Patient data privacy using wireless medical Sensor data

S.DilipKumar[1], A.Kabir Ahamed[2], M.Mohamed Malik[3]

Assistant professor[1]
,Department of CSE, Arasu
Engineering College
Kumbakonam

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.*

Keywords**:** *Eavesdropping, Paillier and ElGamal cryptosystems, patient's privacy.*

I. INTRODUCTION:

Wireless sensor network (WSN) consists of spatially distributed autonomous A 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. A typical example of healthcare applications with WSNs is Alarm-Net developed in University of Virginia for assisted-living and residential monitoring. The architecture of Alarm- Net is shown in Fig.

II. RELATED WORKS:

A k-anonymity privacy-preserving approach in wireless medical monitoring environments. This paper presents the design and prototype of a wireless health monitoring system using mobile phone accessories. We focus on measuring real time Electrocardiogram (ECG) and Heart rate monitoring using a smartphone case. With the increasing number of cardiac patients worldwide, this design can be used for early detection of heart diseases. Unlike most of the existing methods that use an optical sensor to monitor heart rate, our approach is to measure real time ECG with dry electrodes placed on smartphone case. The collected ECG signal can be stored and analyzed in real time through a smartphone application for prognosis and diagnosis. The proposed hardware system consists of a single chip microcontroller (RFduino) embedded with Bluetooth low energy (BLE), hence miniaturizing the size and prolonging battery life. The system called "Smart Case" has been tested in a lab environment. We also designed a 3D printed smartphone case to validate the feasibly of the system. The results demonstrated that the proposed system could be comparable to medical grade devices.

Framework for Fast Privacy-Preserving Computations:

Electric vehicles (EVs) can contribute to reducing carbon emissions and facilitate renewable integration. However, EVs are not competitive with fuel-based vehicles, particularly for long distances, because of their limited range and long charging times. We propose a smart scheduling approach for EVs to plan charging

stops on a highway with limited charging infrastructure. This approach aims to minimize the total travel time for each EV based on the A* algorithm with constraint verification and a peer-to-peer scheduling system. By considering the estimated state of the charging stations, we achieve indirect coordination between EVs. We introduce a simulation framework with trips generated using a data-driven approach and support for time-varying highway parameters. Furthermore, we apply our approach to a use case for the German highway A9 from Munich to Berlin. The computation and communication requirements of the proposed solution remain moderate and privacy preserving, contributing to its applicability. Results show that the smart scheduling approach significantly reduces the total travel times. In addition, by dynamically adjusting the schedules, the proposed approach can account for changing highway conditions, for example, slow traffic on a given segment. Our approach can be generalized beyond fast charging to different technologies, such as hydrogen or battery swapping stations.

A Programmable Service Architecture for Mobile Medical Care:

This paper introduces MobiCare - a novel service architecture that enables a wide range of health-related services for efficient and mobile patient care. These services include: (1) health-related services in medical devices and sensors to remotely install, self-activate, reconfigure or even self-repair with new health services and applications, (2) secure and reliable dynamic software upgrade or update services applied to the native code of the clinical device, and, (3) remote registration and (re)configuration of body sensors as well as remote health-data services such as patient health report downloads and diagnosis data uploads with provider servers. Collectively these services address a range of patient medical monitoring needs by accelerating deployment of new health- related services, thus reducing medical costs and improving the quality of patient care. We are currently implementing a proof-of-concept prototype. Early experiences with MobiCare do show that it has the potential to become a feasible and a useful infrastructure paradigm for the next generation healthcare

Privacy-Preserving Telecardiology Sensor Networks:

Recently, a remote-sensing platform based on wireless interconnection of tiny ECG sensors called telecardiology sensor networks (TSN) provided a promising approach to perform low-cost real-time cardiac patient monitoring at any time in community areas (such as elder nursing homes or hospitals). The contribution of this research is the design of a practical TSN hardware/software platform for a typical U.S. healthcare community scenario (such as large nursing homes with many elder patients) to perform real-time healthcare data collections. On the other hand, due to the radio broadcasting nature of MANET, a TSN has the risk of losing the privacy of patients' data. Medical privacy has been highly emphasized by U.S. Department of Health and Human Services. This research also designs a medical security scheme with low communication overhead to achieve confidential electrocardiogram data transmission in wireless medium.

III. EXISTING SYSTEM:

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.

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.

IV. DISADVANTAGE:

In the wireless medical sensor network, each medical sensor can securely send the patient data to the distributed database system.

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. 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. In the patient data analysis system, the authorized user can get the statistical analysis results only.

The patient data cannot be disclosed to any data server and even to the user during the statistical analysis.

V. PROPOSED SYSTEM:

Because the medical sensors are usually lowpower and low-cost, we can choose the lightweight encryption scheme and the message authentication code (MAC) generation scheme proposed in for the secure channel. Both schemes are built on the smallest version of the 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 as shown in . In our data collection protocol, we can use the lightweight encryption scheme and MAC generation scheme proposed in .

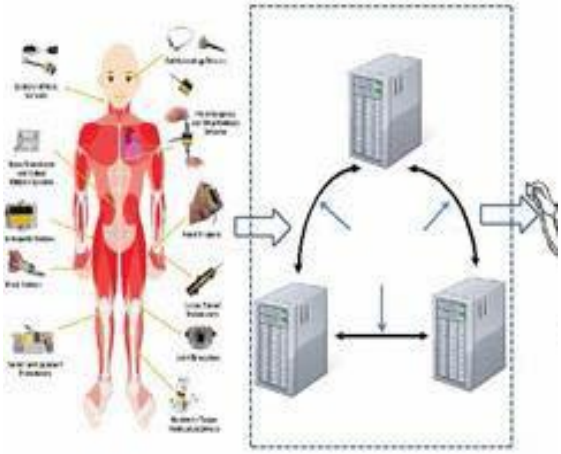
In addition, our random number stream generation scheme is also based on SHA All security mechanisms in the sensor can be implemented with the same This design is suitable for wireless sensor networks where area is particularly important since it determines the cost of the sensors. we used the lightweight encryption scheme and MAC generation scheme based on SHA- 3 proposed in. 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.

VI. ADVANTAGE

Our model considers two types of attacks, the outside attack and the inside attack. The outside attacker does not know any secret key in our system, but attempts to learn the patient data from the views of our protocol, or modify the patient data, or impersonate a medical sensor. The inside attacker is a malicious data server or a coalition of two malicious data servers who know some secret keys in our system and attempt to learn the patient data.

To prevent the patient data from the inside attacks, we propose a new data collection protocol, where a sensor 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. 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 outside attacks can be effectively prevented by encryption, authentication and access control.

VII. SYSTEM ARCHITECTURE



VIII.

IX. 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. 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 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 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.

REFERENCES:

[1]. Advanced Encryption Standard (AES). FIPS PUB 197,November26,2001.

[2]. 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.

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

[4]. R. Chakravorty. A Programmable Service Architecture for Mobile Medical Care. In Proc. 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop

[5]. J. Daemen, G. Bertoni, M. Peeters, G. V. Assche, Permutation-based Encryption, Authentication and Authenticated Encryption, DIAC'12, Stockholm, 6 July2012.

[6]. 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.

[7]. W. Diffie and M. Hellman. New Directions in Cryptography.IEEE Transactions on Information Theory, 22 (6): 644-654, 1976.