International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Preserving Confidentiality in Wireless Medical Data

Ch. Sai Siva Durga[1] , Smt. P. Neelima[2]

[1]M.Tech, Department of Computer Science and Technology, SRKR Engineering College, Bhimavaram, West Godavari, Andhra Pradesh, India.

[2]Assistant Professor, Department of Computer Science and Technology, SRKR Engineering College, Bhimavaram, West Godavari, Andhra Pradesh, India.

ABSTRACT

In recent times, healthcare applications are widely being used for remote patient monitoring and in hospitals using wireless sensor networks. Wireless medical sensor networks are highly vulnerable to different kind of attacks such as eavesdropping, modification, data breach etc which is a potential threat to patient sensitive physiological data. Security for wireless medical sensor networks is one of the major requirements in order to attain few issues like authentication, integrity and confidentiality. A considerable measure of work has been done to secure wireless medical sensor networks. The existing healthcare solutions can protect information amid transmission but in any case fails to stop inside attack where the sensitive patient data will be revealed by the malicious database administrator. The proposed system presents a practical approach to overcome this issue by making use of multiple data servers for storing patient sensitive data. The primary contribution of this system is secure transmission of patient sensitive data to multiple data servers and performing statistical analysis on the patient data using Paillier cryptosystem and EIGamal cryptosystems by ensuring patients' privacy.

Keywords : Wireless Medical Sensor Network, Patient Data Privacy, Paillier Cryptosystem, Statistical Analysis, Eigamal Cryptosystems.

I. INTRODUCTION

Wireless Sensor Networks are widely used in medical fields which are referred to as wireless medical sensor networks (WMSNs). The healthcare applications use medical sensors to sense the patient's physiological data and transmit them wirelessly across the public channels and store in the back-end databases. They are considered as promising fields where the patients can be monitored continuously in hospitals and also at home. The physicians can monitor their patients remotely by accessing patients' health data through wireless medical sensor networks. The medical researchers can use the healthcare application for their research purpose and perform statistical analysis on patient physiological data. The patients' data will be transmitted to data server and stored in some back-end systems.

The patients' privacy becomes vulnerable if the healthcare applications are deployed without considering the security. Therefore, a paramount necessity for healthcare application is security, particularly in the account of patient's privacy. Wireless medical sensor networks conclusively improve patients' nature of care without exasperating their solace. There exist a lot of potential security threats to the patient's sensitive health data during transmission from the medical sensors to the physicians or medical researchers. Various security threats to healthcare applications that affect patients' data privacy are summarized as follows. Impersonation attack is a threat to the authenticity of patient's data. In a healthcare application, an adversary might impersonate a wireless access point, while data is being sent to a remote location.

As a result, this will lead to false alerts and the physicians could start an emergency rescue operation for an individual who is non-existent. This will even defeat the reason of wireless healthcare application. Eavesdropping is a threat to the data privacy of patients when attacker performs this type of attack. An eavesdropper may be equipped with intensively powerful receiving antenna and can retrieve the sensitive patient data from medical sensors and examines the patient's health information. The eavesdropper might even post the sensitive patient data on social networking sites which is a genuine risk to patient privacy. Modification is a threat to the data integrity of patient data. The intruder can intercept the patient's sensitive health data during transmission from the public channels and perform some alterations on the data. This could be a threat to patients when this altered data is sent to the doctors for monitoring which could result in false readings.

In order to protect the patient's remote medical sensor data against different attacks, the existing solutions are providing encryption based approaches for data transmission. They include public key encryption or secret key encryption. In secret key based mechanisms, it is assumed that the symmetric keys are pre-deployed in servers and sensors in advance. In this type of solution, AES cryptosystem is used for encryption and Message authentication code for authentication. In public key based mechanisms, RSA or Diffie-Hellman key exchange protocol is used for generating secret keys and for encryption. The Paillier cryptosystem is used for providing assured security for patient data during transmission. This cryptosystem has an added benefit in its Homomorphic properties where by providing only a set of plaintexts and the public key parameters, the product of the plaintexts is achieved.

