WIRELESS MEDICAL SENSOR DATA PRIVACY PROTECTION

Mrs. Ch. Sandhya[1], Dr. V. Anantha Krishna[2], M. Ramyasri[3], B.Rachana[4], I. Nithya[5]

Article History: Received: 14.02.2023 **Revised:** 31.03.2023 **Accepted:** 15.05.2023

Abstract:

The development of WSNs in recent years have been extensively employed in healthcare applications including patient monitoring in hospitals and at home. In comparison to wired networks, wireless medical detector networks are more susceptible to assaults that include replaying, impersonation, manipulation, and eavesdropping. Several efforts have been made to protect wireless medical technology. Sensing systems. The current technologies can save patient data during transmission, but they are unable to thwart an insider attack in which the patient database administrator accidentally divulges private patient information. Using numerous data servers to hold patient data is the practical strategy we suggest in this study for preventing the inside assault. The safe distribution of patient data over various data waiters and the use of Paillier and ElGamal cryptosystems for statistical analysis of the case data without compromising patient sequestration.

Keywords: Paillier and Elgamal Cryptosystems, Data Servers, Encryption, Decryption.

[1]Assistant Professor, Sridevi Women's Engineering College Hyderabad, India
[2]Professor, Sridevi Women's Engineering College Hyderabad, India
[3,4,5]Computer Science and Engineering, Sridevi Women’s Engineering College, B.Tech IVYear Hyderabad, India

Email address: [1]chirrasandya@gmail.com, [2]krishnaananthav@gmail.com

DOI: 10.31838/ecb/2023.12.s3.321

1. INTRODUCTION

One that uses wireless detectors(WSN) is made up of geographically dispersed independent detectors that work together. Military uses, similar as battleground surveillance, served as the motivation for the creation of wireless detector networks, which are now utilised in a wide range of marketable and consumer operations, including machine health monitoring, process control, and monitoring of artificial processes.

Wireless medical sensor networks, one of the most pr omising uses for wireless sensor networks (WMSNs), allow watching/supervising of patients in hospitals a nd even at home.Several WSN-based healthcare apps, including CodeBlue, have been created in recent years. UbiMon, MEDiSN, Alarm-Net, and MobiCare. Healthcare

applications using WSNs typically include those developed by School of Comp Sci and Computer Systems at RMIT Melbourne University, Victoria, 3001, Australia's Zhen Yi, AthmanBouguettaya, DimitriosGeorgakopoulos, & Andy Song; Cybernetica's Jan Willemson, Ulikooli 2, Tartu, Estonia. University of Virginia researchers created Alarm-Net for residential and assisted living monitoring.

2. RELATED WORK

2.1. In wireless medical monitoring settings, a privacy-preserving method called k-anonymity

Because to the proliferation of wireless sensors and mobile technology as a whole, it is now possible to deliver better medical services whilst simultaneously reducing costs and controlling the shortage of expert staff. The use of sensors to track a person's health has the potential to improve care while also raising privacy concerns. An untrustworthy or negligent data supplier may leak this information to an unauthorized third party. One technique to protect a patient's privacy is to make it difficult to link specific measurements to a specific identifier. The study presents a secure system design based on k-anonymity. As compared to alternative, more expensive, cryptography-based methods, the provided algorithm lowers energy usage, demonstrating its resource awareness.

2.2. A Framework for Fast Privacy-Preserving Computations

3. METHODOLOGY

Sensitive data must be collected and processed carefully. The essential information systems cannot be built using any standard formula. In order to solve this issue, we provide a general-purpose compute system that is both efficient and provably safe in this study. A virtual computer called SHAREMIND, part of our approach, uses share computing methods to analyse data while maintaining anonymity.

It is the standard practice for evaluating functions securely in a distributed computing environment. Our approach to secret sharing, as well as the creation of t he connected rules of conduct suite, distinguishes our solution. We took so me practical to allow largescale shared figuringout. I n the three-party figuring calculating of the honest-but-curious way of thinking, the SHAREMIND rules of conduct secure/make sure of information-theoretic safety,Unlike conventional, centralized databases, the honest-but-curious architecture greatly increases privacy preservation even if it does not accept bad members.

Existing System

- Modification is a security trouble to the case data integrity.
- Data breach is a security trouble to the case data sequestration.
- These data threats are been sloved in the existing system.

Disadvantage

The results can cover the case data during transmission, but cannot stop the inside attack where the director of the case database reveals the sensitive case data.

