Privacy Protection of Wireless Data

Prof. Vijay More[1], Dhiraj Durge[2], Nikhil Deokar[3], Ajit Gawade[4], Yogesh Pujari[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] AISSMS IOIT PUNE

Abstract- *Now a day's, wi-fi networks are widely used in university data programs, along with banking and military applications such as battlefield surveillance such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Wireless networks are greater liable to eavesdropping, change, impersonation and replaying attacks than the wired networks. A lot of work has been done to secure wireless networks. The existing solutions can protect the user data during transmission, but cannot stop the inside attack where the administrator of the user database reveals the sensitive user data. Our proposed system is practical approach to prevent the inside attack by using multiple data servers to store user data. Moreover securely distributing the user data in multiple data servers and employing the Advanced Encryption Standard to perform statistical analysis on the user data without compromising the user privacy,is the another major factor of concern.*

Keywords- Wireless network, user data privacy, Advanced Encryption Standard

I. INTRODUCTION

A wireless network comprises of equally distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc and to mutually pass their data through network to primary location. The development of wireless networks was triggered by military applications such as battlefield surveillance; today such networks are used in many consumer and industrial applications. It is extensively used in healthcare, medicine as well as banking processes.

In recent years, many applications of wireless networks have been developed such as CodeBlue, Alarm-Net, Ubi-Mon, MEDiSN and MobiCare. A typical example of applications with wireless networks is Alarm-Net developed in University of Virginia for assisted-living and residential monitoring. The architecture of Alarm-Net is shown in the following figure.

Alarm-Net is composed of mobile body network placed in network. Alarm-Gate applications are back-end systems, and user interfaces as follows:

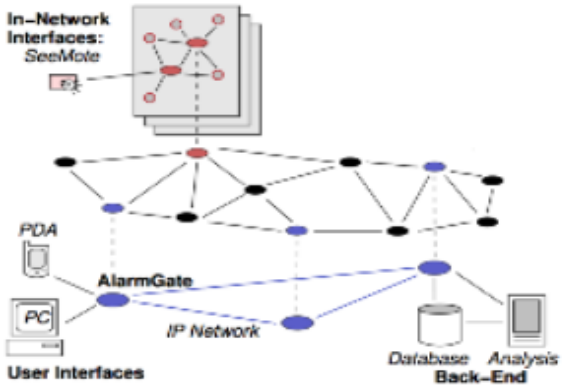

Fig 1: Alarm-Net Architecture

Mobile body network has a wireless devices worn by a person which provide physiological sensing. Data from the body network is transmitted to user interfaces and back end systems. Alarm-Net applications serve as application level gateways between wireless networks and IP networks. Back-end systems provide online analysis of data and long term storage of data .User interfaces allow any legitimate user of system to query sensor data. Wireless medical networks certainly improve user's quality of care without disturbing their comfort. Typical security threats to healthcare applications with wireless networks with wireless networks are the following. Eavesdropping is a security threat to the user data privacy. An eavesdropper, in possession of strong antennae may be able to capture the user data and use it for malicious purpose. He may even post the data on social network, which can become a potential threat to patient privacy.

Impersonation is a security threat to user data authentication. In a home care application an attacker may impersonate a wireless network and copy sensitive information of the user. It may also lead to false alarms to remote sites and also carry out security operations which would give futile results. Data breach is another major threat in which sensitive, protected or confidential data from the user. For example, a malicious patient administrator may use the user data for frauds such as credit card frauds, insurance frauds and sometimes even may pose life-threatening activity. To protect wireless networks against various attacks a lot of research has been done.

II. PRELIMINARIES

One basic building blocks of our solution are the Advanced Encryption Standard (AES) public key cryptosystem, which is described in this section.

(A) Advanced Encryption Standard

The Advanced Encryption Standard (AES Algorithm) is a symmetric key cryptographic algorithm published by National institute of standards and technology in December 2001. The algorithm was proposed by Rijndael the reason it is also called as Rijndael encryption algorithm. The algorithm was proposed by Rijndael encryption algorithm and is a block cipher meaning that it operates on an input block of data of data which is the same size. An input key is also required as input to the AES algorithm. It also the data length of 128,192 and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used both to encrypt and decrypt a message. Also the cipher text produced by the algorithm is the same size as the plain text message. The working of AES is explained in the following image.

