Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Privacy Protection Of Sensitive Data By Using Pallier Cryptography

[1]Sachin, [2]Sagar, [3]Ganesh, [4]Shubham, [5]Prof.Dipti Chaudhari.

[1]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[2]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[3]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[4]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[5]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India

Abstract - *Healthcare applications are careful as assured lees for wireless device systems, where patients can be check using wireless medical sensor networks (WMSNs). Present WMSN healthcare investigation trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, establishing new services in healthcare requests without permitting for security makes patient privacy susceptible. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. This project discusses the security and privacy issues in healthcare application using WMSNs. We highlight some popular healthcare projects using wireless medical sensor networks, and discuss their security the existing systems solutions can simply protect the patient data during transmission, but cannot protect the confidential occurrence where the manager of the patient database reveals the sensitive patient data. So we are proposing a approach to prevent the inside attack by using multiple data servers to store patient data. 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 compromising the patient's privacy. It will trace the hacker information such as IP address, MAC address, time, date by using honey checker.*

I. INTRODUCTION

A wireless sensor network is a network to display corporeal or conservation conditions such as temperature, sound, pressure, etc. The development of wireless sensor networks was motivated by air pollution monitoring, water quality monitoring, land side detection, forest fire detection, habitat monitoring and so on. Though there are many applications in wireless sensor network domain, human healthcare applications takes the major role. In human healthcare, sensors 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.

LITERATURE SURVEY

Sr. No.	Paper Name	Author Name	Published Year	Advantages	Disadvantages
1.	A survey on provide security to wireless medical sensor data	Kiran More, Prof. Jyoti Raghatwan	2017	A practical approach to prevent the inside attack by using several data servers to store patient data.	The present solutions can cannot protect the patient data during transmission
2.	Privacy Protection for Wireless Medical Sensor Data	Xun Yi, Athman Bouguettaya	2016	The lightweight and secure system for MSNs is proposed. The system employs hash-chain based key updating mechanism	Required symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes not for large sensor nodes.

				and proxy-protected signature technique to achieve efficient secure transmission and data access control although the system to provide backward secrecy and privacy preservation.	
3.	A novel and lightweight system to secure wireless medical sensor networks	D. He, S. Chan, and S. Tang	2014	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.	Time synchronization and low-energy communication are two challenging issues for BSNs.
4.	An energy efficient key management scheme for body sensor networks	H. Zhao, J. Qin, and J. Hu	2013	Present WMSN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing	There is security and privacy issues in healthcare application using WMSNs.
5.	Security issues in healthcare applications using wireless medical sensor networks: A survey	P. Kumar and H. J. Lee	2012	Proposed a Staff shortages and an increasingly aging population are straining the ability of emergency departments to provide high quality care.	It cannot address the complex challenge of reliably delivering large volumes of data
6.	MEDiSN: Medical emergency detection in sensor networks	J. Ko, J. H. Lim, Y. Chen, R. Musaloiu	2010	Telecardiology sensor networks, Recently the remote-sensing platform based on wireless interconnection of tiny ECG sensors called Telecardiology Sensor Networks (TSN).	TSN has the risk of losing the privacy of patients' data.