Problem Statement

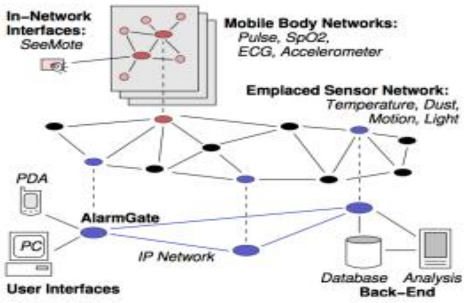
Unauthorized collection and use of patient data can beget life- hanging pitfalls to the case, or make the case’s private matters intimately available.

Proposed System

- We assume that the wireless medical detector network is composed of some medical detectors.
- The Paillier and ElGamal cryptosystems are used in order to keep the privacy.
- The case data can be saved as long as at least one of three data waiters isn't compromised.

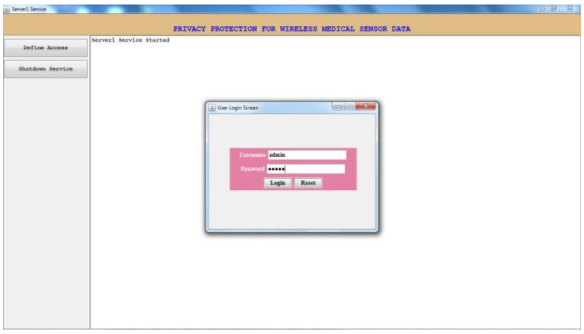
Advantage

The patient’s data can be secured using encryption.


In–Network Interfaces: SeeMote
Mobile Body Networks: Pulse, SpO2, ECG, Accelerometer
Emplaced Sensor Network: Temperature, Dust, Motion, Light
PDA
AlarmGate
PC
IP Network
User Interfaces
Database
Analysis
Back–End

User interfaces, rear systems, a mobile bodily network, and an embedded sensor network make up the Alarm-Net system. • Wireless sensor devices worn by patients to monitor physiological data are included in the portable body network. The installed sensor network keeps tabs on things like temperature, humidity, air quality, motion, and lighting in the home. When people move about the room, integrated sensors maintain contact with their bodies using mobile body networks. In order to connect Internet protocol and wireless sensor networks, AlarmGate applications act as gateways at the application level. These hubs provide data analysis in real time and give access to long-term data storage through a database. Without a question, wireless medical sensor nodes improve patient care while keeping patients comfortable. at serious risk if he were to reveal the patient's. Eavesdropping poses a threat to the confidentiality of patient information. With a powerful receiving antenna, an eavesdropper might get patient information from the sensing devices and learn about the patient's health status. The patient's privacy is health state on social media. Impersonation poses a threat to the reliability of patient information. A hacker might pose as a wireless connection during transmission of patient data from a home health application to a remote location. This might lead to unnecessary rescue missions being launched for nonexistent victims because of misleading alarms being sent to remote regions. This might be harmful to the field of wireless healthcare in certain situations. The patient's physiological data might be intercepted and altered by a threat while it travels through wireless networks on its way to the doctor. Patient safety may be at stake if the physician receives the altered data. In the event of a data breach, patients' personal information could be at risk. A data breach occurs when potentially sensitive, proprietary, or private patient information is accessed, stolen, or used without the owner's permission. This can lead to medical fraud, bogus insurance claims, or death threats by a physician using patient data. There have been several attempts to protect wearable medical sensor networks from various dangers. In 2012, Kumar and Lee conducted a review of the most recent research on wireless networks of sensors for safe healthcare monitoring It is likely that the encryption and authentication keys are pre-installed on the server and medical sensors in secret key systems) is used for authentication. Popular approaches using hidden keys include. These methods usually work well. Nevertheless, the efficiency of private key distribution is lower than that of public-key based methods. Key distribution and updates are simplified by these methods. Yet, they are generally ineffectual and do not directly apply to such networks because of the limited transmission and processing capabilities of wearable medical sensor networks. Most of the current options focus with protecting wireless medical smart sensors against attacks when the attacker requires access to the network's secret keys. It is possible to prevent external attacks with the use of access restriction, authentication, and encryption. Each sensor uses one of three unique secret keys to interact with the servers in the Sharemind network [3], which is used to store patient data. Sharing sensitive patient data (such a temperature measurement) is made possible by the Sharemind system's use of three separate data servers, each of which receives its own encrypted copy of the data over a separate channel. Sharemind is a computing system that can perform operations on input data without disclosing the data itself.three Sharemind's web server may work together to manage certain user requests for patient information without disclosing the data itself, for example, from doctors, nurses, as well as other medical professionals. The method can protect patients' privacy as far as there is just one hacked data server. To transmit patient data, each sensor speaks with the same three data servers. Our system will continue to work frequently even if both of our data servers are attacked. Our contribution to this study are summarized below. To protect the confidentiality of patient information based on the Fillers and ElGamal cryptographic protocols; the protocol allows an individual (for example, a doctor) to connect computer. Users (like medical researchers) are able to conduct statistical analyses on patient data using these methods without compromising confidentiality. In contrast to the method given, which utilizes the Sharemind system to carry out data analysis without taking into account data server cooperation, these contributions take a radically different approach. In Section 3 we explain our answer in full. Evaluations of functionality and safety are carried out in Part 4. The last section is where the overall impression is created.