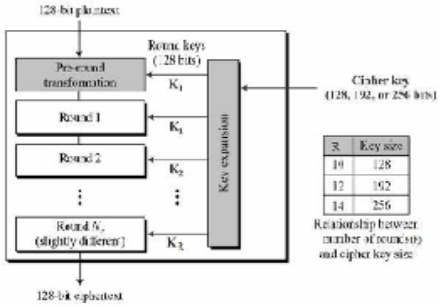

Fig 2: Working Of AES

The plaintext is divided into 128-bit block as consisting of 4*4 matrix of bytes. Therefore the first four bytes occupy the second column and so on. AES operates on column major order matrix of bytes; called as state array shown in the figure. AES also has the notion of a word. A word consists of four bytes that is 32 bits. The number of rounds are 10, is for the case when encryption is 128 bit long. Before any round-based processing foe encryption can begin each byte of the state (plaintext) is combined with the round key using bitwise XOR operation and depends on number of rounds. AES divide plaintext into 16 byte blocks and treats each block into 4*4 state arrays. It then performs four operations in each round which consists of several processing like substitution step, a row wise permutation step and addition of the round key.

III. PRIVACY-PRESERVING WIRELESS NETWORK

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

- A wireless medical network which senses the patient's body and transmits the patient data to a patient database system.
- A patient database system which stores the user data 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.

There may be a middleware between the wireless medical network and the patient database system. If so, the role of the middleware is simply forwarding the encrypted patient data to the database system. The following diagram depicts the working of our proposed system

The security requirements for our model include:

- Data collection security: In the wireless network,securely send data to the distributeddatabase system.
- Data store security: In the distributed patient database system, the patient data cannot be revealed even if two of three data servers are compromised by the inside attackers.
- Data access security: In the patient access control system, only the authorized user can get access to the patient data. The patient data cannot be disclosed to any data server during
- the access.
- Data analysis security: In the patient data analysissystem, the authorized user can get thestatistical analysis results only.
- The patient datacannot be disclosed to any data server andeven to user using statistical user.

IV.SECURITY ANALYSIS

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 application and each data server is through a secure channel, which is implemented by a public key cryptosystem. The user data over the secure channel is encrypted with the public key pre-shared between the data server. Without the public key, the attacker cannot eavesdrop the patient data. Because the medical data are usually low power and low-cost, we can choose the light weight encryption scheme and the message authentication code (MAC) generation scheme proposed in for the secure channel

In our solution, the communication between the user and each data server is also through a secure channel. Because the three data servers and the user's computing device are usually much more powerful in computation and communication, we choose the Advanced Encryption Standard (AES) for the secure channel. For data authentication and integrity. By AES, we can achieve data confidentiality, authenticity and integrity between the user and each data server.

In our solution, the communications among three data servers can be also through secure channels. Like the secure communication between the user and the data servers, any two of the three data servers can establish a public key cryptosystem. Then the communication between the two data servers can be encrypted with AES based on the public key.

V. CONCLUSION

In this paper, we have thoroughly investigated the privacy issue in wireless networks and also taken an example of medical data collection storage. The security and privacy issues in the medical data collection storage and queries and presented a complete solution for privacy-preserving network. To secure the communication between system and data servers. To keep the privacy of the user data, we proposed a new data collection protocol which splits the user 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 user data can be preserved. For the legitimate user e.g. physician to access the patient data.

REFERENCES

[1] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson Privacy Protection for Wireless Medical Sensor Data.

[2] Advanced Encryption Standard (AES). FIPS PUB 197, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[3] 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.

[4] D. Bogdanov, S. Laur, J. Willemson. Sharemind: a Framework for Fast Privacy-Preserving Computations. In Proc. ESORICS' 08, pages 192-206, 2008

[5] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Real-Time and Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, doi: 10.1155/2008/135808.