \gamma) \ \cdot \ e \left(P_{pub}, Q_A\right) \big) \cdot P$

After receiving the sent message, the recipient checks the signature by comparing α to $M_i \cdot H_2 (r_{i-1} \oplus e (P, Q_B)^k)$. If the check doesn't hold, this indicates that the received packets are modified and must be discarded. On the other hand, if the check holds, then the recipient recovers message blocks $M_i = r_i \cdot [H_2 \ (r_{i-1} \oplus [e (S, \theta) \cdot e (S_B, Q_A)])]^{(-1)}$. Finally, the recipient checks if the message blocks have been reconstructed correctly by comparing γ to $H_2(M_1, \ldots, M_n , \alpha, e(S, \gamma) \cdot e(P_{pub}, Q_A)) \cdot P$. For Public verification, the recipient B just needs to reveal (M, S, α, γ, θ). Then, any verifier can check whether (S, γ) is the sender A's signcrypted message by comparing γ to $H_2(M_1, \ldots, M_n , \alpha, e(S, \gamma) \cdot e(P_{pub}, Q_A)) \cdot P$. This equation links the message M, A's public key Q_A, and the signcrypt quadruple (S, α, γ, θ) together. If the equation holds, the recipient (verifier), B, concludes that (S, γ) is a valid signcrypt for the message M by the sender (signer), A. The proposed protocol provides both confidentiality and authenticity simultaneously. Therefore, the computation overhead decreases, this makes the proposed protocol appropriate for big data applications. To decrease the communication overhead, which is considered one of the major disadvantages of using signcryption techniques, we use bilinear pairings and identity-based cryptography. Bilinear parings and Elliptic Curve Cryptography (ECC) use smaller key size than RSA cryptosystems for the same level of security. Moreover, identity-based cryptography solves the centralization problem in the PKI that needs continuous updates for the revocation list in PKI. Furthermore, the proposed protocol eliminates the need to encrypt the message using each recipient's public key and as a result, lowers the communication overhead. Other advantage of the proposed protocol is that it could resist both packet loss and pollution attacks with low computation and communication overheads. It allows the recipient (verifier) to recover the message blocks upon receiving their corresponding signature blocks. The scheme is perfect for some application requirements and it is designed for packet switched networks. In the next section, the security analysis of the proposed protocol is detailed.

V. SECURITY ANALYSIS

The security of the proposed protocol is based on the intractability of reversing the secure cryptographic hash function and the Elliptic Curve Discrete Logarithm (ECDL)

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

problem. We analyze the security of the proposed protocol as follows:

***Correctness*:**

$$e(S,\theta) = e(\beta^{-1} \cdot k \cdot P - \beta^{-1} \cdot S_A,\ \beta \cdot Q_B)$$
$$= e(kP, Q_B) \cdot e(S_A, Q_B)^{-1}$$
$$= e(P, Q_B)^k \cdot e(S_A, Q_B)^{-1}$$

Then,

$$e(P, Q_B)^k = e(S,\theta) \cdot e(S_A, Q_B)$$

But,

$$e(S_A, Q_B) = e(sQ_A, Q_B) = e(Q_A, sQ_B) = e(Q_A, S_B)$$

Then,

$$e(P, Q_B)^k = e(S,\theta) \cdot e(S_B, Q_A)$$

This means that the receiver, B, can calculate α as follows:

$$\alpha = H_2\ (r_1, \dots, r_n,\ e(P, Q_B)^k)$$
$$= H_2\ (r_1, \dots, r_n, e\ (S,\theta) \cdot e\ (S_B, Q_A))$$

Also,

$$e(S,\gamma) = e(\beta^{-1} \cdot k \cdot P - \beta^{-1} \cdot S_A,\ \beta \cdot P)$$
$$= e(kP, P) \cdot e(S_A, P)^{-1}$$
$$= e(P, P)^k \cdot e(Q_A, P_{pub})^{-1}$$

Then,

$$e(P,\ P)^k = e(S,\gamma) \cdot e(Q_A, P_{pub})$$

This means that the receiver, B, can calculate γ as follows:

$$\gamma = H_2(M_1, \dots, M_n, \alpha, e(P, P)^k) \cdot P$$
$$= H_2\big(M_1, \dots, M_n, \alpha, e\ (S,\gamma) \cdot e\big(Q_A, P_{pub}\big)\big) \cdot P$$

Given that the sender, A, generates (using the SignCrypt algorithm) and sends the signcrypted blocks and signature to B. The receiver, B, can recover the message M correctly using the Un-SignCrypt algorithm in the proposed protocol.

***Authenticity/Unforgeability*:**

The proposed protocol generates (S, α, γ, θ, r_1, … , r_n) and β. The sender A keeps β and sends (S, α, γ, θ, r_1, … , r_n) to the recipient B where $\gamma = \beta \cdot P$. Any adversary, who aims to get β from γ, has to solve the Elliptic Curve Discrete Logarithm problem. Therefore, neither the recipient B nor any other adversary can forge the valid signcrypted blocks (S, α, γ, θ, r_1, … , r_n) for any message M in a way that satisfies the verification of the Un-SignCrypt algorithm. The recipient B cannot forge (M, S, α, γ, θ) for a verifier such that (M, S, α, γ, θ) satisfies $\gamma = H_2\big(M_1, \dots, M_n, \alpha, e\ (S,\gamma) \cdot e\big(Q_A, P_{pub}\big)\big) \cdot P$. This is due the fact that γ appears as exponent and discrete logarithm (over elliptic curve), at the same time. Furthermore, the exponent is a cryptographic hash function that has γ as input. Thus, the attacker has to break both the cryptographic hash function and the discrete logarithm problem over elliptic curve. The attacker must get the sender (signer) S_A' secrete key. Only the sender knows this secrete key.

***Confidentiality*:**

The attacker must get $e(P, Q_B)^k$ to recover the message M from the signcrypt quadruple and signcrypted blocks (S, α, γ, θ, r_1, … , r_n). In the proposed protocol, k is a random number the kept secret by the sender and $e(P, Q_B)^k$ is a random value that is unknown to the attacker. Without the recipient B' secrete key, the attacker cannot calculate$e(P, Q_B)^k$. Thus the proposed protocol preserves the confidentiality property.

***Forward Secrecy*:**

The proposed protocol makes use of the identity-based cryptography. So, certificate revocation lists (CRLs) problems do not exist in the proposed protocol. Hence, there is no need to reveal the secrete key of the sender (singer/encryptor). Therefore, there is no forward secrecy problem in the proposed protocol.

***Non-repudiation*:**

In the case of a dispute takes place between the sender and the recipient over signcrypted blocks, a trusted third party can ask the recipient B to reveal (M, S, α, γ, θ). Then, the trusted third party can check whether signcrypted blocks (S, α, γ, θ, r_1, … , r_n) is generated by the sender A by comparing γ to $H_2(M_1, \dots, M_n, \alpha, e(S,\gamma) \cdot e(P_{pub}, Q_A)) \cdot P$. This equation links the message M, A's public key Q_A, and the signcrypt quadruple (S, α, γ, θ) together. If the equation holds, the trusted third party concludes that (S, γ) is a valid signcrypt for the message M by the sender (signer), A, to the recipient (verifier), B. Thus, the non-repudiation property is accomplished in the proposed protocol.

VI. LOGICAL ANALYSIS OF PROPOSED PROTOCOL USING BAN LOGIC

Authentication protocols are the basis of security in many distributed systems, and it is therefore essential to ensure that these protocols function correctly. Unfortunately, their design has been extremely error prone. Most of the protocols found in the literature contain redundancies or security flaws [72]. In [72], M. Burrows *et. al* proposed a method that uses the logic to describe the authentication protocols. They transformed each message into a logical formula which is an idealized version of the original message. In this section, a logical analysis of the proposed protocol using BAN logic is presented. For a successful verification of the protocol, the belief state of communicating parties should

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

satisfy the protocol goals. We will consider the proposed protocol is completed between principals A and B, if there is a data packet "X" which the recipient B believes that it is sent by the sender (signer), A. Thus, authentication between A and B will be completed if $B \mid\equiv A \mid\equiv$ X, and $B \mid\equiv$ X, where the symbol $\mid\equiv$ means believes. First, the basic rules of the BAN logic are listed below:

- The interpretation rule

$$\frac{B \mid\equiv (A \mid\sim (X,Y))}{B \mid\equiv (A \mid\sim X), B \mid\equiv (A \mid\sim Y)}$$

The above rule means that if B believes that A once said a message containing both X and Y, therefore it believes that A once said each statement separately.

- Message Meaning Rule

$$\frac{B \equiv \xrightarrow{Q_A} A, B \lhd [X]_{S_A}}{B \mid\equiv A \mid\sim X}, A \neq B$$

This means that if B believes that Q_A is the public key of A, and B sees a message X signed by S_A, this implies that B believes that A once said X.

- Nonce Verification Rule

$$\frac{B \mid\equiv \#(X), B \mid\equiv A \sim X}{B \mid\equiv A \mid\equiv X}$$

The above rule means that if B believes that X is a recent message and A once said X, therefore it believes that A believes in X.

- Jurisdiction Rule

$$\frac{B \mid\equiv A \Rightarrow X, B \mid\equiv A \mid\equiv X}{B \mid\equiv X}$$

This rule means that if B believes that A has jurisdiction over X, and B believes that A believes in X, then B believes in X.

- Freshness Rule

$$\frac{B \mid\equiv \#(X)}{B \mid\equiv \#(X,Y)}$$

The above rule means that if B believes in the freshness of X and Y, therefore it believes in the freshness of each statement separately. The analysis is undertaken for the message exchanged between the sender, A, and recipient, B. The authentication is considered completed between A and B, if the following goals are achieved:

Goal 1: $B \mid\equiv A \mid\equiv r_i$

Goal 2: $B \mid\equiv r_i$

Where, r_i represents the block sent by A. In order to complete the analysis, the following assumptions are made:

$$B \mid\equiv \xrightarrow{Q_A} A \quad (1)$$

$$B \mid\equiv A \Rightarrow r_i \quad (2)$$

$$B \mid\equiv \#\gamma \quad (3)$$

Equation (1) indicates that B believes that Q_A is the public key of A. Then, equation (2) indicates that both B believes that A has jurisdiction over the block sent. Finally, equation (3) indicates that B believes in the freshness of γ (since it is changed for each message). After making the assumptions, the messages transferred in the initial phase are transformed into logical formulas. Finally, the basic rules of the BAN logic will be applied to the logical formulas. Following is the transformation of the proposed protocol into logical formulas:

$$A \longrightarrow B: \{\{r_i\}_{S_A}, \gamma, \alpha, \theta\} \quad (4)$$

The analysis of the protocol can now be performed. By applying message meaning rule to equation (4) and using equation (1), the following can be deduced:

$$B \mid\equiv A \mid\sim (r_i, \gamma)$$

But, B believes in the freshness of γ (equation (3)). Thus, applying nonce verification rule, the following is obtained:

$$B \mid\equiv A \mid\equiv r_i \quad (5)$$

Then, by applying jurisdiction rule using equation (2), the following is obtained:

$$B \mid\equiv r_i \quad (6)$$

From equations (5) and (6), one can deduce that the proposed protocol achieves the goals of authentication without bugs or redundancies.

VII. CONCLUSIONS

As the need for cloud forensics security arises, the need to reduce the execution time and computation overhead associated with the execution of cryptographic protocols increases. In this paper, we propose an identity-based signcryption protocol to reduce the computation, communication, and implementation overheads in evidence colleting in cloud forensics. Signcryption protocols have the

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

advantage of achieving the basic goals of encryption and signature protocols in more efficient way than Sign-Encrypt-Sign and Encrypt-Sign-Encrypt techniques. At the same time, the proposed protocol does not require the verifier/recipient to process the signcrypted packets in sequence. The aim of the proposed protocol is to ensure confidentiality, authenticity and chain of custody for the digital forensics process in the cloud in an efficient way. Signcryption protocols allow the confidential and authentic delivery of evidences to digital forensic examiners in the cloud computing environment. As such, it is a very interesting mechanism for digital forensics applications that deliver streamed big data content over insecure channels. Utilizing signcryption techniques lowers the communication and computation overheads. But, due to the fact that some digital evidences have huge volume of data and need to be transmitted over the cloud securely, special signcryption protocols that consider the digital forensics requirements in the cloud is needed. The proposed protocol allows the sender to divide the transmitted data into blocks to overcome the big data problem in cloud evidence acquisition. The proposed signcryption protocol is based on bilinear pairings and utilizes the identity-based cryptography. Protocols that make use of bilinear parings use cryptographic keys with key-length less than other protocol that do not implement bilinear pairings. Less key-length means less storage, computation, and implementation overheads. Identity-based cryptography provides the proposed protocol with less communication overhead advantage over protocols that rely on PKI. As a result, the proposed protocol has a simpler structure and easier in implementation than non-signcryption techniques. In addition, the proposed protocol is analyzed using security analysis and BAN logic to ensure that it achieves the goals of encryption and digital signature. The analysis shows that it achieves those goals without bugs or redundancies.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, 2010, pp. 7-18.

[2] S.P. Abirami and R. Shalini, "Linear Scheduling Strategy for Resource allocation in Cloud Environment," International Journal on Cloud Computing and Architecture, vol. 2, no. 2, 2012, pp. 9-17.

[3] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy,vol.9, no.2, 2011, pp. 50-57.

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, 2011, Special Publication 800-145.

[5] M.A. Caloyannides, N. Memon, and W. Venema, "Digital Forensics," IEEE Security & Privacy, vol. 7, no. 2, 2009, pp. 16-17.

[6] S. Hou, T. Uehara, S.M. Yiu, L.C.K. Hui, and K.P. Chow, "Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers," Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, pp. 378-383.

[7] S. Hou, T. Uehara, S.M. Yiu, L.C.K. Hui, and K.P. Chow, "Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics," Third International Conference on Multimedia Information Networking and Security, 2011, pp. 595-599.

[8] S. Hou1, R. Sasaki, T. Uehara, and S. Yiu, "Verifying Data Authenticity and Integrity in Server-Aided Confidential Forensic Investigation," Lecture Notes in Computer Science 7804, Springer, 2013, pp. 312-317.

[9] M. Nasreldin, M. El-Hennawy, H. Aslan, and A. El-Hennawy, "Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing," International Journal of Computer Science Issues, vol. 12, issue 1, no. 1, 2015, pp. 153-160.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST, 2006, Special Publication 800-86.

[11] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, Elsevier, vol. 7, 2010, pp. S64-S73.

[12] E. Casey, "Handbook of Digital Forensics and Investigation," Academic Press, 2009.

[13] B.D. Carrier, "Basic Digital Forensics Investigation Concepts," http://www.digital-evidence.org/di_basics.html, 2006.

[14] N. Beebe, "Digital Forensic Research: The Good, the Bad and the Unaddressed," IFIP Advances in Information and Communication Technology, 2009, vol. 306, Springer, pp. 17-36.

[15] B. Martini and K.-K. Choo, "Cloud storage forensics: ownCloud as a case study, Digital Investigation," vol. 10, no. 4, 2013, pp. 287-299.

[16] K. Ruan, "Cybercrime and Cloud Forensics: Applications for Investigation Processes," Information Science Reference, 2013.

[17] A. Saxena, G. Shrivastava, and K. Sharma, "Forensic Investigation in Cloud Computing Environment," The International Journal of Forensic computer Science, vol. 2, 2012, pp. 64-74

[18] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," In proceedings of the 7th IFIP International Conference on Digital Forensics, 2011, pp.16-25.

[19] R. Adams, "The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice," Murdoch University, 2013.

[20] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011, pp. 1-10.

[21] J. Vacca, "Computer forensics: computer crime scene investigation," Delmar Thomson Learning, 2005.

[22] M. Sudha and M. Monica, "Enhanced security framework to ensure data security in cloud computing using cryptography," Advances in Computer Science and its Applications, vol. 1, no. 1, 2012, pp. 32-37.

[23] K. W. Nafi, T. S. Kar, S. A. Hoque and M. M. A. Hashem, "A newer user authentication, file encryption and distributed server based cloud computing security architecture," International Journal of Advanced Computer Science and Applications, vol. 3, no. 10, 2012, pp. 181-186.

[24] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information Processing Letters, vol. 68, Elsevier Inc., 1998, pp. 227-233.

[25] C.P. Schnorr, "Efficient identification and signatures for smart cards," Advances in Cryptology - Crypto '89, Springer-Verlag, 1990, Lecture Notes in Computer Science, nr 435, pp. 239-252.

[26] M. Rasslan and H. Aslan, "On the Security of Two Improved Authenticated Encryption Schemes," International Journal of Security and Networks, vol. 8, no. 4, 2013, pp. 194-199.

[27] G. El-Kabbany, H. Aslan, and M. Rasslan, "An Efficient Pipelined Technique for Signcryption Algorithms," International Journal of Computer Science Issues, vol. 11, issue 1, no. 1, 2014, pp. 67-78.

[28] T.-Y. Wu, T.-T. Tsai and Y.-M. Tseng "A Revocable ID-based Signcryption Scheme", Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212, vol. 3, no. 3, 2012, pp. 240-251.

[29] D.R.L. Brown, "Deniable authentication with RSA and multicasting," Cryptology ePrint Archive, http://eprint.iacr.org/2005/056.pdf, Feb 2005.

[30] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Information Theory, vol. it-22, 1976, pp. 472-492.

[31] L. Kohnfelder, "On the siganture reblocking problem in public key cryptosystems," Communications of ACM, vol.31, no.19, 1995, pp.1656-1657.

[32] K. Nyberg and R. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," Designs, Codes and Cryptography, vol. 7, no. 1-2, 1996, pp. 61-81.

[33] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of ACM, vol.21, no.2, 1978, pp.120-126.

[34] Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," Proc. of CRYPTO'97, LNCS 1294, Springer-Verlag, 1997, pp. 165-179.

