Hiding Sensitive Medical Data Using Encryption

Mayur Lagad[1], Akhilesh Chaudhari[2]

[1]Information Technology Department, PDEA's COEM, Pune, Maharashtra, India
[2]Information Technology Department, PDEA's COEM, Pune, Maharashtra, India

---***---

Abstract – *Healthcare applications are considered as promising fields for wireless networks, where patients can be monitored using wireless medical networks (WMNs). Current WMN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual is highly sensitive. The main contribution of this paper is to distribute patient's data securely in multiple data servers and performing the Paillier cryptosystems to perform statistical analysis on the patient data without affecting the patient's privacy.*

Key Words – Categories and Subject Descriptors:

*C.2.1[Computer-Communication Networks]: Network Architecture and Design—Wireless communication;

*J.3 [Life and Medical Sciences]: Medical Information Systems General Terms:

*Wireless medical network, patient data privacy, Paillier encryption.

1.INTRODUCTION

A wireless network is a network to monitor physical or environmental conditions such as temperature, sound, pressure, etc. The development of wireless networks was motivated by air pollution monitoring, water quality monitoring, water quality monitoring, land side detection, forest fire detection habitat monitoring and so on. Though there are many applications in wireless network domain, human healthcare applications takes the major role. In human healthcare, are used to monitor the patients' health status such as temperature level, sugar level, heart beat rate, blood pressure. For instance, if the patient's sugar level is monitored 10 times per day then the data is updated in the database which is present in the local server. Likewise the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, stealing and updating, storing the wrong values. Suppose if the intruder is trying to hack the patient details, there are many chances for the misuse of data which may lead to severe consequences. The data can also be modified by the hackers due to lack of security. The treatment prescribed by the doctors can be hacked which may even lead to death of the patients. Patients are the victims because of the above issues. To prevent these issues, the intrusion detection system is proposed. An intrusion detection system is a system used to check the malicious activities and produces electronic reports to a management station. It consists of Paillier algorithm key cryptosystems. The algorithm is used to encrypt the patient details before storing it in the database and perform decryption when needed by the physician.

1.1 Related Work:

For real-world implementation, wireless networks and healthcare networks may employ different topologies, while the trusted IDS principles are still the same. Therefore, this section introduces existing approaches on how to establish trust management for wireless networks and distributed IDS networks.

Intrusion detection systems (IDSs): These systems are usually deployed to identify any behavioral anomalies or policy violations through monitoring the protected networks and systems. Typically, an IDS can be classified into two categories: signature-based IDS and anomaly-based IDS. The former detects attacks by matching network or system events with available signatures. A signature (or rule) is a kind of descriptions of a known attack or exploit, which determines the detection capability in real-world applications (i.e., its detection accuracy would not be better than its available signatures). The latter first builds a profile for typical activities on the target computer and network, and then identifies potential anomalies if the deviation between the monitored events and the normal profile exceeds a predefined threshold. Alarms will be generated if anomalies are discovered. To improve the detection performance, distributed and collaborative IDSs are often applied in real-world environments.

Trust management for wireless networks: The notion of trust in computer science derives mainly from the field of social science, aiming to predict and judge the situations of an object. In literature, many trust-based approaches with intrusion detection technology have been developed and studied.

Trust management for distributed IDS networks: To enhance the detection performance of a single IDS, distributed or collaborative IDS networks have been widely developed through enabling the information collection and exchange among a set of IDS nodes.

1.2 Architecture:

Like most of healthcare applications with wireless medical network, our architecture has four systems as follows:

- A patient database system which stores the patient data from medical 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.

WMNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Networks have direct human involvement are deployed on a small scale must support mobility (a patient can carry the devices), and WMNs requires high data rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical motes. These medical are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate.

WMNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless networks. Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job.

To prevent the patient data from the inside attacks, we propose a new data collection protocol, where a splits the sensitive patient data into three components according to a random number generator based on hash function and sends them to three servers, respective, via secure channels.

To keep the privacy of the patient data in data access, we propose a new data access protocol on the basis of the Paillier cryptosystem. The protocol allows the user (e.g. physician) to access the patient data without revealing it to any data server.

To preserve the privacy of the patient data in statistical analysis, we propose some new privacy-preserving statistical analysis protocol on the basis of the Paillier cryptosystems. These protocols allow the user (e.g., medical researcher) to perform statistical analysis on the patient data without compromising the patient data privacy.

2. DATA MODEL & DESCRIPTION

Privacy is the major design constraint in the health care application for providing security to patient's sensitive data from hacker. Our system uses Java as a front end with Apache web server/ Apache Tomcat/ IIS as the webserver. And MySQL as the back end of the system.

2.1 Mathematical Model:

Let W be the whole system which consists:

W= {IP, PRO, OP}

Where,

IP is the input of the system.

A) IP= {P, SD, SN, PD, U}

P is the number of patients in the system.

SN is the set of number of sensing nodes in the system.

