International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Privacy Protection for Medical Sensed Data

Nithesh R[1], Ravikumar H R[1], Sachin M S[1], Vimal Raj M[1], Yuvaraj B N[2]

[1] *BE, Department of CSE, NIE Mysuru,, Karnaraka, India.*
[2] *Professor, Department of CSE, NIE Mysuru,, Karnaraka, India.*

Abstract – *Wireless sensor networks is used in healthcare applications, such as hospitals and home patient monitoring. These are susceptible to attacks like eavesdropping, modification, impersonation and replaying attacks. Here, the practical approach to prevent the inside attack is done by distributing the patients' sensed data in multiple servers and using the Paillier and ElGamal Cryptosystems to perform static analysis on the sensed data of the patients without compromising the privacy of the patients' sensed data.*

Key Words: *Wireless sensor network, patient data privacy, Paillier and ElGamal encryption.*

1. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions and to pass their data through the network to the main location. Health care applications are considered as promising field for wireless sensor networks, where patients can be monitored in hospitals and even at home using wireless medical sensor networks. Many applications of healthcare have use wireless sensor networks, such as Codeblue[1], Alarm Net[2]. Threats to patients' sensed data are: One is Eavesdroppig. It is done by using the powerful receiver antenna, which captures the patients' data from medical sensor and knows the patients' health condition. Second is Impersonation, here an attacker may impersonate a wireless rely point while patient data is transmitting to the remote location and thus setting the false alarms. Third is Modification, here during the transmission of patients' data an attacker may capture the data from the wireless channel and alters.

The goal here is to prevent the data from the above inside attacks. So the steps taken are

- The sensor splits the sensed data into three components and sends them to multiple (here it is three) servers.
- A new data access protocol is used which is on the basis of Paillier[3] cryptosystem. This protocol allows the user (e.g., physician) to access the patient data without revealing it to any other data servers.
- A new privacy-preserving statistical analysis protocol on the basis of Paillier[3] and ElGamal[4] cryptosystems. These protocols allow the user to perform the analysis statistically without affecting the patient data privacy.

2. PAILLIER CRYPTOSYSTEM AND ELGAMAL CRYPTOSYSTEM

These are the two basic building blocks of the solution that is proposed here.

2.1 Paillier Public-Key Cryptosystem

The Paillier encryption scheme [3] is a probabilistic public key encryption algorithm. It consists of key generation, encryption and decryption algorithms as follows.

2.1.1 Key Generation Algorithm

It works as follows:

- Select two large prime numbers p and q randomly which are independent of each other such that

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

- Compute

$$N=pq,\ \lambda=lcm(p-1,q-1),$$

Where lcm stands for least common multiple.

- Select random integer g where $g \in Z^*_{N2}$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

$$\mu=(L(g^{\lambda}(mod\ N^2)))^{-1}(mod\ N),$$

where function L is defined as

$$L(u)=(u-1)/N.$$

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 (λ, μ).
If using p,q of equivalent length one can simply choose

$g=N+1$, $\lambda=\varphi(N)$, $\mu=\varphi(N)^{-1}(mod\ N)$,
where $N=pq$ and $\varphi(N)=(p-1)(q-1)$.

2.1.2 Encryption Algorithm

It works as follows:

- Let m be a message to encrypt, where $m \in Z_N$.
- Select random r where $r \in Z^*_N$.
- Compute ciphertext as

$$c=g^m . r^N (mod\ N^2).$$

2.1.3 Decryption Algorithm

It works as follows:

- Let c be the ciphertext to decrypt, where the ciphertext $c \in Z^*_{N2}$.
- Compute the plaintext message as

$$m=L(c^\lambda (mod\ N^2)) . \mu (mod\ N).$$

2.2 ElGamal Public-Key Cryptosystem

The ElGamal encryption scheme [4] is a probabilistic public key encryption algorithm. It consists of key generation, encryption and decryption algorithms as follows.