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

[35] C.-K. Li and D.-S. Wong, "Signcryption from randomness recoverable public key encryption," Inform. Sci., vol. 180, Elsevier Science, 2010, pp.549-559.
[36] W. He and T. Wu, "Cryptanalysis and improvement of Petersen-Michels signcryption schemes," IEE Computers and Digital Communications, vol. 146, no. 2, 1999, pp. 123-124.
[37] H. Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes," IEE Computers and Digital Communications, vol. 145, no. 2, 1998, pp. 149-151.
[38] Y. Zheng and H. Imai, "Efficient signcryption schemes on elliptic curves," Inform. Process Lett., vol. 68, no. 5, Elsevier Science, 1998, pp. 227-233.
[39] J.-H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," Proc. of EUROCRYPT'02, LNCS 2332, Springer-Verlag, 2002, pp. 83-107.
[40] H. Krawczyk and T. Rabin, "Chameleon signatures," Proc. of NDSS 2000, 2000, pp. 143-154.
[41] J.-B. Shin, K. Lee, and K. Shim, "New DSA-verifiable signcryption schemes," Proc. Of ICISC'02, LNCS 2587, Springer-Verlag, 2002, pp. 35-47.
[42] J. Zhang and J. Mao, "A novel ID-based designated verifier signature scheme," Inform. Sci., vol. 178, no. 3, Elsevier Science, 2008, pp. 766-773.
[43] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," Proc. of EUROCRYPT'03, LNCS 2656, Springer-Verlag, 2003, pp. 416-432.
[44] M. Rasslan, "A stamped hidden-signature scheme utilizing the elliptic curve discrete logarithm problem," Int. J. Network Security, vol. 12, no. 3, 2011, , pp. 250-258.
[45] M. Rasslan and A. Youssef,"Cryptanalysis of Hwang-Lo-Hsiao-Chu authenticated encryption schemes", IEICE Trans. Inform. and Syst., vol. e93-d, no. 5, 2010, pp. 1301-1032.
[46] M. Rasslan and A. Youssef, "A bilinear pairing based hidden-signature scheme," Communications in Computer and Information Science, vol. 84, no. 3, Springer-Verlag, 2010, pp. 389-397.
[47] M. Rasslan and A. Youssef, "Comments on the security of Chen's authenticated encryption scheme," Computers and Electrical Engineering, vol. 37, no. 1, Elsevier Science, 2011, pp. 71-75.
[48] M. Rasslan and A. Youssef, "Cryptanalysis of a public key encryption scheme using ergodic matrices," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. e94-a, no. 2, 2011, pp. 853-854.
[49] M. Rasslan and M. Nasreldin, "Identification Protocols Based on Discrete Log Representation Problem," Procedia Computer Sciences, vol. 21, Elsevier Science, 2013, pp. 368-373.
[50] M. Rasslan, "Cryptanalysis of an identity-based strong designated verifier signature scheme," Lecture Notes in Electrical Engineering, vol. 164, no. 1, Springer-Verlag, 2012, pp. 359-365.
[51] C. Adams and S. Lloyd, Understanding PKI: Concepts, Standers, and Deployment considerations, Second Edition. Addison-Wesley, 2002.
[52] A. Shamir, "ID-based cryptosystems and signature schemes," Proc. of CRYPTO'84, LNCS 196, Springer-Verlag, 1985, pp. 47-53.
[53] Y. Desmedt and J. Quisquater, "Public-key systems based on the difficulty of tampering," Proc. of CRYPTO'86, LNCS 263, Springer-Verlag, 1986, pp. 111-117.
[54] U. Maurer and Y. Yacobi, "Non-interactive public-key cryptography," Proc. Of CRYPTO'91, LNCS 547, Springer-Verlag, 1991, pp. 498-507.
[55] D. Huhnlein, M. Jacobson, and D. Weber, "Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders,"Proc. of SAC 2000, LNCS 2012, Springer-Verlag, 2000, pp. 275-287.
[56] S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," IEEE Journal on Selected Areas in Communication, vol. 7, no. 4, Springer-Verlag. 1989, pp. 467-473.
[57] H. Tanaka, "A realization scheme for the identity-based cryptosystem," Proc. Of CRYPTO'87, LNCS 293, Springer-Verlag, 1987, pp. 341-349.
[58] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. Of CRYPTO'01, LNCS 2139, Springer-Verlag, 2001, pp. 213-229.
[59] C. Cocks, "An identity based encryption scheme based on quadratic residues," Proc. Of Cryptography and Coding, LNCS 2260, Springer-Verlag, 2001, pp. 360-363.
[60] J.-C. Cha and J.-H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," Proc. of PKC'03, LNCS 2567, Springer-Verlag, 2003, pp. 18-30.
[61] N. P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," Electronics Lett., vol. 38, 2002, pp. 630-632.
[62] F. Heb, "Efficient identity based signature schemes based on pairings," Proc. of SAC 2002, LNCS 2595, Springer-Verlag, 2003, pp. 310-324.
[63] P. Barreto, "The pairing based crypto lounge," Available at http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html
[64] M. Joye and G. Neven, Cryptology and Information Security Series on Identity-Based Cryptography, IS Press, Dec 2008.
[65] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil airing," Proc. of ASIACRYPT'01, LNCS 2248, Springer-Verlag, 2001, pp. 514-532.
[66] F. Bao, R. Deng, and H. Zhu, "Variations of Diffie-Hellman problem," Proc. of Information and Communications Security, LNCS 2836, Springer-Verlag, 2003, pp. 301-312.
[67] M.-S. Hwang, J.-Y. Hsiao, and Y.-P. Chu, "Improvement of authenticated encryption schemes with message linkages for message flows," IEICE Trans. Inform. and Syst., vol. e89-d, no. 4, 2006, pp. 1575-1577.
[68] Z. Zhang, S. Araki, and G. Xiao, "Improvement of authenticated encryption schemes with message linkages for message flows," Applied Mathematics and Computation, vol. 162, no. 3, Elsevier Science, 2005, pp. 1475-1483.
[69] B.-H. Chen, "Improvement of authenticated encryption schemes with message linkages for message flows," Computer and Electrical Engineering, vol. 30, Elsevier Science, 2004, pp. 465-469.
[70] Y.-M. Tseng, J.-K. Jan, and H.-Y. Chien, "Authenticated encryption schemes with message linkages for message flows," Computers and Electrical Engineering, vol. 29, no. 1, Elsevier Science, 2003, pp. 101-109.
[71] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," Proc. of ACISP'04, LNCS 3108, Springer-Verlag, 2004, pp. 313-324.
[72] L. Kohnfelder, "On the siganture reblocking problem in public key cryptosystems," Communications of ACM, vol.31, no.19, 1995, pp.1656-1657.

AUTHORS PROFILE

Mahmoud M. Nasreldin is a Ph.D. student at the Electronics and Telecommunication Department in Ain Shams University, Cairo, Egypt. He received his B.Sc. degree in Electronics and Telecommunications Engineering from the Faculty of Engineering, Cairo University, Egypt.

Magdy El-Hennawy is a Computer Science & Information Technology Professor at Shorouk Academy, Cairo, Egypt. He received his B.Sc. degree from the Faculty of Engineering, Ain Shames University, Cairo, Egypt. He obtained his Master degree in Performance Evaluation of Security and Integrity Measures for Database Systems from the same Faculty, as well as, his Ph.D. degree in Cryptographic Engineering for Securing Information Exchanged over the Internet. During his professional career, he was a senior engineer, deputy manager, and the manager of an Information System Centre, that is specialized in building, rolling out, operating, supporting and maintaining distributed systems over geographically distributed locations.

Heba K. Aslan is a Professor at Electronics Research Institute, Cairo-Egypt. She received her B.Sc. degree, M.Sc. degree and Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering, Cairo University, Egypt in 1990, 1994 and 1998 respectively. Aslan has supervised several masters and Ph.D. students in the field of computer networks security. Her research interests include: Key Distribution Protocols, Authentication Protocols, Logical Analysis of Protocols and Intrusion Detection Systems.

Adel El-Hennawy is a Telecommunication and Electronics Engineering Professor at Ain Shams University, Cairo, Egypt.

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

TECHNICAL SOLUTIONS TO RESOURCES ALLOCATION FOR DISTRIBUTED VIRTUAL MACHINE SYSTEMS

Ha Huy Cuong Nguyen
Departmentof
InformationTechnology,
Quangnam University
Quang Nam, Viet Nam

Van Thuan Dang
Departmentof
InformationTechnology,
Industrial University of HCM City
Quang Ngai, Viet Nam

Van Son Le
Departmentof
InformationTechnology,
Danang University of Education
The university of Danang
Da Nang, Viet Nam

***Abstract*— Virtual machine is built on group of real servers which are scattered globally and connect together through the telecommunications systems, it has an increasingly important role in the operation, providing the ability to exploit virtual resources. The latest technique helps to use computing resources more effectively and has many benefits, such as cost reduction of power, cooling and, hence, contributes to the Green Computing. To ensure the supply of these resources to demand processes correctly and promptly, avoiding any duplication or conflict, especially remote resources, it is necessary to study and propose a reliable solution appropricate to be the foundation for internal control systems in the cloud. In the scope of this paper, we find a way to produce efficient distributed resources which emphasizes solutions preventing deadlock and proposing methods to avoid resource shortage issue. With this approach, the outcome result is the checklist of resources state which has the possibility of deadlock and lack of resources, by sending messages to the servers, the server would know the situation and have corresponding reaction.**

Keywords— Virtual machine, best-effort, lease, deadlock detection, distributed environments, virtual resources.

I. INTRODUCTION

In the early 1980s, Cloud Computing (Clouds) has changed from large computer models to client - server model. Details infrastructure is abstracted from the users, they do not need to know about IT infrastructure and resources are easily accessible in the cloud. Client use of cloud computing applications while computing resources or data placed in the cloud environment. Most cloud computing infrastructure consists of services delivered through data centers and built on the virtual machine. Cloud computing resources are often a single points of access to all cloud computing servers. At the moment, the Internet retains its traditional role as a means of communication and at the same time, it is also a means to share resources. The current trend shows the need to build more flexibility infrastructure in scalability, resilience of security and network congestion. Virtualization technology provides the abstract and isolates the lower level functions, allowing greater mobility and gathering physical resources [2].

These problems have prompted researchers, expertist in the field of computer science looking for better solutions to meet capacity requirements of information technology service from users. In this article, we present solutions to virtual machine model which needs to provide information resources, preventing deadlock in resources supply. Deadlock problems in resources supply on distributed platforms has always been an interest of advanced researchers. However, there are still many things to do with the challenge of future trends.

In the past, grid computing and batch scheduling have both been commonly used for large scale computation. Cloud computing presents a different resource allocation paradigm than either grids or batch schedulers [4,5]. In particular, Amazon C2 [10], is equipped to, handle may smaller computer resource allocations, rather than a few, large request as is normally the case with grid computing. The introduction of heterogeneity allows clouds to be competitive with traditional distributed computing systems, which often consist of various types of architecture as well. In a heterogeneous cloud environment. Recently, reports have appeared many of the studies provide cloud computing resources, the majority of this research to deal with variability in resource capacity for infrastructure and application performance in the cloud. In this paper, we develop a method to predict the lease completion time distribution that is applicable to making a sophisticated trade off decisions in resource allocation and scheduling. Our evaluation shows that these methods deadlock detection using algorithm two ways search can improve efficiency and effectiveness of the cloud computing allocation resource heterogeneous systems.

The work is organized in the following way: in section 2, we introduce the related works; in section 3, we introduce existing models; in section 4, we present solutions in resource allocation heterogeneous distributed vitual machine, in section 5, we present the results from our assessment in section 6, we present our conclusions and suggestions for future work.

II. RELATED WORKS

Large distributed system [6.10] using the virtualization technology to enable the creation of dynamic range of virtual resources which can meet the computing needs of users with specific applications, grid computing.

Resource allocation in cloud computing has attracted the attention of the research community over last few years. Srikantaiah et al. [8] studied the problem of request scheduling for multi-tiered web applications in virtualized heterogeneous systems in order to minimize energy consumption

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

while meeting performance requirements. They proposed a heuristic for a multidimensional packing problem as an algorithm for workload consolidation. Garg et al. [10] proposed near optimal scheduling policies that consider a number of energy efficiency factors, which changes across different data centers depending on their location, architectural design, and management system. Warneke et al. [11] discussed the challenges and opportunities for efficient parallel data processing in cloud environment and presented a data processing framework to exploit the dynamic resource provisioning offered by IaaS clouds. Wu et al. [12] proposed a resource allocation for SaaS providers who want to minimize infrastructure cost and SLA violations. Addis et al. [13] proposed resource allocation policies for the management of multi-tier virtualized cloud systems with the aim to maximize the profits associated with multiple class SLAs. A heuristic solution based on a local search that also provides availability, guarantees that running applications has been developed.

Distributed intelligent model has been proposed to support for large complex distributed systems with smart algorithms. The concept of distributed intelligence model aims to provide information resources based on middleware components which can meet the growing and challenging request from customer that they do not necessarily have to change the system.

The trend in building virtual machine network model in order to manage resources effectively include the following useful purposes:

- The hardware resources in distributed system consists of separate compute nodes connected together via communications networks. At each node, resources include CPU, memory, disk, network, computers, clusters, grids. The special thing is, it cannot communicate directly to the resources of other nodes at this node. The physical architecture components can be the same or different ... These buttons can be distributed on any geographical surface and in separate governance areas, management by the resource management system.
- For resources information including system of programs and data, a vital key requirement of the system is to ensure the coherence of data in multiple host systems.

The process of resource providing under virtualization mechanism is illustrated in Figure 1. Grouping the cloud computing service providers activate based on the need for additional resources and the need for collaboration which has been explained in the basic functions of the cloud computing architecture, and in the structure of the cloud.

Multi-agent system in resources providing based on virtualization mechanism

III. SYSTEM MODEL RESOURCE ALLOCATION IN HETEROGENEOUS DISTRIBUTED PLATFORMS

Resource allocation in cloud computing has attracted the attention of the research community in the last few years. Cloud computing presents a different resource allocation paradigm than either grids or batch schedulers[2]. In particular, Amazon C2 [10], is equipped to, handle may smaller computer resource allocations, rather than a few, large request as is normally the case with grid computing. The introduction of heterogeneity allows clouds to be competitive with traditional distributed computing systems, which often consist of various types of architecture as well.

Like traditional distributed system before we can see a heterogeneous distributed system consists of a set of processes that are connected by a communication network. The communication delay is finite but unpredictable [21,22].

A. The application

A heterogeneous distributed program is composed of a set of n asynchronous processes $p_1, p_2,\ldots,p_n$ that communicates by message passing over the communication network. We assume that each process is running on a different processor. The processor does not share a common global memory and communicate solely by passing messages over the communication network. There is no physical global clock in the system to which processes have instaneous access. The communication medium may deliver messages out of order, messages may be lost garble or duplicated due to timeout and retransmission, processors may fail and communication links may go down. The system can be modeled as a directed graph in which vertices represent the processes and edge represent unidirectional communication channels.

Example 1 Resource allocation on heterogeneous distributed platforms

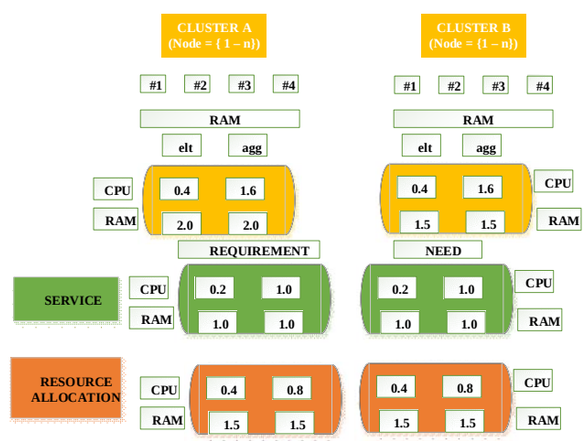


Figure 1. Example problem instance with two nodes and one service, showing possible resource allocations.

Figure 1 illustrates an example with two nodes and one service. Node A, B are comprised of 4 cores and a large memory. Its resource capacity vectors show that each core has elementary capacity 0.8 for an aggregate capacity of 3.2. Its memory has a capacity of 1.0, with no difference between elementary and aggregate values because the memory, unlike cores, can be partitioned arbitrarily. No single virtual CPU can run at the 0.9 CPU capacity on this node. The figure shows two resource allocations one on each node. On both nodes, the service can be allocated for memory it requires.

Informally speaking, a deadlock is a system state where requests are waiting for resources held by other requesters

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

which, in turn, are also waiting for some resources held by the previous requests. In this paper, we only consider the case where requests are processors on virtual machine resource allocation on heterogeneous distributed platforms. A deadlock situation results in permanently blocking a set of processors from doing any useful work.
There are four necessary conditions which allow a system to deadlock[3]: (a) Non – Preemptive: resources can only be released by the holding processor; (b) Mutual Exclusion: resources can only be accessed by one processor at a time; (c) Blocked Waiting: a processor is blocked until the resource becomes available; and (d) Hold – and – Wait: a processor is using resources and making new requests for other resources that the same time, without releasing held resources until some time after the new requests are granted.

Example 2 A examble simple platform

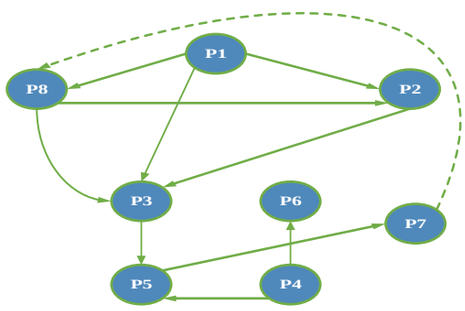


Figure 2. A examble simple platform

We use the platform graph, for the grid platform. We model a collection of heterogeneous resources and the communication links between them as the nodes and edges of an undirected graph. Seea example in Figure 2 with 8 processors and 11 communication links. Each node is a computing resource (a processor, or a cluster, or node).
A process can be in two states: running or blocked. In the running state (also called active state), a process has all the needed re and is either executing or is ready for execution. In the blocked state, a process is waiting to acquire some resource.

B. The architecture

The target heterogeneous platform is represented by a directed graph, the platform graph.
There are p nodes $P_1, P_2, \ldots, P_n$ that represent the processors. In the example of figure 1 there at eight processors, hence n = 8.
Each edge represents a physical interconnection. Each edge e_{ij}: $P_i \rightarrow P_j$ is labeled by value $c_{i,j}$ which represents the time to transfer a message of unit length between P_i and P_j, in either direction: we assume that the link between P_i and P_j is bidirectional and symmetric. A variant would be to assume two unidirectional links, one in each direction, with possibly different label values. If there is no communication link between P_i and P_j we let $c_{i,j} = +\infty$, so that $c_{i,j} < +\infty$ means that P_i and P_j are neighbors in the communication graph.

C. Wait – For – Graph (WFG)

In distributed systems, the sate of the system can be modeled by directed graph, called a wait for graph (WFG) [21,22,23,24,25]. In a WFG, nodes are processors and there is a directed edge from node P_1 to mode P_2 if P_1 is blocked and is waiting for P_2 to release some resource. A system is deadlocked if and only if there exists a directed cycle or knot in the WFG.
Let us first of all describe the deadlock condition problem more precisely.
A set $S = \{s_1, s_2, \ldots s_k\} \subseteq \mathcal{E}$ of $k > 1$ entities is deadlocked when the following two conditions simultaneously hold:
Each entity $s_i \in S$ is waiting for an event permission that must be generated from another entity in the set;
No entity $s_i \in S$ can generate a permission while it is waiting.
If these two conditions hold, the entities in the set will be waiting forever, regardless of the nature of the permission and of why they are waiting for the "permission"; for example, it could be because s_i needs a resource held by s_j in order to complete its computation.
A useful way to understand the situations in which deadlock may occur is to describe the status of the entities during a computation, with respect to their waiting for some events, by means of a directed graph $\overline{W}$, called wait-for graph.

IV. SOLUTIONS IN RESOURCE ALLOCATION HETEROGENEOUS DISTRIBUTED VIRTUAL MACHINES

In cloud computing model as introduced above, the resources provided is gathered in so many complicated steps. The development of a solution to prevent deadlock need to ensure that at least one of the following conditions cannot occur: Resources cannot be shared.Occupied and the additional resources required. No recovery resources. Exist in a cycle or knot.

