I J C T A, 9(3), 2016, pp. 1633-1640

Privacy Protection for Transmission of Medical Data through Wireless Network

M.C. Jemima Gracia* and R. Dhanalakshmi**

Abstract: Recently, The use of Wireless Sensor Network (WSN) in health care applications is growing rapidly because it has got several advantages over the traditional wired systems such as ease of use, reduced risk of infections, reduced risk of failures, reduced user discomfort and it provides enhanced mobility, but providing security and privacy is a major concern. There are several solutions in order to protect the patient data during transmission, but it cannot stop the inside attacker from revealing the patient sensitive data. The inside attacker can be a patient database administrator. The main aim of this paper is to prevent the inside attack by distributing the patient data securely in multiple servers and to employ the Paillier cryptosystem to carry out statistic analysis on the patient data without compromising the privacy of the patient's data.

Keywords: privacy protection;paillier cryptosystem ;patient data privacy.

1. INTRODUCTION

The application areas of wireless sensor networks are growing widely, as the cost and size of sensor devices are decreasing rapidly. The major application domains are home, office, transportation, environmental monitoring, healthcare, security and surveillance, tourism and entertainment.

Wireless Medical Sensor Network (WMSN) technology has invaded medical equipments to replace thousands of wires connected to various equipments found in hospitals. The development of Wireless Medical Sensor Networks has the potential to transform the way of human life. The wireless sensor network consists many sensor nodes that are scattered throughout a physical environment and can be used to closely monitor the physiological conditions of the patients. Each sensor device is capable of monitoring, sensing and displaying the information that includes monitoring the blood pressure, glucose level, pulse rate, measuring the heart rates and analyzing the body temperature etc. Some of the examples of health care applications that use WSN are HealthGear, Vital Jacket, and eWatch.

HealthGear [14] is a product of Microsoft Research. It consists of a set of physiological sensors connected via Bluetooth to a mobile phone. It is a wearable real-time health system for observing and analyzing the physiological signals.

eWatch sensor [13] that is inserted into the wrist watch form making it highly available, immediately viewable, and widely acceptable. eWatch gives tactile, audio and visual notification while sensing and recording light, temperature and sound.

The Vital Jacket mobile device is an wearable garment that is able to constantly monitor electrocardiogram (ECG) waves and Heart Rate.

Wireless medical sensor networks helps in upgrading patient's quality-of-care without disturbing their comfort zone. However, there exist many possible security threats to the patient sensitive confidential data transmitted over the public channels and stored in the back-end systems. The WSN are prone to various

* KCG College of Technology Chennai, India, *Email: jemimagracia@gmail.com*

** KCG College of Technology Chennai, India, *Email: dhanalakshmi.cse@kcgcollege.com*

security threats that would be harmful for the wireless healthcare success. The various security threats are as follows:

Eavesdropping-It is a common threat to the patient privacy where an adversary can easily discover the patient information from communication channels. An eavesdropper, consists of a powerful receiver antenna, and will be able to capture the patient confidential data from the medical sensors and thereby knows the patient's health condition.

Data modification-The attacker can delete or change a part or all of eavesdropped information and send the modified information back to original receiver to achieve some illegal purpose. Health data are important. Modifying them may result in serious problems.

Data breach-It is a security threat to the patient data privacy. A data breach is where the confidential patient data is used by an unauthorized user.

Due to sensitive nature of healthcare applications and to protect the wireless medical sensor networks against various attacks encryption of data, and constant monitoring of the network is done.

Most of the solutions focuses on how to protect the wireless medical sensor networks against the outside attacks, where the attacker does not know any details about the secret keys whereas this paper deals with the inside attacker who knows some secret keys in our system and use them to get the patient data.

2. RELATED WORKS

A survey on secure healthcare monitoring using wireless sensor networks was done by Kumar and Lee [9] [10] where they make use of trusted server protocol for key management. Trusted server based scheme provide stronger security, but in real time environment, it could become a single point for the entire network failure. Trusted server is not suited for critical applications because there may occur problems like providing less storage space, poor scalability, bottleneck problem etc. In order to solve this issue, the data is distributed across muliple servers to achieve high scability, providing more memory than one server can provide, improved load balancing and helps in avoiding bottleneck problems.

