International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Data Security and Privacy in Wireless Sensor Devices

Meekhal Solomon[1], Eldo P Elias[2]

[1] *Student, Mar Athanasius College of Engineering Kothamangalam, India*
[2]*Second Assistant Professor, Dept. of CSE, Mar Athanasius College of Engineering Kothamangalam, India*

Abstract - *The wireless medical sensor network has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters to be collected by small wearable and communicated using short-range wireless communication techniques. It has shown great potential in improving healthcare quality, and thus has found a wide range of applications which includes ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. But, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications. A practical approach for secure data storage, and fine-grained distributed data access control for sensitive and confidential patient medical data is proposed in this work. Here, for security, the sensor data is splitted and stored in three different servers. RSA algorithm is used for digital signatures for different users. Most importantly, we use homomorphic encryption scheme to access and to perform statistical analysis on the data collected. Also we use attribute based encryption for fine grained access control for personal as well as medical data of the patient.*

Key Words: **WSN, DSS, Paillier Cryptosystem, ABE**

1. INTRODUCTION

Wireless medical sensor networks (WMSNs) is a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters to be collected by wearable biosensors. Recently, interest in wireless systems for medical applications has been rapidly increasing. With a number of advantages over wired alternatives, including: ease of use, reduced risk of infection, reduced risk of failure, reduce patient discomfort, enhance mobility and low cost of care delivery, wireless applications bring forth exciting possibilities for new applications in medical market. Wireless medical sensor networks certainly improve patient's quality-of-care without disturbing their comfort. However, there exist many potential security threats to the patient sensitive physiological data transmitted over the public channels and stored in the back-end systems. The common threats are eavesdropping, spoofing, altering and replaying attacks. The aim of the proposed work is to develop a new method to prevent the inside attack by using multiple data servers to store patient data, analyze the medical data from body worn sensors, provide authorized access to each part of the patient data and perform statistical analysis on the data without compromising the patient's privacy. The data collection protocol is based on a random number generator which splits the patient data into three and sent it to the three servers. To access the patient data without revealing it to any data server, a new data access protocol is proposed on the basis of the Paillier cryptosystem and attribute based encryption. Privacy preserving statistical analysis are also done using these protocols.

This paper is organized as follows: Section II describes the related works. Section III describes working of the proposed system and in Section IV the conclusions of this research is presented.

2. RELATED WORKS

Healthcare applications are considered as promising elds for wireless sensor networks. In recent years, several WMSN projects have been proposed and a a lot of work has been done to protect the wireless medical sensor networks against various attacks. Some among them are listed here. CodeBlue [2], [3] is a popular healthcare research project based on WMSN developed at the Harvard Sensor Network Lab. In the architecture, several medical sensors (e.g., pulse oximeter, EMG, EKG, and SpO2 sensors) are placed on the patient's body. These medical sensors sense the patient body and transmit it wirelessly to the end-user devices (PDAs, laptops, and personal computers) for further analysis. Furthermore, the Code Blue architecture facilitates RF-based localization, which is accurate enough to locate a patient's or medical professional's position.

In [11], a secure, lightweight public key - based security scheme, Mutual Authentication and Access Control based on Elliptic curve cryptography (MAACE) is described. MAACE is a mutual authentication protocol where a healthcare professional can authenticate to an accessed node (a PDA or medical sensor) and vice versa. This is to ensure that medical data is not exposed to an unauthorized person. On the other hand, it ensures that medical data sent to healthcare professionals did not originate from a malicious node. MAACE is more scalable and requires less memory compared to symmetric key-based schemes. Furthermore, it is much more lightweight than other public key-based schemes.

Dagtas et al. [16] proposed a real time and secure architecture for health monitoring in smart homes using ZigBee technology. The proposed framework has the following features: (a) the ability to detect signals wirelessly within a body area sensor

network (BSN); (b) low-power and reliable data transmission using ZigBee technology; (c) secure transmission of medical data over BSN; (d) efficient channel allocation over wireless

networks, and (e) optimized analysis of data using an adaptive framework

that maximizes the processing and computational capacity. A secure key management protocol was proposed to establish secure session keys in body sensor networks and the cryptographic keys facilitate security services, e.g., condentiality, authentication, and data integrity. An authentication protocol was used between the body sensors and the handheld device of the mobile patient.

3. PROPOSED WORK

Figure 1 shows the health care application using wireless medical sensor networks.