A. The proposed algorithm for distributing virtual machines

Virtual machine distribution on physical nodes at a specific time. To determine the distribution capabilities of all VM's of a lease on physical nodes at required times, starting at time t and lasting d seconds is very difficult. When combining best-effort and algorithm 2, we can find that the time before and algorithms used to provide resources in distributed environments is underutilized, as we cant schedule and best-effort request.

Algorithm 1 Best-effort

Input: A lease l, a Boolean allow_future
Output:A lease l
m ← map (l,now, duration[l])
Step 1 if m ≠ 0 then
VMrr ← new reservation
start[VMrr] ←now
end[VMrr] ←now + duration[l]
res[VMrr} ←..
add VMrr to reservations[l] and to slot table.
State[l] ← Scheduled
Step 2 else if m=0 and not allow_future

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

State[l] ←Queued
else changepoints ←t
For all cp € changepoints do
m ←map(l,cp,duration[l])
if m≠ 0 then
break
end if
end for
Step 3 return l

When the nodes have been sorted, the model uses the best-effort algorithm to distribute all VM's.

Aforementioned algorithm has the ability to distribute multiple VM's on the same node. With this research aiming to provide efficient distribution of resources, we propose the following technique in distributed environments. In this case, the algorithm tries to distribute as many VM's as possible on multiple physical nodes.

B. The proposed for techique solution distributed environments

When a lease (l) requests resources to create a virtual machine VM (including software, data operating systems, etc.) of any Data Center DC_i.

Step 1 If DC_i already has VM then l_k already has resources, no deadlock detects and algorithm ends.

Else, if DC_i does not have VM but l has been issued for transaction l_j then send message l_j block l_k for $DC(l_j)$ and $DC(l_k)$. The message content is (l_j, l_k).

When any DC_i received a notification message for blocked pair (l_j, l_k) then:

Step 2 If $DC=DC(l_k)$ then add l_j to set P(DC) if l_j does not belong to T(DC).

Step 3 If $P(DC) \cap T(DC) = \{j\}$ then deadlock detection succeeds and algorithm ends..

Else, send message (l_j, l') for all servers DC(l'), with each l' being a member of set B(S).

Else if $DC \neq DC(l_k)$ then add l_k to T(DC).

From the above algorithm, it can be concluded that the proposed solution is of computational complexity. For every deadlock detection, the algorithm exchanges e request messages and e reply messages, where e=n(n-1) is the number of edges.

On consideration of resources required, we imposed some information about time that lease contracts are submitted, elapsed duration, the number of nodes required. We also set up more information: p = 1, m = 1024 (which means each node requires 1 CPU and 1024 MB of memory).

We conduct studies to evaluate the ability to provide resources, namely CPU hardware resources. In the future we will conduct additional analysis capabilities of virtualized resources such as storage drives, availability and completion time upon lease contract submission. p, the percentage of CPU being used by a given request. (Value of p can be 10%, 20%, 30%, 40% and 50% - because the percentage of CPU for using the greedy algorithm is calculated as approximately 49.20%).

VM, the number of nodes required. These are approximately as follows: small (1-24), medium (25-48), large (49-72). With the above two parameters, the research team determined the times to collect the results of the time when it requires to use the greedy algorithm within 1 lease contract in 1 DC and the time when the deadlock detection algorithm detected on deadlocks.

V. THE RESULTS FROM OUR ASSESSMENT

This section presents the results to the simulation experiments on simulated scheduling software Haizea.

Table 1. *Average time a contract ends with greedy algorithm, together with the CPU usage at local environment.*

The ability of the CPU p	10%	20%	30%	40%	50%
NOVM with NO suspension/recovery	4,5	14,3	15,5	10,5	18
NOVM with suspension/recovery	2,4	2,6	6,5	16,5	20
Can create VM	2,8	2,8	27,3	37,3	90

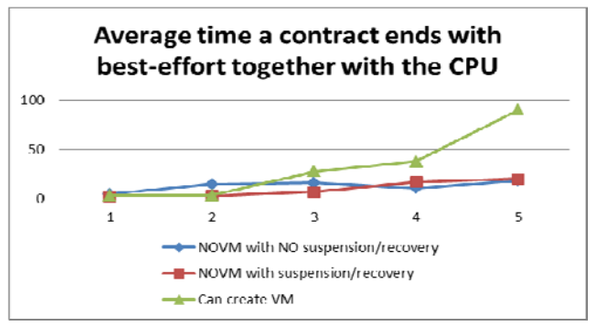
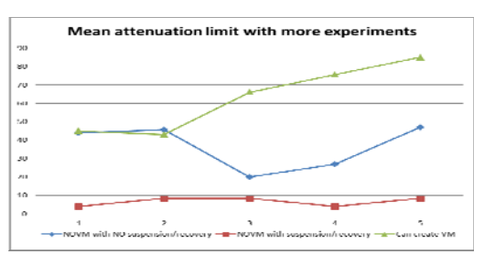


Figure 3. Graph showing the ability of CPU to each lease contract with best-effort algorithm

Through chart 1, by applying scheduling using greedy algorithm with the ability to provide resources for one lease contract (given the condition that the ability of CPU is predetermined), we realized that the rates between failure and successful creation of virtual machines is the same. At CPU's ability of 50%, we can clearly see the that difference between these rates greater, with failure creation at 18 % and success creation at 90%.

Table 2. *Mean attenuation limit with more experiments*

The ability of the CPU p	10%	20%	30%	40%	50%
NOVM with NO suspension/recovery	43,95	45,65	20	26,95	47
NOVM with suspension/recovery	4,05	8,40	8,46	4,05	8,40
Can create VM	45	43	66	75,5	85



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

Figure 4. Graph showing mean attenuation limit after 10 trials, each lasted 180 minutes.

Through chart 2, by applying scheduling using greedy algorithm with the requirement to provide resources for 10 lease contracts (given the condition that the ability of CPU is pre-determined), we found that the success rate to create VM is high with the CPU's ability at 20%. As for CPU's ability at 10%, the success and failed rate are almost the same. At CPU's ability of 50%, we can clearly see that differences between these rates are greater, with failure creation at 47 % while success creation at 85%.

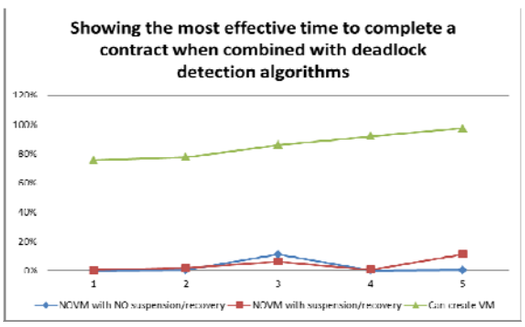


Figure 5. Graph showing lease contract completion time for each CPU capability in distributed environments, using deadlock detection algorithm.

Through chart 3, by applying scheduling using greedy algorithm combined with deadlock detection algorithm to the requirement to provide resources for 10 lease contracts (given the condition that the ability of CPU is pre-determined), we found that the success rate to create VM is very high with the CPU's ability at 50%. As for CPU's ability at 10% and 20%, the success creation is also higher than that of failure creation.

VI. Conclusion

In the context of this paper, we are interested primarily in the criteria of readiness, because it affects preparing costs the most. The use of virtualization technology has great potential to meet the requirements of complex computing systems.

Two algorithms proposed in this research on providing efficient resources for virtual workspaces can grow up by utilizing the above advantages. Security problems, isolation, and the ability to adjust resources can impact positively on the standard of environmental quality by ensuring sufficient workspace resources (CPU, RAM, etc.) to support execution. Independence ability also improves the standard of resources openness, expanding pool of physical resources to run certain workspaces.

Our main approach focuses on applying scheduling algorithms for each type of lease contracts and applying the proposed algorithm in the distributed resources system. There were previous studies on the topic like that of author Borja Sotomayor, but it limited at researching local stations. We have also conducted experiments on distributed environments, given the ability of CPU, in some data centers – which yielded some positive results. It is the assessment that compares between the ability to create VM as requirements, or reject the request of creating a VM as other VM's cannot be suspended, or to stop the CPU in the data centers. Through this research we found that the application of appropriate scheduling algorithms would give optimal performance to distributed resources of virtual machine systems.

References

[1] Ha Huy Cuong Nguyen, Van Son Le, Thanh Thuy Nguyen, "Algorithmic approach to deadlock detection for resource allocation in heterogeneous platforms", Proceedings of 2014 International Conference on Smart Computing, IEEE Computer Society Press, 3 - 5 November, Hong Kong, China, page 97 – 103.

[2] B.Sotomayor, R.Santiago Montero, I.Martín Llorente, I.Foster. Virtual Infrastructure Management in Private and Hybrid Clouds, IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sep./Oct. 2009.

[3] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D.,Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commune. ACM53(4), 50–58 (2010)

[4] M. Andreolini, S. Casolari, M. Colajanni, and M. Missouri, "Dynamic load management of virtual machines in a cloud architectures," inCLOUDCOMP, 2009.

[5] P. Shiu, Y. Tan and V. Mooney "A novel deadlock detection algorithm and architecture", Proc. CODES 01, pp.73 -78, (2001).

[6] Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: towards a cloud definition. SIGCOMM Comput. Commune. Rev. 39(1), 50–55 (2009)

[7] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D.,Rabkin, A., Stoica, I., Zaharia, M.: Above the Clouds: A Berkeley View of Cloud Computing.Technical Report No. UCB EECS-2009-28, University of California at Berkley, USA, Feb 10, 2009

[8] Kaur P.D., Chana I.: Enhancing Grid Resource Scheduling Algorithms for Cloud Environments. HPAGC 2011, pp. 140–144, (2011)

[9] Vouk, M.A.: Cloud computing: Issues, research and implementations. In: Information Technology Interfaces. ITI 2008. 30th International Conference on, 2008, pp. 31–40, (2008)

[10] Srikantaiah, S., Kansal, A., Zhao, F.: Energy aware consolidation for cloud computing. Cluster Comput. 12, 1–15 (2009)

[11] Berl, A., Gelenbe, E., di Girolamo, M., Giuliani, G., de Meer, H., Pentikousis, K., Dang, M.Q.:Energy-efficient cloud computing. Comput. J. 53(7), 1045–1051 (2010)

[12] Garg, S.K., Yeo, C.S., Anandasivam, A., Buyya, R.: Environment-conscious scheduling of HPC applications on distributed cloud-oriented data centers. J Distrib Comput. Elsevier Press,Amsterdam, (2011)

[13] Warneke, D., Kao, O.: Exploiting dynamic resource allocation for efficient data processing in the cloud. IEEE Trans. Distrib. Syst. 22(6), 985–997 (2011).

[14] Wu, L., Garg, S.K., Buyya, R.: SLA-based Resource Allocation for a Software as a Service Provider in Cloud Computing Environments. In: Proceedings of the 11th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid 2011), Los Angeles, USA, May 23–26, (2011)

[15] Addis, B., Ardagna, D., Panicucci, B.: Autonomic Management of Cloud Service Centers with Availability Guarantees. 2010 IEEE 3rd International Conference on Cloud Computing, pp 220–207,(2010)

[16] Abdelsalam, H.S., Maly, K., Kaminsky, D.: Analysis of Energy Efficiency in Clouds. 2009 Computation, World: Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns,pp. 416–422, (2009)

[17] Yazir, Y.O., Matthews, C., Farahbod, R.: Dynamic Resource Allocation in Computing Clouds using Distributed Multiple Criteria Decision Analysis. IEEE 3rd International Conference on Cloud Computing, pp. 91–98, (2010)

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

[18] M. Stillwell, D. Schanzenbach, F. Vivien, and H. Casanova, “Resource allocation algorithms for virtualized service hosting platforms,” JPDC, vol. 70, no. 9, pp. 962–974, (2010).

[19] S. Benin, A. I. Bucur, and D. H. Epema, “A measurement-based simulation study of processor co-allocation in multi-cluster systems,” inJSSPP, pp. 184–204, (2003).

[20] A. Buttery, J. Kurzak, and J. Dongarra, “Limitations of the PlayStation 3 for high performance cluster computing,” U Tenn., Knoxville ICL, Tech. Rep. UT-CS-07-597, (2007).

[21] S. Banen, A. I. Bucur, and D. H. Epema, “A measurement-based simulation study of processor co-allocation in multi-cluster systems,” inJSSPP, pp. 184–204, (2003).

[22] A. Buttari, J. Kurzak, and J. Dongarra, “Limitations of the PlayStation 3 for high performance cluster computing,” U Tenn., Knoxville ICL, Tech. Rep. UT-CS-07-597, (2007).

[23] D. P. Mitchell and M. J. Merritt, “A distributed algorithm for deadlock detection and resolution,” in Proc.ACM Symposium on Principles of Distributed Computing, pp. 282–284,1984.

[24] Ajay D. Kshemkalyani, Mukesh Singhal. “*Distributed Computing Principles, Algorithms, and Systems”*, Cambridge University Press, 2008.

[25] Bondy JA, Murty USR (2008) Graph theory. Springer graduate texts in mathematics. Springer,Berlin. ISBN 978-1-84628-970-5.

[26] Fournier JC (2009) Graph theory and applications. Wiley, New York. ISBN 978-1-848321-070-7.

[27] Greg N. Frederickson, Fast algorithms for shortest paths in planar graphs, with applications, SIAM Journal on Computing, v.16 n.6, p.1004-1022.

AUTHORS PROFILE

HA HUY CUONG NGUYEN received his B.S. degree in information technology from Van Lang University, Ho Chi Minh, Viet Nam, in 2003, the M.S. degree in Computer Science from DA Nan University, DA Nang, Viet Nam, in 2010. He was a lecturer, with Department of Information Technology, Quang Nam University, in 2003 so far. From 2011 until now, he studied at the center DATIC, University of Science and Technology - The University of Da Nang. At the center of this research, he doctoral thesis "Studies deadlock prevention solutions in resource allocation for distributed virtual systems". His research interests include network, operating system, distributed system and cloud computing.

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

COMPARATIVE ANALYSIS OF DISCRETE LOGARITHM AND RSA ALGORITHM IN DATA CRYPTOGRAPHY

Abari Ovye John
Computer Science Department
Federal University Lokoja
Kogi State, Nigeria

P.B.Shola
Computer Science Department
University of Ilorin, Ilorin
Kwara State, Nigeria

Simon Philip
Computer Science Department
Federal University kashere,
Gombe State, Nigeria

Abstract: Due to its speed, spread and ease of use, the internet has now become a popular means through which useful data and information are transported from one location to another. This shift in the way data and information is being transported then calls for a new or different approach to security issues to save data in-transit from hackers. Cryptography is one of the approaches that have been explored for data security on the internet. RSA and El-Gamal (based on concepts of discrete logarithm) cryptographic algorithms are mostly employed to handle data security on the internet. This research work present a fair comparison between RSA and Discrete Logarithm algorithms along this direction; efficiency (time and space) by running several encryption setting to process data of different sizes. The efficiency of these algorithms is considered based on key generation speed, encryption speed, decryption speed, and storage requirement of the cipher text. In this paper, simulation has been conducted using Java programming language. Texts of different sizes were encrypted and decrypted using RSA and El Gamal during the testing. Based on the result of the simulation, El Gamal is faster than RSA in terms of key generation speed but consumes more memory space than RSA. RSA is faster than El Gamal in terms of encryption and decryption speed.

Keywords: Cryptography, Algorithm, RSA, El-Gamal, Encryption, Decryption, Discrete Logarithm, Plain text, Cipher text.

1. INTRODUCTION

Steganography and Cryptography are the two approaches that have been explored for data security on the internet.

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes that there is a hidden message [1]. Pure, secret key and public key steganography are the basic three main categories of steganography. In pure steganography, the secret lies in the embedding and extracting algorithms that only the message sender and intended receiver should know [2]. In secret key steganography, it is assumed that a party other than the sender and intended receiver knows the embedding and extraction algorithms. The sender embeds a message in a cover-object using a secret key known as a stego-key. Therefore, even if a third party intercepts the stego-object and extracts the information, the result will appear to be a random, garbled mess. Only the intended receiver who possesses the same key can extract the original message [2]. In a public key steganography system, two keys are used: a private key and a public key. The public key is used in the embedding process, and the private key is used in the extraction process. Public key steganography allows the sender and receiver to avoid exchanging a secret key that might be compromised [2].

Cryptography on the other hand is one of the methods used to ensure confidentiality and integrity of information in a communication system. It is derived from the Greek word "kryptos" which means secret-writing. Cryptography is the science and art of

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

transforming messages to make them secure and immune to attack [3].

Cryptography basically works on the principal of mathematics that generates different algorithms known as cryptographic algorithm [4]. A cryptographic algorithm (or cipher) is a mathematical function used in the encryption and decryption process. The cryptographic algorithm works in combination with a key to encrypt the plaintext. The set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context is known as the Cryptosystem [RFC2828]. Basically, cryptographic techniques are categorized into two namely; Secret Key (Symmetric) Cryptography, and Public Key (Asymmetric) Cryptography.

2. SECRET KEY (SYMMETRIC) CRYPTOGRAPHY

This type of cryptography uses a single (one) key for both encryption and decryption. Both the sender and the receiver of the message have to meet or establish a secure channel for exchanging the key. This method is therefore mostly used in olden days and is regarded as risky and is not efficient. The encryption techniques using secret key cryptography are the Data Encryption Standard (DES), Advanced Encryption Standard (AES) e.t.c.

Figure 1 shows a private (symmetric) key cryptosystem where the Dean convert a plain text into a cipher text using a key and the HOD convert the cipher text back to its original plain text using the same key.

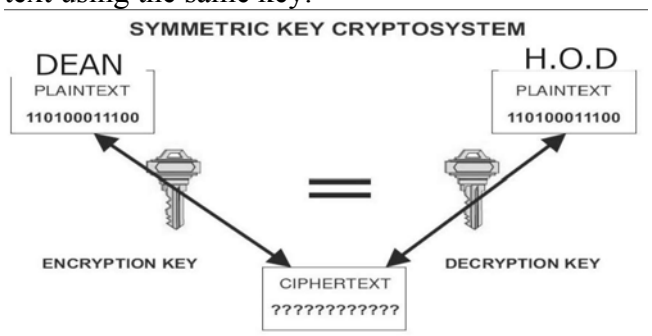


Fig. 1: Private (Symmetric) key cryptosystem

Symmetric key encryption algorithm (secret key algorithm) though easy and simple to implement, has observable shortcomings [6]. These include:

- The communicating parties must agree upon a secret key.
- The need for a new key for every correspondence.
- Origin or receipt Authenticity cannot be confirmed since the key is shared.
- The symmetric keys management becomes difficult.

3. PUBLIC KEY (ASYMMETRIC) CRYPTOGRAPHY

The idea of public key cryptography was brought about by Whitfield Diffie and Martin Hellman at Stanford University in 1976 [7]. This type of cryptography uses two keys; one for encryption and the other for decryption and hence it is called modern cryptographic method.

