Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.478 – 488

Advanced Protection for Patient Information in Medical Database

Shruthi Ramdas[1], Ankitha K[2]

[1]Department of Computer Science & Engineering

[2]Assistant Professor, Department of Computer Science & Engineering

[1,2]Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

[1] shruthiramdas@gmail.com, [2] ankitha.cs@sahyadri.edu.in

Abstract*— *In the current society, the transfer of information using internet is rapidly raising up, because it is easier and faster and has also proved security to transfer the data to destination. Security is a very important issue while transferring the sensitive data via internet because any unauthorized user can tamper the data and may make it useless or obtain the information unintended to him, especially in telemedicine. With the proliferation of patient's digital health records, and an increasing number of data breaches, protecting patient information is of utmost importance, with this respect lot of work has been done to secure medical data. Patient's health information confidentiality was an issue even when it was stored on paper. An unauthorized person could enter the hospital and steal the paper documents. Moreover, even any hospital staff can read paper documents which are not supposed to be viewed, as long as they have physical access to the document. So it is very important to protect patient's private information against unauthorized viewers by using cryptosystem confidentiality of these documents is enforced by putting them under some lock state and thereby enforcing physical access control to the document. So in this work, an attempt is made to provide high end security for the patient's sensitive data .This approach dealt with the security for medical data by using a cryptography mechanism named as Paillier cryptosystem , which is having a unique homomorphic property.

Keywords*— *Security, Sensitive data, Patient information, Paper documents, Paillier cryptosystem, Homomorphic property

I. INTRODUCTION

A booming trend in hospitals is digitalization, where documents consisting of sensitive patient information are stored digitally. Digitized medical data are shareable, flexible, can react in real time and also saves resources .This raises need of security of the documents being stored. Digital medical data & images are also frequently been exchanged throughout the world every second through Internet. These data can be viewed or manipulated during their transmission via a non-controlled channel. However the existing solutions can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data.

Day by day, confidential medical records are increasingly being stored at data centers by hospitals or firms. Many sophisticated algorithms are developed for predictive analysis of medical data so in fact, more and more operations will be done over private patient data. So there's need of concerns about the privacy for sensitive information since medical data are stored externally, off- premise data centers.

In particular in any of the health sector, a sensitive patient record has to be kept confidential. Privacy of such sensitive information can only be guaranteed, if it is encrypted by the data owner before it is being stored in data centers. Thereby, only the authenticated data owner will be able to access the data by decrypting it using given private decryption key. Encryption process restricts the possibility to outsource computation over the externally stored data, especially if the data centre have no access to the decryption key, since the key is very much essential, for any standard encryption schemes, to decrypt the data by performing certain computation upon it. This system authorizes the physician and medical researcher.

Cryptography is area which allows security engineering meet mathematics. It provides the most modern security protocols. Conventionally, Cryptographic techniques provide protection for data and information transmitted over the network. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity so on. Modern cryptography includes the disciplines of mathematics as well as computer sciences and engineering. A cryptosystem performs a pair of transformations called encrypting and decrypting. Encryption means encoding the data so that it cannot be intercepted by anyone except the one who is intended receiver after transforming back to plaintext.

There are different variations of message encryption, either using single secret key encryption called 'symmetric encryption' or using public key encryption called 'asymmetric encryption'.

1) Tasks such a evaluating or searching in an encoded database, without decoding the entries first, will require sophisticated types of encryption method with large computational expense involved, and also trivial statistical analysis becomes difficult with standard encryption method.

2) There may be need of evaluating hospital performance based on its patients' health records, without disclosing the details of all patient records.

3) Patient may want to use a web service that stores , maintains all his/her medical records in a centralized place, but may not trust the cloud service to keep his/her private health data confidential. But still want to obtain information about her health status such as a prediction of whether or not she will contract a specific disease.

All such scenarios can be realized using homomophic encryption, since a homomorphic encryption scheme allows computations over encrypted data without even decrypting it.