On the decrypting side, the user can decrypt the received data and obtain the sum of the plaintexts. Paillier cryptosystem can be useful for those applications which need top of the line security and summation of the set of plaintexts. The existing solutions can provide privacy to the patients' data by ensuring protection against outside attacks but fails to provide protection against the inside attacks. Some of the existing solutions don't provide security at all and some solutions do provide security for the data transmitted over channels. The existing solution deals with security of patient data by using three servers to store patient information [1]. They split the received data from sensors into three parts and sends to three servers using a secure channel where the secret keys are pre-deployed in sensors and servers. This solution can provide protection to the sensitive patient data as long as only one data server is compromised. If the attacker is successful in compromising two of the three data servers then the existing solution is a failure. The proposed system provides a practical approach to overcome this issue and also provides protection against inside attacks. In the proposed system, even if the attacker is successful in compromising two of the three data servers, the solution is still secure.

II. RELATED WORK

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 multiple servers to achieve high stability, 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 Share mind 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 share mind 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.

III. IMPLEMENTATION

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.

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.

IV. ELGAMAL CRYPTOSYSTEM

Key aspects:

- Based on the Discrete Logarithm problem
- Randomized encryption

Application:

1. Establishing a secure channel for key sharing
2. Encrypting messages

ElGamal Cryptosystem - Key Generation

Participant A generates the public/private key pair

1. Generate large prime p and generator g of the multiplicative Group Z∗p pf of the integers modulo p.
2. 2. Select a random integer a, $1 \le a \le p - 2$, and compute ga mod p.
3. A's Public key is (p, g, ga); A's Private key is a.

ElGamal Cryptosystem - Encryption Procedure

Participant B encrypts a message m to A

1. Obtain A's authentic public key (p, g, ga).
2. Represent the message as integers m in the range $\{0, 1, \ldots, p - 1\}$.
3. Select a random integer k, $1 \le k \le p - 2$.
4. Compute γ = gk mod p and δ = m ∗ (ga)k. 5. Send ciphertext c = (γ, δ) to A

ElGamal Cryptosystem - Decryption Procedure

Participant A receives encrypted message m from B

1. Use private key a to compute ($\gamma p-1-a$) mod p.
   Note: $\gamma p-1-a = \gamma-a = a-ak$
2. Recover m by computing ($\gamma-a$) $*$ δ mod p.

V. 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, Υ, pk, sk

Output: p= $\alpha + \beta + \Upsilon$

1. The data server S1 picks a random r1 ε Z* N and computes

C1 = Encrypt (α, pk) = g ε r1 N (mod N2)

And sends C1 to the server S2

2. The data server S2 picks a random r2 ε Z* N and computes C2 = Encrypt (β, pk) = g r2 N (mod N2) And

sends C1 C2 to the server S3.

3. The data server S3 picks a random r3 ε Z* N and computes C3 = Encrypt (Υ, pk) = g r3 N (mod N 2) And replies C1 C2 C3 to the user

4. The user computes p = Decrypt(C1 C2 C3, sk)

5. Return p

Because of the Homomorphic properties of the Paillier Cryptosystem, $\alpha + \beta + \Upsilon$

C1 C2 C3` = E (α, pk) E (β, pk) E (Υ, pk)

= (g α r1 N) (g β r2 N) (g Υ r1 N) (mod N2)

= g $\alpha + \beta + \Upsilon$ (r1 r2 r3) N (mod N2)

= E ($\alpha + \beta + \Upsilon$; pk)

Therefore,

p = Decrypt (C1 C2 C3 ; sk) = $\alpha + \beta + \Upsilon$

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. 1.

