Privacy Protected and Secured Wireless Sensor Network based E-Healthcare Monitoring System

M.Jayalakshmi[1],K.Maharajan[2], Dr.B.Paramasivan[3]

[1,2]Assistant Professor (SG)/CSE, [3] Prof&Head/CSE
National Engineering College
Tuticorin, Tamilnadu, (India)

ABSTRACT

This paper focus on how a wireless sensor network is used to sense the patient's body condition and how to transmit and receive the patient data to the patient database in a secured environment. The patient details including temperature, heartbeat, and blood pressure are sensed using appropriate sensors and stored in the server. The details are encrypted using Elgamal and Paillier key cryptosystem to ensure security. From the server, the encrypted data is fetched and decrypted after authentication. To secure the patient data from the inside attacks, a new data collection protocol[DCP] is proposed, where a sensor splits the sensitive patient data into three components according to a random number generation based on hash function and send them to servers via secure channels. Statistical analysis on the firmly distributed patient data which are accessible from the cloud environment can be performed without compromising the patients' privacy by using Paillier and Elgamal cryptosystems. By this approach, secure storage and communication to store and retrieve the patient data can be performed in a confidential mode.

Keywords-Wireless medical sensor network, patient data privacy, Paillier and Elgamal key cryptosystem.

I.INTRODUCTION

A wireless sensor network is a sensor network used to monitor physical or environmental conditions such as temperature, pressure, etc. and cooperatively pass the sensed data through the network to the main location [1]. The growth of wireless sensor network was supported by many industrial and consumer applications, such as industrial process monitoring, human healthcare monitoring, pollution and water quality monitoring, land slide detection, habitat monitoring and so on. Though there are many applications in the field of wireless sensor network, human healthcare applications takes the major role. In human healthcare, sensors are used to monitor the patient's health status such as temperature level, sugar level, heart beat rate, blood pressure. For instance, if the patient's sugar level is monitored 10 times per day then the data is updated in the database which is present in the local server. Likewise the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, viewing, updating, and storing the wrong values. Suppose if the intruder is trying to hack the patient details, there are many chances for the misuse of data which may lead to severe consequences. The data can also be modified by the hackers due to lack of security. The treatment prescribed by the doctors can be hacked which may even lead to death of the patients. Patients are the victims because of the above issues. This paper focuses on preventing these issues by developing a system which securely transmits the data. With the help of the proposed method it is possible to monitor network or system activities to identify the malicious activities and produces electronic reports to a management station. This is implemented by using two algorithms Paillier and ElGamal [2]key cryptosystems. Both the algorithms are used to encrypt the patient details before storing it in the database and perform decryption when needed by the physician. In order to propose the system effectively, the data is stored in the centralized server which is helpful for accessing the patient data any where any time when ever needed. The history of the patient details can be retrieved even after several years. Because of this type of secured environment in accessing the patient data in a centralized manner, the growth of medical application using wireless sensor has been rapidly increasing. Also wireless network has several advantages over wired network such as usability, reducing risk of infection and failure, comfortably in using the device by the patient, wireless applications produces possibilities for new applications in medical market. The rest of the paper is organized as follows. Papers related to this were discussed in Section II. Section III illustrates framework and architecture of the system for monitoring of patients. The working principle and implementation methodology of this proposed method is described in Section IV. Prospects of this system and its applications are briefed in the concluding section.

II. RELATED WORK

Xunyi et al [2] prevent the patient data from the inside attack by using multiple data servers to store patient data. The main contribution is securely distributing the patient data in multiple data servers and employing the paillier and ElGamal cryptosystem. To perform statistical analysis on the patient data without compromising the patient's privacy, a new data collection protocol is proposed; where a sensor splits the sensitive patient data into three components according to a random number generation based on hash function and sends them to three servers via secure channels. To keep the privacy of the patient data a new data access protocol on the basis of the paillier cryptosystem. The protocol allows the user to access the patient data without revealing it to any data servers.

