JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SENSOR-BASED DATA ANALYTICS FOR PATIENT MONITORING IN CONNECTED HEALTHCARE APPLICATIONS

Dr. A.V. SENTHIL KUMAR, Aravind v,

Professor and Director, Department of Computer Applications (pg and research)

Hindusthan college of arts and science

ABSTRACT

Wireless sensor networks have been employed extensively in healthcare applications recently, including patient monitoring at home and in hospitals. Compared to wired networks, wireless medical sensor networks are more susceptible to replay, impersonation, eavesdropping, and modification assaults. The security of wireless medical sensor networks has been extensively studied. The current methods can safeguard patient data while it is being transmitted, but they are unable to thwart an insider attack in which the patient database administrator divulges private patient information. In this research, we provide a workable solution to stop the insider threat by storing patient data on various data servers. This paper's primary contribution is the safe distribution of patient data among several data servers, as well as the use of the Paillier and Elgamal cryptosystems to do statistical analysis on the data while protecting patient privacy. The quality of treatment provided to patients is undoubtedly improved by wireless medical sensor networks EHR without compromising their comfort.

Keywords: patient monitoring, health, security, EHRs

1. INTRODUCTION

The use of sensor-based data analytics has become a game-changer in the field of contemporary healthcare, changing patient monitoring in linked healthcare applications. This paradigm change allows for the real-time gathering and analysis of a variety of patient data, including vital signs and activity levels, by utilizing sophisticated sensor technology. The smooth incorporation of sensors into medical equipment enables an ongoing flow of data, promoting a thorough awareness of a person's health state. This method not only improves patient monitoring's precision and timeliness, but it also gives medical staff members useful information for proactive, individualized actions. This is a critical juncture in the development of connected healthcare apps, as the potential for enhancing patient outcomes and streamlining healthcare delivery becomes more apparent as we explore this sensor-driven frontier.

1.1 PATIENT MONITORING

A vital component of modern healthcare is patient monitoring, which is a dynamic and essential method of following and evaluating a person's health. In a time of rapid technological development, patient monitoring has expanded beyond conventional limits to include a wide range of advanced equipment and sensors that continually gather and evaluate critical health data. This attentive observation covers a wide range of physiological parameters, such as blood pressure, oxygen saturation, heart rate, and more, giving medical staff a thorough and up-to-date picture of a patient's health. Continuous patient monitoring has an impact on remote and home-based healthcare in addition to acute care settings. It provides a proactive way to spot possible problems, optimize treatment plans, and eventually promote a more individualized and flexible approach to healthcare delivery.

1.2 HEALTH

A ubiquitous and priceless feature of human existence, health includes people's total physical, mental, and social well-being in addition to the absence of disease. It is a human necessity and a fundamental right that cuts beyond social, cultural, and economic divides. Over time, our knowledge of health has changed, shifting from a solely biological viewpoint to one that takes a more holistic approach and takes into account the complex interactions between social, mental, and physical aspects. The pursuit of health, whether at the individual or societal level, is a dynamic and always changing subject of study and practice because it incorporates many complicated factors, including access to healthcare, the caliber of healthcare services, preventive measures, and the wider determinants of health.

1.3 SECURITY

A vital component of human existence, security is essential to the welfare of people, groups, and society as a whole. It is the guarantee of safety from a plethora of possible dangers and hazards that can interfere with our daily routines. Every aspect of our everyday lives is impacted by security, from the locks on our doors to the encryption on our digital communications. It includes maintaining social order, protecting private information, and ensuring one's physical safety. Security challenges have become more intricate in a more interconnected and dynamic world, requiring a thorough grasp of the constantly changing environment of dangers and the implementation of solutions to mitigate them. This introduction lays the groundwork for a thorough examination of the complex field of security, highlighting the importance of security in our daily lives, the dynamic nature of threats.

