Protection and Security for Wireless Medical Sensor Data

DHARMARAJ CHAVAN, TUKARAM DUKARE, SUMAN SAKSAMUDRE, HEMLATA VAIDYA

Lecturer, Computer Department, Aditya Polyechnic College, Maharashra, India
Lecturer, Computer Department, M S Polyechnic College, Maharashra, India
Lecturer, Computer Department, Aditya Polyechnic College, Maharashra, India
Lecturer, Computer Department, M S Polyechnic College, Maharashra, India

ABSTRACT

In recent years, wireless sensor networks are widely used in healthcare applications, such as hospital monitoring. Wireless medical sensor networks are more effective to eavesdropping, modification, replaying attacks and impersonation than the wired networks. A lot of efforts have been done to secure wireless medical sensor networks. The existing systems can protect the patient data during transmission, but cannot drop the inside attack where the administrator of the patient database requires the sensitive patient data. In this paper, we propose a practical approach for preventing 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 statistical analysis on the patient data without compromising the patients' privacy.

Keyword: - *Wireless medical sensor network, patient data privacy, Paillier encryption, and ElGamal encryption.*

---

1. INTRODUCTION

A 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.

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. 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. Back-end systems provide online analysis of sensor data and long-term storage of data. User interfaces allow any legitimate user of the system to query sensor data.

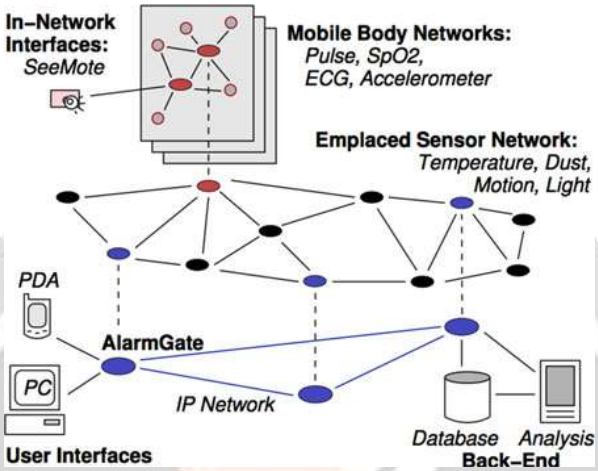

Fig 1: Alarm-net architecture.

2. PRELIMINARIES

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

2.1 Paillier Public-Key Cryptosystem

The Paillier encryption scheme [25], 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.

2.1.1 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 gcd (pq, (p-1)(q-1)) = 1.

- Compute

  N = pq, v = lcm (p -1, q -1),

  Where LCM stands for the least common multiple.

- Select random integer g where g 2 Z_N2 and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

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).

2.1.2 Encryption

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m 2 ZN.
- _ Select random r where r 2 Z_N.
- _ Compute ciphertext as

2.1.3 Decryption

The decryption algorithm works as follows.

- Let c be the ciphertext to decrypt, where the ciphertext.
- Compute the plaintext message.

2.1.4 Homomorphic Properties

A notable feature of the Paillier cryptosystem is its homomorphic properties.

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

2.2 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.

2.2.1 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 and compute
- The public (encryption) key pk (G, q, g, y).
- The private (decryption) key sk is x.

2.2.2 Encryption

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m == G.
- Choose a random r.
- Compute the ciphertext c = (A;B), where
  A = g

  B = m * y

2.2.3 Decryption

The decryption algorithm works as follows.

- Let c = (A, B) be a ciphertext to decrypt.
- Compute m = B/Ax:

The decryption algorithm produces the intended message.

2.2.4 Homomorphic Property

ElGamal encryption scheme has homomorphic properties.

3. CONCLUSION

In this paper, 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 proposed in [31]. 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.

4. 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.