Privacy Protection for Medical Data in Distributed Server

Thorat Nikhil V[1] Wabale Ashwini H[2] Salgat Piraji R[3] Kardile Pratiksha A.[4] Prof. S.S.Gore[5]

[1,2,3,4]B.E. Student [5]Project Guide

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]Jaihind College of Engineering Kuran Pune, India

Abstract—Remote sensor systems have been broadly utilized as a part of social insurance applications, for example, healing facility what's more home patient observing. Remote medicinal sensor systems are more powerless against listening in, adjustment, mimic and replaying assaults than the wired systems. A considerable measure of work has been done to secure remote medicinal sensor systems. The current arrangements can secure the patient information amid transmission, however can't stop within assault where the persisting chairman database uncovers the delicate patient information. we propose a functional way to deal with keep within assault by utilizing various information servers to store tolerant information. The principle commitment of this paper is safely conveying the patient information in different information servers and utilizing the Paillier and ElGamal cryptosystems to perform measurement investigation on the patient information without bargaining the patients security.

Key words: Wireless medical sensor network, patient data privacy, Paillier encryption, and ElGamal encryption

I. INTRODUCTION

Data collection security in the wireless medical sensor network, each medical sensor can securely send the patient data to the distributed database 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 analysis system, the authorized user can get the statistical analysis results only. Health care technologies are moving from isolated and autonomous solutions to more interoperable ones. The main expectations of this change are to provide better ways to exchange and share medical information and to improve the quality of services offered to the patients. In this context, medical data is supposed to be available online where healthcare professionals can access it at any time and from any place. Basically, it will be transmitted over Internet, dedicated Virtual Private Networks (VPN), and hospital networks. The on-line access to medical information can have two major consequences: it can support healthcare professional to take better decisions; it can increase the risk of loss of privacy and malicious attacks. The goal of designing and implementing eHealth platforms is to reinforce the former consequence and to reduce or eliminate the second one. This paper focuses on the strategy to widely reduce the malicious attacks' risk and to assure the privacy of patients during the storing and exchange (sharing) of medical information by using the e Health platform. Some cryptographic protocols have proved their efficiency to provide data-security for communications over networks but they do not fully prevent attacks to users computers or servers. An e Health platform has to deal with these risks, control authentication, authorization, and integrity. Several countries are implementing different solutions to satisfy these needs, but the evolution of the applications, methods and laws had forced some of them to review partially or completely their approaches.

II. EXISTING SYSTEM

Numerous social insurance applications utilizing WSNs have been produced, such as CodeBlue,Alert Net, UbiMon , MEDiSN, and MobiCare. A regular illustration of medicinal services applications with WSNs Caution Net created in University of Virginia for helped living and private checking. The construction modeling of Alarm-Net is appeared in Fig. 1. Caution Net is made out of versatile body system, emplaced sensor system, Alarm Gate applications, back-end frameworks, and client interfaces as takes after:

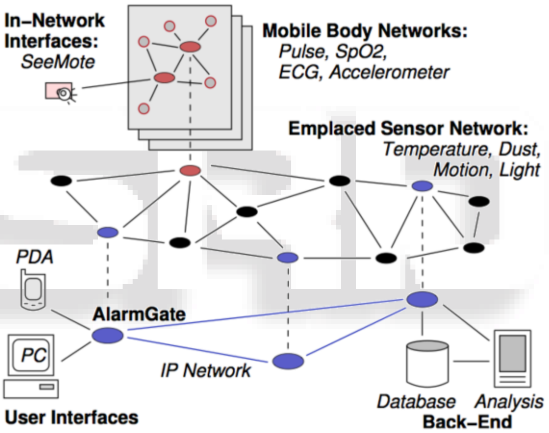

Fig. 1: Alarm-Net Architecture

Versatile body system has remote sensor gadgets worn by a patient which give physiological detecting. Information from the portable body system is transmitted through the emplaced in the living space to sense ecological quality or conditions, for example, temperature, dust, movement, and light.

Emplaced sensors keep up associations with versatile body systems as they travel through the living space Alarm Gate applications serve as application level passages between the remote sensor systems and IP systems. These hubs permit client interfaces and an association with a back-end database for long haul stockpiling of information.

Back-end frameworks give online examination of sensor information and long haul stockpiling of information. User interfaces permit any honest to goodness client of the framework to inquiry sensor information. Remote restorative sensor arranges surely move forward quiet's nature of-consideration without aggravating their solace. Be that as it may, there exist numerous potential security dangers to the patient delicate physiological information transmitted over people in general channels and put away in the back-end frameworks. Common security dangers to social insurance applications with WSNs can be outlined as takes after.

Remote restorative sensor organizes surely move forward Persistent nature of-consideration without irritating their solace. Be that as it may, there exist numerous potential security dangers to the patient touchy physiological information transmitted over people in general channels and put away in the back-end frameworks. Run of the mill security dangers to human services applications with WSNs can be condensed as takes after. Listening in is a security danger to the patient information protection. A busybody, having a capable recipient radio wire, may have the capacity to catch the patient information from the restorative sensors and in this manner knows the understanding's wellbeing condition. He may even post the understanding's wellbeing condition on informal organization, which can represent a genuine risk to patient protection. Mimic is a security risk to the patient information validness.

