A SURVEY ON PROVIDE SECURITY TO WIRELESS MEDICAL SENSOR DATA

Kiran More[1], Prof. Jyoti Raghatwan[2]

1 Kiran More, RMD Sinhgad School of Engineering, Pune

2 Prof. Jyoti Raghatwan , RMD Sinhgad School of Engineering,Pune

Abstract- *Now a days, wireless sensor networks have been widely used in healthcare applications, such as hospital and home patient monitoring. Wireless medical sensor networks are more vulnerable than the wired networks to eavesdropping, modification, impersonation and replaying attacks. A lot of work has been done to secure wireless medical sensor networks. The present solutions can protect the patient data during transmission, but cannot stop the inside attack wherever the administrator of the patient database reveals the sensitive patient data. Here we propose a practical approach to prevent the inside attack by using several data servers to store patient data. The main contribution is securely distributing the patient data in numerous data servers by using the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy.*

***Key words*: Paillier cryptosystem, ElGamal cryptosystem, Wireless medical sensor network, healthcare application, statistic analysis, Wireless Sensor network.**

1. INTRODUCTION

Wireless sensor networks (WSN), also called as wireless sensor and actuator networks (WSAN) are spatially scattered autonomous sensors to monitor environmental or physical conditions, such as temperature, sound, pressure, etc. and to helpfully pass their data through the network to destination. The development of wireless sensor networks was aggravated by military applications such as battlefield surveillance. Now a days, such networks are used in many industrial and consumer applications, For Example industrial process monitoring, machine health monitoring, and so on.

Healthcare applications are considered as promising fields for wireless sensor networks, In which patients can be monitored using wireless medical sensor networks (WMSNs). Current WMSN healthcare research trends focus on patient reliable patient mobility, communication, and energy-efficient routing. Deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. The physiological data of an individual are highly sensitive. So, that the security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease.

Any unauthorized collection or leakage of patient data could harm the patient. However,
an unauthorized person may use the patient data (such as, patient identity) for their personal benefit, such as for fraudulent insurance claims, medical fraud, and sometimes this may even pose life-threatening risks. This motivated to provide security to Patient data when data is share on distributed system.

In this paper we have surveyed on Privacy protection for wireless medical sensor data. Section 2 of this paper deals with literature survey and Section 3 presents proposed system. Section 4 concludes this paper.

2. LITRATURE SURVEY

A comprehensive literature survey is performed in the support of the Wireless Medical Sensor Data. In literature, several techniques have been presented for securing wireless medical sensor data by using Paillier and ElGamal cryptosystems.

System [1] Wireless medical sensor networks (MSNs) are a useful technology in e-healthcare which allows the data of a patient's vital body parameters is collected by the wearable biosensors. However, the security and privacy protection of the collected data is a major unsolved issue, and the high demand for both security/privacy and practicality. So, The lightweight and secure system for MSNs is proposed. The system employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and data access control ,although the system to provide backward secrecy and privacy preservation. Here we required symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes. Among the all previous servey, this is the first secure data transmission and access control system for MSNs.

In [2] Energy efficient key management scheme is proposed to the distributed systems like Body Sensor Networks(BSNs) where biosensor nodes are scattered in different positions to collect health data from the human body and transport the information to a remote medical center. As per the medical data policy, security of BSNs is very important. The operational resources are very limited of the biosensor nodes which are located in BSNs and traditional security technologies are not directly applicable to BSNs. Time synchronization and low-energy communication are two challenging issues for BSNs. A fuzzy commitment technology with weak time synchronization mechanism for keys negotiation is developed, with a multi-hop route key management scheme used for efficient energy consumption management. The Security analysis and performance evaluation is provided to authenticate the proposed scheme.

Present WMSN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing [3]. Though, an Introducing new technology in healthcare applications without considering security makes patient privacy vulnerable. Furthermore, the physiological data of an individual are highly sensitive so, the security is a paramount requirement of healthcare applications, mainly in the case of patient privacy or if the patient has an embarrassing disease. Here we discussed the security and privacy issues in healthcare application using WMSNs.