4. RESULT AND DISCUSSION



Server1 Service

PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

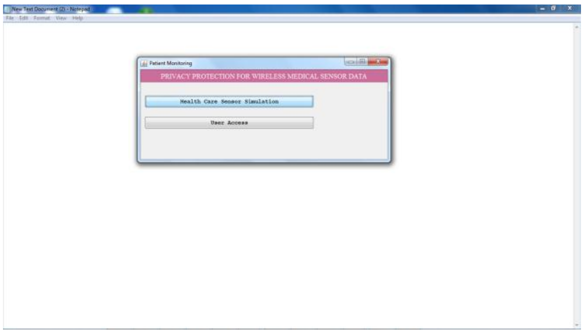
Server1 Service Started

User Login Screen

Username: admin

Password: •••••

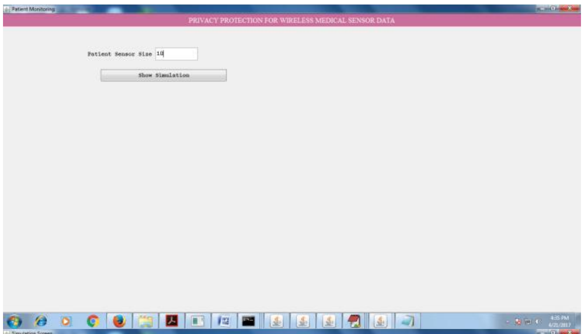
Users of either the average analysis technique or patient information retrieval access should be included



Patient Monitoring

PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

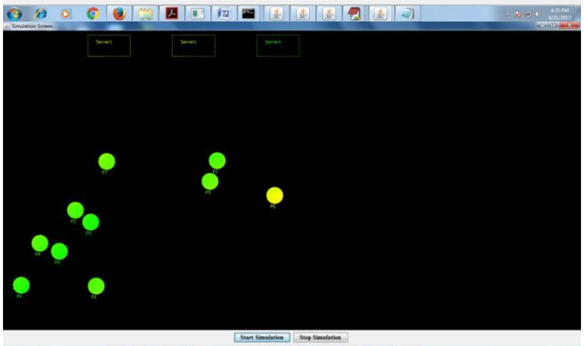
Health care sensor simulation: Choose Show Simulation and enter the patient sensor size.