D. Bogdanov, S. Laur, J. Williamson proposed a Sharemind system [2], which is a virtual machine for privacy-preserving data processing that depend on the shared computing techniques to protect the patient data. In this solution, the sharemind system [19] can protect the patient data privacy as long as the number of the compromised data servers is at most one. If two of the three servers are compromised by the inside attack, the solution becomes insecure.

A. Siva Sangari and J. Martin Leo Manickam[18] proposed Light weight security and authentication in wireless body area network using Skipjack, a secret key encryption algorithm that provides the secure communication between sensor node and mobile node. Skipjack is a block cipher that supports a 64 bit block size and a 80 bit key**.** Since skipjack algorithm uses key length of 80 bits it is subject to brute force attack.

In 2013, Dan Baehr et al. [3] used TinyECC to secure the wireless communication between sensor nodes, in a real-time sensor network. TinyECC is a public key algorithm which uses Elliptic Curve Cryptography to solve the issues of power consumption and slow processor speeds, but it increases the size of the encrypted message. The ECC algorithm is highly complex and more difficult to implement.

J. Misic and V. Misi proposed a technique that relies on a Central Trusted Security Server (CTSS) [14] to authenticate that participants belong to the particular patient's group and to generate the session key. CTSS makes uses of central trusted security server which leads to central point of failure and it is easy for the inside attacker to hack the server.

The energy-efficient access control scheme based on ECC to overcome security limitations such as not providing mutual authentication and is strictly exposed to Denial-of-Service attacks is discussed in [11].

Public-key cryptography based access control scheme has more benefits than symmetric-key cryptography based scheme because of better scalability, low memory demand, assigning of new nodes easily, and no key pre-distribution. The limitation is that the sensor must commune with the Key Distribution Centre (KDC) to authenticate the user and verify the access request. First, this requires an on-line KDC every time. Any failure of the KDC will lead to serious problem to the network. Secondly, interacting with the KDC requires a significant extra overhead to the network.

The main aim of this paper is to prevent the inside attack by distributing the patient data securely in multiple servers and to employ the Paillier cryptosystem to perform statistic analysis. In this paper, an efficient solution for privacy preserving WMSNs based on a symmetric key cryptosystem is implemented by Advanced Encryption Standard (AES) algorithm.

3. SYSTEM ARCHITECTURE

Data collection-Health care involves a variety of public and private data which includes health reviews, administrative enrollment, billing records, sensitive patient data which are used by the hospitals, doctors, physicians etc. A data collection protocol is used where a sensor collects and splits the sensitive patient data into multiple components and sends them to multiple servers.

In the wireless medical sensor network, each medical sensor sends the sensitive patient data to the distributed database system in a protected manner.