The paillier cryptosystem is a probabilistic & asymmetric algorithm under public key cryptography It applies an additive homomorphic cryptosystem, i.e., using public-key and the encryption of m1 and m2, we can compute encryption of m1+m2.

II. RELATED WORK

Several modern cryptography mechanisms have been proposed and implemented in recent works. However providing a high end security and maximising the privacy for the patient's data becomes very much essential. So many experiments are going on with this regard.

L Zhang *et al.* [1] have demonstrated that authentication scheme may suffer from different attacks and may fail to provide several security characteristics. Later, proposed a authenticated key agreement scheme by applying "chaotic map-based cryptography" to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process, allowing the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis & performance analysis has been proved for various attacks and better performance and thus its more suitable for practical applications in TMIS environments.

In [2], Shu-Di Bao *et al.* considering the sensitive healthcare information in cloud environments, and proposed in a special data scrambling method for healthcare application, where a tiny part of data is used to scramble the remaining data for the purpose of encryption. This method improves in terms of security performance and practicability. ECG signals from both "MIT-BIH arrhythmia" database and "elf-collected" database are used. Conversion into decimal format is based on a quantization resolution of eight bits.

W Zhao *et al.* [3] introduced a novel system for healthcare professionals to enhance their compliance with best practice and regulations using 'Microsoft Kinect sensor' and smart watches while protecting patient privacy. A contribution for this study will be registration mechanism for a healthcare professional to explicitly give their system the permission to monitor his/her activities. Multiple Kinect sensors are used for improved tracking accuracy and better coverage for bigger workplaces. Finally, their system generates alerts through designated smart watch according his or her personal preference.

Lingjia Liu *et al.* [4] consider a three tier medical body area network (MBAN): inter-MBAN, intra-MBAN, and beyond-MBAN. The intra-MBAN transmit sensors' data to a controller, and in turn transmits them to inter-MBAN tier to an access device like a PDA or tablet device, which is usually connected to a patient's medical database. This access device used as a means of communication for intra-MBAN and beyond-MBAN to uses hospital information systems. This is widely deployed in hospitals places security and privacy violation threats .Results show that this scheme achieves much higher privacy protection, at expense of reduced coverage.

In [5], Min Chen *et al.* introduced a cloudlet based healthcare system, where they consider privacy of users' physiological data and efficiency of data transmission. They use NTRU, Number Theory Research Unit for data protection during data transmission to the cloudlet. To share data in the cloudlet, they use users' similarity and reputation to build a trust model. Based

on measured users' trust level, the system finds out whether data sharing is performed. They divide data in remote cloud into various kinds and apply encryption mechanism to protect them respectively. They also proposed collaborative IDS, intrusion detection system against malicious attacks based on cloudlet mesh to protect the whole healthcare system.

Abdelali El Bouchti *et al.* [6] has contributed to appeal to 'Data encryption in healthcare cloud computing environment' .They suggest a hybrid architecture based on Cryptography as a Service(CaaS) includes the private cloud OpenStack platform. Cryptographic operations control the healthcare cloud clients and they prevail keys in the cloud independent of the cloud provider. Firstly, they summarize cloud computing for healthcare, and provide survey about important concepts regarding cryptography. Then, they investigate optimized realization of homomorphic encryption, RSA and Elliptic based additive homomorphic encryption, which offers better reporting. Finally, they propose a architecture to solve the privacy problem in healthcare cloud which offers a fast point multiplication, while featuring small code and memory requirements.

III. IMPLEMENTATION

A. Methodology:

In hospitals, documents consisting of sensitive patient information, that is stored digitally and security of such documents are very much essential. Privacy of such sensitive information can only be guaranteed, if it is encrypted by the data owner before it is being stored in data centers. In this work, the high end security is provided for the patient's sensitive data thereby ensuring maximum privacy for the patients.

