PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

Mrs. N. BHAGYA LAKSHMI

Assistant Professor, Department of CSE, Sri Mittapalli College of Engineering,
Tummalapalem, NH-16, Guntur, Andhra Pradesh, India.

1) P. KRISHNA VENI , 2) B. PRASANNA , 3) V.LAKSHMI KAVYA , 4) V. SOWJANYA

B. Tech Students, Department of CSE, Sri Mittapalli College of Engineering,
Tummalapalem, NH-16, Guntur, Andhra Pradesh, India.

Abstract:. In recent years, wireless sensor networks have been widely used in healthcare applications, such as hospital and home patient monitoring. Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. A lot of work has been done to secure wireless medical sensor networks. 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. In this paper, we propose a practical approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy.

I. INTRODUCTION

wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored in hospitals and even at home using wireless medical sensor networks (WMSNs). In recent years, many healthcare applications using WSNs have been developed, such as CodeBlue. Alarm-Net, UbiMon MEDiSN , and MobiCare . A typical example of healthcare applications with WSNs is Alarm-Net developed in University of Virginia for assisted-living and residential monitoring Typical security threats to healthcare applications with WSNs can be summarized as follows.

Eavesdropping is a security threat to the patient data privacy. An eavesdropper, having a powerful receiver antenna, may be able to capture the patient data from the medical sensors and therefore knows the patient's health condition. He may even post the patient's health condition on social network, which can pose a serious threat to patient privacy.

Impersonation is a security threat to the patient data authenticity. In a home care application, an attacker may impersonate a wireless rely point while patient data is transmitting to the remote location. This may lead to false alarms to remote sites and an emergency team could start a rescue operation for a non-existent person. This can even defeat the purpose of wireless healthcare.

Most of current solutions focus on how to protect the wireless medical sensor networks against the outside attacks, where the attacker does not know any information about the secret keys. The solution 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 data servers are compromised by the inside attack, the solution becomes insecure. we assume that the wireless medical sensor network is composed of some medical sensors, three data servers, and some users. Each sensor sends the patient data to the three data server in the same way as . Unlike , the three data servers process the queries, such as statistical analysis on the patient data, from the users on the basis of the Paillier and ElGamal cryptosystems instead of the Sharemind system.

The patient data privacy can be preserved as long as at least one of three data servers is not compromised. Even if two data servers are compromised but one data server is not compromised, our solution is still secure.

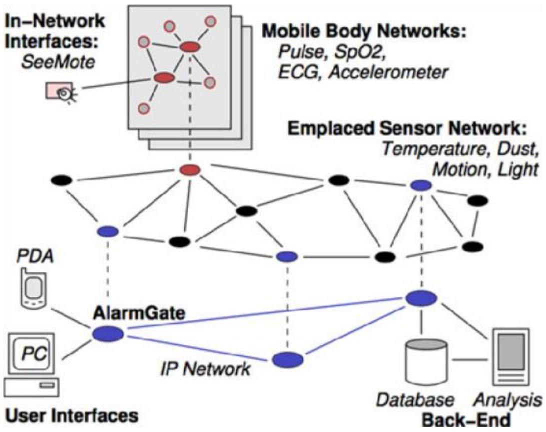

Fig. 1. Alarm-net architecture.

II. PRELIMINARIES

Two basic building blocks of our solution are the Paillier and the ElGamal public key cryptosystems which are described in this section.

A. Paillier Public-Key Cryptosystem

The Paillier encryption scheme named after and invented by Pascal Paillier in 1999, is a probabilistic public key encryption algorithm. It is composed of key generation, encryption and decryption algorithms as follows.

1) Key Generation

The key generation algorithm works as follows.Choose two large prime numbers p and q randomly and independently of each other such that N ¼ pq; ¼ lcmp 1;q 1Þ

where lcm stands for the least common multiple.

Select random integer g where g 2Z$_{N2}$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse: m¼ðLðgðmod N^{2}ÞÞÞ^{1}ðmod NÞ; where function L is defined as1 LðuÞ¼ : N Note that the notation a=b does not denote the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divided by b.

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

The private (decryption) key sk is (;m).

If using p;q of equivalent length, one can simply choose

g ¼ N þ 1; ¼’ðNÞ;m¼’ðNÞ^{1}ðmod NÞ;

where N ¼ p q and ’ðNÞ¼ðp 1Þðq 1Þ.

2) Encryption

The encryption algorithm works as follows.