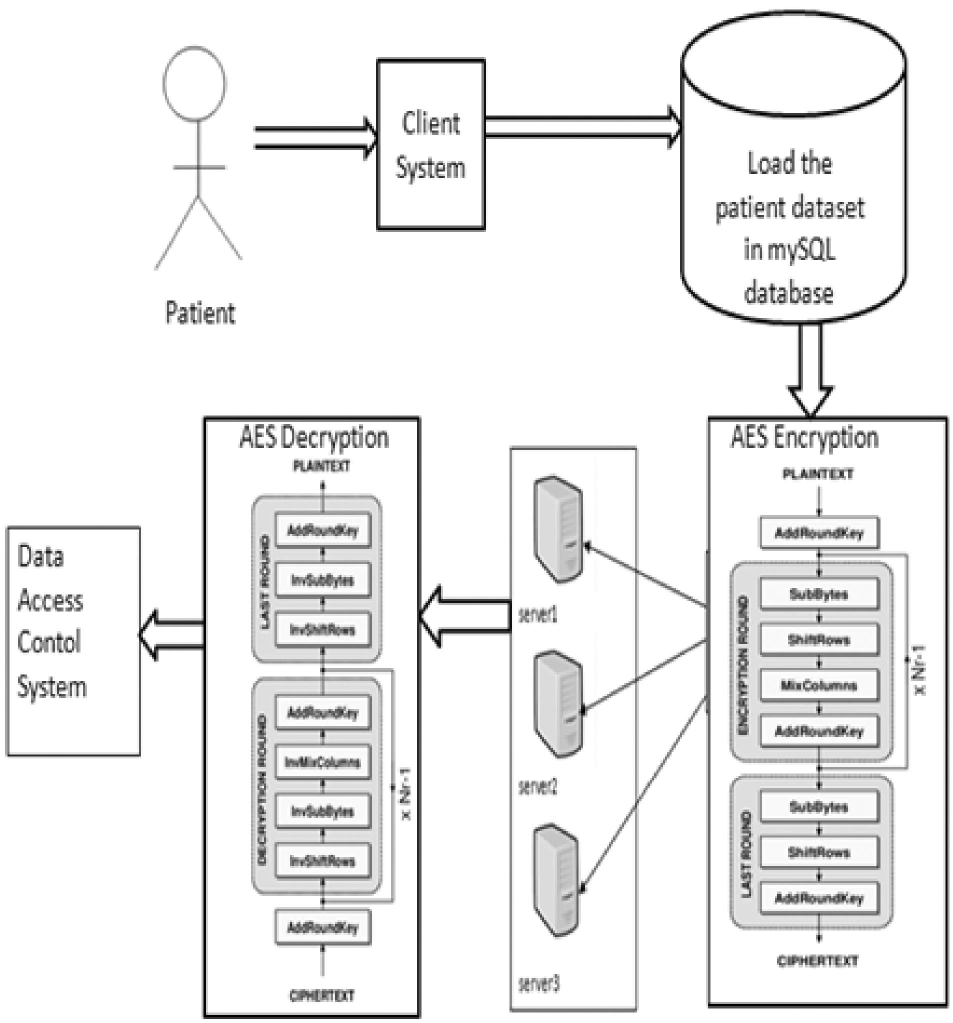

Figure 1: System Architecture

Data store security-The patient database system consists of multiple database servers. Assuming that all data servers are semi-honest, often called honest but curious". That is, all data servers run protocol exactly as specified, but tries to learn as much as possible about the patient data. In addition, assuming that at least one data server is not compromised by the inside attackers.

Data Access security-In the patient access control system, only the person who are authorized can get access to the sensitive patient data. The patient data cannot be disclosed to any data server during the access. Paillier Public-Key Cryptosystem is used by the user (e.g., Doctor) to access the patient data and monitor the patient's health condition. The user sends the request including the patient's identity, attribute of the data, the signature of the user on the query, and the certificate of the user to the three data servers through secure channels. The secure channels is used for the user to place his queries because the patient's personal details in the queries needs to be protected against outside attackers. If the user's request passes the signature verification and meets the access control policies, then the servers can identify the shares of the data according the patient's identity and the attribute of the data.

AES are symmetric-key algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. AES is more secure than its predecessors such as DES and 3DES, as the algorithm is stronger and uses longer key lengths. AES is built for three key sizes 128,192,256 bits. The communication between the user and each data server is through a secure channel. Because the three data servers and the user's computing device are usually much more powerful in computation and communication. By using AES, we can achieve data confidentiality, authenticity and integrity between the user and each data server. The sensitive patient data which is stored in the database is encrypted using AES algorithm and it is stored in multiple servers.

Paillier Public-Key Cryptosystem

The Paillier encryption scheme invented by Pascal Paillier in 1999, is public key encryption algorithm. It is consists of key generation, encryption and decryption algorithms as follows:

Key generation

The key generation algorithm works as follows:

1. Choose any two large prime numbers p and q such that they are independent of each other

$$gcd(pq, (p-1)(q-1)) = 1$$

2. Compute $N = pq$, $\lambda = lcm\ (p-1, q-1)$

   Where lcm stands for the least common multiple.

3. Select random integer g where $g \in Z^{*}_{N}{}^{2}$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

$$\mu = (L(g^{\lambda}\ (mod\ N^{2})))^{-1}\ (mod\ N)$$

Where function L is defined as

$$L(u) = u - 1/N$$

The notation a/b does not denote the modular multiplication of a times the modular multiplicative inverse of b but rather it denotes the quotient of a divided by b.

The public (encryption) key pk is (N, g).

The private (decryption) key sk is (λ, μ).