II. EXISTING SYSTEM

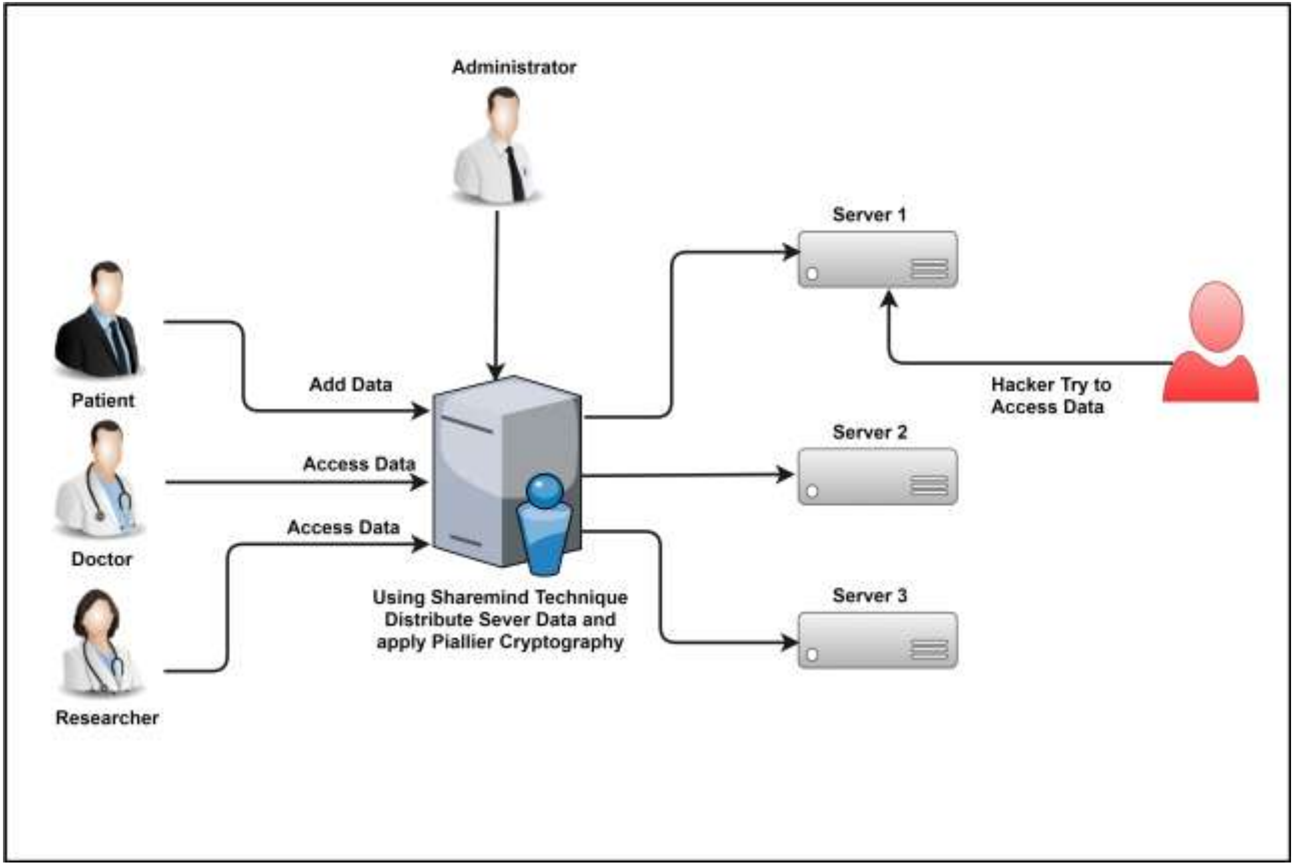
The security is a overriding must of healthcare applications, particularly in the case of patient privacy, if the patient has an uncomfortable disease. This project discusses the security and privacy issues in healthcare application using WMSNs. We highlight some popular healthcare projects using wireless medical sensor networks, and discuss their security the existing systems solutions can simply protect the patient data during transmission, but cannot protect the inside attack where the administrator of the patient database reveals the sensitive patient data.

Disadvantages of Existing System

1. Less secure.
2. Cannot protect inside attacker.
3. If any hacker get data from one DB server then whole data will be get to hacker.

III. PROPOSED SYSTEM

In this study, we focus on 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. 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. It will trace the hacker information such as IP address, MAC address, time, date.



Advantages of Proposed System

- Practical approach to prevent the inside attack by securely distributing the patient data in multiple data servers.
- Employing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patients' privacy.
- In Proposed system, Due to secured distributed database architecture we can achieve data storage & data analysis security.
- Proposed data retrieval technique allow to retrieve the data compromised server(s)

IV. CONCLUSION

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 net-work through the ad-hoc network. To keep the privacy of the patient data, we proposed a novel data group protocol which splits the patient data into three statistics and stores them in three data servers, respectively. As long as one data server is not compromised, the confidentiality of the patient data can be conserved. For the real user e.g. medical doctor to access the patient data, we planned a charge regulator protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. In case any two of three servers are given in the proposed system provides a proxy based data retrieval system.

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.