SD is the sensing data sensed from the medical SD.

PD is the patient's database system which consists of number of databases.

U is the set of number of user in the systems that are accessing the data from patient's database server.

B) PRO is the procedure of our proposed system:

Step 1: At first the wireless medical network which senses the patient's body and transmits the patient data to a patient database system.

Step 2: A patient database system which stores the patient data from medical and provides querying services to users (e.g., physicians and medical professionals).

Step 3: A patient data access control system which is used by the user (e.g., physician) to access the patient data and monitor the patient.

Step 4: 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.

OP is the output of the system:

The system provides the privacy to the patient's sensible data available on the patient's database system in the sense of inside attacks.

2.2 Algorithms:

A) Paillier Public-Key Cryptosystem:

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

Where lcm stands for the "least common multiple".

- Select random integer g where g $\in Z^{¿}_{N^2}$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:
$$\mu=\left(L\left(g^{\lambda}(mod\,N^2)\right)\right)^{-1}(mod\,N)$$

where function L is defined as;
$$L(u)=\frac{u-1}{N}$$

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

2)Encryption:

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m $\in Z_N$
- Select random r where r $\in Z^{¿}_N$
- Compute cipher text as:
$$C=g^m.r^N(mod\,N^2)$$

3)Decryption:

The decryption algorithm works as follows.

- Let c be the cipher text to decrypt, where the cipher text; c $\in Z^{¿}_{N^2}$.
- Compute the plain text message as:
$$m=\left(c^{\lambda}(mod\,N^2)\right).\mu(mod\,N)$$

4)Homomorphic Properties:

A notable feature of the Paillier cryptosystem is its homomorphic properties. Given two cipher texts;
$$E(m_1,pk)=g^{m1}r_1^N(mod\,N^2)$$
$$E(m_2,pk)=g^{m2}r_2^N(mod\,N^2)$$
where r1,r2 are randomly chosen for $Z^{¿}_N$,we have the following homomorphic properties –
$$D\left(E(m_1,pk_1).E(m_2,pk_2)\right)=m_1+m_2(mod\,N)$$

The product of a cipher text with a plain text raising g will decrypt to the sum of the corresponding plain texts;
$$D\left(E(m_1,pk_1).g^{m2}\right)=m_1+m_2(mod\,N)$$

An encrypted plain text raised to a constant k will decrypt to the product of the plain text and the constant;
$$D\left(E(m_1,pk_1)^k\right)=km_1(mod\,N)$$

2.3 Major Constraints:

The patient data may be decimal numbers with several digits after the point. In this case, the information should convert it to an integer and sends the shares of the data together with the unit of the data to three data servers, respectively.

2.4 Functional Model and Description:

Patient: The patient sensitive data is stored in multiple servers by using some new crypto systems protocols.

System: The system will protects the patients data from hacker while data transmission by administrator.

2.5 Data Design:

A description of all data structures including internal, global, and temporary data structures, database design (tables), file formats.

A. Internal software data structure –
When SQL returns the results of the query sent to it by user, the results of the query will be passed back to user using the built in data structures.

B. Global data structure –
We are not using any global data structure.

C. Temporary data structure –
We will be using a cookie saved on the user's machine to temporarily store the user's query entry. This is so the user can go back to the query page and easily modify their last query to refine or widen their search as needed.

D. Database description –

MySQL: MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. The MySQL Web site (http://www.mysql.com/) provides the latest information about MySQL software.

MySQL is a database management system. A database is a structured collection of data. It may be anything from a simple shopping list to a picture gallery or the vast amounts of information in a corporate network. To add, access, and process data stored in a computer database, you need a database management system such as MySQL Server. Since computers are very good at handling large amounts of data, database management systems play a central role in computing, as standalone utilities, or as parts of other applications.

REFERENCES

[1] Yi, Xun, et al. "Privacy Protection for Wireless Medical Sensor Data." IEEE Transactions on Dependable and Secure Computing 13.3 (2016): 369-380.

[2] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Net-work. In Proc. TrustCom13, pages 118-125, 2013.

[3] D. He, S. Chan and S. Tang. A Novel and Lightweight System to Secure Wireless Medical Sensor Networks. IEEE Journal of Biomedical and Health Informatics, 18 (1): 316-326, 2014.

[4] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchi-cal Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.

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

[6] P. Belsis and G. Pantziou. A k-anonymity privacy-preserving approach in wireless medical monitoring environments. Journal Personal and Ubiquitous Computing, 18(1): 61-74, 2014.

[7] T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Loga-rithms. IEEE Transactions on Information Theory, 31 (4): 469-472, 1985.

[8] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT99, pages 223-238, 1999.

BIOGRAPHIES

Mr. Mayur Lagad
(BE Information Technology 2019)
PDEA'S College of Engineering,
Manjari(Bk) Pune – 412307

Mr. Akhilesh Chaudhari
(BE Information Technology 2019)
PDEA'S College of Engineering,
Manjari(Bk) Pune - 412307