If using p, q of equivalent length, then

$$g = N + 1,\ \lambda = \varphi(N)\ ,\ \mu = \varphi\ (N)^{-1}(mod\ N)$$

Where $N = pq$ and $\varphi\ (N) = (p - 1)\ (q - 1)$.

Encryption

The encryption algorithm involves the following steps:

1. Let m be a message to encrypt, where $m \in Z_{N}$.
2. Select a random r such that $r \in Z^{*}_{N}$.
3. The ciphertext is computed as:

$$c = g^{m}.\ r^{N}\ (mod\ N^{2})$$

Decryption

The decryption algorithm involves the following steps:

1. Let c be the ciphertext to decrypt, where the ciphertext

$$c \in Z^{*}{}_{N}{}^{2}$$

2. Compute the plaintext message as:

$$m = L\ (c^{\lambda}\ (mod\ N^{2}))\cdot \mu\ (mod\ N)$$

Homomorphic Properties

A remarkable feature of the Paillier cryptosystem is its homomorphic properties. Given two ciphertexts

$$E\ (m_{1}, pk) = g^{m1}r_{1}{}^{N}\ (mod\ N^{2})$$

$$E\ (m_{2}, pk) = g^{m2}r_{2}{}^{N}\ (mod\ N^{2})$$

Where $r1, r2$ are randomly chosen for Z^{*}_{N}

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

$$D\ (E\ (m_{1}, pk_{1})\cdot E\ (m_{2}, pk_{2})) = m_{1}+ m_{2}\ (mod\ N)$$

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

$$D\ (E\ (m_{1}, pk_{1}).\ g^{m2)} = m_{1}+ m_{2}\ (mod\ N)$$

An encrypted plaintext raised to a constant k will decrypt to the product of the plaintext and the constant,

$$D\ (E\ (m_{1}, pk_{1})^{k}) = k\mathrm{m}_{1}\ (mod\ N)$$

However, given the Paillier encryptions of two messages, there is no known way to compute an encryption of the product of these messages without knowing the private key.

Paillier cryptosystem: Patient information access control protocol

The data access protocol is used to maintain privacy of the sensitive patient data during access by the physician without revealing to any servers

Input: α, β, γ, pk, sk

Output: $\rho = \alpha + \beta + \gamma$

1. The data server S_1 picks a random $r_1 \in Z^*_N$ and computes
   C_1 = Encrypt (α, pk) = $g^{\alpha} r_1^N \ (mod\ N^2)$
   And sends C_1 to the server S_2
2. The data server S_2 picks a random $r_2 \in Z^*_N$ and computes
   C_2 = Encrypt (β, pk) = $g^{\beta} r_2^N \ (mod\ N^2)$
   And sends C_1 $C_{2\ \text{to}}$ the server $S_{3.}$
3. The data server S_3 picks a random $r_3 \in Z^*_N$ and computes
   C_3 = Encrypt (γ, pk) = $g^{\gamma} r_3^N \ (mod\ N^2)$
   And replies C_1 C_2 C_3 to the user
4. The user computes
   ρ = Decrypt(C_1 C_2 $C_{3,}$ sk)
5. Return ρ

Because of the homomorphic properties of the Paillier

Cryptosystem,

$$
\begin{aligned}
C_1C_2C_{3'} &= E(\alpha, pk)\, E(\beta, pk)\, E(\gamma, pk) \\
&= (g^{\alpha} r_1^{N})\, (g^{\beta} r_2^{N})\, (g^{\gamma} r_1^{N})\ (mod\ N^2) \\
&= g^{\alpha+\beta+\gamma}\, (r_1 r_2 r_3)^{N}\ (mod\ N^2) \\
&= E(\alpha + \beta + \gamma; pk)
\end{aligned}
$$

Therefore,

ρ = Decrypt($C_1C_2C_3$; sk) = $\alpha + \beta + \gamma$

The Wireless Sensor Network involve in collecting the patients sensitive data by data collection protocol and splits the sensitive patient data randomly and sends them to multiple servers through secure channels as shown in Fig. 2.