Let m be a message to encrypt, where m 2Z$_{N}$.

Select random r where r 2Z $_{N}$.

Compute ciphertext as

c ¼ g^{m} r^{N}ðmod N^{2}Þ

3) Decryption

The decryption algorithm works as follows

Let c be the ciphertext to decrypt, where the Ciphertext c 2Z$_{N2.}$ Compute the plaintext messages as m ¼ Lðcðmod N^{2}ÞÞmðmod NÞ:

4) Homomorphic Properties

A notable feature of the Paillier cryptosystem is Homomorphic properties. Given two ciphertexts Eðm$_{1}$;pkÞ¼ g^{m_1}r^{N}$_{1}$ ðmod N^{2}Þ

Eðm$_{2}$;pkÞ¼ g^{m_2}r^{N}$_{2}$ ðmod N^{2}Þ;

where r$_{1}$;r$_{2}$ are randomly chosen for Z$_{N}$, we have the following homomorphic properties.

B. ElGamal Public-Key Cryptosystem

The ElGamal encryption scheme, named after and invented by Taher ElGamal in 1985, is a probabilistic public key algorithm. It is composed of key generation, encryption and decryption algorithms as follows

1) Key Generation

The key generator works as follows. Generate a cyclic group G, of large prime order q, with generator g. Choose a random x 2f1;...;q 1g and compute

y ¼ g^{x}:

The public (encryption) key pk is ðG;q;g;yÞ. The private (decryption) key sk is x. The encryption algorithm works as follows.

Let m be a message to encrypt, where m 2 G. Choose a random r 2f1;...;q 1g.

Compute the ciphertext c ¼ðA;BÞ, where

A ¼ g^r B ¼ m y^r:

2) Decryption

The decryption algorithm works as follows. Let c ¼ðA;BÞ be a ciphertext to decrypt.

Compute

m ¼ B=A^x:

The decryption algorithm produces the intended message, since

B=A^x ¼ m y^r=g^{rx} ¼ m gxr=grx

3) Homomorphic Property

ElGamal encryption scheme has homomorphic properties. Given two ₂ encryptions₂ ðA$_1$;B$_1$Þ¼ðg^{r1};m$_1$y^{r1}Þ and ðA$_2$;B$_2$Þ¼ðg^r ;m$_2$y^r Þ, where r$_1$;r$_2$ are randomly chosen from f1;2;...;q 1g and m$_1$;m$_2$ 2 G, one can compute

ðA$_1$;B$_1$ÞðA$_2$;B$_2$Þ¼ðA$_1$A$_2$;B$_1$B$_2$Þ

¼ðg g ;ðm$_1$y Þðm$_2$y ₂ÞÞ

¼ðgr1þr2;ðm1m2Þyr1þr2Þ

which is the encryption of m$_1$m$_2$.

III. PRIVACY-PRESERVING WIRELESS MEDICAL SENSOR NETWORK

A. Our Model

Like most of healthcare applications with wireless medical sensor network, our 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.

To query the patient database system and analyze the patient data statistically.

There may be a middleware between the wireless medical sensor network and the patient database system. If so, the role of the middleware is simply forwarding the encrypted patient data to the database system. In our model, the patient database system is composed of multiple database servers. We assume that all data servers are semi-honest, often called “honest but curious”. That is, all data servers run our protocol exactly as specified, but may try to learn as much as possible about the patient data from their views of the protocol. In addition, we assume that at least one data server is not compromised by attackers. For simplicity, we assume that the number of data servers is three. In fact, it can be any number more than three. The architecture of our model with three data servers can be shown in Fig. 2.

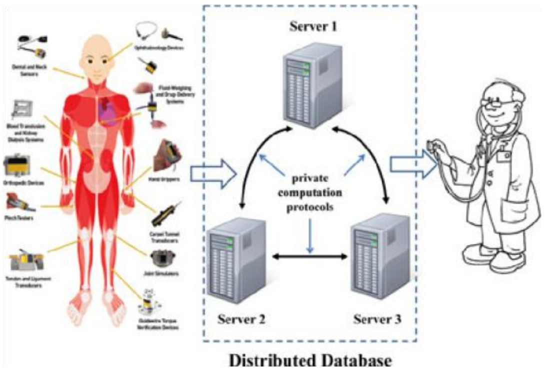

Fig. 2. Our model.