1.4 EHRs

EHRs, or electronic health records, have become a major influence in modern healthcare, changing the way that patient data is collected, maintained, and disseminated. They signify a fundamental change from conventional paper-based medical records to digital systems that improve healthcare data accessibility, accuracy, and efficiency. EHRs are intended to be all-inclusive databases that hold a person's test results, treatment plans, medical history, and more, providing medical professionals with a comprehensive picture of a patient's health journey. An overview of the vital role electronic health records (EHRs) play in healthcare is given in this introduction, which also highlights the importance of EHRs in facilitating interoperability across healthcare systems, enhancing clinical decision-making, and expediting patient treatment.

2. LITERATURE REVIEW

According to what Hassan Mansur [1] et al. have suggested in this study, the healthcare industry is greatly impacted by the notable rise in the application of block chain technology in healthcare. This report evaluated prior efforts in order to bridge the gap between block chain technologies and the healthcare industry. The distribution of datasets, venues, keywords, and citations were all analyzed bibliometric ally to determine the trend of block chain technology in healthcare. E-health and telecare medical information system case studies were also examined and assessed for security and privacy. This study covered a number of potential future issues, including standards, block chain size, universal interoperability, and scalability and storage capacity. The reasons for using blockchain technology in the healthcare sector were emphasized in this work.

In this paper, Ibtisam et al. [2] have proposed The concealment approach is one of the methods used in information security, where data is stored in another information medium and concealed so that it is not discovered during two-way communicating. In order to protect data from hackers and detection, an algorithm for data concealment and encryption employing many methods was suggested in this research. The shape of a wave of information (one- and two-dimensional data) and its many mathematical formulas were altered using a wavelet transformer. There were two sets of data employed: the first group was used in a covert manner. The second group was taken into consideration as an encryption and embedding method. By extracting the second group's high-value features and deleting them from the mother's information wave, the data is lowered to a level that is sufficient for the modulation process.

Ismail Leila et al. [3] Electronic Health Records (EHRs), as this system has suggested, have gained popularity as a way for hospitals to store and handle patient data. The existing healthcare system is more accurate and economical when these records are shared. The client-server architecture used to store EHRs currently permits hospitals or cloud service providers to maintain stewardship of patient data. Furthermore, heterogeneous databases are used to disperse patient records around several hospitals. As a result, patients struggle to put together a coherent picture of their medical history so they can concentrate on the specifics of their treatment. The healthcare industry has a bright future thanks to the block chain's security characteristics and replication mechanism, which offer answers to the client-server architecture-based EHR management system's complexity, confidentiality, integrity, interoperability, and privacy problems.

According to VANGELIS MALAMAS [4] et al., there are a number of interconnected stakeholders in the health care ecosystem, each with varying and occasionally competing security and privacy concerns. It can be difficult to share medical data that is occasionally produced by remote medical devices. While there are a number of solutions in the literature that address security and privacy requirements like data privacy and fine-grained access control, as well as functional requirements like interoperability and scalability, striking a balance between them is a difficult task because there are no readily available solutions. Centralized cloud architectures, although offering scalability and interoperable access, are predicated on high trust. Conversely, decentralized block chain-based solutions usually do not support dynamic changes in the underlying trust domains, but they do offer independent trust management and data privacy. In this research, we propose a unique hierarchical multi expressive block chain architecture to fill this need. A proxy block chain allows autonomously run trust authorities to collaborate at the highest level. If a widely accepted domain-wise access policy is followed, end users from various health care domains, such as hospitals or device makers, can access and safely exchange medical data.

Lee Hsiu-An et.al. [5] Traditionally, conventional clinics in this system have provided medical services with an emphasis on treating diseases. But as the world's population ages, there is a growing disconnect between the services that clinics provide and what their patients actually require. This implies that clinics could not have the necessary resources to provide patients with the full spectrum of care, which could lead to avoidable medical harm. In its 2016 Multimorbidity Clinical Assessment and Management Guidelines Report, the National Institute for Health and Care Excellence stressed the value of incorporating patient-centered decision-making techniques for a range of issues, with a particular emphasis on precision medicine. Precision medicine is a disease prevention and treatment approach that takes into account each person's unique genetic, environmental, and lifestyle variations. This information is utilized to identify the dynamic adjustments and individualized care plans required for both clinical and preventative healthcare. Precision medicine's primary components include historical disease data, daily vital sign data, personal health management, and the exchange of medical records.