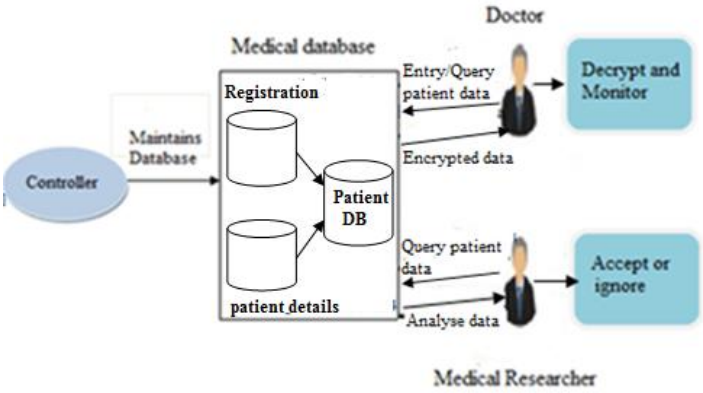

Figure 1: System Architecture

The users of this system are doctors and researchers. For registration, doctor needs to provide his username and password. Thereafter doctor can either view or needs to enter the patient's details such as name, age, health type etc.

The users should be able to perform the following functions using this system:

By Doctor

- Register to medical database
- Login using a user name and password
- View all the patients' record.
- Enter patients details [name, age, health type etc]

By Researcher

- Register to medical database
- Login using a user name and password
- View his or her patients record based on required health type
- Add or delete patients record based on required health type

Controller (Admin): Controller is the administrator who is the owner of this system. The administrator is responsible for maintaining medical database. Admin will assign user name and password. The administrator can perform the following functions:

- Register genuine doctor and researchers
- Maintains patients database

B. Mathematical Functions and Notations used in the Algorithms

In order to understand Paillier cryptosystem working, we should have knowledge on the following basic mathematical concepts:

Euler's totient function (phi function): The totient of positive integer n is defined to be number of positive integer less than or equal to n that are relatively prime to n.

Example : φ(9)= 6 (since 1,2,4,5,7 and 8 are relatively prime to 9).

If n can be factorized to distinct prime numbers a and b then φ(n)=(a-1)(b-1).

Example: φ(15)= φ (3*5) = (3-1)(5-1)

Carmichael's function **(λ function)** is given by the least common multiple (lcm) of all the factors of the totient function Φ(n). If n can be factorized to prime number a and b then $\lambda(n) = lcm(a-1,b-1)$.

Modular multiplicative inverse of an integer b modulo m is an integer y such that $b^{-1} \equiv x \bmod m$ is equivalent to $bx \equiv 1 \bmod m$. The multiplicative inverse of *b* modulo *m* exists iff *b* and *m* are coprime (i.e.,if *g*cd(b, *m*)= 1).

Notations used in Paillier Cryptosystem explanation

$\mathbb{Z}_n$ → set of n integers

$\mathbb{Z}_{n^*}$ →integers coprime to n - this set consists of $\Phi(n)$ numbers

$\mathbb{Z}_{n^2*}$ → integers coprime to n^2 - this set consists of $n\Phi(n)$ numbers.

Two basic building blocks of solution are the Paillier and homomorphic scheme.

Algorithm 1: Paillier Cryptosystem

---

1. Choose two big prime numbers 'a' and 'b' randomly ,such that gcd(ab,(a-1)(b-1))=1, This property assures ,if both primes are of same length.

2. Compute n=ab and Carmichael function λ=lcm(a-1,b-1) , which can be computed using λ=(a-1)(b-1)/gcd(a-1,b-1)

3. Select generator g where $g \in Z^*_{n^2}$ there are two ways of selecting the g.

a. Randomly select g from a set $Z^*_{n^2}$ where

$$\gcd\left(\frac{g^{\lambda} \bmod n^2-1}{n}, n\right) = 1$$

there are φ (n)* φ (n) number of valid generators ,thereby the probability of choosing them out of n φ (n) elements of $Z^{*}{}_{n}{}^{2}$ set is relatively high for big n.

b. Select α and β randomly from a set Z_n^* then calculate $g = (\alpha n+ 1)^n \bmod n^2$

In this case the selected generator always meets the condition above

4. Calculate the following modular multiplicative inverse

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$$

Where the function *L* is defined as (u) = (u-1)/n

This multiplicative inverse exists if and only if valid generator was selected in previous step.