B. Data Collection Protocol

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

Fig. 3. Data collection

C. Access Control Protocol

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 (pk;sk) for the Paillier cryptosystem as described in Section 2.1 and a signature verification and signing key pair (pk ;sk) 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 (pk;pk) for the user in a digital certificate. In addition, we assume that the user establishes three secure channel with three data servers, respectively.

IV. SECURITY AND PRIVACY ANALYSIS

A. Security Analysis

In our architecture as shown in Fig. 2, there are three parts of communications as follows.

The communications between the medical sensors and the three servers;

The communications between the user (e.g., physicians or medical professional) and three servers; The communications among the three servers.

In our solution, 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 low-cost, we can choose the lightweight encryption scheme and the message authentication code generation scheme proposed in for the secure channel. Both schemes are built on the smallest version of the SHA-3 with r ¼ 40;c ¼ 160, which can provide a security level sufficient for many applications. In addition, the random numbers in our data collection protocol are also generated with SHA-3.

V. PERFORMANCE ANALYSIS

In our data collection protocol, we can use the lightweight encryption scheme and MAC generation scheme proposed in. In addition, our random number stream generation scheme is also based on SHA-3. All security mechanisms in the sensor can be implemented with the same SHA-3. This design is suitable for wireless sensor networks where area is particularly important since it determines the cost of the sensors.Our access control protocol is built on the Paillier cryptosystem , where the dominated computation is the modular exponentiation, i.e., a^xðmod N^2Þ where x 2Z_N. In each data server computes two modular exponentiations and exchange jN^2j¼ 2jNj bits, where jNj is the length of N. The user computes one modular exponentiation and exchanges 2jNj bits.

Our average analysis protocol is also built on the Paillier cryptosystem. In Algorithm 2, the computation and communication complexities for each data server and the user are the same as those in Algorithm 1 In our correlation analysis protocol, with the help of the three data servers, the user compute $s_x;s_y$ by Algorithm 2 and compute $s_{xy};s_{x^2};s_{y^2}$ by Algorithm 3 or Algorithm 4 and then computes the correlation r_{xy}. Algorithm 3 is based on the Paillier cryptosystem and can be used when the user is permitted to access the individual patient data. Algorithm 4 is based on the combination of the ElGamal and Paillier cryptosystems and can be used when the user is not permitted to access any individual patient data.

Each data server computes 4n modular exponentiations and exchanges 8jNjn bits in average, where n is the number of patients. The user computes one modular exponentiation and exchanges 2jNj bits. In Algorithm 4 , each data server computes 8n modular exponentiations and exchanges 20jNjn bits in average. The user computes one modular exponentiation and exchange 4jNj bits.

VI CONCLUSION

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. 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.

7 REFERENCES

[1] Advanced encryption standard (AES). (2001, Nov. 26). FIPS PUB 197 [Online]. Available: http://csrc.nist.gov/publications/fips/ fips197/fips-197.pdf

[2] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," J. Personal Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014.

[3] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security, 2008, pp. 192–206.

[4] R. Chakravorty, "A programmable service architecture for mobile medical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop, Pisa, Italy, Mar. 13–17, 2006, pp. 532–536.

[5] Crypto++ 5.6.0 Benchmarks [Online]. Available: http://www. cryptopp.com/benchmarks.html, 2009.

[6] J. Daemen, G. Bertoni, M. Peeters, and G. V. Assche. (2012, Jul. 6). Permutation-based encryption, authentication and authenticated encryption. Proc. Directions Authenticated Ciphers, Stockholm, Sweden [Online]. Available: http://www.hyperelliptic.org/DIAC/ slides/PermutationDIAC2012.pdf.

[7] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, and N. Challa, "Real-Time and secure wireless health monitoring," Int. J. Telemed. Appl., pp. 1–10, Jan. 2008.

[8] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[9] (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS. 186-4.pdf

[10] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[11] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 316–326, Jan. 2014.

[12] F. Hu, M. Jiang, M. Wagner, and D. C. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign," IEEE Trans. Inf. Tech. Biomed., vol. 11, no. 6, pp. 619–627, Nov. 2007.

[13] Y. M. Huang, M. Y. Hsieh, H. C. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 400–411, May 2009.

[14] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terzis, and G. M. Masson, "MEDiSN: Medical emergency detection in sensor networks," ACM Trans. Embedded Comput. Syst., vol. 10, pp. 1–29, 2010.

[15] P. Kumar, Y. D. Lee, and H. J. Lee, "Secure health monitoring using medical wireless sensor networks," in Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage., Seoul, Korea, Aug. 16–18, 2010, pp. 491–494.