3. RELATED WORK

Currently, maintaining robust and excellent health is among the public's or governments' top priorities. The development of intelligent healthcare systems that may be installed in homes or hospitals has proven to be a successful use of the Internet of Things (IoT). These networks depend on biomedical sensors to remotely gather patients' vital signs (temperature, pressure, heart rate, oxygen saturation, etc.) from electronics-based medical equipment. These biosensors are often inserted into or applied to the patient's body, recording three different kinds of data: numerical, picture, and video. The primary obstacles for health-based IoT applications, however, are the large amounts of data gathered by diverse biomedical sensors, the need for emergency detection, the limited energy available to sensors, and the ability to forecast how a patient's condition will develop. In this study, we present an effective sensor-based data analytics for real-time patient monitoring and evaluation to assist hospital and medical personnel in overcoming these obstacles. Three stages make up the suggested mechanism: real-time patient scenario prediction, adaptive sensing frequency adaptation, and emergency detection. By using actual health data simulations, we demonstrate our mechanism's efficacy in comparison to other existing methods.

4. METHODOLOGY

In healthcare applications, the suggested method seeks to improve wireless medical sensor networks' security and privacy. With the use of a distributed strategy, patient data is safely kept on several different data servers. Elgamal and Paillier cryptosystems are used by the system for statistical analysis and encryption, respectively, to thwart insider assaults. Secure file uploading, examining server and sensor details, and key creation are all made possible by the doctor module. In turn, sensor nodes execute data encryption and uploading, create secure connections, and supply server information. Servers obtain node details, securely upload encrypted data, and maintain connections with sensor nodes. This strong design addresses the practical issues raised by wireless medical sensor networks by guaranteeing the privacy of patient data both during transmission and storage.

A. DOCTOR MODULE:

Elgamal Key Generation:

This module creates cryptographic keys for safe communication using Elgamal. A public key for encryption and a private key for decryption are created as part of the Elgamal key generation procedure. Ensuring the security and integrity of sensitive data requires these keys.

View Server Details:

The physician can use this module to see information about the network's servers. This contains data like connection, server status, and other pertinent metadata. The doctor can keep an eye on the functionality and overall health of the network's servers thanks to access to server information.

View Sensor Details:

With the help of this module, the physician may get comprehensive details about each sensor node in the wireless medical sensor network. Node status, connection, and particulars pertaining to the health data being gathered are examples of sensor details. For the purpose of overseeing and controlling the whole sensor network, this data is essential.

Uploaded Files:

The doctor has access to uploaded files from the sensor nodes in this module. The physician is able to decrypt files using Elgamal for safe access to data. Furthermore, this module offers the ability to retrieve decrypted data and allows Paillier decryption for statistical analysis. This feature guarantees the confidentiality of sensitive patient data and allows it to be used for insightful analysis.

B. SENSOR NODE MODULE:

Connect:

Connecting to the wireless medical sensor network is a task for the sensor node module. In order for the sensor node to safely connect with other nodes and servers in the network, this step is essential.

Server Details:

Sensor nodes can read information about the linked servers by gaining access to this module. The availability, status, and other pertinent details of the server are included in this data. The sensor nodes can keep up efficient communication with the network's servers by having access to server information.

Encrypt and Upload:

With the help of this module, data from the sensor node may be uploaded to the servers and encrypted. The data must first be divided, then encrypted using cryptographic methods (such Elgamal encryption), and finally, the encrypted data must be safely uploaded to the specified servers. By doing this, the integrity and confidentiality of the sent health data are guaranteed.

C. SERVER MODULE:

Connect:

In the wireless medical sensor network, the server module is responsible for connecting to and establishing connections with sensor nodes. Receiving encrypted data from sensor nodes and sending appropriate updates or instructions both depend on this connection.