In this method, the encryption key is made public, so a person can publish his encryption key to the general public and keep his/her decryption key private (hence his/her decryption key is only known to him/her). Therefore, the only person that can be able to decrypt the message is the owner of the private key. The sender himself cannot be able to decrypt the message.

For instance, you have a box which can only be unlocked with a key and you are the only person that has the key; you can decide to send the box unlocked (opened) to the general public. When someone wants to send a message to you, he can put it in the box and lock it. Therefore, the box can only be unlocked by you because you are the only person who has the key.

Figure 2 shows a public (asymmetric) key cryptosystem where the Dean convert a plain text into a cipher text using a key (HOD's public key) and the HOD convert the cipher text back to its original plain text using another different key (his private key).

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

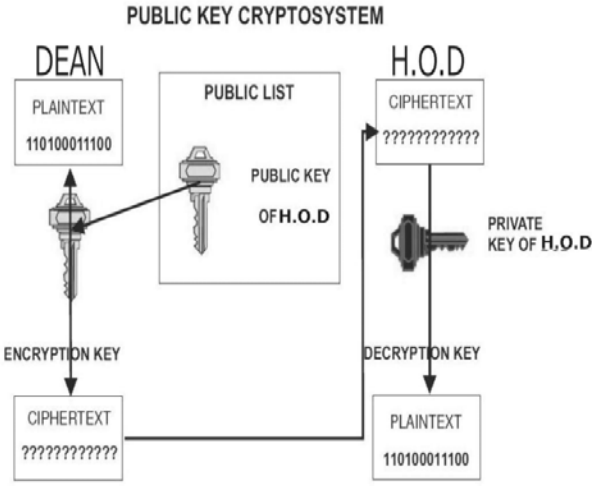


Fig.2: Public (Asymmetric) Key Cryptosystem

Like secret key cryptography, the security of a message depends on the key size i.e. larger key provides high security but slow speed of encryption/decryption. Also 80 bits key length of secret key cryptography is equivalent to 1024 bits key length in public key cryptography.

In public key cryptography, encryption and decryption is slow compared to secret key cryptography. Since public key cryptography uses two keys, it is regarded as more secure and efficient. Also the establishment of secure channel for exchanging the key is not necessary. Unlike secret key cryptography, public key cryptography is not limited to only encryption/decryption of data, but can also be used in digital signatures.

4. RELATED WORK

- Reference [8] has done an analysis of the Mathematics of the RSA Public-Key Cryptosystem. He discussed how the Prime Generation and Integer Factorization, Modular Exponentiation and Roots of RSA algorithms can be derived.
- Reference [9] has done an efficient implementation of RSA algorithm using gmp library from GNU. The authors also analyzed the changes in the performance of the algorithm by changing the number of characters. At the end, an efficient implementation of RSA is shown by using various functions of the GMP library. Feasibility analysis is done by comparing the time taken for encryption and decryption.
- Reference [10] has done a comparative study between some symmetric and asymmetric techniques(AES, DES, 3DES, Blowfish, RSA, Diffie-Hellman Algorithm) based on effectiveness, flexibility and security.
- Reference [11] has proposed a new comparative study between three encryption algorithms such as DES, 3DES and AES within Nine Factors achieving an effectiveness, and security, which is at the challenge of researchers.
- Reference [12] has analyzed DES , Triple DES and RSA three algorithm. DES and Triple DES is symmetric key algorithm and RSA is an asymmetric key algorithm, they have been analyzed on their ability to secure data, time in use to encrypt data and throughput the algorithm requires. Performance of algorithms is different according to the inputs size.
- Reference [13] used an object-oriented model to design and implement the RSA where Unified Modeling Language (UML) was used as the design technique.
- Reference [14] presented a comparison between the DES private key based Algorithm and RSA public key based algorithm based on the speed of encryption and decryption of the input plain text and encryption throughput and decryption throughput

5. ANALYSIS OF RSA ALGORITHM

The RSA algorithm is a public key cryptosystem that offers both encryption and digital signatures (authentication). Its name stands for the first letters of its creators' names *Rivest*, *Shamir* and *Adleman.*

For a person to encrypt a plain text into a cipher, and then decrypt the cipher using RSA technique, three phases have to be followed accordingly: key generation phase, encryption phase and decryption phase.

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

Take for instance, the DEAN wants to send a message M_i to HOD, then HOD has to generate a pair of keys (public and private/secret key) as described below:

5.1 Key Generation Algorithm

1. Generate two large random prime integers "p" and "q" of approximately equal size such that their product is the required bit length (e.g. 1024 bits) but p should not be equal to q i.e. $p \neq q$
2. Compute: $n = p \times q$
3. Compute phi φ(n): $\varphi(n) = (p - 1)(q - 1)$
4. Choose an integer "e" between 1 and φ(n) such that "e" and φ(n) are coprime
   i.e. $1 < e < \varphi(n)$ such that: $\gcd(e, \varphi(n)) = 1$
5. Compute the secret exponent "d":
   i.e. $1 < d < \varphi(n)$ such that: $e \cdot d \equiv 1 \pmod{\varphi(n)}$
   Meaning $de \% \varphi(n) = 1$
   or $d = e^{-1} \bmod \varphi(n)$
6. The public key is $K_P = (n, e)$
7. The private key $K_S = (n, d)$

Where

"n" is the system modulus or simply modulus

"e" is the public or encryption exponent

"d" is the private or decryption exponent

"p, q and φ(n)" are kept private

After the keys are generated, the HOD can publish the public key $K_P = (n, e)$ to the public and keep his private (Secret) key $K_S = (n, d)$ secret. The DEAN can now encrypt his message with the HOD's public key using the below algorithm:

5.2 Encryption Algorithm

1. The DEAN obtains the HOD's public key $K_P = (n, e)$
2. Represents his message M_i as positive integer such that $M_i < n$
3. Compute the cipher $C_i = M_i^e \bmod n$
4. The cipher C_i is then reconverted from number to text (cipher text)

The cipher C_i is then sent to the HOD. The HOD can now decrypt the cipher C_i with his private/secret key $K_S = (n, d)$ using the decryption algorithm as described below.

5.3 Decryption Algorithm

1. The HOD obtains the DEANS ciphered text C_i
2. Represent the ciphered text as a positive integer
3. Use his private key K_P to compute $M_i = C_i^d \bmod n$
4. The plain number M_i is then reconverted from number to text (plain text)

6. ANALYSIS OF DISCRETE LOGARITHM

Discrete logarithm is the principle used in encryption and digital signature. By itself, it is not an encryption algorithm, rather its principles is used in encryption algorithms. Taher ElGamal in 1984 was the first to use this concept in his algorithm known as El – Gamal encryption algorithm.

Like RSA algorithm, El – Gamal encryption algorithm is also a public key cryptosystem and encryption of text has three phases. The three stages of El - Gamal encryption algorithm i.e. key generation, encryption and decryption are described below.

Using the above example, suppose the DEAN wants to send a plain text M_i to the HOD, the HOD generates a pair of keys (public & private/secret keys). The key generation is done as follows:

6.1 Key Generation Algorithm

1. Generate a random large prime number p (≥ 1024 bits) such that p – 1 is divisible by another randomly large prime number q (> 160 bit) i.e. (p-1)% q=0
2. Compute a generator g of the multiplicative group of order q in GF(p)*, using:
   $g \equiv r^{(p-1)/q} \bmod p$ (using some random r until $g \neq 1$)
3. Choose a random integer a between 1 and q – 1 i.e. $1 \leq a \leq q - 1$
4. Compute h using: $h \equiv g^a \bmod p$

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

5. Public key $K_P = (p, q, g, h)$
6. Secret (Private) key $K_S = a$

After the keys are generated, the HOD can publish his public key $K_P = (p, q, g, h)$ to the public and keep his private (Secret) key $K_S = a$ secret. The DEAN can now encrypt his message using the HOD's public key using the below algorithm:

6.2 Encryption Algorithm

1. The DEAN obtains the HOD's public key $K_P = (p, q, g, h)$
2. Generate a random number k between 1 and q – 1 such that k and p – 1 are coprime i.e. $1 < k < q - 1$ such that $\gcd(k, p - 1) = 1$
3. Represents his message M_i as positive integer such that $0 \leq M_i \leq p - 1$
4. Compute r: $r \equiv g^K \bmod p$
5. Compute s: $s \equiv h^K M_i \bmod p$ $(0 \leq M_i \leq p - 1)$
6. The cipher text C_i: $C_i = (r, s)$

The cipher text C_i can now be sent to the HOD. The HOD can now decrypt the cipher C_i with his secret key $K_S = a$ using the below algorithm.

6.3 Decryption Algorithm

1. The HOD obtains the DEANS ciphered text C_i
2. Represent the ciphered text as a positive integer
3. Use his private key K_S to compute $z \equiv r^{p-1-a} \bmod p$
4. Compute the message $M_i \equiv z \cdot s \bmod p$
5. The plain text M_i is then reconverted from number to text (plain text)

7. SIMULATION RESULTS

The algorithms were implemented using java programming language. The result of the comparison of the two algorithms in terms of key generation speed, encryption speed, decryption speed, and storage requirement of the cipher text is presented in following the tables and graphs.

A. Efficiency

i. Speed Of Generating Keys

The table 1 shows the time taken to generate keys (i.e. 512 & 1024) by these algorithms:

Table 1: Key Generation Time

Algorithm Name	512 bits Time (sec)	1024 bits Time (sec)
RSA	0.09524	0.78711
El Gamal	0.00789	0.01482

Graph

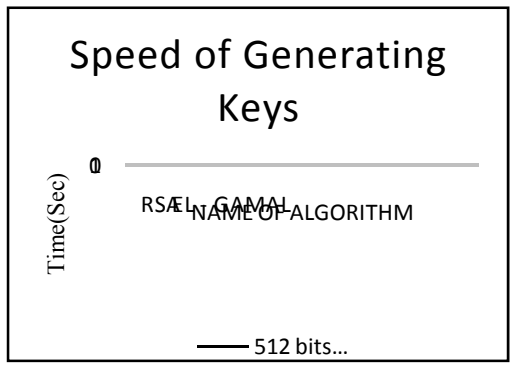


Fig. 3a: Graph of Key Generation

Graph

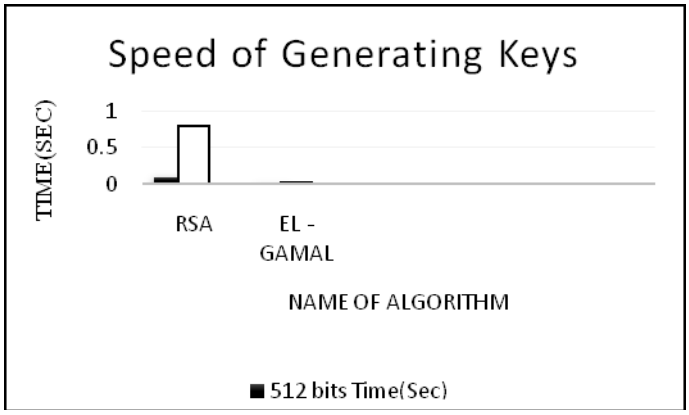


Fig. 3b: Bar Chart of Key Generation

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

ii. Speed Of Encryption

Table 2 shows the time taken to encrypt text of various sizes.

Table 2: Encryption Execution Time

Number of characters (Input Data)	Encryption Execution Time (Seconds)	
	RSA	El Gamal
1	0.00214	0.30976
10	0.00405	0.38016
100	0.00471	0.48655
1000	0.02047	0.56299
10000	0.08785	1.15767

Graph

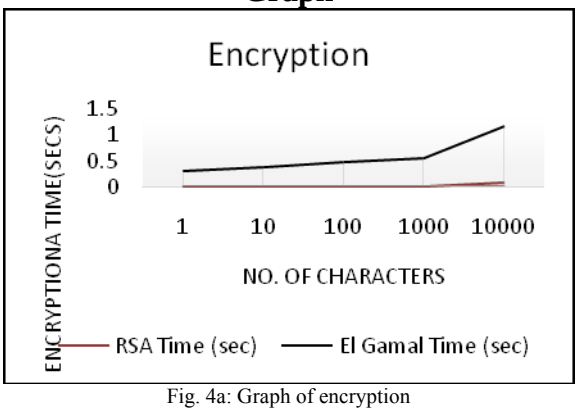


Fig. 4a: Graph of encryption

iii. Speed Of Decryption

The table 3 shows the time taken to decrypt cipher text to plain text of various sizes.

Table 3: Decryption Execution Time

Number of characters (Input Data)	Decryption Execution Time (Seconds)	
	RSA	El Gamal
1	0.03460	0.04840
10	0.05496	0.06154
100	0.06072	0.06249
1000	0.32294	0.76274
10000	1.09979	1.79132

Graph

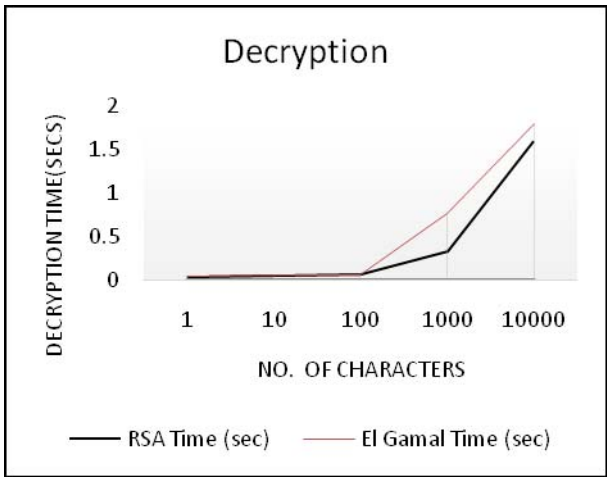


Fig. 5: Graph of decryption

iv. Storage Requirement

By storage requirement, the researchers mean the space occupied by a cipher text produced by these algorithms. Table 4 shows the sizes of cipher text produced by these algorithms.

Table 4: Storage requirement

Number of characters (Input Data)	Space Occupied by Cipher Text (Bytes)	
	RSA	El Gamal
1	309	619
10	309	638
100	308	818
1000	2169	4470
10000	20752	41015

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

Graph

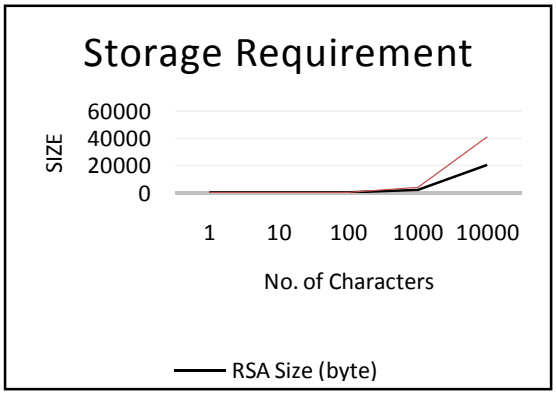


Fig. 6: Graph of Storage Requirement

8. RESULT AND FINDINGS

The following are the results and findings of this research work:

- It takes longer time to generate keys in RSA algorithm than in El Gamal algorithm. Therefore, in terms of key generation speed, El Gamal algorithm is better than RSA algorithm.
- It takes longer time to encrypt text in El Gamal algorithm than in RSA algorithm. Therefore, in terms of encryption speed, RSA algorithm is better than El Gamal algorithm.
- It takes longer time to decrypt text in El Gamal algorithm than in RSA algorithm. Therefore, in terms of decryption speed, RSA algorithm is better than El Gamal algorithm.
- The cipher text produced by El Gamal algorithm is almost twice the cipher produced by RSA algorithm and hence, El Gamal algorithm consumes more storage space than RSA. Therefore, in terms of memory consumption RSA algorithm is better than El Gamal algorithm.
- Based on mathematical assumptions, El Gamal algorithm is stronger than RSA algorithm while in terms of the key concept, RSA and El Gamal algorithm are of the same strength since Diffie-Hellman keys are as strong as RSA keys.

8.1 SUMMARY OF RESULT AND FINDING

Table 5: Comparison Summary Table

CRITERIA	RSA ALGORITHM	EL GAMAL ALGOTIRHM
Key Generation Speed		✓
Encryption Speed	✓	
Decryption Speed	✓	
Memory Consumption	✓	

9. CONCLUSION AND FUTURE WORK

The presented simulation results showed that RSA is generally favored over El-Gamal for practical reasons. This is because RSA produces small cipher and therefore saves memory, reduces traffic and saves bandwidth in a network. Encrypted El Gamal cipher text is much larger than the original plain text input, so it will not be suitable for use in places where bandwidth is a limiting factor, such as over slow Wide Area Network (WAN) links. Both RSA and El Gamal algorithms are very secure since up to date, no efficient algorithm is found for breaking them. El Gamal algorithm is considered more secured than RSA even though RSA algorithm has survived over 30 years of attack. However, RSA is significantly faster than El-Gamal.

Therefore, RSA and El Gamal algorithms are secured and recommended for use. Their keys size should be at least 1024 bits for a reliable security. For those interested in extremely high security, El Gamal algorithm should serve their needs while for those interested in extremely high speed of operation and small memory/bandwidth consumption, RSA should be considered. In order to derive the benefits of both, the cipher text produced by one algorithm should be encrypted using the other algorithm. This ensures the highest

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

security but wastes time and therefore requires 4 keys (2 private keys & 2 public keys).

The next step of our future work is to adopt another different approach (mathematical approach) to carry out the comparative analysis of the two encryption algorithms to see if it will give us a better result than the approach adopted in this paper (Naive approach).

REFERENCES

[1] Steganography- Wikipedia, the free encyclopedia

[2] www.Snotmonkey.com

[3] B. A. Forouzan "Data Communication and Networking (4 Edition)", McGraw Hill Inc. New York, 2008.

[4]. P. Chaitanya and Y. R. Sree "Design of New Security using Symmetric and Asymmetric Cryptography Algorithms." World Journal of Science and Technology. Vol 2. Issue 10. pp. 83-88, 2012, 2012.

[6] RSA Data Security, Inc. The RSA Factoring Challenge. http://www.rsa.com/rsalabs/node.asp?id=2092, 2010

[7] http://www.wikipedia.com/au/rsa_alg.html, Accessed May 25, 2010.

[8] B. Kaliski "The Mathematics of the RSA Public-Key Cryptosystem", RSA Laboratories.

[9] B. Rajorshi S. Bandyopadhyay, and A. Banerjee, "A Fast Implementation Of The RSA Algorithm Using The GNU MP Library".

[10] R. Tripathi, and S. Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC), ISSN 2348 - 4853,Volume 1, Issue 6, June 2014.

[11] O.A. Hamdan, B.B.Zaidan, A.A.Zaidan, Hamid, A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

[12] M. Marwaha, R. Bedi, A. Singh, and T. Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[13] N. C. Ashioba, and R. E. Yoro "RSA Cryptosystem using Object-Oriented Modeling Technique", International Journal of Information and Communication Technology Research, Volume 4 No. 2, February 2014.