Jong Hyun Lim et al [12] proposed staff shortages and an increasingly aging population is straining the ability of emergency departments to provide high-quality care. Moreover, there is a growing concern about the ability of hospitals to provide effective care during disaster events. Tools that automate patient monitoring would greatly improve efficiency, quality of care, and the volume of patients treated. Towards this goal, they have developed MEDiSN, a wireless sensor network for monitoring patients' vital signs in hospitals and disaster events. MEDiSN consists of Patient Monitors which are custom-built, patient-worn motes that sample, compress and secure medical data, and Relay Points that form a static multi-hop wireless backbone for carrying patient data. Moreover, MEDiSN includes a back-end server that persistently stores medical data and presents them to multiple GUI clients. MEDiSN's heterogeneous architecture enables it to address the compound challenge of reliably delivering large volumes of data while meeting the application's QoS requirements.

Neikato et al [1] proposed Scheme against global eavesdropping is used to avoid eavesdropping in the e-Health system and also it will provide privacy against a strong global adversary. It can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. Content oriented privacy concerns whether an adversary has the capability in disclosing the patients' PHI that he cares about by observing and manipulating the data transmitted over the communication networks. In an eHealth system, if any adversary has no ability to reveal the patient PHI, then the content oriented privacy is achieved. Contextual privacy means an adversary has the ability to link the source and the destination of a message. In eHealth systems, if an adversary can link the patient with a specific physician, then the patient privacy will be disclosed. Using SAGE the patient's privacy is secured.

Khaliq-ur-Rahman Raazi Syed Muhammad et al [10] proposed a Wireless body area networks (WBAN) consist of resource constrained sensing devices just like other wireless sensor networks (WSN). However, they differ from WSN in topology, scale and security requirements. Due to these differences, key management schemes designed for WSN are inefficient and unnecessarily complex when applied to WBAN. Considering the key management issue, WBAN are also different from WPAN because WBAN can use random biometric measurements as keys. They highlight the differences between WSN and WBAN and propose an efficient key management scheme, which makes use of biometrics and is specifically designed for WBAN domain.

KriangsiriMalasri et al [11] A medical sensor network can wirelessly monitor vital signs of humans, making it useful for long-term health care without sacrificing patient comfort and mobility. For such a network to be viable, its design must protect data privacy and authenticity given that medical data are highly sensitive. They identify the unique security challenges of such a sensor network and propose a set of resource-efficient mechanisms to address these challenges. Their solution includes (1) a novel two-tier scheme for verifying the authenticity of patient data, (2) a secure key agreement protocol to set up shared keys between sensor nodes and base stations, and (3) symmetric encryption/decryption for protecting data confidentiality and integrity. They have implemented the proposed mechanisms on a wireless mote platform, and their results confirm their feasibility.

Pengfei You et al [7] proposed sensor information system is a specific distributed information management system for applying sensor data and aims to effectively process, manage, and analyze data emanating from sensor networks. Recently, with the development of sensor networks, sensor information system encounters many challenges, such as huge and diverse data, heterogeneous clients, scalability, and security. In this paper, they propose an extensible and secure cloud architecture model for sensor information system. Firstly, they describe the composition and mechanism of the architecture model using cloud paradigm. Secondly, they design the security solution for accessing sensor data and information services inside the architecture. This security solution ensures legal access and use for sensor data and information services and avoids illegal breach for user data in the cloud environment. In particular, a certificate authority (CA) based Kerberos protocol is proposed to provide strong identity authentication. The simulation experiment results show that the architecture gets high performance and stability throughout, while keeping scalability and flexibility brought by cloud.

R.Rekha et al [9] proposed the body sensor node to base station communication has been secured using these symmetric key cryptographic algorithm AES and message authentication code. Data integrity is maintained by using the MAC function and hacking will be solved by using AES key distribution algorithm. SHA-1 algorithm will use for high performance for the wireless body sensor network. Stegnography is used for securing the data transfer between base station and medical server. In this work, we have embedded the medical data (Blood Pressure) within the patients' facial image. The face image is selected as a cover image in order to provide authentication. The pixel positions for embedding the medical data are determined by fixing a threshold level (120-126). This threshold value is chosen so as to have high random distribution throughout the image.