- The public (encryption) key is (n , g).
- The private (decryption) key is (λ , μ).

A simpler variant of the above key generation steps would be to set g=n+1 ,λ=φ (n) ,

$\mu=\varphi(n)^{-1} \bmod n$ where φ (n) =(a-1)(b-1)

Encryption

1. Let m be a message to be encrypted where $m \in \mathbb{Z}n$

2. Select random r where $r \in Z_n^*$

3. Compute ciphertext as: $c=g^m * r^n \bmod n^2$

Decryption

1. Ciphertext $c \in Z^{*}{}_{n}{}^{2}$

2. Compute message: $m = L\,(c^{\lambda} \bmod n^2) * \mu \bmod n$

Homomorphic Properties

A prominent feature of the Paillier cryptosystem is using homomorphic properties. As the encryption scheme is additively homomorphic, described as follows:

• **Homomorphic addition of plaintexts**

The product of two ciphertexts will decrypt to the sum of their corresponding plaintexts,

$$D(E(m_1,r_1)*E(m_2,r_2) \bmod n^2)=m_1+ m_2 \bmod n$$

The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D\,(E(m_1,r_1)*g^{m_2} \bmod n^2)= m_1+ m_2 \bmod n$$

Practically, this leads to the following identities: Where $\forall \boldsymbol{m_1}$, $m_2 \in \mathbb{Z}\boldsymbol{n}$ and $\boldsymbol{k} \in \mathbb{N}$

$$D\,(E(m_1,r_1)*E(m_2,r_2) \bmod n^2)=m_1+ m_2 \bmod n$$

$$D\,(E(m_1,r_1)*g^{m_2} \bmod n^2)= m_1+ m_2 \bmod n$$

$$D\,(E(m)^k \bmod n^2)= km \bmod n$$

$$D\,(E(m_1)^{m_2} \bmod n^2)= m_1m_2 \bmod n$$

$$D\,(E(m_2)^{m_1} \bmod n^2)= m_1m_2 \bmod n$$

Algorithm 2: Homomorphic Scheme

---

1. Key Generation (λ)

- Input: Security parameter λ
- Output: A tuple (S_i, P_i) consisting of the secret key S_i and public key P_i.

2. Encryption (P_i, P_t)

- Input: A public key P_i and a plaintext P_t
- Output: ciphertext C_t

3. Decryption (S_i, C_t)

- Input: a secret key S_i and a ciphertext C_t
- Output: the corresponding plaintext Pi

4. Evaluation (P_i, C, C_t)

- Input: a public key P_i a circuit C with x inputs and a set P_t of x ciphertext,P_t1,P_t2,P_t3,..,.$P_{t\ x}$
- Output: a ciphertext C_t.

Input Data

The following URL is utilized to give patients health type details for this system :

→http://developer.ihealthlabs.com/index.htm

→http://ihealth.sepdek.net/

{"healthData":[{"sensor":"Airflow","value":"1.71","metric":"%","timeStamp":"20161114062954"}, {"sensor":"Body temperature", "value":"36.24", "metric":"deg.C", "timeStamp":"20161114062954"}, {"sensor":"ECG", "value":"0.00", "metric":"%", "timeStamp":"20161114062954"}, {"sensor":"Oxygen saturation", "value":"98.75", "metric":"%", "timeStamp":"20161114062954"}, {"sensor":"Heart rate", "value":"65.90", "metric":"bpm", "timeStamp":"20161114062954"}, {"sensor":"Systolic pressure", "value":"99.24", "metric":"mmHg", "timeStamp":"20161114062954"}, {"sensor":"Diastolic pressure", "value":"76.21", "metric":"mmHg", "timeStamp":"20161114062954"}, {"sensor":"Pulse", "value":"65.90", "metric":"bpm", "timeStamp":"20161114062954"}, {"sensor":"EMG", "value":"0.00", "metric":"%", "timeStamp":"20161114062954"}, {"sensor":"Skin conductance","value":"1.06", "metric":"Î¼s", "timeStamp":"20161114062954"}, {"sensor":"Skin resistance", "value":"1018.35", "metric":"KOhms", "timeStamp":"20161114062954"}