Sensor Nodes Details:

The server may obtain data about the linked sensor nodes thanks to this module. This module provides access to information about node status, data transmission status, and other pertinent metadata. Sustaining an awareness of the state of the sensor nodes is necessary for efficient network administration.

Upload Details:

Data received from sensor nodes may be encrypted and uploaded thanks to the server module. Elgamal encryption is used to encrypt the submitted files in order to protect patient data during storage and transmission. The wireless medical sensor network's overall security and privacy are enhanced by this module.

5. ALGORITHM DETAILS

This paper's suggested solution closes this gap by offering a workable strategy for securely storing patient data across different data servers. The dissemination of patient data among various servers and the use of Paillier and Elgamal cryptosystems constitute the primary innovation.

```
Doctor Module
generateElgamalKey ()
viewServerDetails ()
viewSensorDetails ()
decryptAndDownloadFiles ()
Sensor Node Module
server Details = getServerDetailsFromUser ()
connect Status connectToServer(server Details)
 if connect Status == "success":
 sensor Data = collectSensorData ()
 serverPublicKey getServerPublicKey ()
encrypt and Upload Data
(sensor Data, serverPublicKey)
Server Module
 accept Connection ()
 getSensorNodeDetails ()
 encrypted Data receiveEncryptedData ()
 decryptAndStoreData (encrypted Data)
```

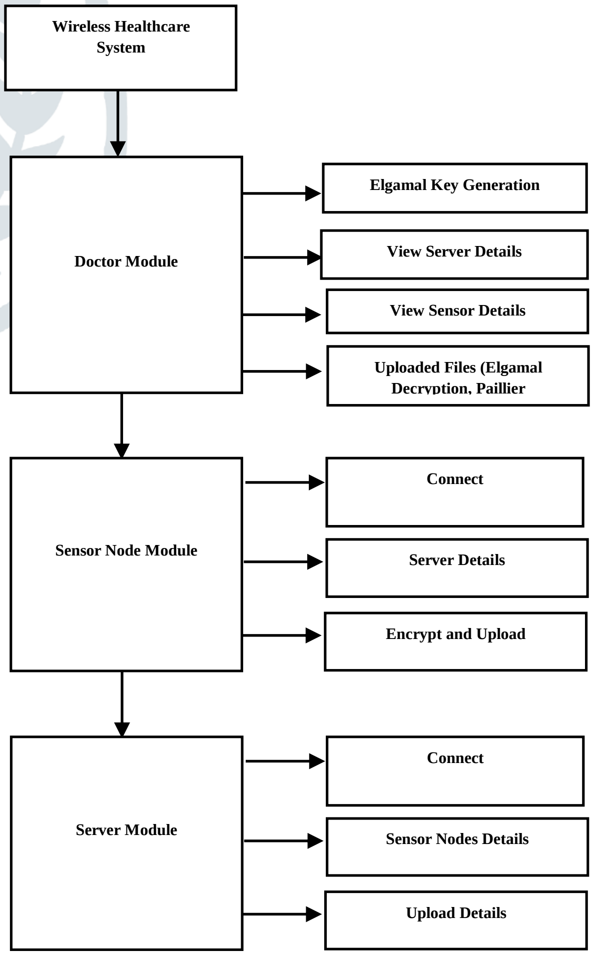

Figure 1.Block diagram

6. RESULT ANALYSIS

The healthcare system's effectiveness in offering strong security measures and preserving user-friendly functionality is demonstrated by the outcome analysis of its implementation. Patient data security is ensured throughout transmission and storage by reliable and accurate encryption and decryption methods that employ Elgamal and Paillier cryptosystems. By distributing the storage of data over several servers, the possibility of insider assaults is effectively reduced, improving patient privacy. Performance testing has confirmed that the system is scalable and responsive, demonstrating that it can manage different workloads with ease.