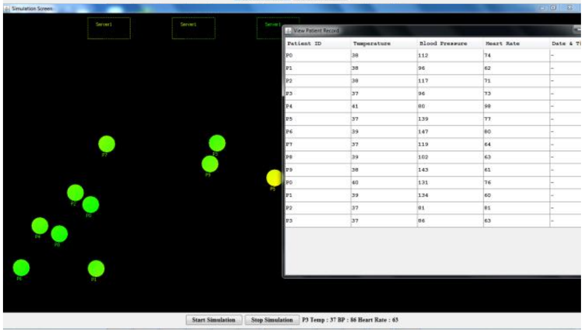
Patient Monitoring

PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

Patient Sensor Size: 10



Simulation Screen

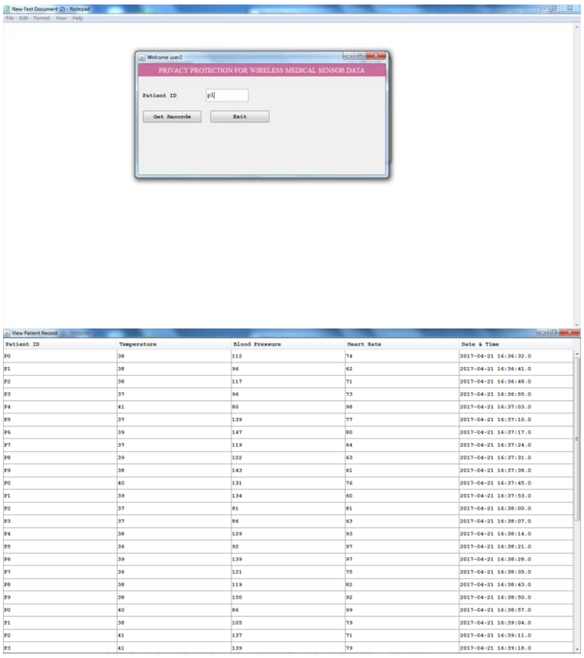


Simulation Screen

View Patient Record

Patient ID	Temperature	Blood Pressure	Heart Rate	Date & Ti
P0	38	112	74	-
P1	38	96	62	-
P2	38	117	71	-
P3	37	96	73	-
P4	41	80	98	-
P5	37	139	77	-
P6	39	147	80	-
P7	37	119	64	-
P8	39	102	63	-
P9	38	143	61	-
P0	40	131	76	-
P1	39	134	60	-
P2	37	81	81	-
P3	37	86	63	-

P3 Temp : 37 BP : 86 Heart Rate : 63



PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

Patient ID p1

Patient ID	Temperature	Blood Pressure	Heart Rate	Date & Time
P0	38	112	74	2017-04-21 16:36:32.0
P1	38	96	62	2017-04-21 16:36:41.0
P2	38	117	71	2017-04-21 16:36:48.0
P3	37	96	73	2017-04-21 16:36:55.0
P4	41	80	98	2017-04-21 16:37:03.0
P5	37	139	77	2017-04-21 16:37:10.0
P6	39	147	80	2017-04-21 16:37:17.0
P7	37	119	64	2017-04-21 16:37:24.0
P8	39	102	63	2017-04-21 16:37:31.0
P9	38	143	61	2017-04-21 16:37:38.0
P0	40	131	76	2017-04-21 16:37:45.0
P1	39	134	60	2017-04-21 16:37:53.0
P2	37	81	81	2017-04-21 16:38:00.0
P3	37	86	63	2017-04-21 16:38:07.0
P4	38	129	93	2017-04-21 16:38:14.0
P5	36	92	97	2017-04-21 16:38:21.0
P6	39	139	97	2017-04-21 16:38:28.0
P7	36	121	75	2017-04-21 16:38:35.0
P8	38	119	82	2017-04-21 16:38:43.0
P9	38	150	92	2017-04-21 16:38:50.0
P0	40	86	99	2017-04-21 16:38:57.0
P1	38	105	79	2017-04-21 16:39:04.0
P2	41	137	71	2017-04-21 16:39:11.0
P3	41	139	79	2017-04-21 16:39:18.0

5. CONCLUSION

We address the security and sequestration issues related to the collection, storehouse, and reclamation of medical detector data in this research by suggesting a comprehensive solution for a secure medical sensor network. Lightweight techniques and an SHA -3 based approach to generate MAC were used to protect data transmissions between sensor devices and servers. To protect patient privacy, we proposed a unique data-collection approach that divides patient data into three parts and keeps them in various servers. If even an individual data source is not the confidentiality of patient information is not breached. We devised an access mechanism through which only authorized users (such as doctors) may see patient records. Control protocol in which three data servers join to provide the user with patient information, while the protocol remain secret. We handed new protocols for average, correlation, friction, and retrogression analysis in which the three data waiters unite to dissect patient data while guarding the case's sequestration and also offer the statistical analysis findings to the stoner. It offers a path for the authorized user to conduct statistical analysis on the patient data. Our approaches are safe against external and internal threats as long as just one data server is attacked, according to security and privacy studies. The investigation of our methods' performance demonstrates that they are also practically useful. As long as one of the three data servers is not hacked, our system can protect the very private nature of patient information.

6. REFERENCES

Advanced Encryption Standard (AES). FIPS PUB 197, November 26, 2001.

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.

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

R. Chakravorty. A Programmable Service Architecture for Mobile Medical Care. In Proc. 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06), Pisa, Italy, 13-17 March 2006.

Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com / benchmarks.html. [6] J. Daemen, G. Bertoni, M. Peeters, G. V. Assche, Permutation-based Encryption, Authentication and Authenticated Encryption, DIAC'12, Stockholm, 6 July 2012. Available at http://www.hyperelliptic.org/DIAC/slides /PermutationDIAC2012.pdf

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.

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

Digital Signature Standard (DSS). FIPS PUB 186-4, July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, 31 (4): 469-472, 1985.

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.

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.

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

J. Ko, 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. [

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 Information Management, pages 491-494, Seoul, Korea, 16-18 August 2010.

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