Table 1: Table of ihealth data from ihealth website

Benefits of this System

1) Doctors need not worry about the security of patients data
2) Doctors can access patient data remotely using modern encryption method.
3) Researchers can view and use patients records for their research purpose.
4) Provides secured storage and communication of hospital data using modern cryptosystems and performs statistical analysis on the patient's data.

IV. PERFORMANCE ANALYSIS

Performance analysis on RSA, ElGamal, Paillier algorithms based on the following parameters on local system for different input size:

a. Evaluation Parameters: Performance of encryption/decryption algorithm is evaluated considering the following parameters:

1. Encryption Time: Considers the time taken by encryption process to produces cipher text from a plain text.

2. Decryption Time: Considers the time taken by decryption process to produces plain text from a cipher text.

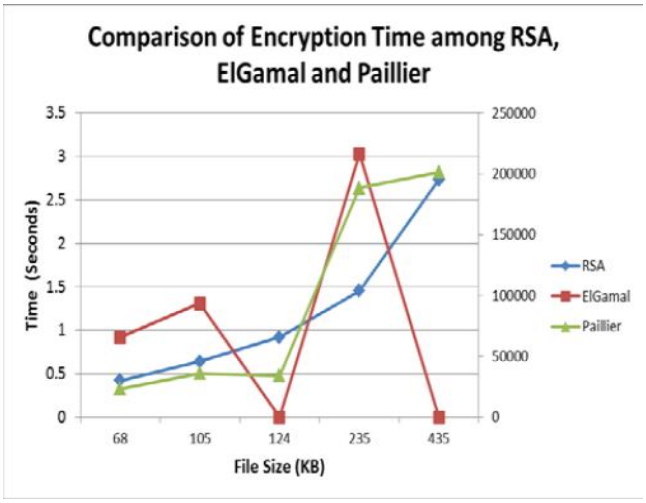

Figure 2: Comparing RSA, Elgamal and Paillier Encryption Time

Paillier encryption time is fast for smaller file size but provides very strong security since its embedded with homomorphic property.

b. Evaluation Platforms: Performance of encryption/decryption algorithm is evaluated considering the following system configuration:

1. Software Specification: Experimental evaluation on NetBeans IDE 8.1 with Java Development Kit 8 Update 65, with XAMPP (Apache, Mysql), Windows 7 , 32 bit Operating System.

2. Hardware Specification: All the algorithms are tested on Intel Core i5 (2.20 GHz) fourth generation processor with 2GB of RAM with 1 TB-HDD.

c. Evaluation Factor: In this system, evaluation of different algorithms key size is considered:

1. Symmetric Algorithms: DES uses 56-bitkey (8 bit parity) and produce output of 64 bit block. In AES, key length varies from 128, 192, to 256 bits .In Triple Data Encryption algorithm, use 192 bits key size.

2. Asymmetric Algorithms: RSA uses 1024-bit keys but its not secure, and it works only if it is correctly implemented and good key management is employed. So here in my system, paillier with homomorphic property containing mathematical operation over encrypted data is utilized, encrypted with 308 bit of keys with advanced technology to protect the data. Hackers will find it difficult to decrypt such encrypted data. Hence paillier cryptosystem is proved to be a stronger mechanism.