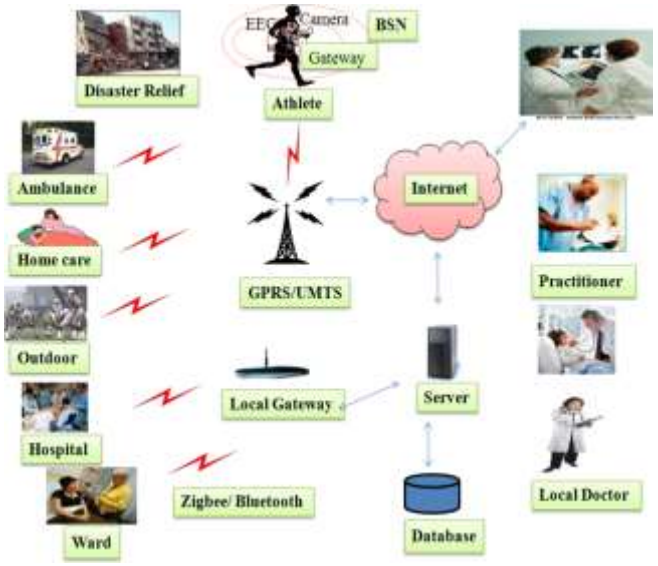

Fig 1: Healthcare application using wireless medical sensor networks.

The proposed system has four stages as follows

- A medical sensor network which wireless senses the patient's body and transmits the patient data to a database system.
- A patient database system which stores the patient data from medical sensors and provides services to users (e.g., physicians and medical professionals).
- A patient data access control system which is used by the user (e.g., physician) to access the patient data and monitor the patient.
- A patient data analysis system which is used by the user (e.g. medical researcher) to query the patient database system and analyze the patient data statistically.

The communications between the medical sensors and the three servers are secured using lightweight encryption scheme.

Thus data confidentiality, authenticity and integrity are achieved between each medical sensor and each data server. Any inside attacker, including each data server, cannot guess the two random numbers without the secret key as the medical sensor splits the patient data into three numbers and sends them to the three data servers, respectively, through secure channels. Two of the three numbers are generated by SHA-3 with a secret key K and an initial vector IV. In the access control protocol and the statistical analysis protocols, the patient data is always encrypted by the public key of the user. Without the private key of the user, even if two data servers are compromised by the inside attacks, the attacker can never obtain the patient data. To provide more security to the personal details of the patient, it is encrypted using CP-ABE scheme. Therefore only users whose credentials satisfy the policy requirements can decrypt the encrypted data.

The communication between each medical sensor and each data server is through a secure channel, which is implemented by a secret-key cryptosystem. The patient data over the secure channel is encrypted with the secret key pre-shared between the sensor and the data server. Without the secret key, the attacker cannot eavesdrop the patient data. Because the medical sensors are usually low-power and lightweight encryption scheme and the message authentication code generation scheme is proposed in for the secure channel. Both schemes are built on the smallest version of the SHA-3 with r= 40 and c= 160, which can provide a security level sufficient for many applications. In addition, the random numbers in data collection protocol are also generated with SHA-3. To get access to the patient data, the user sends a request including the patient's identity, the data attribute, and the signature of the user on the query to the three data servers through the three secure channels, respectively. Secure channels are established for the user to submit his queries because the patient's personal information 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, the three servers send the shares of the data according the patient's identity and the attribute of the data.

Data Collection

The wireless medical sensor network senses the patient's body and transmits the patient data to a patient database system. There is an initial deployment phase between each medical sensor and each data server. For each medical sensor, three secret keys are pre deployed and pre-shared with three data servers, respectively. Each secret key is used to create a secure channel between the sensor and one data server. In addition, one more secret key is pre-deployed in each sensor in order to generate random numbers. Note that different medical sensors are deployed with different secret keys. The data from the sensors is split into three using a random number generator and sent to three servers respectively.