[14] S. Singh, S. K. Maakar, and S. Kumar "A Performance Analysis of DES and RSA Cryptography ", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN 2278-6856, Volume 2, Issue 3, May – June 2013.

AUTHORS' PROFILE

Mr. Abari Ovye John is a Graduate Assistant in Departmengt of Computer Science, Federal University Lokoja, Kogi, Nigeria. He obtained his B.Sc Computer Science at Nasarawa State University, Keffi, Nigeria. He is currently undergoing his Master programme at University of Ilorin, Nigeria. He has finished his master's thesis and awaits his final examination.

Dr. P.B. Shola is an Associate Professor in Department of Computer Science, University of Ilorin, Nigeria. He obtained his PhD at University of Essex, Essex, England, United Kingdom. He is a member of Computer Society of Nigeria.

Mr. Simon Philip is a Graduate Assistant in Departmengt of Computer Science, Federal University Kashere, Gombe. He obtained his B.Sc Computer Science at Gombe State University, Gombe, Nigeria. He is currently undergoing his Master programme at University of Ilorin, Ilorin, Nigeria. He has finished his master's thesis and awaits his final examination.

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

Ensuring consistent Patient Data flow in a low Bandwidth environment with Mobile Agent

Akomolafe Oladeji Patrick
Department of Computer Science
University of Ibadan
Ibadan, Nigeria

***Abstract*-The present technological advancement in pervasive computing and the widespread of the internet and wireless networks and mobile communication systems can be harnessed by E-health to bring better monitoring of patients to obtain a more efficient health care delivery, cost reduction and reduction in medical errors. Health care applications can take outstanding advantage of the intrinsic characteristics of multi-agent systems because of notable features that most health care applications share. This paper presents a patient monitoring system where context can be easily gathered from patient to caregivers. All the functionalities involved in transmitting data or contextual values from one end (patient) to another end (Doctor or Care givers) were abstracted into a middle ware using mobile agent technologies.**

Keywords- Mobile data, Local Patient Information, Mobile Agents, Context Aware, Middleware

I. INTRODUCTION

The health care sector is not only widely distributed and fragmented but it also exhibits a high degree of heterogeneity with strong local autonomy [1]. In addition to these, the data intensive nature of patient monitoring systems and dynamic nature of both care givers and patients in terms of physical mobility have made researchers to accept mobile agent paradigm as a better approach to context-aware services delivery in patient monitoring [2].

The present technological advancement in pervasive computing and the widespread of the internet and wireless networks and mobile communication systems can be harnessed by E-health to bring better monitoring of patients to obtain a more efficient health care delivery, cost reduction and reduction in medical errors .

To be able to serve the user efficiently, mobile applications must be able to discover services, manage and adapt to their changing contexts so that users can focus on their primary objectives or assignments [3]. Context awareness is a design approach in computer science that creates computer applications that take the situation (specific needs) of its users into account. Context is any information that can be used to characterize the situation of entities (that is, whether a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the applications themselves with the other attributes (world) such as sensor, activator networking facilities and user profiles [4].

Meaningful contextual information like patient blood pressure, heart beat rate, body temperature which can be derived from raw data acquired by sensors placed on user's body or monitoring devices at the user's environment and these, when processed by context-aware systems can improve the quality of medical care especially remote patient monitoring. Health care applications can take outstanding advantage of the intrinsic characteristics of multi-agent systems because of notable features that most health care applications share:

(i) They are composed of loosely coupled (complex) systems;

(ii) They are realized in terms of heterogeneous components and legacy systems;

(iii) They dynamically manage distributed data and resources; and

(iv) They are often accessed by remote users (synchronous) collaboration [5][6].

Mobile agents are software abstraction that can move from host to host on a network to perform specialized services. Apart from providing mobility, agents possess the unique characteristics of adapting to changes in their execution environment and hence have a higher chance of survival and achieving application objectives over a large, distributed and heterogeneous network when compared against traditional techniques which make its adoption for the present research a viable option in this local context [7]. Mobile agents have also proved very effective in supporting asynchronous execution of client's request, weak connectivity and poor bandwidth management [8].

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

In this work mobile agents transfer vital signals or context data like patient blood pressure, heart beat rate, body temperature which are being derived from raw data acquired by sensors placed on user's body or monitoring devices at the user's environment to agent on patients mobile device (readers). The agents that transfer contextual information were abstracted into a middleware. This middleware manages the interaction and complexity between disparate applications across the heterogeneous computing platforms to facilitate the design, development, integration and deployment of both mobile and desktop distributed applications in heterogeneous networking environments. The middleware also automatically replicates the same data for back up purpose consequently providing application designers full location visibility to perform application-specific optimizations and to adapt to local resource availability.

II. RELATED WORKS

[9] developed a context-aware system that helps in monitoring patients diagnosed with brain tumour health care application. They used a button up approach to collect data from various hardware, sensors and notifications are generated by the system to doctors whenever there are deviations from the expected medical recommend actions. This work does not adopt a mobile agent approach to remote patient monitoring.

[10] developed intelligent context- aware monitoring home health care system. In this system sensors are used to collect data from patient and then sent to a centre for supervision. They introduced intelligence to the system by using fuzzy logic model and rules based on medical recommendations to analyze and identify critical situations of the patient locally at home. The identification of patient abnormal situation can activate a local device or start interaction with the person or issue on emergency message. Although this work contributed to the vision of home health care, it does not utilize the mobile agent approach to remote patient monitoring.

[11] proposed and consequently implemented a policy based architecture that allows autonomous and continuous monitoring of patient thereby providing continuous necessary medical information to hospital personnel by utilizing software agents and wireless sensor technologies. Although this work introduced mobile agent but it was implemented as a direct application and not at middleware level.

[12] developed a web based framework for patient monitoring comprising of a worst models called Biote which houses an accelerometer and different bio-potential sensors interfaces, a invero controller and RF communication transceiver. This hardware receives patient's medical signals and transmits to their website which is integrated to Microsoft Health vault. Care providers are able to view these patients reading by navigating to the desired patients reading page. This work does not take context awareness into consideration.

[13] presented a telephone care system using mobile telephony for remote patient monitoring. Their system takes advantage of the serial port available in new mobile phones to implement a generic interface for patient monitors. Vital signals are acquired from electro medic devices using RS232 interface and transmitted through the internet. This work also does not adopt the mobile agent technology.

A mobile agent framework for telecardiology was proposed by [14] they combined both mobile agent and object request broker mechanism in their framework so that it can support interoperability and optimize monitoring process. [15] also produced a patient vital signal measuring devices called Tyndal mole, a non-intrusive patient monitoring equipment that does localized processing. Both works are not done at middleware level. Other similar works but with the same demerit mentioned above were done by [16] listed several multi agents projects and initial for e-health. Of much interest is the work of [17] called Ubimedic.

III. REQUIREMENTS AND ARCHITECTURAL GUIDELINES

At an abstract level the most basic functional requirement of the proposed system is to serve as an effective conduit for transferring physiological and contextual data from any application sitting on it to specified server location, therefore template of contextual data must be defined completely from the abstract definition provided.

The middleware promises to help simplify remote patient monitoring application(RMP) development. Based on analysis of many different RPM applications we developed a framework shown in figure 1, the requirements identified are: Data capturing and delivering both discrete and continuous physiological and contextual data ,data transmission, node failure management to maintain system integrity ,messaging, portability, simplicity of code integration, good performance.

What we have done is to abstract all the functionalities involved in transmitting data or contextual values from one end (patient)to another end (Doctor or Care givers) into a middleware using mobile agent technologies –Jade Agent Development Environment (JADE)

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

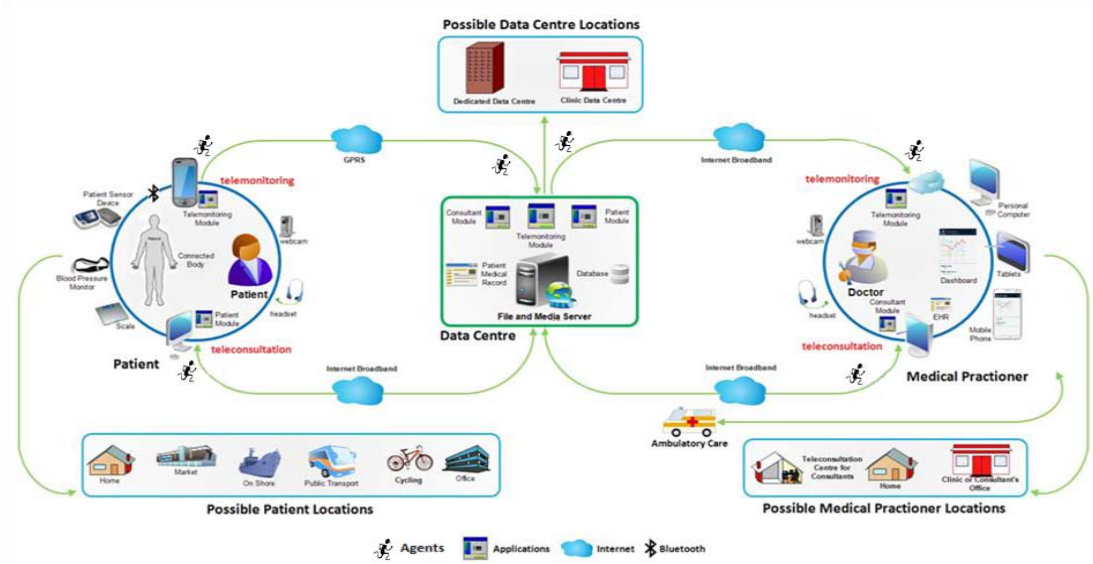


Figure 1: Framework for Remote Patient Monitoring

IV. MODEL OF THE CONTEXT AWARE MOBILE AGENT MIDDLEWARE

The Model of the developed middleware is shown in Figure 2.

It shows the internal modules of the middleware and how they interact to form a unified whole. The different components in the model are explained below.

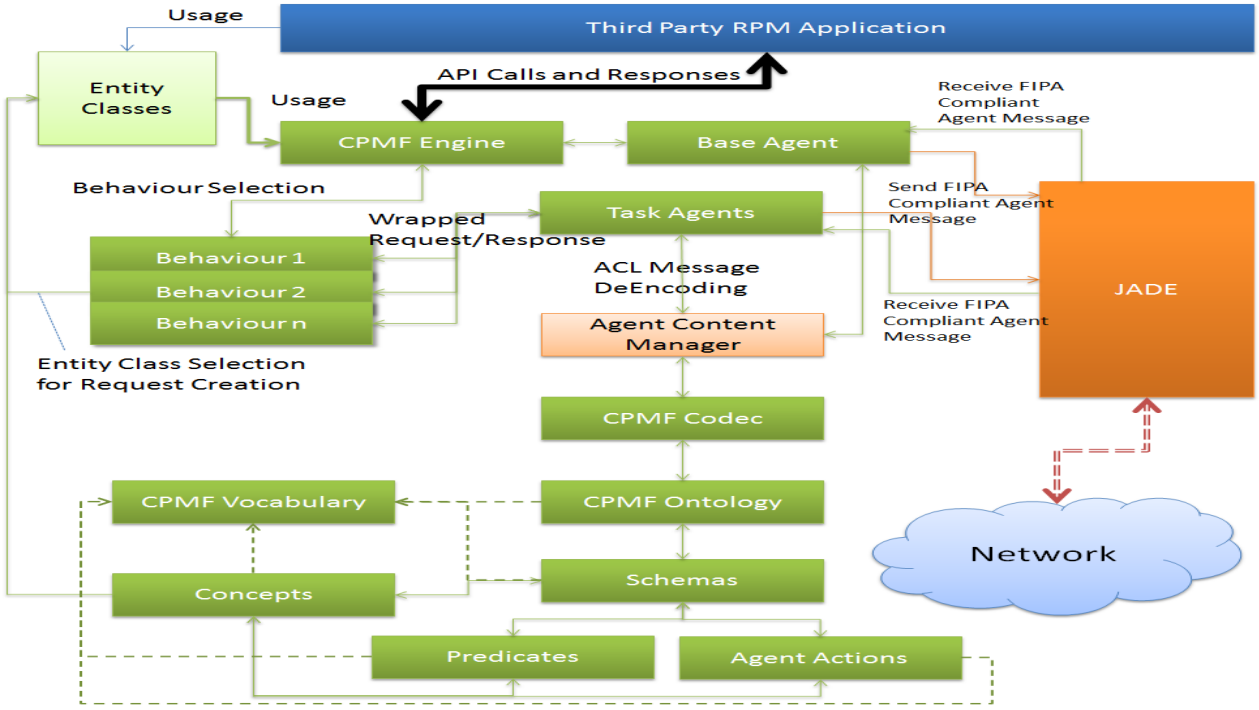


Figure 2 Model of the Context Aware Mobile Agent Middleware

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

Behaviour represents a task that an agent can carry out. It extends predefined behaviour in JADE and implements an atomic task or functionality. The middleware on the initiator sides of the system (patient or caregiver) selects the behaviour that implements a requested task and schedules it for onward processing by a task agent, these task agents communicate with the server base agent by sending various messages and getting responses as described by the running behaviour. On the responder side (Server) all behaviours are added to the base agent and each of them respond to incoming requests as appropriate.

We have two basic agents that are doing all the plumbing work inside the middleware .A complete process of sending data is put into a session and that is initiated by an agent that we called Task Agent .Transport Service is the actions provided by the base agent to consistently transport contextual values from the source PDA to the server after a session has been successfully initialized by a task agent As we move data across.

As we move data across PC and mobile devices data are persisted using JPA Data Persistence on server and RMS Data Persistence on J2ME devices ,we have to persist some information on the Reader devices(mobiles devices) so that continuous reading wont required continuous login procedure.

The Base Agent is an agent that is started when a session starts and runs continuously until the session stops. They perform tasks that are to be repeated and processed continuously. Most typical of such task is the patient sensor data processing (forwarding/receiving ,that is continuous sending of patient context values to the server as soon as it is read by sensors or inferred by the system the server, the base agent exhibits all the behaviours that respond to initiators.

Task Agent performs a specific one-off tasks. On starting, they pick up the behaviour that defines the required task, execute it and are destroyed when the task completes. Task agents exist only on the initiator side of the middleware, they send requests to the base agent on the server as specified by the behaviour assigned to them and are destroyed when a response is received, the response is handed over to the middleware engine for onward delivery to the third party application.

The Agent Content Manager Handles the wrapping and unwrapping of agent communication concepts (Communicative acts, performatives, actions, expressions etc.) into or from a string. It converts between internal objects and FIPA compliant agent message content string. It serves as an interface between the middleware and its associated entities and the underlying agent-based framework.

Application developer using the middleware will only use the API exposed by the middleware to develop a remote patient monitoring application without necessarily having knowledge of Agent oriented programming could defined the context of interest that can be measure using sensor using the entity class, the entity class also is used to model the actors, actions and data that move around the system. The classes have a consistent definition across all modules of the framework. There is also automatic context generation on the layered diagram (where we target context awareness) this automatically generates the location and time

V. ACTIVITIES OF A TYPICAL REMOTE PATIENT APPLICATION

Figure 3 shows the activity diagram section of a generic patient monitoring application,, it shows the individual actions and checks perform by the middleware to initialise the session. To start monitoring a patient or send some agent to the server, or essentially, for a client application to use the middleware, a "Session" must be setup. It begins by checking if a session is currently running that is, if it has been previously been initialized and terminates successfully if one is in progress. Otherwise, it proceeds to setup the session. It retrieves patient information from the data store, then retrieve the patients contexts. If it is running in detached mode, the "Agent" system is not activated, it proceeds next to initialize the policy manager and the location manager. Otherwise, the Agent system starts , the middleware ontology is first initialized, then a connection is made to the server to create the mobile agent backend. If the operation succeeds, it performs a "login" using the patient data retrieved from local storage. On successful login, if the patient record was found on the server, then, the base agent is started, ready to receive contextual data (as provided by the client application) from sensors connected to

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

the PDA and pump them to the server. Policy manager and location handler are afterwards initialized and the session setup completes successfully. otherwise, the patient record is not found on the server, the initialization halts and terminates successfully.

The activity diagram of the Patient registration task is shown in Figure 4, it shows the individual actions and checks perform to register a patient session. At the very beginning, the patient ID is supplied and the local (on device) storage is queried in the "Retrieve Registered Patient from Persistence" process.

If the record is found, then the patient has been registered on the device before now, therefore, nothing else to do, the operation terminates successfully. If the record is not found, and If the system is running in "Detached Mode, then the system requests for the patient context info and persists it locally. otherwise, a task agent is started, to go to the server and retrieve the patients (previously collected) context info. The result returned by the agent is persisted in the local storage and the base agent is started. Then registered policies are retrieved, the policy manager initialized and the registration process completes.