When a medical sensor sends a sensitive numerical patient data ρ (e.g., Blood pressure reading) to multiple servers, to prevent any data server from understanding the patient data and revealing the patient

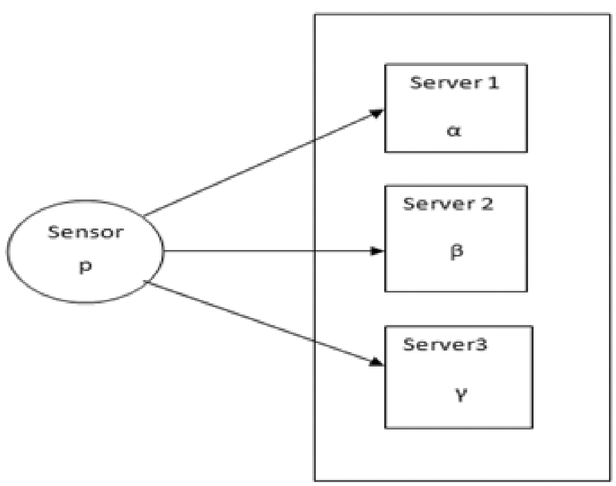

Figure 2: Data Distribution

privacy (the inside attack), the medical sensor splits the confidential patient data ρ (an integer)into three integers α, β, γ in such a way that α + β+ γ = ρ and sends them to the three data servers through three secure channels.

When a doctor wishes to get access the patient data, he needs to send a request to the three data servers, each of them checks the doctor's credential with the access control list and then replies the doctor with the patient data. If the doctor's credential passes authentication and meets the access control policies, the three servers reply α, β, γ to the doctor through three secure channels. Finally, the doctor combines the three integers to obtain the patient data ñ as shown in Fig. 3

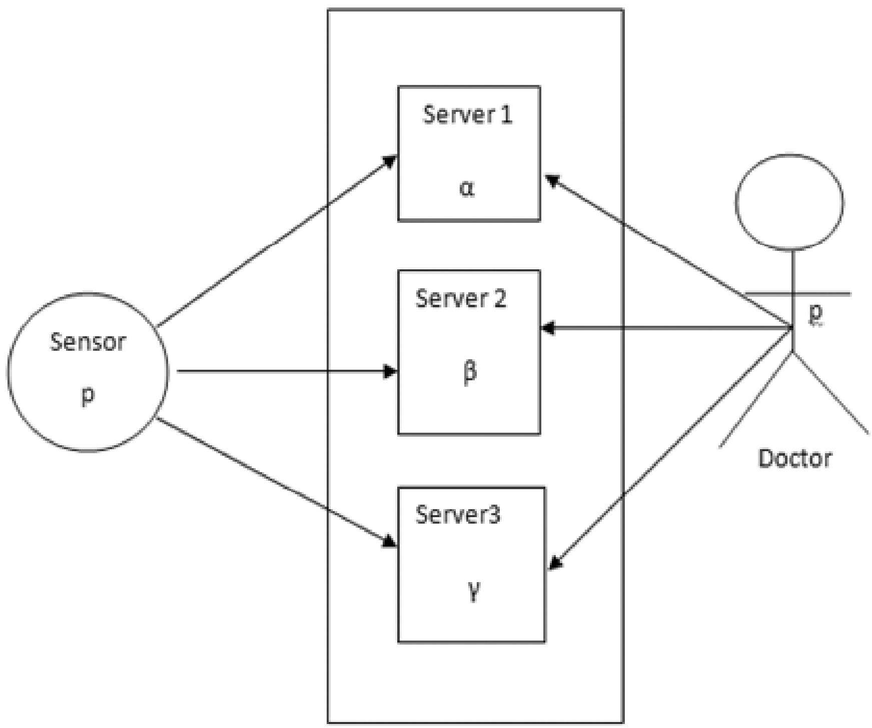

Figure 3: Data Distubution and Access

4. PRIVACY AND PERFORMANCE ANALYSIS

In patient information access control protocol, the sensitive patient data is always encrypted by the public key of the user. The attacker cannot access the patient data even if two of the three data servers are compromised by the inside attack without the private key of the user(eg:physician). Even if the user gets the encrypted data, he will not be able to decrypt without the cooperation of all the three servers.