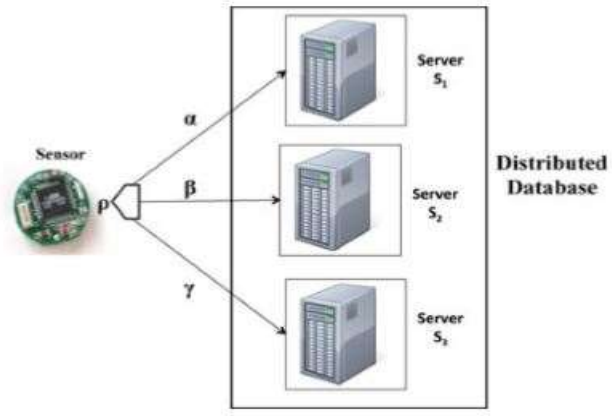

Fig. 1 Data collection

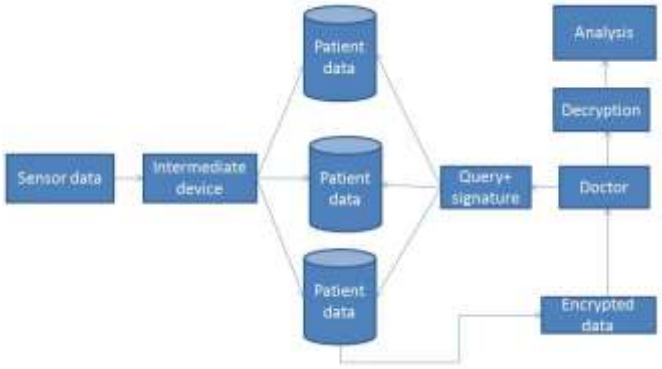

Fig. 2 Proposed System Architecture

Access control

There is an initialization phase before any user (physician) can get access to the patient data. In this phase, the user generates a public and private key pair (p_k, s_k) for the Paillier cryptosystem and a signature verification and signing key pair (p_k^*, s_k^*) for the digital signature standard (DSS). For security reason, the size of N in the Paillier cryptosystem is required to be more than 1024 bits. Assume that there exists a public key infrastructure (PKI), where there exists a certificate authority (CA) which certifies the public keys. In addition, we assume that the user establishes three secure channel with three data servers, respectively. To get access to the patient data, the user sends a request including the patient's identity, the data attribute, the signature of the user on the query, and the certificate of the user to the three data servers through the three secure channels, respectively. Only the concerned doctor of a patient can view his personal data. Other doctors can only access the medical details of the patient for analysing the treatment of other similar patients. This can be achieved using attribute based encryption that enables secure data sharing by multiple users. The data is encrypted using an access policy based on credentials (i.e., attributes). Only the users whose credentials satisfy the access policy can access data.

Statistical analysis

Privacy-preserving statistical analysis is done on the patient data for medical research, where the three data servers cooperate to help the medical researcher analyze the patient data without revealing the patient privacy. The different stsistical analysis done are average analysis, correlation analysis, variance analyis and regression analysis.

4. CONCLUSION

In this work, we have investigated the security and privacy issues in the medical sensor data collection, storage and queries and presented a complete solution for privacy preserving medical sensor network. To secure the communication between medical sensors and data servers, we used the lightweight encryption scheme and MAC generation scheme based on SHA-3. To keep the privacy of the patient data, we proposed a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g.,physician) to access the patient data, we proposed an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher) to perform statistical analysis on the patient data, we proposed some new protocols for average, correlation, variance and regression analysis, where the three data servers cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results. The access control module involves the implementation of Paillier cryptosystem and Digital signature standard for for data authentication and integrity. Attribute based encryption which is a public-key encryption that enables secure data sharing by multiple users is to be implemented to encrypt the personal details of the patient. The data is encrypted using an access policy based on credentials (i.e., attributes). Only the users whose credentials satisfy the access policy can access data. CP-ABE scheme provides a ne-grained access control to encrypted data. Private key of a user is associated with user credentials. Ciphertexts specify an access policy and only users whose credentials satisfy the policy requirements can decrypt them.Statistical analysis module allows the statistical analysis on the patient data. for medical research, where the three data servers cooperate to help the medical researcher analyze the patient data without revealing the patient privacy. This module will be also implemented in the second phase which involves several analysis such asaverage analysis, correlation analysis, variance analysis and

regression analysis etc. Security and privacy analysis has shown that our protocols are secure against both outside and inside attacks as long as one data server is not compromised. Performance analysis has shown that our protocols are practical as well.

REFERENCES

1. Xun Yi, Athman Bouguettaya , Dimitrios Georgakopoulos, Andy Song, and Jan Willemson "Privacy Protection for Wireless Medical Sensor Data",IEEE transactions on dependable and secure computing, VOL. 13, NO. 3, MAY/JUNE 2016.

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

3. D. Malan, T. F. Jones, M. Welsh, S. Moulton. " CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care". In Proc. MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES'04), Boston, MA, USA, 69 June 2004.

4. K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shayder, G. Mainland, M. Welsh. "Sensor Networks for Emergency Response: Challenges and Opportunities". Pervas. Comput. 3: 16-23, 2004.

5. A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He,S.Lin,J.Stankovic. "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring". Technical Report CS-2006-01; Department of Computer Science, University of Virginia: Charlottesville, VA, USA, 2006.

6. J. Ng, B. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Z. Yang. "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors(UbiMon)". In Proc. 6th International Conference on Ubiquitous Computing (UbiComp04), Nottingham, UK, 7-14 September 2004.

7. 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.Syst.10:1-29,2010.

8. R. Chakravorty. "A Programmable Service Architecture for Mobile Medical Care".In Proc. 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW06), Pisa, Italy, 13-17 March 2006.

9. T. Dimitriou, K. Loannis. "Security Issues in Biomedical Wireless Sensor Networks". In Proc. 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL08), Aalborg, Denmark, 25-28 October 2008.

10. 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. 27: 400-411, 2009.

11. K. Malasri, L. Wang. "Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors" 9: 6273-6297, 2009.

12. X. H. Le, M. Khalid, R. Sankar, S. Lee. "An Efcient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare". J. Networks 27: 355-364, 2011.

13. Misic, V. Misic. "Enforcing Patient Privacy in Healthcare WSNs Through Key Distribution Algorithms". Secur. Commun. Network 1: 417-429.