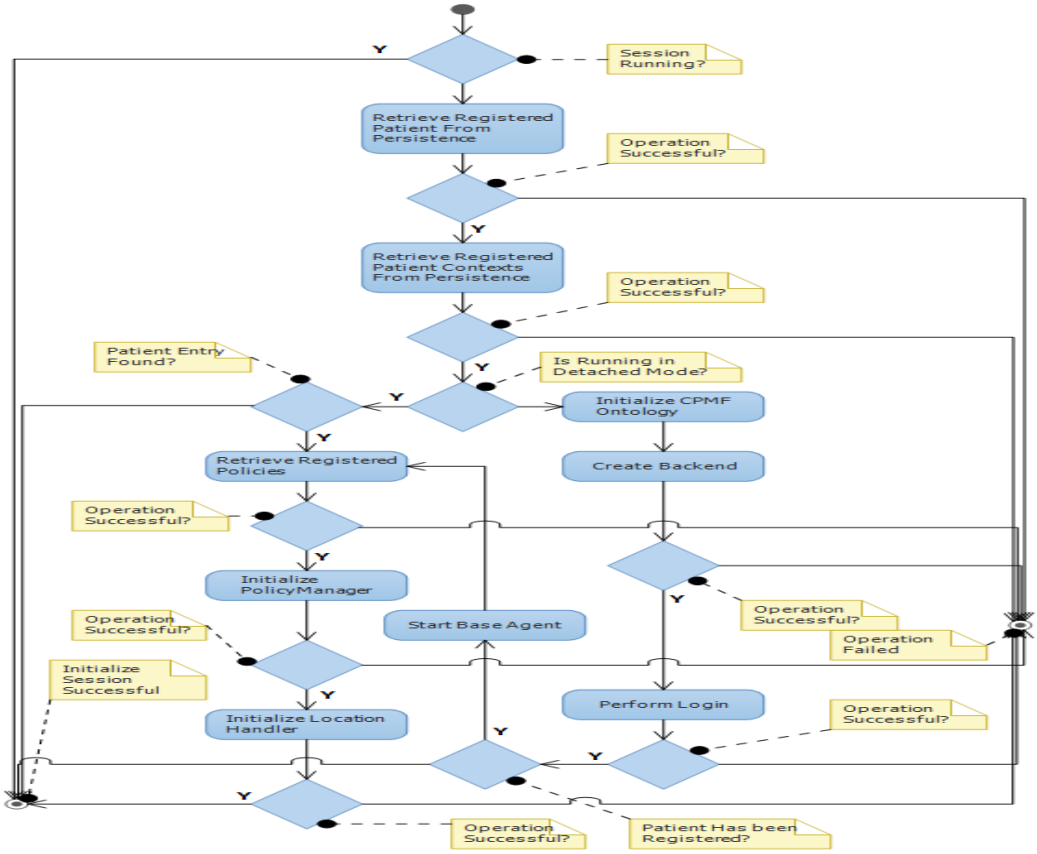


Figure 3 Activity Diagram for the initialisation session method on the SPDA

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

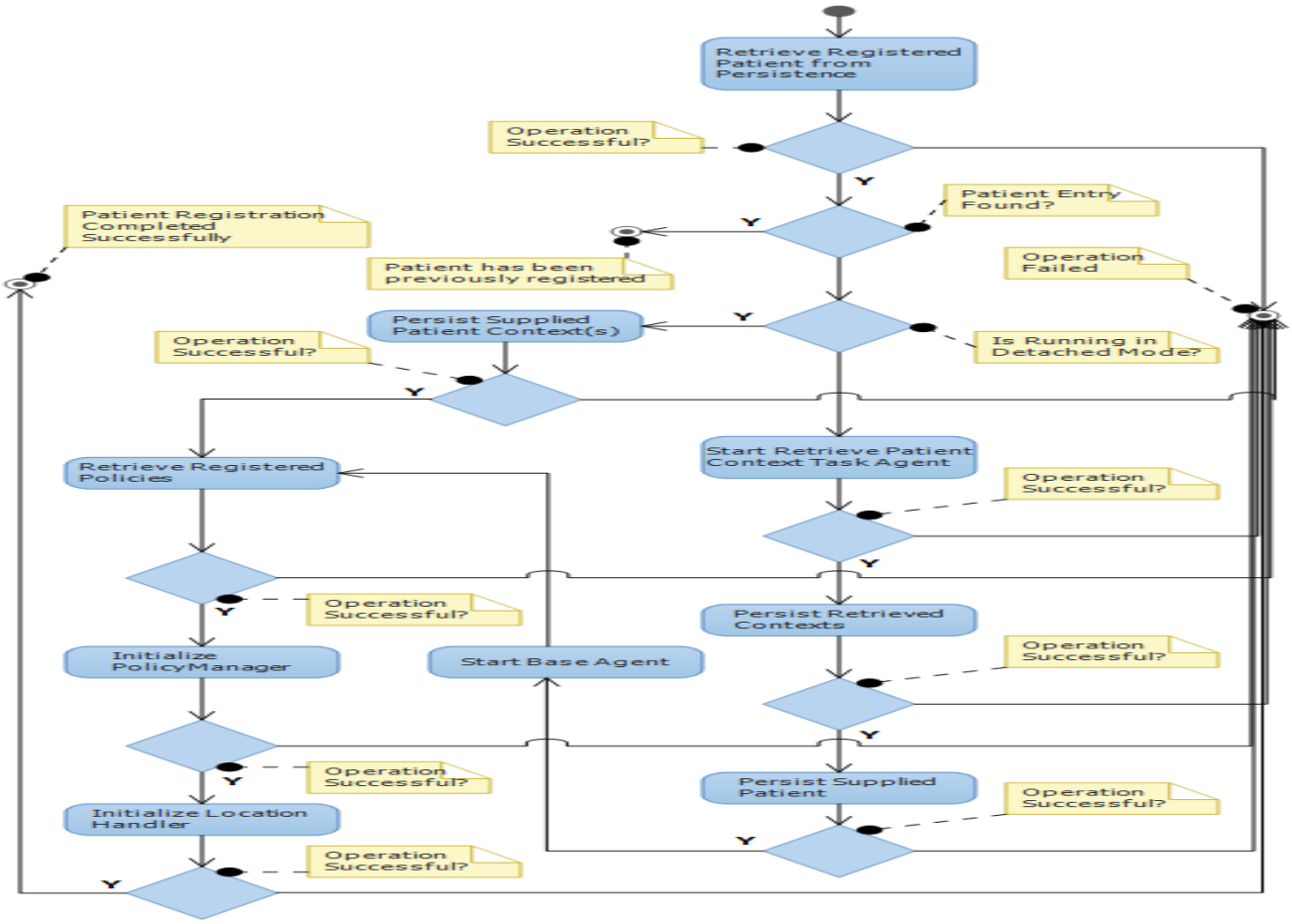


Figure 4. Activity Diagram for the Patient registration task

VI. RESULTS

A simple scenario was implemented using the developed framework. A sample medical patient to be monitored is registered first on the server front end which mimics the process of registering a patient as shown in Figure 5. On successful registration, the patient is given a unique id that will be used for future correspondence. Next, on the PDA that will be used for receiving sensor data, an application that uses the middleware is installed. The application on startup, checks if a patient has been previously registered on the phone.

If no, the id of the patient is requested and the full information for the patient is retrieved from the central server. After confirmation of the retrieved information, the contexts registered for the patient is retrieved and persisted. After successful execution of these processes, the patient and his/her registered . Figures 6 show a registered patient and Figures 7 and 8 show the context data sent and received. These data are automatically logged into the backup server by the replicator agent part of the middleware.

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

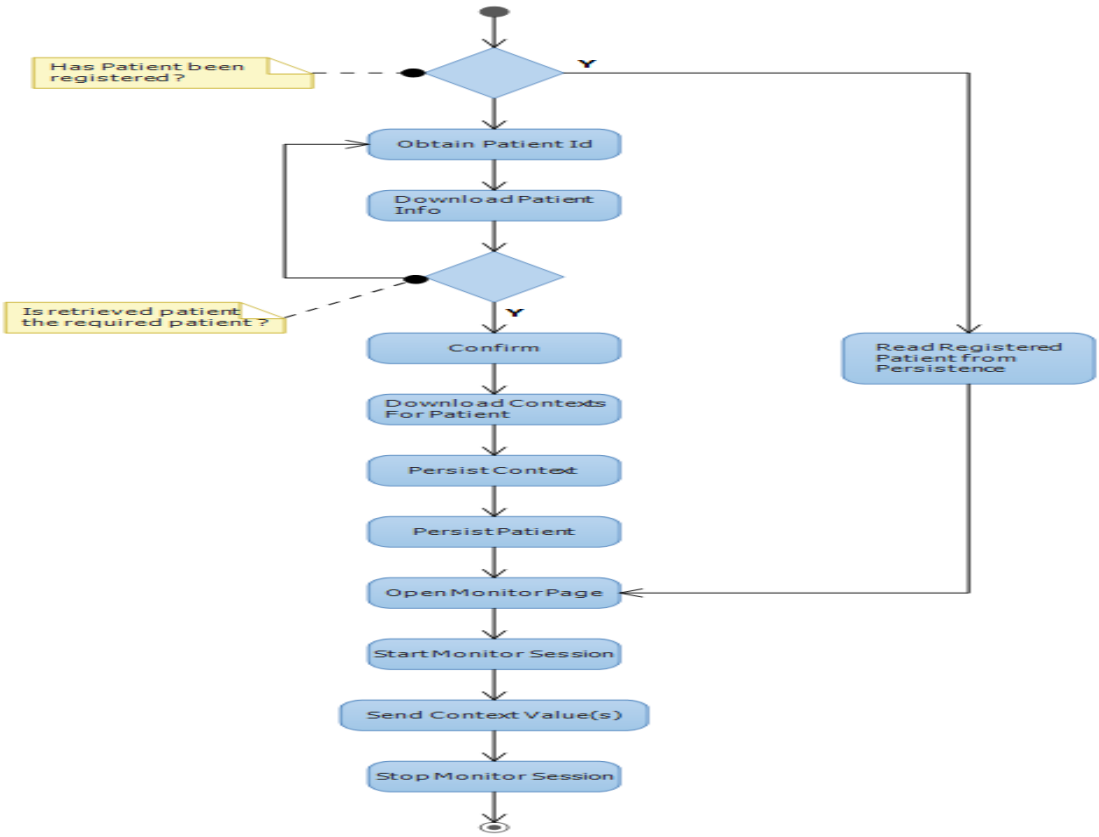


Figure 5 Activity Diagram for Test Scenario

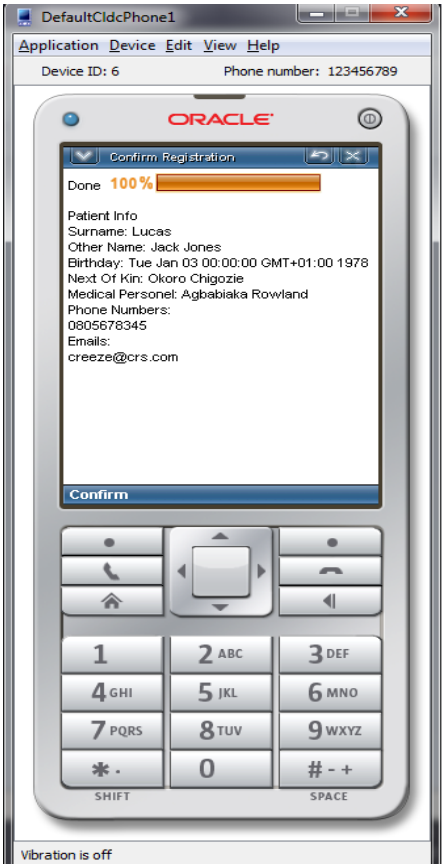


Figure6 Patient Confirmation

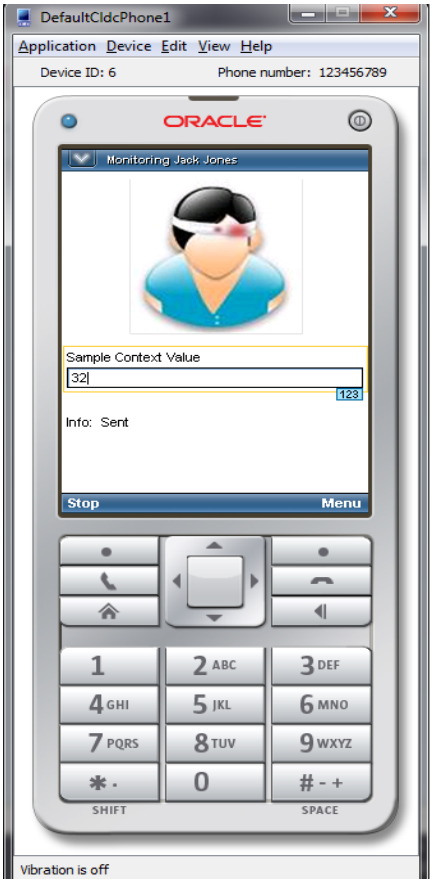


Figure 7Patient Monitoring

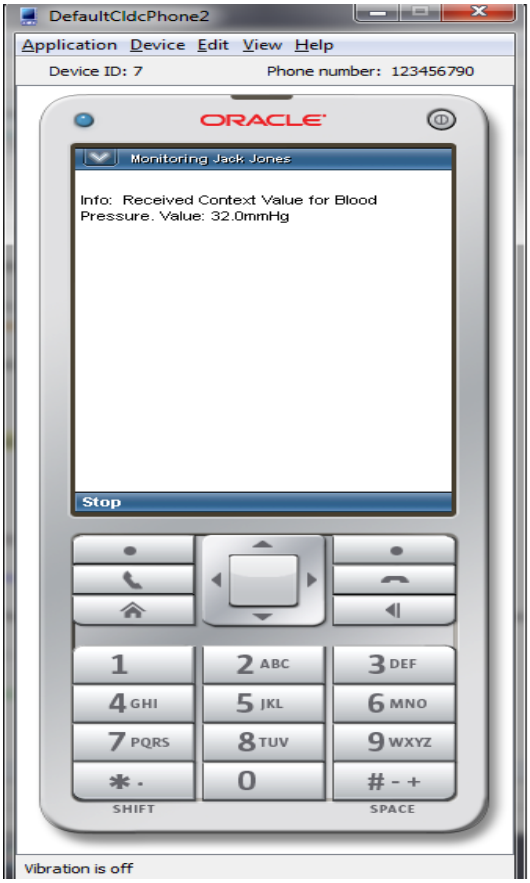


Figure 8 Patient Real-time data

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

VII. CONCLUSION

We presented a framework that allows for easy patient monitoring embedding mobile agents technology on a middleware, using this framework we succesfully implement a platform for healthcare monitoring , the applications shows that mobile agent can be used to remotely monitor patient in low or poor bandwidth areas and automatically replicate these data for backup purposes. In the future ,we plan futher to abstract the functionaliteis of the agent into a middleware layer so that application developers can concertrate on service logic of collecting vital physiological signals only.

REFERENCES

[1] Grimson, J., Stephens, G., Jung, B., Grimson, W., Berry, D., and Pardon, S. (2001),"Sharing Health-care Records over the Internet, "IEEE Internet Computing,5(3),pp.47-58.

[2] Juan, A. F., Dante, I. T., Jesús, A. R., and Óscar, G. (2010), "Agents to Help Context Aware System in Home Care" PAAMS Special Sessions and Workshops.71, pp. 501-508.

[3] Abowd, G. D, Anind K. Dey, P. J., Brown, N. D., Mark, S. & Pete,S. (1999). "Towards a Better Understanding of Context and Context-Awareness, HUC '99: " Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, London, UK pp. 304–307.

[4] Vlasveld, J. (2009), "On designing context-aware applications - Past the phenomenological perspective."Master Essay, University of Twente, Enschede,Netherlands

[5] Annicchiarico, R., Cortés, U., and Urdiales, C. (2008)," Agent Technology and e- Health. Whitestein Series in Software Agent Technologies and Autonomic Computing," M.Calisti, Ed. Basel, Switzerland, BirkhäuserVerlag.

[6] Moreno, A., and Nealon, J. L. (2003), "Application of Software Agent Technology in the Health Care Domain.", Whitestein Series in Software Agent Technologies and Autonomic Computing (Vol. V), Birkhäuser Basel.

[7] Danny, B. L., and Mitsuru, O. (1999), "Seven good reasons for mobile agents," Communications of the ACM, 42 (3), pp. 88-89.

[8] Spyrou, C., Samaras, G., Pitoura, E., &Evripidou, P. (2004), "Mobile Agents for Wireless Computing: The Convergence of Wireless Computational Model with Mobile-Agent Technologies." Journal of ACM/Baltzer Mobile Networking and Applications (MONET).

[9] Bhattacharyya, S., Saravanagru, R. A. K., Thangavelu, A. (2011), "Context-aware Health Care Application," International Journal for Advances in Computer Science, 2 (2), pp.1-6.

[10] Alessandro, C., Loques,O and Leite, J.C.B (2008), "Intelligent Context-aware Monitoring in Home Care," 2nd International Conference: E-Medical Systems. TUNISIA: E- MEDISYS 2008.

[11] Vassis D., Belsis P., Skourlas C., Pantziou G.: A pervasive. (2008)," A Pervasive architectural framework for providing remote medical."1st International Conference on Pervasive Technologies Related to Assistive Environments, Greece p. 23

[12] Walker, W P, Aroul, A. L Praveen, Bhatia, Dinesh K.,(2009) "Mobile health monitoring systems" EMBC,2009 Annual International Conference of the IEEE pp. 5199-5202, IEEE,Minneapolis, MN

[13] Figueredo M.V.M and Dias J.S. (2004), "Mobile telemedicine system for home care and patient monitoring," 26th Annual International Conference of the IEEE EMBS.San Francisco, CA, USA (2), pp. 3387-3390.

[14] Chao K M, Anane R, Plumley J, Godwin N, Naguib R N G,(2001), "A Mobile Agent Framework for Telecardiology",Proceeding of the 23rd Annual EMBS InternationalConference, Istanbul, Turkey

[15] O'Donoghue, J., Herbert,J.and Stack P. (2006), "Remote Non-Intrusive Patient Monitoring," 4th International Conference on Smart Homes and Health.IOS Press.

[16] Burstein, F. A., Zaslavsky, A. B., and Arora, N. B. (2005), "Context-aware Mobile Agents for Decision-making Support in Healthcare Emergency Applications", Workshop on Context Modeling and Decision Support. Paris.

[17] Francesco D. M., Giacomo C., Nicola M., Raffaele Q., Franco Z.(2006), "The UbiMedic Framework to Support Medical Emergencies by Ubiquitous Computing, "International Transactions on Systems Science and Applications, I(1), pp.15-26.

AUTHORS PROFILE

Akomolafe Oladeji Patrick (Ph.D) is a Lecturer at the Department of Computer Science , University of Ibadan . He obtained a Bachelor of Technology (B.Tech) in Computer Engineering at Ladoke Akintola University of Technology, Ogbomoso (LAUTECH) in 1999, a Master of Science Degree (M.Sc) in Computer Science at the University of Ibadan in 2004 and a Ph.D Degree in Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2014. His research interests include Pervasive and Mobile Computing, Mobile Agent Technology, Context Aware Computing and Software Engineering. He can be reached at akomspatrick@yahoo.com.

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

State of the Art: Vehicle-to-Vehicle Information Exchange

Abdelsalam Obeidat
Software Engineering Dpt., College of Information Technology
World Islamic University for Science and Education
Jordan, Amman

Adnan Shaouot
The Electrical and Computer Engineering
The University of Michigan-Dearborn
Dearborn, MI 48128

Atef Nsour
Computer Engineerng Dpt., College of Engineeering
Yarmouk University ,Irbid, Jordan on sabbatical leave in
World Islamic University for Science and Education
Jordan, Amman

Nidal Al-Omari
Software Engineering Dpt., College of Information Technology
World Islamic University for Science and Education
Jordan, Amman

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

ABSTRACT

As with most 'new' ideas and technologies, there is not much 'new' involved in the basic concept but just with the implementation. The idea of vehicle-to-vehicle communication dates back to the widespread implementation of wireless communication devices and the need for passengers of one vehicle to communicate with those of another. The purpose of this paper is to explore the past, present and potential future application of technologies that enable occupants of two separate vehicles to exchange messages. Whether the intent is safety, courtesy or emergency notifications, there is opportunity to provide this message exchange over a distributed system via a low cost portable device.

1.0 INTRODUCTION

Vehicle-to-vehicle communication is not a new concept. Like the notion of the when the first race occurred between motorized transportation devices, the first attempts at communication between two vehicles most likely occurred when at least two of them came in close proximity. Airplanes, trains, ships, heavy trucks, construction equipment, motorcycles and automobiles have been outfitted with a variety of devices and technologies to facilitate inter-vehicle communication.

Sailing ships relied on flags, Morse code via pencil beam lights and finally wireless. The technological path holds similar parallels for trains and airplanes. Regarding automobiles and heavy trucks, to provide commercial advantages, the path most likely started with the two-way radio transceiver utilizing the Citizen's Band of frequency ranges.

Over the road vehicles, such as heavy trucks, have the distinct need for relaying information. This information can consist of current road conditions, a potential equipment safety hazard, and a series of friendly exchanges to pass time or alternative routing information resulting from unexpected road delays.