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

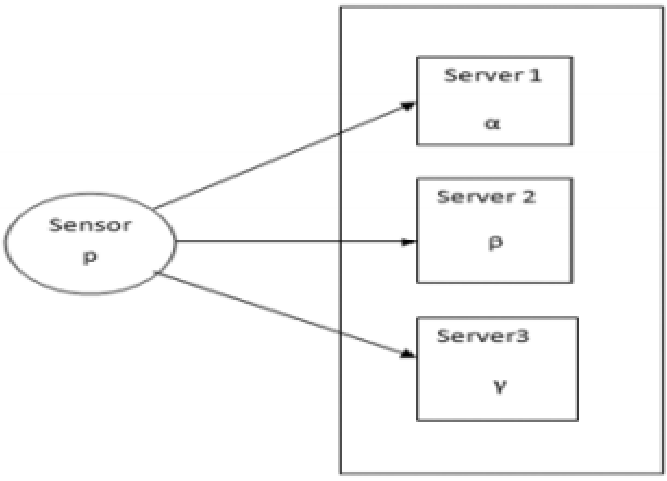

Figure 1: Data Distribution

Privacy (the inside attack), the medical sensor splits the confidential patient data p (an integer)into three integers α , β , Υ in such a way that $\alpha + \beta + \Upsilon = p$ 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 , Υ to the doctor through three secure channels. Finally, the doctor combines the three integers to obtain the patient data ñ as shown in Fig. 2

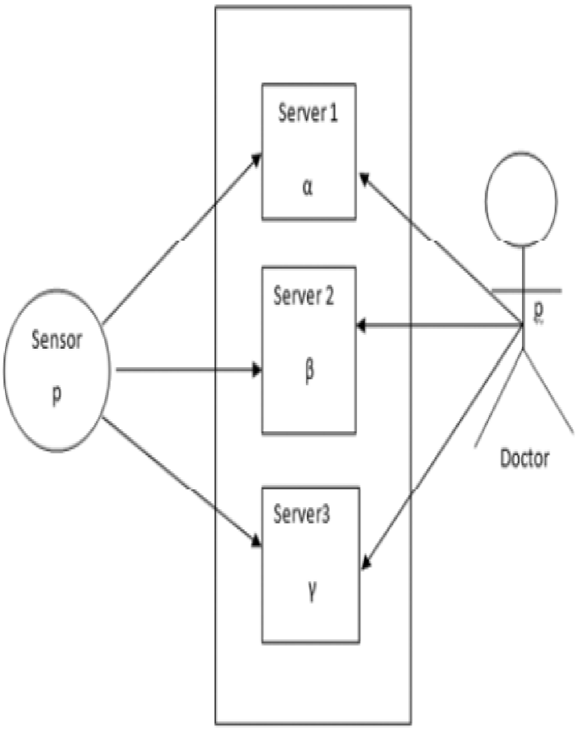

Figure 2: Data Distubution and Access

VI. EXPERIMENTAL RESULTS

The proposed method is expected to secure the patient physiological data during transmission and this solution is secure even though two of the three data servers are compromised by the adversary. That is, as long as one of the three servers is not compromised, the proposed system assures high end security to the patients. This solution is successful in providing protection against outside attacks and also inside attacks where the malicious administrator of the database of patients may capture the patient health data and perform medical frauds for his personal advantages. Hence the proposed system accomplished to provide patient privacy using the Paillier cryptosystem mechanism.

VII. CONCLUSION

This paper presents an efficient approach to provide high end security for wireless medical sensor data. Unlike other healthcare solutions, this system utilizes three data servers to store the split values of patient physiological data thereby providing more security to the patient data. The communication between the medical data server and the three data servers for processing is secured using the lightweight encryption method and SHA-3 based hashing technique. To preserve the privacy of the data, data collection protocol is implemented to split the patient health data into three random parts and store in three data servers. Access control protocol is used where the three data servers provide the doctor with the patient health data. Statistical analysis protocol is used where the three data servers process some queries and produce the analysis results for the medical researcher. This solution requires that at most one data server can be compromised. This solution can protect the privacy of patient data even if two data servers are compromised.

VIII. 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.