III.PROPOSED WORK

The proposed work consists of three phases such as Data Collection, User Authentication Module for Encryption and decryption and Patient Data Storage Phase. The proposed architecture shown in Fig.1 explains the overall system design. In Data Collection Phase the proposed algorithm is tested with three data sets. In the first dataset, the measurement of estimated average glucose, HBA1C, pp is given for the patient at different intervals. In the second dataset, the measurement of Red blood cell (RBC), White blood cell (WBC), Platelet Count, Haemoglobin is given for the patient at different intervals. In the third dataset, the measurement of Glucose, cholestrol, triglycerides is given for the patient at different intervals. Figure1 shows how the sensed patient's data collected from home and hospital are stored in database and the encrypted details are sent to the local server through wifi.

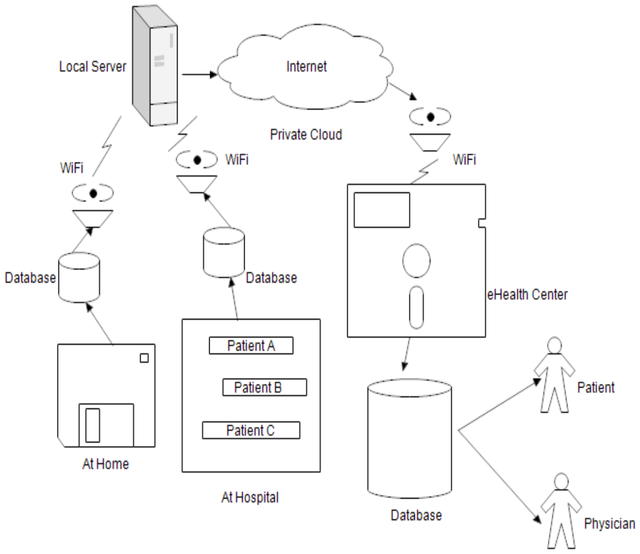


Fig.1. Depiction of System Design for Healthcare Analysis

In Authentication Phase Encryption has been performed using Paillier and ElGamal Key Cryptosystem Phase, the collected datasets are encrypted using paillier and elgamal key cryptosystem and stored in the local server. The patient details from the dataset can be retrieved from the local server by authenticated users. The doctor, patient, patient's family members are considered as authenticated users.

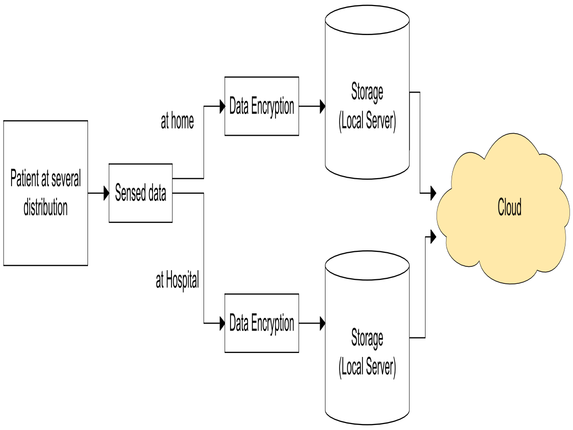


Fig. 2. Client side

The details are stored in local server, so that the authenticated user can retrieve the details even without internet connection. Then the encrypted details are stored in the private cloud. Figure 2 shows that the patient's data are sensed at home and hospital and then encrypted using Paillier and Elgamal key cryptosystem for security purposes. The encrypted data are stored at local servers. The encrypted data are then stored in private cloud

at decryption side the user can get the intermediate encryption results and obtain the individual patient data because the user can get the decrypted details whenever the retrieval process takes place. To prevent the user from learning the individual patient data, an improved solution on the basis of a combination of the Paillier and the ElGamal cryptosystems is provided. Figure 3 shows that the data stored at the private cloud are decrypted and the patient's details are displayed as per patient's or physician's request after proper authentication. The data stored at the private cloud are decrypted and the patient's details are displayed as per patient's or physician's request after proper authentication. Sensor enabled RFID tags are used to monitor the patient body condition. RFID which has tags or labels attached to the patient's body parts to be monitored. RFID readers send a signal to the tag and read its response. The RFID reader transmits an encoded radio signal to read the tag and the RFID tag receives the message and responds with its identification and other measured medical information. Various bio-signals are checked through RFID tags as blood pressure, temperature, heart rate. The health data that are collected through RFID tags are amplified and transmitted through RFID readers and sent to the local work station. Then it is transmitted and stored in a data base server.