The purpose of this paper is to explore past, present and potential future technologies that provide motorists, commercial and private, with the means to exchange information vehicle to vehicle while traveling. This information can be in the form of messages or emergency alerts that contribute to improved traffic flow, safety and shared understandings between drivers.

The scope of this paper will be limited to road going vehicles and will start with the Citizen's Band radio as this was the first readily accessible, widely applied inter-vehicle communication device that enabling motorists to exchange any information they felt relevant to the current situation.

The paper will start with past information exchange practices in section 2. Section 3 will cover the current vehicle communication services. Section 4 will explore the near-term future implementation of Dedicated Short Range Communication (DSRC). Section 5 provides the conclusion of the paper.

2.0 INFORMATION EXCHANGE OF THE PAST

CITIZENS BAND RADIO HISTORY

Citizens band radios have their roots in small two way radios that were first used in World War II. The citizens band (CB) radio was born out of the idea that there was a market for inexpensive two way radio service for private aircraft, boats and businesses. As businesses and individuals became licensed to use the frequency by the Federal Communications Commission (FCC), they found that there were all types of people, including truckers, interested in using the frequency.

CBs evolved into a mass market product in the 1970s during the oil crisis, independent trucker strikes, and it was popularized by TV, movies and songs. CB jargon and the appeal of the independent image of truckers appealed to many motorists who purchased CBs.

On the highway, truckers use it to relay information on road emergencies, traffic conditions and to stay in touch with the "road community" or base units at truck stops or in the home [2].

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

CITIZENS BAND DEFINITION

The Federal Communication Commission defines the Citizens Band (CB) Radio Service as a private two-way voice communication service for use in personal and business activities of the general public. Its communications range is from one to five miles.

There are 40 shared CB channels used on a "take-turns" basis. There are no channels authorized in the CB Radio Service above 27.405 MHz or below 26.965 MHz. Table shows general information about CB.

Citizens Band at a Glance	
Two-way voice communications service for use in personal and business activities. Its communications range is from 1 to 5 miles.	
Also Known As	CB
Service Rules	CFR, 95.4
Part Of	Personal Radio
Related Services	
General Mobile Radio Low Power Radio	
Included Services	
Family Multi-Use Radio Service	
Band Plan	
Band(s)	26.965-27.405 MHz

Table 1. Citizen Band Radio General Information

No CB channel is assigned to any specific individual or organization. Some fundamental rules of CB operation are:

- Be cooperative
- Keep your communications short.
- Users must never talk with another station for more than 5 minutes continuously and then must wait at least one minute before starting another communication.
- Channel 9 is used only for emergency communications or for traveler assistance [1].

CITIZENS BAND 'LANGUAGE'

The message exchange via CB radios follows natural language, CB "slang" and the FCC recognized standardization of CB Ten Codes.

Table 2 shows a sample of standardized CB Ten codes for the purpose of understanding the information normally shared via CB radios [3].

10-13 = Advise Weather/Road conditions
10-20 = My location is
10-23 = Stand by
10-30 = Does not conform to FCC rules
10-33 = EMERGENCY TRAFFIC
10-34 = Trouble at this station
10-35 = Confidential information
10-36 = Correct time is
10-37 = Wrecker needed at
10-38 = Ambulance needed at
10-42 = Traffic accident at
10-43 = Traffic tie up at
10-45 = All units within range please report
10-70 = Fire at
10-200 = Police needed at

Table 2. Standardized Citizens Brand 'Ten' code.

BENEFITS AND DRAWBACKS OF CB RADIOS

Following are some of the benefits of a CB radio:

- No license or subscription is required
- Basic understanding is required for operation
- Low cost and portable
- Network is local by nature
- Information is real-time and relevant
- Non-commercial and self-governing
- A free, dynamic and effective 'network'

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

Following are some of the drawbacks of a CB radio:

- User must constantly monitor – unable to interact with other passengers/all information is real time
- User must query for information – no queue or filter of information
- Information quality and depth is variable (ask for directions and you may or may not receive data)
- Transmit and receive quality can be marginal – radio interference or power variances
- Range is limited and dependent on user's equipment
- Popularity among non-professional motorists is low

SUMMARY

The Citizens Band Radio was, and still is, an effective low cost method of vehicle-to-vehicle communication for commercial and private applications. As noted in the drawbacks there are user interface and quality issues that have room for improvement.

Vehicle to Vehicle - Arbitrary

Amazingly, there have not been any significant advances in mass market vehicle to vehicle communication devices. To scope this statement, currently there does not seem to be any devices available, other than the CB radio, that allow a user to arbitrarily broadcast and receive messages to or from vehicles in close proximity. In addition, the probability of a fellow, non-commercial, motorist having a CB Radio in their vehicle is low.

Popularity of these devices has declined significantly from their days when they had become so ubiquitous that automotive manufacturers included them as factory options in many models. The CB Radio was offered as an integrated factory option as recently as 1985. Today, no automotive manufacturer is offering a CB Radio as a regular production option

However, the story is not the same for commercial applications. Professional heavy truck operators still rely on the Citizen's Band Radio for on the road exchange of important proximate information between each other while on the highway.

General Broadcast

General Broadcast is defined as a receive only scenario where information sent to a receiver, such as a standard car AM/FM car radio tuned to a user selected frequency. The user is dependent on the broadcasters at this frequency to relay information of local conditions such as traffic flow, traffic accidents or general emergencies.

The listener must interpret the information in real-time to understand any potential impacts to their intended direction of travel. The quality and depth of information is dependent on the broadcaster which is usually covering a wide geographic area. The user cannot query for information regarding their proximity.

The primary form of General Broadcast is via an audible format. There is another format that has been available for a few years mostly in General Motors products. This format is called RDS or Radio Data System.

RDS was developed by Swedish Telecom in 1976 as a method of sending data to radio pagers. In the early 1980s, the European Broadcasting Union changed it to the Radio Data System (RDS). The U.S. National Association of Broadcasters (NAB) adopted a standard for it in 1993. British Broadcasting System (BBC) is also a user of the system.

In the United States, FM radio stations are allocated 200 KHz of bandwidth. (In Europe, it is 100 KHz.) The station does not fill all of this bandwidth with music. RDS is a completely separate radio signal that fits within the station's frequency allocation. It carries digital information at a frequency of 57 KHz, with a data rate of 1187.5 bits per second. RDS transmits data simultaneously with a standard FM stereo (or monophonic) radio broadcast. Possible uses include transmitting song titles, station call signs, and signaling when traffic or weather reports are being broadcast [4].

The primary benefit of this system is that the vehicle operator is able to receive information without the need for a query and will receive notification vehicle an indicator on their car radio's display. The user can then push a button to obtain a text display of the information being broadcasted. The information is continually broadcasted so the user can re-query the information if some part of the broadcast is missed.

Again, though, the user is dependent on the quality of information being broadcasted. Fundamentally, the United States utilization of this system is limited to manufacturers who install the RDS reception capability and the exploitation of this system's usage has been limited to song titles, station call letters and the occasional tagline or seasonal greeting message.

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

The European implementation of this technology is more extensive where users notified the pertinent information is being broadcast and directed to a pre-defined RDS station where the information will be broadcast. The following description illustrates Europe's expanded utilization of this system [5]:

RDS Travel News

Apart from the station name, this is probably the most useful and visible part of the RDS system. When a radio station starts a travel report, they instruct their transmitter site to switch on the RDS TA travel flag. Radios with RDS can see this flag, and get the radio to tell the listener that there's a travel report. A radio can do this by interrupting the tape or CD that's playing, or by increasing the volume, to get the listener's attention. This is an incredibly useful service for motorists, and by listening to a local radio station, you can keep up-to-date with local road conditions and travel flashes, without having to listen to the station's DJs, music and commercials.

3.0 CURRENT METHODS OF INFORMATION EXCHANGE

Telematics

Telematics is a combination of telecommunication and informatics: a telematics service is one that provides information to a mobile source, like a cell phone, PDA or car. Today telematics often describes vehicle systems that combine GPS and cellular technologies with onboard electronics. They can include safety, communication, vehicle diagnostic capability, and entertainment features [6].

The adoption and long-term commercial viability of these services has been somewhat questionable. Initially, the excitement of this new term 'telematics' and the promises surrounding it were viewed as the future of motoring in regard to efficiency, safety and productivity. Significant capital was poured into development of systems that were thought of as a new revenue opportunity for **O**riginal Equipment Manufacturers (OEMs) that would build loyalty and revenue. In many cases, however, this did not prove true.

The idea behind telematics is that millions of car owners eventually will pay monthly subscription fees for all sorts of telecom-related services, which can include anything from customized traffic reports to the automatic reporting of accidents. But, as with so many other telecom-related profit schemes hatched in the 1990s, telematics has found itself on a rocky road to mass consumer acceptance. It has not yet been proven that people who already pay for cell-phone service will eagerly sign up for a telematics offering, even if it includes services they cannot get via their handset [16].

Per comments of Jerry Flint, an established automotive journalist for Forbes magazine, "General Motors (nyse: GM - news - people) puts its OnStar telematic equipment in many of its new vehicles for free (meaning the cost of the equipment is buried in the car price) and gives a year of free service. But the money only comes when owners sign up after that initial year. So far, the renewal rate isn't terrific.

People do like phones in their cars, that's for sure. But almost everyone already seems to own a cell phone, and many folks even use them in their cars, despite various new laws.

Lots of people may also want the new satellite radio service and be willing to pay extra for it, but that's still unknown. But the other services just haven't caused much excitement.

There's also some feeling that the auto companies shouldn't be the providers of telematic hardware or services, that they should make the cars and leave the wireless business to the experts. Advances in electronics often come faster than new vehicle development, which means that carmakers could be installing outdated or incompatible electronic technology." [17]

One such example is the failed Wing Cast joint venture and its telematics product that was to be offered by Ford Motor Company. Wingcast was to deliver information services, voice, entertainment, Internet access, and safety services to cars and trucks. The general idea being that a driver would have a computer generated voice that out of the blue as you're driving down the freeway saying you needed brake fluid and that a service station is two miles west at the next exit. Ford dissolved the joint venture in 2002.

General Motor's OnStar system was one of the first North American mass-market offering of a telematics service. Today, it is developing new services and evolving its technology. Other OEMs, such as Honda and Audi contracted with OnStar to offer the service in their products. However, as of this model year, General Motors is not renewing those contracts to keep OnStar as a GM product exclusive feature.

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

General Motors began offering OnStar in 1996 as an automotive safety tool -- a way for people to get help easily and quickly in an emergency. Instead of trying to find your cell phone, you push a button on a console and are instantly connected with an OnStar advisor. The advisor can pinpoint your exact location and relay your problem to emergency services. If you're in an accident, your car can "tell" OnStar without you having to do a thing [6].

OnStar consists of four different types of technology: cellular, voice recognition, GPS and vehicle telemetry. All of the services that OnStar provides are a result of one or more of these technologies working together [7].

As an interesting side note, OnStar, available in Europe via the Opel brand, closed down in November 2005 resulting from poor sales. This poses an interesting theoretic correlation between Europe's more extensive implementation of the free Radio Data System and its overlap with some of the services offered by OnStar [6].

Other automobile manufacturers have similar systems marketed under with their own brand name. These telematics services offer a great deal of features and the added sense of security by always having someone to contact for the trivial to the serious. Table 3 provides an overview of the OEM telematic products currently available.

Current OEM Telematics Offerings and Features					
Product Name	Onstar	RESCU (Remote Emergency Satellite Cellular Unit)	VCS (Vehicle Communication System)	ASSIST	On-Call
Year Introduced	1996	1996-2001	2001 (No Longer Offered)	2001	2002
Manufacturer	General Motors OnStar Division	Ford Motor Company/ Motorola	Ford Motor Company/ ATX Technologies/ Sprint PCS	BMW/ Vodaphone	Volvo
Form Factor	Integrated with Vehicle/ Not Portable	Integrated with Vehicle/ Not Portable	Fully transportable digital/analog Motorola Timeport phone	Integrated/ Not Portable	Integrated/ Not Portable
Features					
Hands Free Cellular Phone	x		x	x	
Automatic Emergency Notification	x		x	x	x
Driver-initiated emergency	x	x	x	x	x
Roadside Assistance	x	x	x	x	x
News and Information Service	x		x	x	
Routing/Directions (non-Real Time)			x	x	x
Real Time Navigation	x				
Internet/Email access	x				
Stolen Vehicle Recovery	x			x	
Vehicle Service Scheduling				x	
Vehicle Diagnostic Capability	x				

Table 3. Current OEM telematics product offerings

However, as sophisticated and providing as these services are, there are significant drawbacks. The user must pay monthly fee for use of the telematics system. There is no facility to contact the person in the vehicle traveling next to you or, to that end, contact the driver of any vehicle. Localized information is available based on your

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

current geographic position but all communication is via the telematics subscriber and the telematics provider representative – which, aside from the technical investment, is a contributor for the monthly subscription cost.

Cellular Phone with 'Walkie-Talkie' feature

A current service offering from the major cellular service providers is a 'walkie-talkie' which can be summarized as on demand digital two way communication among subscribers. This cellular phone based communication medium is no different, in concept, than original Police Dispatch radio communication system.

The digital two-way radio service uses a half-duplex signal. A normal cell phone call uses two separate frequencies, one to send and one to receive, for each call while the two way system uses only a single frequency.

The system uses the proven technology of Push To Talk (PTT), commonly used in dispatch radio systems. PTT requires the person speaking to press a button while talking and then release it when they are done. The listener then presses their button to respond. This way the system knows which direction the signal should be traveling in.

The cellular service subscriber defines the intended recipient(s) of their 'broadcast' messages, of whom, must be subscribers to the same system.

This method of communication is now common practice among businesses where direct, responsive information exchange is necessary. Examples of a vehicle to vehicle application would be a landscaping or waste hauling business where it is critical and efficient for drivers or dispatchers to contact other drivers for real-time routing and/or coordination information.

Nextel, the first major cellular provider to offer this feature, uses a network based on Motorola's Integrated Digital Enhanced Network (iDEN) and makes, what Nextel has branded as, Direct Connect possible. It uses the 800 MHz portion of the radio spectrum assigned to specialized mobile radio (SMR) service. The iDEN network uses TDMA technology to split a 25 KHz frequency into six separate time slots [7].

TDMA technology is short for Time Division Multiple Access, a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA is used by the GSM (Global System for Mobile Communications) digital cellular system [8].

GSM is one of the leading digital cellular systems and uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency. GSM was first introduced in 1991. As of the end of 1997, GSM service was available in more than 100 countries and has become the de facto standard in Europe and Asia [8].

Verizon wireless, another major cellular service provider, utilizes CDMA technology in its version of a PTT (Push To Talk) network [9]. CDMA stands for Code-Division Multiple Access, a digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which third generation wireless technologies (the first being analog and the second being digital Personal Communication Service) are built [10].

This 'Walkie-Talkie" communication schema is the closest known digital based method emulating the fundamental vehicle to vehicle communication services of the CB Radio. However, like current telematics services, the users of the system must also be subscribers, via monthly services and using dedicated equipment, to the same service provider. In addition, the users are 'locked' into a predefined network of contacts. The broadcaster is targeting the message to known nodes on the network.

On December 17, 2003 the Commission adopted a Report and Order establishing licensing and service rules for the Dedicated Short Range Communications (DSRC) Service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850-5.925 GHz band (5.9 GHz band).

The DSRC Service involves vehicle-to-vehicle and vehicle-to-infrastructure communications, helping to protect the safety of the traveling public. It can save lives by warning drivers of an impending dangerous condition or event in time to take corrective or evasive actions. The band is also eligible for use by non-public safety entities for commercial or private DSRC operations [11]. Table 4 provides general information regarding DSRC.

Dedicated Short Range Communications (DSRC) Service at a Glance	
Facilitates the use of radio-based technologies to improve traffic flow and traffic safety as well as to assist the traveling public.	
Also Known As	DSRC
Established	2004

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

Service Rules	CFR, Part 90 and 95
Part Of	Intelligent Transportation Service
Related Services	
Location and Monitoring Service	
Band Plan	
Band(s)	5.850-5.925 GHz
Block Size	10 MHz channels some of which can be aggregated to 20 MHz
Market Areas	MSA/RSA
Licensing	
Non-exclusive for area of operation with site registration	

Table 4. DSRC General Information.

The adoption of the DSRC standard under the umbrella of services provided by the Intelligent Transportation System (ITS) has provided guidelines to continue development of a roadway available communication system to be used for the purpose of integrating radio-based technologies into the nation's transportation infrastructure and to develop and implement the nation's intelligent transportation systems [12].

The standard has spurred numerous special interest groups, studies, proposed standards that are building a foundation for protocols, robustness and practical application of a network that will enable occupants and the vehicles themselves to share information while traveling on the roadways.

4.0 FUTURE VEHICLE TO VEHICLE COMMUNICATION METHODS

Starting in 2004, a Special Interest Group (SIG) of the Association for Computing Machinery (ACM), SIGMOBILE holds an annual conference called VANET or Vehicular Ad Hoc NETworks. VANET applications will include on-board active safety systems leveraging vehicle-vehicle or roadside-vehicle networking. These systems may assist drivers in avoiding collisions. Non-safety applications include real-time traffic congestion and routing information, high-speed tolling, mobile infotainment, and many others [13].

The goal of the workshops is to explore the development of wireless vehicular ad hoc networking (VANET) technologies. Enabled by short- to medium-range communication systems (vehicle-vehicle or vehicle-roadside), the VANET vision includes vehicular real-time and safety applications, sharing the wireless channel with mobile applications from a large, decentralized array of commercial service providers [14].

In addition to the VANET workshops, the idea of vehicle to vehicle communication has been a topic of study for some time. A technical paper authored in October of 2000, "Disseminating Messages Among Highly Mobile Hosts based on Inter-Vehicle Communication", used direct radio communication between moving vehicles on the road that requires no other infrastructure.

The authors propose a communication network that is decentralized using omni-directional antennas to allow senders to transmit to multiple hosts simultaneously. The authors study a road accident as an example and the potential number of vehicles "in a zone of relevance" would be informed [15]. There is no question that this is a modern, more intelligent version of the CB radio as a tool for information exchange on roadways.

Appendix 1 contains a table identifying other technical papers relating to DSRC and a categorization of the paper's fundamental focus for quick reference.

As shown in the Appendix 1 table, there has been much research and many proposals to address the challenges presented by the implementation of a wireless, digital, ad-hoc vehicle to vehicle communication system.

Ad-hoc networks are a popular choice for implementation of DSRC because of their ease of deployment. There is no wired infrastructure to support and hosts communicate via packet radios [18].

Based on the collection of papers in Appendix 1, the areas of traffic prediction and analysis are the foundation to understanding the potential security threats and real-time operating constraints for protocol development.

The variability of mobility, bandwidth and power constraints pose the greatest challenges to establishing and maintaining single and multi-hop routes. Some studies show that on-demand protocols are better suited for mobile networks because of low overhead and efficient management. Simulations indicate providing multiple routes aid robustness [18].