2.2.1 Key Generation Algorithm

It works as follows:

- Generate a cyclic group G, of large prime order q, with generator g.
- Choose a random $x \in \{1,. . . . ,Q-1\}$ and compute

$$y=g^x.$$

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

2.2.2 Encryption Algorithm

It works as follows:

- Let m be a message to encrypt, where $m \in G$.
- Choose a random $r \in \{1, ... , q-1\}$.
- Compute the ciphertext $c =(A,B)$, where

$$A = g^r$$
$$B = m . y^r.$$

2.2.3 Decryption Algorithm

It works as follows:

- Let $c = (A,B)$ be a ciphertext to decrypt.
- Compute

$$m = B/A^x.$$

The decryption algorithm produces the intended message, since

$$B/A^x = m . y^r/g^{rx}$$

$$= m . g^{xr}/g^{rx}$$

$$= m .$$

3. PROPOSED SYSTEM

Here the wireless medical sensor network consists of some medical sensors, three data servers and some users. Here in this solution, it is going to improve the solution which was given by Yi et al. [5]. Unlike [5], here the three data servers process the queries, such as statistical analysis on the patient data, from the users on the basis of Pailler[3] and ElGamal[4] cryptosystems instead of Sharemind System[6]. The flow diagram of the proposed system is as shown in figure 3.1.

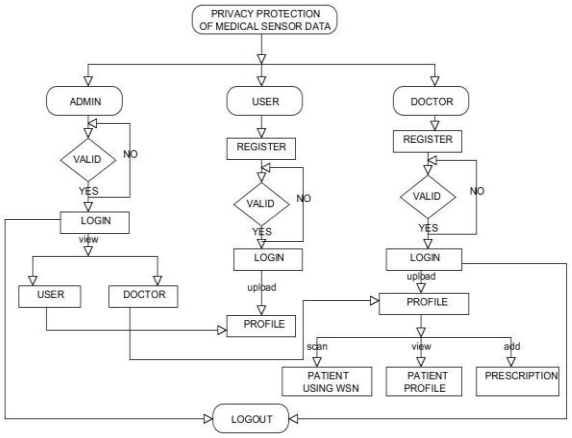

Fig.3.1 Flow diagram of the proposed system

There are three modules in this system. They are admin, users and doctors.

- Admin provides the authorization to user and doctors. The users and doctors are given a unique login IDs and password on the time of registration. Both users and doctors' profiles can be viewed and maintained by the admin.
- Users (patients) can login to their profile and view the prescriptions given by the doctor. User has no authorization to update the medical data in his profile and has the authorization only to view his medical data.
- Doctors can login to their profile by using the unique IDs and passwords given to them. The doctors can view the list of patients to whom he prescribe. The doctors can view the medical data of the patient which is statistically analyzed. Doctor has no authorization to update the medical data of the patient.

The medical data which is sensed through wireless sensors which is deployed in patient's body is divided into three (may be multiple) parts and encrypted using Paillier[3]and ElGamal[4] cryptosystems and then stored in three (multiple) different servers. Whenever the data is retrieved by querying, the data present in all three servers is fetched and then decrypted. The decrypted data which is statistically analyzed data is sent to the requesting authorized doctor or admin. Using this fetched medical data doctor can prescribe the necessary medicine or diet to the patient which is updated in patient's profile. When the patient login to his profile he can see the prescription given by the doctor and follow it.

Advantage of the proposed system over existing system is that the patient data is still secure even if one of the three data servers is not compromised. That is if two servers are compromised and one server is not compromised then the data is still secure. The data is sent to the servers via secured channel. Where as in the existing system can protect the patient data as long as the number of the compromised servers is at most one. That is if two of the data servers are compromised by the inside attacks then the data is insecure.

4. CONCLUSION

Here we use lightweight encryption scheme and MAC generation scheme based on SHA-3 proposed in [5] to secure the communication between the data servers and medical sensors. A new data collection protocol is proposed which splits the patient data into three numbers and stores hem in three data servers to keep the privacy of patient data. A new access control protocol is proposed for authorized doctor where three data servers cooperate to provide the user with the patient data, but do not know what it is. For authorized users a new protocol is proposed where the three data servers cooperate to process patient data and provide statistical analysis results. In this solution can preserve the patient data privacy as long as any one of the three servers is not compromised.

REFERENCES

[1]. D. Malan, T. F. Jones, M. Welsh, and S. Moulton, "CodeBlue: An Ad-Hoc sensor network infrastructure for emergency medical care," in Proc. MobiSys Workshop Appl. Mobile Embedded Syst., Boston, MA, USA, Jun. 6–9, 2004, pp. 12–14.

[2]. A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Dept. Comput. Sci., Univ. Virginia: Charlottesville, VA, USA, Tech. Rep. CS- 2006-01, 2006.

[3]. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptograph. Techn., 1999, pp. 223–238.

[4]. 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.

[5]. X. Yi, J. Willemson, and F. Nat-Abdesselam, "Privacy-preserving wireless medical sensor network," in Proc. 12th IEEE Int. Conf. Trust, Security Privacy Comput. Commun., 2013, pp. 118–125.

[6]. 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.