System [4] proposed a Staff shortages and an increasingly aging population are straining the ability of emergency departments to provide high quality care. At the same time, there is a rising concern about the hospitals' ability to provide effective care during disaster events. So because of, the tools that automate patient monitoring have the potential to greatly improve efficiency and quality of health care. Towards this target, MEDiSN developed, a wireless sensor network for monitoring patients' physiological data in hospitals and at a time of disaster events. MEDiSN comprises Physiological Monitors (PMs) that are custom-built, patient-worn motes that sample, encrypt, and sign physiological data and Relay Points (RPs). Which then self-organize into a multi-hop wireless backbone for carrying physiological data. Additionally, MEDiSN includes a back-end server that persistently stores medical data and presents them to authenticated GUI clients. The grouping of MEDiSN's two-tier architecture and optimized rate control protocols allows it to address the complex challenge of reliably delivering large volumes of data while meeting the application's QoS requirements.

In [5] telecardiology sensor networks, Recently the remote-sensing platform based on wireless interconnection of tiny ECG sensors called Telecardiology Sensor Networks (TSN). It provided a hopeful approach to perform lowcost real-time cardiac patient monitoring whenever in community areas such as elder nursing homes or hospitals. The contribution of this research is the design of a practical TSN based on 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. Alternatively, 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. The Proposed work also designs a medical security scheme with low communication overhead to achieve confidential electro cardiogram data transmission in wireless medium.

3. PROPOSED SYSTEM

The proposed system is divided into following four systems:

- A wireless medical sensor network which senses the patient's body and transmits the patient data to a patient database system.
- A patient database system that stores the patient data from medical sensors and provides querying services to users such as physicians and medical professionals.
- A patient data access control system which is used by the user examples physician to access the patient data and monitor the patient.
- A patient data analysis system that is used by the user Example medical researcher to query the patient database system and examine the patient data statistically.

We propose various Cryptosystem algorithm such as paillier, ElGamal to Encrypt\Decrypt data and store on several data server.

That various data server are connected by WSN. Here wireless medical sensor network senses the patient's body and then that data is splitted, and store on distributed data server (here we used at least 3 data server). Whenever that data is required by medical researcher or any doctor then they access data in decrypted form by querying to data server. The privacy of the patient data can be preserved as long as one data server is not compromised.

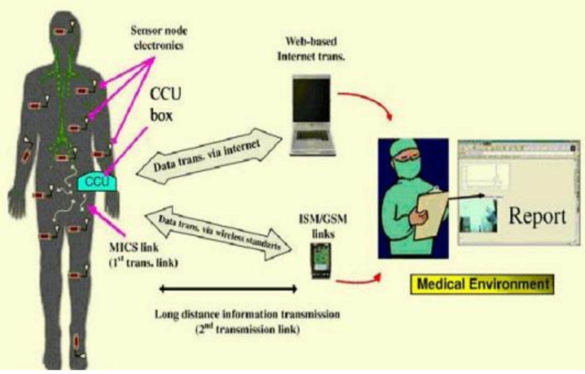
Sensor node electronics
CCU box
CCU
Web-based Internet trans.
Data trans. via internet
Data trans. via wireless standarts
ISM/GSM links
MICS link (1st trans. link)
Long distance information transmission (2nd transmission link)
Report
Medical Environment

Figure 1: Patient Data Transmission over internet.

4. CONCLUSION

We have surveyed different types of security technique to secure the wireless medical sensor data. Here, we also proposed the Paillier cryptosystem and ElGamal cryptosystem to encryption and decryption of data. Proposed solution can preserve the patient data privacy as long as one of three data server is not compromised. Also requires that the number of the compromised data servers is at most one.

ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Jyoti Raghatwan for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my Paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department, RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

REFERENCES

[1] Xun Yi, Athman Bouguettaya, ”Privacy Protection for Wireless Medical Sensor Data”, in IEEE, VOL. 13, NO. 3, MAY/JUNE 2016.

[2] 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.

[3] H. Zhao, J. Qin, and J. Hu, ”An energy efficient key management scheme for body sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2202-2210, Nov. 2013.

[4] P. Kumar and H. J. Lee, ”Security issues in healthcare applications using wireless medical sensor networks: A survey,” Sensors, vol. 12, pp. 55-91, 2012.

[5] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terzis, and G. M. Masson, ”MEDiSN: Medical emergency detection in sensor networks,” ACM Trans. Embedded Comput. Syst., vol. 10, pp. 1-29, 2010.

[6] 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.