In a home care application, an assailant may mimic a remote depend point while understanding information is transmitting to the remote area. This may prompt false cautions to remote locales and a crisis group could begin a salvage operation for a non-existent individual. This cans even thrashing the motivation behind remote social insurance.

Adjustment is a security risk to the patient information trustworthiness. While the patient information is transmitted to the doctor, a foe may catch the physiological information from the remote channels and adjust the physiological information. After the assaulted information (i.e., adjusted information) is sent to the doctor, it could jeopardize the patient.

Information rupture is a security risk to the patient information security. An information rupture is an occurrence in which delicate, ensured or secret patient information has conceivably been seen, stolen or utilized by a person unapproved to do as such. For instance, a noxious patient database head may utilize the patient information, (for example, tolerant character) for their individual advantage, for example, for medicinal extortion, deceitful protection claims, and here and there this may even posture life-undermining dangers.

To secure the remote therapeutic sensor systems against different assaults, a ton of work has been done. In 2012, an overview on the as of late distributed writing on secure social insurance observing utilizing remote sensor systems was led by Kumar also, Lee. Current arrangements are based on either mystery key encryption or open key encryption as takes after:

Mystery key based arrangements accept that the mystery keys for encryption and confirmation are sent in the therapeutic sensors and the servers ahead of time. A mystery key cryptosystem, such as AES [1], is utilized for encryption, while the message confirmation code (MAC) is utilized for confirmation.

III. Proposed System

A. *Privacy-Preserving Wireless Medical Sensor Network:*

1) *System Model:*

Like the greater part of human services applications with remote restorative sensor organize, our structural engineering has four frameworks as takes after.

A remote restorative sensor system which faculties the persistent body and transmits the patient information to a patient database framework;

A quiet database framework which stores the patient information from medicinal sensors and gives questioning administrations to clients (e.g., doctors and restorative experts);

A quiet information access control framework which is utilized by the client (e.g., doctor) to get to the patient information and screen the patient;

A persistent information examination framework which is utilized by the client (e.g., medicinal specialist) to question the patient database framework and investigate the patient information measurably.

There may be a middleware between the remote restorative sensor system and the patient database framework. Provided that this is true, the part of the middleware is simutilize sending the encoded understanding information to the database framework.

In our model, the patient database framework is made out of numerous database servers. We accept that all information servers are semi-fair, frequently called "legit however inquisitive". That is, all information servers run our convention precisely as indicated, yet may attempt to learn however much as could be expected about the patient information from their perspectives of the convention. What's more, we expect that no less than one information server is not bargained by assailants. For straightforwardness, we accept that the quantity of information servers is three. The architecture of our model with three data servers can be shown in Fig.2. The security requirements for system model include:

B. *Data Collection Security:*

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

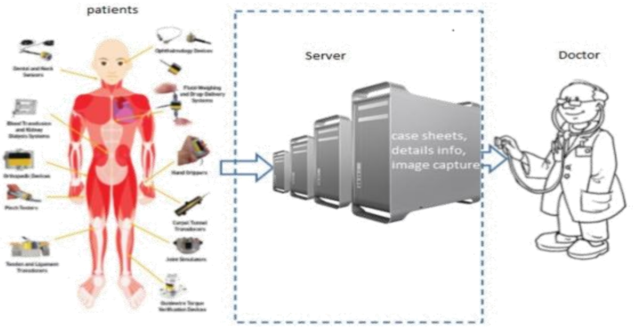

Fig. 2: System Model

1) *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.

2) 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.

3) Data Analysis Security:

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.

Our model considers two types of attacks, the outside attack and the inside attack. The outside attacker does not know any secret key in 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.

IV. Conclusion

In this paper, we have researched the security and protection issues in the medicinal sensor information gathering, stockpiling and inquiries and exhibited a complete solution for protection saving therapeutic sensor system. To secure the correspondence between medicinal sensors and information servers, we utilized the lightweight encryption plan and MAC era plan taking into account SHA-3 proposed in the paper .To keep the quiet's protection information, we proposed another information accumulation convention which parts the patient information into three numbers and stores them in three information servers individually. The length of one information server is definitely not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g., physician) 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 (e.g., 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. Unlike our solution can preserve the patient data privacy as long as one of three data server is not compromised requires that the number.

References

[1] Advanced Encryption Standard (AES). FIPS PUB 197,November26,2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[2] F. Hu, M. Jiang, M. Wagner, D. C. Dong. Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign. IEEE Trans. Inform. Tech. Biomed, 11: 619-627, 2007.

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

[4] J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terzis, G. M. Masson. MEDiSN: Medical Emergency Detection in Sensor Networks. ACM Trans. Embed. Comput. Syst. 10: 1-29, 2010.

[5] P. Kumar, Y. D. Lee, H. J. Lee. Secure Health Monitoring Using Medical Wireless Sensor Networks. In Proc. 6th International Conference on Networked Computing and Advanced Informa- tion Management, pages 491-494, Seoul, Korea, 16-18 August 2010

[6] P. Kumar and H. J. Lee. Security Issues in Healthcare Appli- cations Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012.

[7] X. H. Le, M. Khalid, R. Sankar, S. Lee. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. J. Networks 27: 355-364, 2011.

[8] H. J. Lee and K. Chen. A New Stream Cipher for Ubiquitous Application. In Proc. ICCIT’07, South Korea, 2007.

[9] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato. SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth System. IEEE J. Select. Area Commun. 27: 365-378, 2009.