In patient information access control protocol which is based on the Pailliercryptosystem [16], the dominated computation is the modular exponentiation, i.e., $a^x (\text{mod } N^2)$ where $x \in Z^*_{N.}$ Each data server computes two modular exponentiations and exchange $|N^2| = 2|N|$ bits, where $|N|$is the length of N. The user calculates one modular exponentiation and exchanges $2|N|$ bits.

5. CONCLUSION

Different scheme have been prescribed to implement the Healthcare Architecture but the security and privacy of the medical data is still a concern. Maintenance of the server, upgrading the server, providing storage capacity updating the Software used and their licensing is also a big concern.

Providing security and privacy of Medical data can be achieved by keeping the patient data in Cloud Servers where sensitive data are stored in encrypted format and it is shared with authorized users only. To improve the privacy and security, Proxy Re-encryption technique is used where the intent is to transform the cipher data that the owner uploads into cipher text that the user of the data can decrypt using his or her own private key. The queries forwarded by these users are evaluated on the encrypted data such that the cloud server does not learn any useful information other than the query output. The server is maintained by the cloud service provider itself. Storing the patient data in cloud servers can quicken and improve data transmission and enable remote data collection which can help the doctors to take a better decision in case of emergency.

References

[1] M. Ahmed, X. Huang, and H. Cui, "Smart Decision Making for Internal Attacks in Wireless Sensor Network," International Journal of Computer Science and Network Security,, vol. 12, no. 12, pp. 15–23, Dec. 2012.

[2] D. Bogdanov, S. Laur, J. Willemson. Sharemind: a Framework for Fast Privacy-Preserving Computations. In Proc. ESORICS'08, pages 192-206, 2008.

[3] Dan Baehr, Steve McKinney, Aaron Quirk, and Khaled Harfoush, "On the Practicality of Elliptic Curve Cryptography for Medical Sensor Networks", IEEE, 2013.

[4] X. Du and H.-H. Chen, "Security in wireless sensor networks," IEEE Wireless Communications, vol. 15, no. 4, pp. 60–66, 2008.

[5] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in Wireless Sensor Network," vol. 5, no. 7, pp. 954–960, 2011.

[6] X. Huang, M. Ahmed, and D. Sharma, "Protecting from Inside Attacks in Wireless Sensor Networks," in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), 2011, pp. 186–191.

[7] X. Huang, M. Ahmed, and D. Sharma, "A Novel Algorithm for Protecting from Internal Attacks of Wireless Sensor Networks," in 2011 sIFIP 9th International Conference on Embedded and Ubiquitous Computing (EUC), pp. 344349, 2011

[8] X. Huang, M. R. Ahmed, D. Sharma, and H. Cui, "Protecting wireless sensor networks from internal attacks based on uncertain decisions", in 2013IEEE Wireless Communications and Networking Conference (WCNC), pp. 1854–1859, 2013.

[9] 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, pages 491-494, Seoul, Korea, 16-18 August 2010.

[10] P. Kumar and H. J. Lee. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012.

[11] X. H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M-H. Han, Y-K. Lee, H. Lee. "An Energy-Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography. Journal of Communications and Networks, Special Issues on Secure Wireless Networking", December 2009.

[12] K. Lu, Y. Qian, and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 7, no. 2, pp. 639–647, Feb. 2008.

[13] Maurer U., Rowe A., Smailagic A., and Siewiorek P., "eWatch: a Wearable Sensor and Notification Platform," in Proceedings of International Workshop on BSN, Wearable and Implantable Body Sensor Networks, pp. 144-145, 2006.

[14] J. Misic, V. Misic. Enforcing Patient Privacy in Healthcare WSNs Through Key Distribution Algorithms. Secur. Commun. Network 1: 417-429, 2008.

[15] Oliver N. and Flores F., "HealthGear: A RealTime Wearable System for Monitoring and Analyzing Physiological Signals," International Workshop on Wearable and Implantable Body Sensor Networks, pp. 3-5, 2006.

[16] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT'99, pages 223-238, 1999.

[17] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, p. 53, Jun. 2004.

[18] A. Siva Sangari et al., "light weight security and authentication in wireless body area network", Indian Journal of Computer Science and Engineering, Vol. 4 No. 6, 2014.

[19] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Network. In Proc. TrustCom'13, pages 118-125, 2013.