With the vision of vehicle based ad-hoc networks providing frequent exchange of data by vehicles to facilitate route planning, road safety and e-commerce applications, network security is an important facet of any implementation. In a

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

vehicular ad-hoc network erroneous or intended modification of data can have serious impacts. For example, transmitting fraudulent data about road congestion or vehicle position can have serious impacts [19].

Along with the exploration and proposal of security models, high vehicle densities pose significant challenges in regard to the bandwidth of channels reserved for the exchange of safety-related information. There is a perceived 'fairness' problem that arises in situations in which vehicle send periodic 'beacon' messages to inform other vehicles in the surrounding area (velocity, direction) in order to improve safety conditions [20].

The 'fairness' problem is derived from the idea that every vehicle will be able to send and receive data packets into/from a share medium. For North America (FCC), the DSRC frequency range will be divided into 7 seven different channels, 1 control channel and 6 service channels. The control channel is reserved for the exchange of safety messages. Therefore, all vehicles will have to poll this channel in a timely manner to deliver a safety message to serve the message's intentions. It is assumed that two types, event driven and periodic, of safety messages will be implemented to address priority needs [20].

Event driven messages would be triggered resulting from an unsafe condition like an accident. Periodic messages would fall into a classification of messages that are more preventative in nature like weather alerts or icy conditions reported in the current direction of travel. When vehicular ad hoc networks are fully deployed, high vehicle densities could lead to overloading the control channel capacity to allow both periodic and event-driven safety messages [20].

A proposal to alleviate a potential bandwidth utilization issue is achieved through a 'fair power control' strategy where the transmission power of localized nodes is reduced by the same ratio to reduce the number of receivers of periodic messages in high density areas [20].

There are other proposals/analyses that indicate non-safety (non control channel) messages will not be handled by ad-hoc networks but, instead, by road side units (RSU) using a DSRC hot-spot model.

Table 5 is taken from [21] where message types are classified and associated with preliminary message requirements base on the preliminary evaluations of the authors.

Application	Packet Size (Bytes) /Bandwidth	Allowable Latency (ms)	Network Traffic Type	Comm. Range (m)	Priority
Intersection Collision Warning / Avoidance	~100	~100	Event	50 – 300	Safety of Life
Cooperative Collision Warning	~100/ ~10Kbps	~100	Periodic	50 – 300	Safety of Life
Work Zone Warning	~100 ~1Kbps	~1000	Periodic	50 – 300	Safety
Transit Vehicle Signal Priority	~100	~1000	Event	300 – 1000	Safety
Toll Collection	~100	~50	Event	≤15	Non-Safety
Service Announcements	~100/ ~2Kbps	~500	Periodic	0 – 90	Non-Safety
Movie Download (2 hours of MPEG 1) : 10 min. download time	> 20Mbps	N/A	N/A	0 – 90	Non-Safety

Table 5. DSRC Message classification [21].

The table illustrates a typical latency and range values of 100 and 500 msec and 50 to 300 meters respectively. Since DSRC is based on the IEEE 802.11a standard, 300 meters is the maximum distance a small message can be sent. The authors assume then that 300 meters is a sufficient distance for a safety related message to cover and, therefore, a single hop broadcast is appropriate [21].

The idea of the RSU hot spot causes issues with bandwidth utilization to balance the need of high-priority safety communication but still maintain high levels of information exchange with the RSU. This model indicates that an uncoordinated ad hoc protocol for safety messaging is not ideal. Therefore, a coordinated approach, illustrated by the following figure is one proposal to resolve the theoretical issue.

The fundamental theory of operation is a node can be any one of three states where Ad-Hoc is the default state where vehicle exchange safety messages without the aid of any infrastructure. Once receiving an Access Point (AP) message from an RSU, the state will switch to Ad-Hoc Coordinated where nodes are coordinated and remain quiet unless polled by the AP. A state diagram of this operation is shown in figure 1 [21].

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

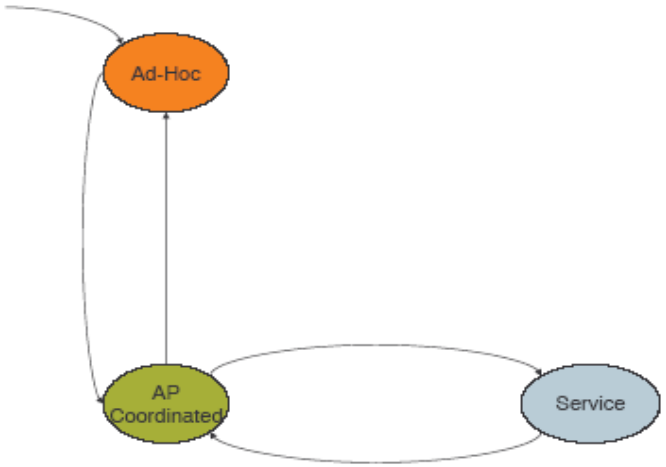


Figure 1. Ad Hoc vs. Ad Hoc Coordinated Operation [21].

Although somewhat conflicting, the two communication bandwidth proposals commonly identify the need to meet messaging requirements for safety critical message transmitted and received on the control channel.

Safety critical messages will need to be serviced under the constraints imposed under a hard real-time operating system. This is true based on the priority of the message but also to meet protocol messaging constraints because of the highly dynamic nature of a vehicular ad-hoc network.

Proposing the scenario of vehicle to roadside communication between an intersection traffic light controller, the authors of [22] identify the need for time constrained communication. The intersection light controller could be informed of a vehicle's impending arrival and change the light sequence to allow the vehicle to pass without interruption. However, with multiple vehicles approaching the same intersection, the need to meet communication deadlines with sound message coordination and arbitration is absolute to prevent potential catastrophe.

The authors focus on a product called RT-STREAM but the concept of a Space-Elastic model is introduced. This core concept is identified as a need for meeting hard deadlines in a vehicular ad hoc network where the dynamics impact the real-time guarantees available within a proximity bound. This Space-Elastic model assumes real-time applications are space aware and a defined proximity bound is adaptable to ensure real time requirements are met [22].

In [23] authors discuss the reliability of inter-vehicle communication in a traffic stream, dependent on the distribution of equipped vehicles. With the assumption that information propagation is instantaneous compared to vehicle movements, the reliability is measured by the probability of
success for information to travel beyond a location; stochastic models are presented for both uniform and general traffic streams.
In the models, the traffic stream is divided into a series of cells based on the transmission range, the structure of possible most-forward-within-range communication chains is clarified, the probabilities for information to travel to and beyond a vehicle at a certain hop are computed regressively, and the lower bound of the absolute success rate for information to travel beyond a point is determined [23].
Based on the models, authors examine the performance of information propagation for different penetration rates, transmission ranges,and traffic scenarios that include gaps and shock waves[23].
Proposing a methodology which is based on a matrix representation that enables the definition of specific metrics,which can then be used for further evaluation[24]. Authors gather relevant project information, then define and apply a methodology for handling this information, and to compare and draw some general conclusions about the nature of projects carried out in Europe, USA and Japan[24].

Authors of [25] Proposed an intelligent traffic system based on intervehicle communication networks and grid technology is
proposed. This system adopts hybrid architecture, and diverse real-time traffic services are provided in a centralized or decentralized way. Grid technology is introduced to provide the high performance computing platform for massive traffic data processing and real-time traffic service presenting.

. Taking advantage of ubiquitous smartphones authors of [26] develop an Inter-vehicle communications (IVC) system based on smartphones, called SPIVC. In this system, smartphones on vehicles communicate with a central server and share traffic information with each other. Field tests are carried out on both WiFi and 3G networks to determine the accuracy of GPS devices and communication delays between vehicles. A communication model is developed to explain communication delays. It is found that location errors are about 4 meters after warm-up, and communication delays are in the order of seconds and depend on the frequency of location updates in GPS devices. The SPIVC system, which can be centralized or decentralized, holds great promises for an array of multimodal transportation applications that are not very sensitive to GPS accuracy and communication delay.
The continuous increase in the number of vehicles in the transportation system calls for an improvement of traffic safety and efficiency of Inter vehicle communication. To achieve this demand, the vehicular communications have been considered to enable various security issues on vehicles is to obtain the traffic safety. Effective implementation of vehicular communication could also improve traffic management system. Inter-Vehicle communications are emerging as a new class of wireless networks enabling mobile users in their vehicles to communicate to the roadside and to each other. Safety related applications require asecure and reliable system[27].

5.0 CONCLUSION

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

Vehicle to vehicle communication is about to be reinvented. The approval of the DSRC frequency range and the governing organizations in place to oversee its utilization will allow significant improvements in information exchange between motorists.

Circling back to initial discussion of CB radios and their benefits and drawbacks, we can evaluate these identified pros and cons from the perspective of a DSRC based ad-hoc communications system implementation. Table 6 presents the various Vehicle to Vehicle communication technologies benefits and drawbacks.

	Citizens Band Radio	Radio Data System	Telematics	DSRC Based Ad-Hoc Network (Proposed Concepts)
Benefits				
No license or subscription is required	x	x		x
Only basic understanding is required for operation	x	x	x	x
Low cost and portable	x	x		x
Network is local by nature	x			x
Information is real-time and relevant	x	Not relevant	x	x
Non-commercial and self-governing	x			x
A free, dynamic and effective network	x			x
Drawbacks				
User must constantly monitor – user unable to interact with other passengers/all information is real time	x			
User must query for information – no queue or filter of information	x		x	Dedicated channel can interrupt for safety related information - user need not query
Information quality and depth is variable (ask for directions and you may or may not receive data)	x	x		True for asynchronous queries by user of other users. Re: Navigation - Road Side Units can/will transmit navigation information locally and GPS based navigation maps supplement
Transmit and receive quality can be marginal – radio interference or power variances	x			Expected to equivalent or superior to modern Cellular phone
Range is limited and dependent on user's equipment	x	x		(Multi-hop Capability extends range)
Popularity among non-professional motorists is low	x	x (North America)	x	Unknown

Table 6. Vehicle to Vehicle Communication Technologies benefits and drawbacks

Based on the above evaluation, it is evident that, if actual implementation occurs as discussed in published technical papers, an ad-hoc DSRC based network will meet all the vehicle to vehicle communication benefits of the original CB radio. In addition, nearly all the identified drawbacks would not be carried through. This includes elimination of the deficiencies in the current RDS and telematics offerings.

The improvements over the original CB Radio will be in the quality of information, delivery methods and the ability for the user to query or arbitrarily receive critical and non-critical information. The significance of this information is that it will be location centric to improve the safety and efficiency of all motorists accessing the network.

The network for communication will be a distributed ad hoc system. Users will have free, passive access to the information and the devices used for access will be low cost or possibly no-cost based on the thought that the standard car radio will most likely incorporate DSRC capabilities as new generations of standard radio chipsets are created.

6.0 REFERENCES

1. Federal Communications Commission, Wireless Telecommunications Board, Services, "Citizens Band (CB) – Service Description and Fundamental Operation", - http://wireless.fcc.gov/services/index.htm?job=service_home&id=cb.
2. Institution, National Museum of American History, "America on the Move Collection", Smithsonian - http://americanhistory.si.edu/onthemove/collection/object_101.html
3. CB Radio Operators Webring, "CB Ten Codes", operated by the defpom - http://www.radiomods.co.nz/10codes.html
4. howstuffworks.com, "How is my radio able to display the station's call letters?", , - http://electronics.howstuffworks.com/question323.htm
5. radioandtelly.com, "RDS - standing for the Radio Data System", http://www.radioandtelly.co.uk/rds.html
6. howstuffworks.com, "How is my radio able to display the station's call letters?", http://electronics.howstuffworks.com/question323.htm
7. howstuffworks.com, "How OnStar Works ", http://auto.howstuffworks.com/onstar.htm
8. webopedia.com, "What is GSM?", http://www.webopedia.com/TERM/G/GSM.html
9. Steve Punter's Southern Ontario Cell Phone Page, "PCS Technologies", http://www.arcx.com/sites/Technical%20Comparison.htm
10. webopedia.com, "What is CDMA?", http://www.webopedia.com/TERM/C/CDMA.html
11. Federal Communications Commission, "Dedicated Short Range Communications (DSRC) Service", http://wireless.fcc.gov/services/index.htm?job=service_home&id=dedicated_src

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

12. Federal Communication Commission, "Intelligent Transportation Systems (ITS)", http://wireless.fcc.gov/services/index.htm?job=service_home&id=intelligent_ts
13. ACM/SIGMobile, "The First ACM International Workshop on Vehicular Ad Hoc Networks - Scope", http://www.sigmobile.org/workshops/vanet2004/
14. ACM/SIGMobile, "The Second ACM International Workshop on Vehicular Ad Hoc Networks - Scope", http://www.sigmobile.org/workshops/vanet2005/
15. Briesemeister, Schaefers, Hommel, "Disseminating Messages Among Highly Mobile Hosts based on Inter-Vehicle Communication", Paper presented for the Vehicular Ad Hoc Networks Workshop 2005.
16. Lewis, Mark , "Ford Grounds Its Wingcast Venture", Forbes Magazine, June, 2002
17. Jerry Flint, "Too Much Car Gadgetry?", Forbes Magazine, May 2002.
18. Lee, Sung-Ju, "Routing and Multicasting Strategies in Wireless Mobile Ad Hoc Networks", Dissertation for Doctorate in Philosophy in Computer Science, University of California, 2000
19. Golle, Greene, Staddon, "Detecting and correcting malicious data in VANETs", ACM/VANET Workshop, 2004
20. Torrent-Moreno, Paolo, Hannes, "Fair sharing of bandwidth in VANETs", ACM/VANET Workshop, 2005
21. Mak, Laberteaux, Sengupta, "A multi-channel VANET providing concurrent safety and commercial services", ACM/VANET Workshop, 2005
22. Hughes, Meier, Cunningham, Cahill, "Towards Real-Time Middleware for Vehicular Ad-Hoc Networks", ACM/VANET Workshop, 2004

23. Wen-Long Jin _and Wilfred W. Recker "Instantaneous Information Propagation in a Traffic Stream through Inter-Vehicle Communication" Wen-Long Jin _and Wilfred W. Recker May 20, 2005

24.Lars Strandén, Elisabeth Uhlemann, and Erik Ström, "Wireless Communications Vehicle to-Vehicle and Vehicle-to-Infrastructure", *Project no: AD4, SAFER - Vehicle and TrafficSafety Centre,* April 2008.

25. Wen-Long Jin1, Candy Kwan, Zhe Sun, Hao Yang, Qijian Gan " A SmartPhone-based Inter-Vehicle Communication System" International Journal of Vehicle Information and Communication Systems, November 15, 2011
26 M.V.B.T.Santhi, K.Deepthi, Ch.Satya Keerthi .N.V.L,P.Lakshmi Prasanna" Security Issues on Inter-Vehicle Communications" International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011.

APPPENDIX 1 – Technical papers related to DSRC.

Select Papers on Vehicular Ad Hoc Network and Dedicated Short Range Communication (DSRC)									
			Focus Area of Paper						
Paper Name	**Author(s)**	**Year Issued**	**Protocol**	**V2V Traffic Prediction and Analysis**	**Network Robustness**	**Security**	**Messaging and Bandwidth Usage**	**Simulation**	**Summary**
Security in VANET: Detecting and correcting malicious data in VANETs	Philippe Golle, Dan Greene, Jessica Staddon	Oct-04				x			An approach to evaluating the validity of Vehicle Ad Hoc Network Data

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

Analyzing the spread of active worms over VANET	Syed A. Khayam, Hayder Radha	Oct-04		x		x			Defines the average degree of a Vehicle Ad Hoc Network node using freeway traffic parameters and the spread of a worm in congested and low-density traffic scenarios.
Fair sharing of bandwidth in VANETs	Marc Torrent-Moreno, Paolo Santi, Hannes Hartenstein	Sep-05	x				x		Addresses the challenge of how to share the limited wireless channel capacity for the exchange of safety-related information in a fully deployed vehicular ad hoc network.
Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks	Marc Torrent-Moreno, Daniel Jiang, Hannes Hartenstein	Oct-04	x		x		x		Attempts to gain an understanding of broadcast message reception probability, establish message priorities for improved reception by another car depending on its proximity to the sender.
Performance evaluation of safety applications over DSRC vehicular ad hoc networks	Jijun Yin, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, Timothy Talty	Oct-04		x	x		x		Simulation study of the DSRC physical layer to judge the link bit error rate performance under a wide variety of vehicles speeds and multi-path delay spreads and simulation test bed for a DSRC vehicular ad hoc network executing vehicle collision avoidance applications.
The security of vehicular ad hoc networks	Maxim Raya, Jean-Pierre Hubaux	Nov-05	x			x			Provides a detailed threat analysis, appropriate security architecture and a set of security protocols.
VITP: an information transfer protocol for vehicular computing	Marios D. Dikaiakos, Saif Iqbal, Tamer Nadeem, Liviu Iftode	Sep-05	x						Introduce the Vehicular Information Transfer Protocol (VITP), an application-layer communication protocol, which is designed to support the establishment of a distributed, ad-hoc service infrastructure over Vehicular Ad Hoc Networks
An integrated mobility and traffic model for vehicular wireless networks	David R. Choffnes, Fabián E. Bustamante	Sep-05		x				x	Analyzes ad-hoc vehicular wireless network performance according to a simplified vehicular traffic model on roads defined by real map data, demonstrates that protocol performance varies with the type of urban environment and identifies the need for and network traffic simulators for ad-hoc network applications.
A multi-channel VANET providing concurrent safety and commercial services	Tony K. Mak, Kenneth P. Laberteaux, Raja Sengupta	Sep-05	x						Proposes a medium access control (MAC) protocol to support the multi-channel operation for dedicated short range communication (DSRC).

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

Vehicle-to-vehicle safety messaging in DSRC	Qing Xu, Tony Mak, Jeff Ko, Raja Sengupta	Oct-04	x				x		Proposes several random access protocols for medium access control which are compatible with the Dedicated Short Range Communications (DSRC) multi-channel architecture.
Disseminating Messages Among Highly Mobile Hosts based on Inter-Vehicle Communication	Briesemeister, L.; Schafers, L.; Hommel, G.;	Oct-00	x	x			x	x	Presents an approach to distributing messages among highly mobile hosts in ad hoc networks using direct radio communication between moving vehicles on the road that requires no additional infrastructure.
Routing and Multicasting Strategies in Wireless Mobile Ad Hoc Networks	Lee, Sung-Ju	Dec-00	x	x			x	x	PhD Dissertation exploring past and current multicast routing strategies and exploration of mobile ad-hoc network simulation and multiple protocol applications
A Multi-Hop Mobile Networking Test-Bed for Telematics	Rahul Mangharam, Jacob J. Meyers, Ragunathan Rajkumar, Daniel D. Stancil, Jayendra S. Parikh, Hariharan Krishnan, Christopher Kellum	Apr-05		x	x				Presents an onboard vehicle-to-vehicle, multi-hop wireless networking system to test emergency and safety messaging, traffic updates, audio/video streaming and commercial announcements to emulate the DSRC standard

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

IJCSIS AUTHORS' & REVIEWERS' LIST

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2015
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, 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/