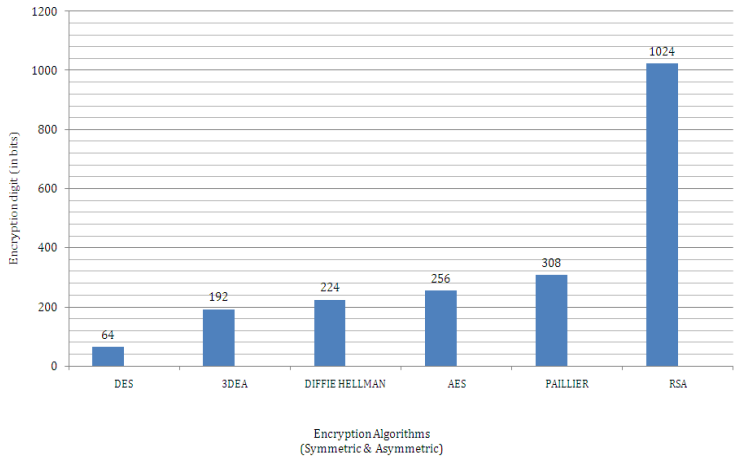

Figure 3: Comparing encryption algorithms, encryption digits (in bits)

V. CONCLUSION

The proposed method is much stronger cryptosystem than the traditional methods. This work, presents an efficient approach to provide well-protected security for patients data. Unlike other healthcare solutions, this system utilizes paillier and homomorphic encryption of patient's health type thereby providing advanced security to the patient data. When comparing with the existing method, there is certain amount of overhead concerning the time required for individual health rate encryption computation but the overall outcome is satisfactory and precise. However using this system, patient's sensitive health data are strongly secured and thereby not easily compromised. Hence this proposed scheme is very efficient both for doctors and medical researchers and they can view patient's records ubiquitously. Doctors are provided with highly secured and efficient storage of hospital data; hence patient's data are accessed securely. This method can solve the issue of protecting patient's private information against unauthorized viewers and provide high level of protection.

Finally this method can be improved by distributing encrypted data to different data servers without being compromised even if any one of the data server gets attacked. Further this system can be improvised so that it can be used for larger and any type of health data for wider coverage.

REFERENCES

[1] Liping Zhang, Shaohui Zhu, and Shanyu Tang, "Privacy protection for Telecare Medicine Information Systems Using a Chaotic Map-Based Three-Factor Authenticated Key Agreement Scheme", IEEE Journal of Biomedical and health informatics, Vol. 21, No. 2, March 2017.

[2] Shu-Di Bao, Meng Chen, Guang-Zhong Yang, "A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications", IEEE, DOI 10.1109/JBHI.2017.2679979, 2017.

[3] Wenbing Zhao, RoannaLun, Connor Gordon, Abou-BakarFofana, Deborah D. Espy, M. Ann Reinthal, Beth Ekelman, and Glenn Goodman, Joan Niederriter, ChaominLuo, XiongLuo, "A Privacy-Aware Kinect-Based System for Healthcare Professionals ", IEEE, February 2016.

[4] Lingjia Liu, RachadAtat and Yang Yi, "Privacy Protection Scheme for eHealth Systems: A Stochastic Geometry Approach", IEEE, September 2016.

[5] Min Chen, YongfengQian, Jing Chen, Kai Hwang, Shiwen Mao, "Privacy Protection and Intrusion avoidance for Cloudlet-based Medical Data Sharing", IEEE Transactions on Cloud Computing, 2016.

[6] Abdelali El Bouchti, Samir Bahsani, TarikNahhal, "Encryption as a Service for Data Healthcare Cloud Security", IEEE 5th International Conference on Future Generation Communication Technologies, July 2016.

[7] Tzu-Wei Tseng, Cheng-Yi Yang, Chien-Tsai Liu, "Designing Privacy Information Protection of Electronic Medical Records", IEEE2016 International Conference on Computational Science and Computational Intelligence, April 2016.