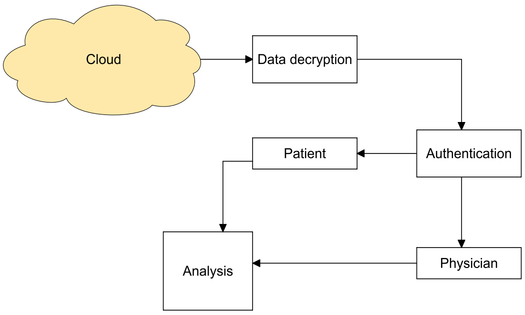


Fig. 3. Server side

IV. IMPLEMENTATION RESULTS

A. Dataset in Local Server

Figure 4 shows the measurement of estimated average glucose, HBA1C, pp is given for the patient at different intervals. Hemoglobin A1c (HbA1c) is a minor component of hemoglobin to which glucose is bound. HbA1c also is referred to as glycosylated or glucosylated hemoglobin. HbA1c is an important average measure of how well a person's diabetes is being controlled over the previous 2 to 3 months. HbA1c or haemoglobin A1c blood test, is also known as the glycated haemoglobin test or glycohaemoglobin.

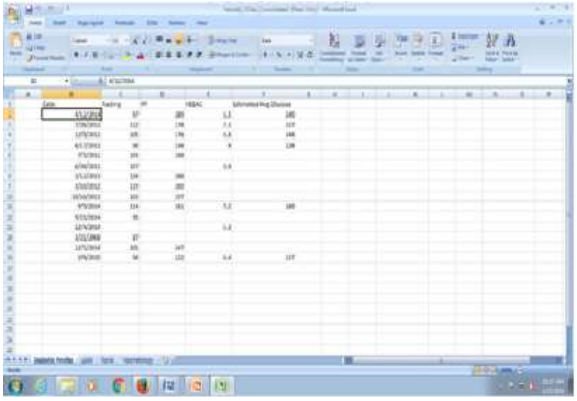


Fig. 4. Dataset in Local Server

Fig 5 shows the data set of heart beat rate of a patient.

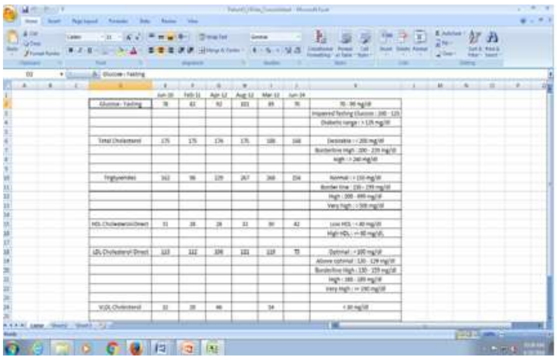


Fig5: DATA SET FOR HEART BEAT RATE DETAILS

B. Encryption

To insert the patient details in microsoft sql server following coding is used.

SqlConnection con=new SqlConnection(constr1);

con.Open(0);

SqlCommand cmd=new SqlCommand(“insert into Dataset(Patientname, Patientid, Date,

RBC, TotalWbc, PlateletCount, MeanPlatletVolume,Haemoglobin)…..

The algorithm for Paillier and ElGamal cryptosystem is a probabilistic public key encryption algorithm. It is composed of key generation, encryption and decryption algorithms.

C. Key generation

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. The key generation algorithm works as follows.

Generate a cyclic group G, of large prime order q, with generator g. Choose a random

x € {1,…,q-1}and compute

$y = g^x$

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m € G.
- Choose a random r € {1,…,q-1}
- Compute the ciphertext c = (A,B), where

$$A = g^r \ , = m.y^r$$

Fig 6 shows the result of encryption algorithm for the patient details

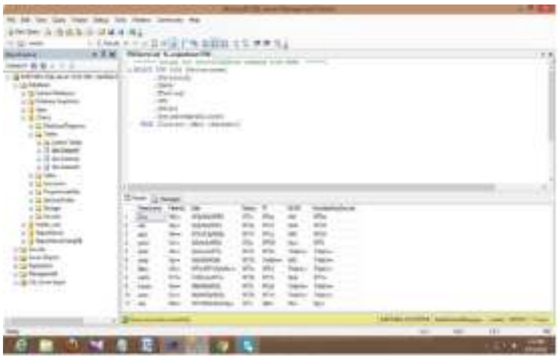
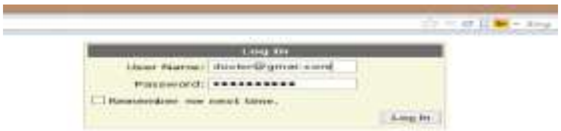


