© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Privacy Protection for Wireless Medical Sensor Data

Meekhal Solomon, Eldo P Elias

Department Computer Science and Engineering Mar Athanasius College of Engineering Kothamangalam, India

ABSTRACT

Health care involves expensive and challenging services that prominently affect the quality of patients' life and economies. The following decade will witness a surge in remote health-monitoring systems that are based on body-worn monitoring devices. These devices record multiple physiological signals, such as ECG and heart rate, or measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG. The medical data that is acquired from patients by the distributed sensor network can be transmitted to a remote location and can be viewed by a health care professional. Although the system has many advantages and it facilitates the patients and health service providers significantly, the possibility of privacy breaches can allow sensitive health care information to move into the wrong hands. To assure the privacy of the personal health information during the transmission from the sensory networks, a sophisticated cryptographic architecture must be designed and it must ensure secure storage, secure sharing and secure computation of the patient data. A practical approach to prevent both inside and outside attacks to the confidential data is proposed in this work. The main contribution is securely distributing the patient data in multiple data servers and employing the homomorphic encryption schemes (Paillier and ElGamal cryptosystems) to perform statistic analysis on the patient data . In real-world health case scenarios, more than one party may need to access the patient data and each may have different access requirements. This can be achieved using cipher text attribute based encryption(CP-ABE). Thus secure storage, secure access and secure computation is achieved without compromising patient' s privacy.

Keywords: Paillier Cryptosystem, Elgamal cryptosystem, CP-ABE.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructureless wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location where the data can be analysed. Currently, WSN is the most standard services employed in commercial and industrial applications, because of its technical development in a processor, communication, and low-power usage of embedded computing devices. This technology is thrilling with infinite potential for many application areas like medical, environmental, transportation, military, entertainment, homeland defence, crisis management and also smart spaces.

Healthcare applications are considered as promising fields for wireless sensor networks. Wireless medical sensor networks (MSNs) is a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters to be collected by wearable or implantable 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. Portable devices such as heart rate monitors, pulse oximeters, spirometers and blood pressure monitors are essential instruments in intensive care.

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. To protect the wireless medical sensor networks against various attacks, a lot of work has been done. The already available solutions can safeguard the patient data during communication, which can be effectively done by encryption, authentication and access control, but unable to terminate the inside attack where the proprietor of the patient database discloses the delicate patient information. Therefore, there is a strong demand for the development of a system that effectively prevent both inside and outside attacks.

The objective 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.

A new data collection protocol is proposed for preventing the patient data from the inside attacks. This 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. To preserve the privacy of the patient data in statistical analysis, some new privacy-preserving statistical analysis protocols on the basis of the Paillier and ElGamal cryptosystems is proposed.

This paper is organized as follows: Section II describes the security requirements of wireless medical sensor networks. Section III describes working of the proposed system and in Section IV the conclusions of this research is presented.

II. SECURITY REQUIREMENT

Security is one of the most important aspects of any system. In general words, the concept of security is similar to safety of the system as a whole. The communications in sensor networks applications in healthcare are mostly wireless in nature. This may result in various security threats to these systems. These threats and attacks could pose serious problems to the social life of an individual who is using the wireless sensor devices. People with malicious intent may use the private data to harm the person. The elementary requirements of secure health monitoring using WSNs are safely exchanging the patient's health information transmitted by WSN devices, and preventing improper use of illegal devices, such as intercepting transferred data, eavesdropping patient health-status data, replaying out-of-date information. In this section, we describe essential security requirements of health monitoring using sensor network as follows:

A. Data confidentiality

Data confidentiality is a major problem for healthcare and medical emergency system since it accumulates significant information. Sharing and transmission of private via Internet leads to easily intercept it by unauthorized parties. Attackers need to access private information by capturing data transmission and forging themselves as authorized user. Cryptography algorithms (encryption schemes) are possible solution to achieve patient confidentiality, to protect the patient data eavesdropping by an adversary.

B. Data authentication

Since the patient health data is very sensitive, it is desirable that proper user authentication should be considered, where each user (doctor, nurse, and etc.)

must prove their authenticity and then access the WMSN data. Data authentication can be achieved by using symmetric and asymmetric techniques.

C. Data Integrity

Data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.Feature extraction is done using discrete wavelet transform. Proper data integrity mechanisms is necessary to ensure that the received data is not altered by an adversary.

III. PROPOSED WORK

The proposed architecture has four systems as follows

- A wireless medical sensor network which senses the patient’s body and transmits the patient data to a patient database system.
- A patient database system which stores the patient data from medical sensors and provides querying 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 sufcient 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 verication 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.

A. Data Collecton

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.

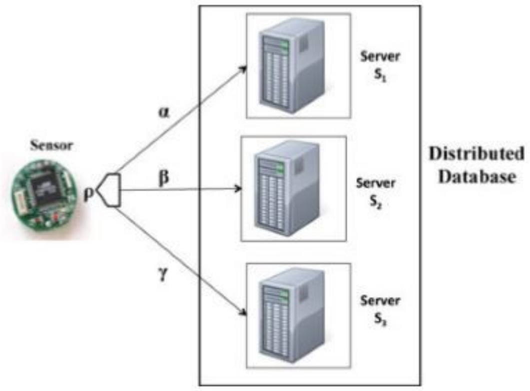

Figure 1. Data collection

B. 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.

C. 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.

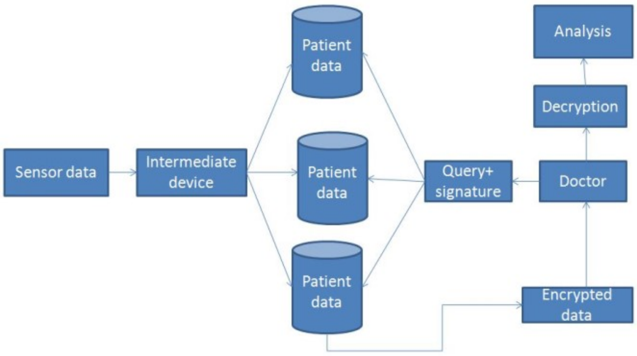

Figure 2. Proposed System Architecture

IV. CONCLUSION

Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. Securing wireless medical sensor networks from different attacks is a challenging task. The proposed method a complete solution for privacy preserving medical sensor network. To keep the privacy of the patient data, a new data collection protocol is implemented which splits the patient data into three numbers and stores them in three data servers, respectively. To assure the privacy of the personal health information during the transmission from the sensory networks,a sophisticated cryptographic architecture is designed for the secure storage, secure sharing and secure compuation of the patient data.

V. 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.