[8] Jisha S, Mintu Philip, "RFID based Security Platform for IOT in Health Care Environment", IEEE Online International Conference on Green Engineering and Technologies ,(IC-GET) 978-1-5090-4556-3/16 , 2016 .

[9] MasumaMammadova, "The Problems of Information Security of Electronic Personal Health Data", IEEE 7th International Conference on Information Technology in Medicine and Education, August 2015.

[10] AlexandruSoceanu, MaksymVasylenko, AlexandruEgner, TraianMuntean, "Managing the Privacy and Security of eHealth Data", IEEE 20th International Conference on Control Systems and Science, 2015.

[11] Chinyang Henry Tseng, Shiau-Huey Wang, and Woei-JiunnTsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection", IEEE Transactions on Reliability, Vol. 64, No. 3, September 2015.

[12] Tohari Ahmad, HudanStudiawan, HafidhSholihuddin Ahmad, Royyana M. Ijtihadie, WaskithoWibisono, "Shared Secret-based Steganography for Protecting Medical Data" IEEE 2014 International Conference on Computer, Control, Informatics and its Applications, July 2014.

[13] Narendra K. Pareek, VinodPatidar, "Medical Image Protection using Genetic Algorithm Operations", Springer, 2014.

[14] Mohamed M. Abd-Eldayem, "Medical Image Authentication Based on Revertible Watermarking",The 9th International Conference on INFOrmatics and Systems,December 2014.

[15] Tohari Ahmad, HudanStudiawan, HafidhSholihuddin Ahmad, Royyana M. Ijtihadie, WaskithoWibisono, "Shared Secret-based Steganography for Protecting Medical Data", IEEE 2014 International Conference on Computer, Control, Informatics and Its Applications, 2014.

[16] Daojing He, Sammy Chan,and Shaohua Tang, "A Novel and Lightweight System to Secure Wireless Medical Sensor Networks", IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 1, January 2014.

[17] G.Nalinipriya ME, R.Aswin Kumar, "Extensive Medical Data Storage With Prominent Symmetric Algorithms On Cloud - A Protected Framework", IEEE International Conference on Smart Structures & Systems, Chennai, India, March 2013.

[18] Jungchae Kim, Byuckjin Lee, and Sun K. Yoo, "Design of Real-time Encryption Module for Secure Data Protection of Wearable Healthcare Devices", 35th Annual International Conference of the IEEE EMBS Osaka, Japan, July 2013.

[19] Zhong Han, Yuqing Sun, Yuan Wang, "Audit Recommendation for Privacy Protection in Personal Health Record Systems", Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, 2013.

[20] ChenglangLu ,ZongdaWu ,Mingyong Liu, Wei Chen ,JunfangGuo, "A Patient Privacy Protection Scheme for Medical Information System", Springer, October 2013.

[21] Moonshik Shin, SunyongYoo, Kwang H. Lee, Doheon Lee, "Electronic Medical Records Privacy Preservation through *k*-Anonymity Clustering Method", IEEE, 2012.

[22] Hsiang-Cheh Huang, Wai-Chi Fang, "Integrity Preservation and Privacy Protection for Medical Images with Histogram-Based Reversible Data Hiding", IEEE, 2011.

[23] Mar´ıa de los A´ ngelesCosioLeo´n, Juan Iv´an Nieto Hip´olito, Jes´us Luna Garc´ıa, "A Security and Privacy Survey for WSN in e-Health Applications", IEEE Electronics, Robotics and Automotive Mechanics Conference,2009.

[24] Yicong Zhou, Karen Panetta, and SosAgaian, "A Lossless Encryption Method for Medical Images Using Edge Maps", 31st Annual International Conference of IEEE, September 2009.

[25] Dickson K.W. Chiu, Patrick C. K. Hung, Vivying S. Y. Cheng, and EleannaKafeza, "Protecting the Exchange of Medical Images in Healthcare Process Integration with Web Services",Proceedings of the 40th Hawaii International Conference on System Sciences IEEE, 2007.