Fig. 6:Encrypted Patient Data

Users can able to view the patient details after completing the authentication process. During this process data is decrypted using the decryption algorithm. Fig7 shows the authentication process.



Log In

User Name: doctor@gmail.com

Password: ●●●●●●●●●●●

□ Remember me next time.

Log In

Fig. 7: Authentication Process

The decryption algorithm works as follows.

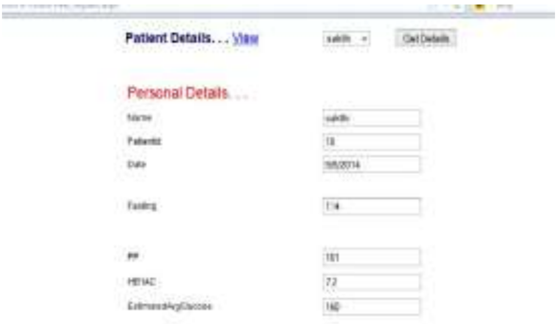
- Let c = (A, B) be a ciphertext to decrypt.
- Compute m = B/A^x

The decryption algorithm produces the intended message, since

$$B/A^x = m.y^r/g^{rx}$$

$$=m.g^{xr}/g^{rx}$$

$$=m$$



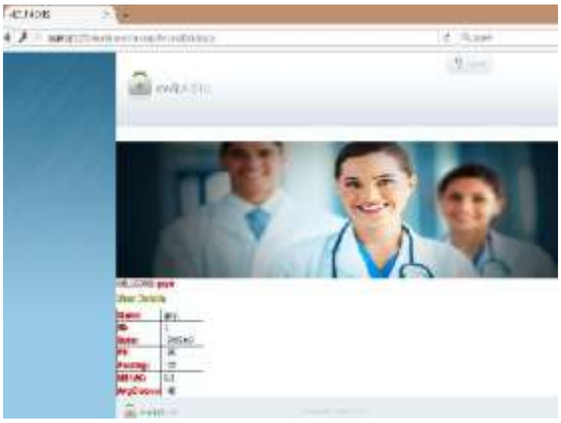
Patient Details. . . View

Personal Details. . .

Name	sakthi
PatientId	18
Date	5/5/2014
Fasting	114
PP	181
HB1AC	7.2
EstimatedAvgGlucose	160

Fig:8 After Decrypting the patient data.

After authentication the patient detail is decrypted and displayed to the user who has requested the data as shown fig 8.Once the patient details are stored in the cloud it can be accessed from anywhere any time. The following fig9 explains the same. Thus the implementation results shows the patient details are stored and retrieved securely from the cloud.



User Details

Name	[illegible]
ID	1
Date	[illegible]
PP	[illegible]
Fasting	[illegible]
HB1AC	[illegible]
AvgGlucose	[illegible]

Fig9: Retrieving the patient data from local server

V.CONCLUSION

Healthcare analysis is an emerging field which has increased the lifetime of many people. The sensed patient details from home and hospital are collected and stored in a database. In home, remote patient monitoring technology enables patients with severe chronic diseases or conditions to monitor their blood pressure and other health factors from the comfort of their homes and share this information electronically with their physicians and other healthcare providers. Health care sensors are playing a vital role in hospitality. This system can help people by providing healthcare services such as medical monitoring, memory enhancement, medical data access, and communication with the healthcare provider in emergency situations through the SMS or GPRS. To prevent the patient data from the inside attacks, a new data collection protocol is proposed, where a sensor splits the sensitive patient data into three components according to a random number generation based on hash function and sends them to servers via secure channels. Thus this work can provide a strong privacy preserving scheme against inside attackers. To prevent the patient data from the inside attacks, a new data collection protocol is proposed, where a sensor splits the sensitive patient data into three components according to a random number generation based on hash function and sends them to servers via secure channels.

VI. FUTURE WORK

In order to propose the system effectively, the data can be stored in the cloud which is helpful in accessing 24*7 anytime, anywhere when needed. The encrypted data is fetched from the cloud and decrypted before authentication. Then the details of patient's can be analyzed by the physician.

REFERENCES

[1] XiaodongLinrongXingluxuemin (Sherman) Shen, Yoshiakinemoto, and neikato, "sage: a strong privacy preserving scheme against global eavesdropping for e-health systems", IEEE journal on selected areas in communications, Vol.27, No.4, pp.365-378, 2012.

[2] Xunyi, AthmanBouguettaya, DimitriosGeorgakopoulos, Andy song and Janwillemson, "privacy protection for wireless medical sensor data", IEEE transaction on dependable and secure computing, Vol.3, No.3, pp.1-14, 2015.

[3] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park," Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks", IEEE J. Select. Areas Commun.. Vol.27, pp. 400-411, 2009.

[4] P. Kumar, Y. D. Lee, H. J. Lee," Secure Health Monitoring Using Medical Wireless Sensor Networks", In Proc. 6th International Conference on Networked Computing and Advanced Information Management, Vol.10, pp.491-494, 2010.

[5] Pardeep Kumar and Hoon-Jae Lee," Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", Department of Ubiquitous-IT, Vol.12, pp. 55-91, 2012.

[6]Ahmed Lounis, AbdelkrimHadjidj, AbdelmadjidBouabdallah, YacineChallal," Secure and Scalable Cloud-based Architecture for e-Health Wireless sensor networks", International Conference on Computer Communication Networks (ICCCN), pp.1-6, 2012.

[7] Pengfei You and Zhen Huang," Towards an Extensible and Secure Cloud Architecture Model for Sensor Information System", International Journal of Distributed Sensor Networks, Vol.12, pp. 1- 12, 2012.

[8]Ahmed Lounis, AbdelkrimHadjidj, AbdelmadjidBouabdallah and YacineChallal," Secure emergency medical architecture on the cloud using wireless sensor networks for emergency detection", International conference on computer communication networks, Vol.5, pp. 22-27, 2013.

[9] R.Rekha, T.GayathriMathambigai, and Dr.R. Vidhyapriya," Secure medical data transmission in body area sensor networks using dynamic biometrics and steganography", Bonfring international journal of software engineering and soft computing, Vol.2, No.1, pp. 5-11, 2012.

[10] Khaliq-ur-RahmanRaazi Syed Muhammad, Heejo Lee, Sungyoung Lee Jun and Young-Koo Lee," BARI: a biometric based distributed key management approach for wireless body area networks", International journal of information technology, Vol.10, No.1, pp.3911-3933, 2010.

[11] KriangsiriMalasri and LanWang,” design and implementation of a securewireless mote-basedmedical sensor network”, International journal of network security and its applications, Vol.4, No.4, pp.6273-6297, 2010.

[12] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terzis, G. M. Masson,” MEDiSN: Medical Emergency Detection in Sensor Networks”, ACM Trans. Embed. Comput..System Vol. 10, pp.1-29, 2010.

[13] Junwu and Shigerushimamoto,” an energy efficient data secrecy scheme for wireless body sensor networks”, Computer science & engineering: an international journal (CSEIJ), Vol.1, No.2, pp. 1-12, 2011.

[14] Priyanka Bhatia and ronaksumbaly,” framework for wireless network security using quantum cryptography”, International journal of computer science and engineering ,Vol.2, No.27, pp.1-17, 2014.

[15] Ying Wang, XinguangPeng and Jing Bian,” key management mechanism for authentication security in wireless sensor network”, An International Journal of Applied Mathematics & Information Sciences, Vol.9, No.2, pp.711-719, 2015.

[16] Mohammed A.Abuhelaleh, Khaled M. Elleithy,” security in wireless sensor networks: key management module in SOOAWSN”, international journal of network security & its applications, Vol.2, No.4, pp. 67-78, 2010.