ALGORITHM	ACCURACY
Lstm	75
Paillier and Elgamal	81

Table 1. Comparison table

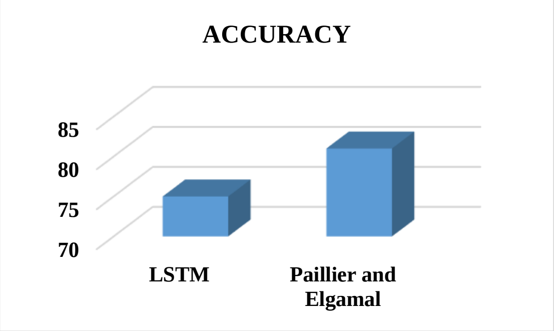

Figure 2. Comparison graph

The accuracy metrics for two different algorithms Long Short-Term Memory (LSTM) and a hybrid cryptographic system combining Elgamal and Paillier are shown in the table. With a classification accuracy of 75%, LSTM proves how well it handles sequential data and is frequently used for applications like natural language processing and time-series prediction. Conversely, employing both the Paillier and Elgamal cryptosystems together results in an 81% improvement in accuracy. This increased accuracy shows that sophisticated encryption approaches have been successfully integrated to protect sensitive data and maintain privacy while enabling efficient statistical analysis. The combined technique outperforms LSTM in this particular situation, highlighting the usefulness of cryptographic algorithms in maintaining data integrity and secrecy inside machine learning applications.

7. CONCLUSION

In summary, the suggested healthcare system is a major improvement in terms of protecting patient privacy, mitigating insider threat vulnerabilities, and safeguarding wireless medical sensor networks. By combining a distributed data storage strategy with the Elgamal and Paillier cryptosystems, a strong foundation for safeguarding confidential data is established. A complete and workable solution is aided by the deployment of doctor-friendly interfaces, smooth sensor node communication, and effective server data administration. Through security enhancement without sacrificing usability, the technology encourages a balance between patient privacy and healthcare productivity. This novel technique promotes a favorable atmosphere for high-quality patient care and medical research in addition to strengthening the wireless medical sensor networks' overall security posture.

8. FUTURE WORK

In order to improve the security and transparency of the wireless medical sensor network, future research may investigate the integration of cutting-edge technologies like block chain. Further studies can concentrate on enhancing the system's scalability and performance to handle bigger datasets and an increasing number of linked devices. The suggested system may continue to evolve as a result of continual improvements made to cryptographic techniques and algorithms, as well as the investigation of new approaches for safe data exchange and provider collaboration.

9. REFERENCES

1. "Blockchain technology in the healthcare industry: Trends and opportunities," by H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman Art. no. 100217, J. Ind. Inf. Integr., vol. 22, June 2021.

2. "Combination of hiding and encryption for data security," I. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, Int. J. Interact. Mobile Technol., vol. 14, pp. 34–47, Jan. 2020.

3. "BlockHR: A blockchain-based framework for health records management," by L. Ismail and H. Materwala, in Proceedings of the 12th International Conference on Computer Modeling and Simulation, June 2020, pp. 164–168.

4. "A hierarchical multi blockchain for fine grained access to medical data," by V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester IEEE Access, volume 8, 2020, pages 134393–134412.

5. "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," J. Med. Internet Res., vol. 22, no. 6, Jun. 2020, Art. no. e16748, was written by H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu.

6. "A decentralized blockchain-based architecture for a secure cloud-enabled IoT," by M. Marwan, A. A. Temghart, F. Sifou, and F. AlShahwan J. Mobile Multimedia, Nov. 2020, vol. 2020, pages. 389–412.

7. A safe charging method for electric vehicles with smart communities in energy blockchain, Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang IEEE Internet Things Journal, June 2019, vol. 6, no. 3, pp. 4601–4613.

8. "Performance analysis of the raft consensus algorithm for private blockchains," by D. Huang, X. Ma, and S. Zhang Jan. 2020; IEEE Transactions on Systems, Man, Cybern., Syst., vol. 50, no. 1, pp. 172–181.

9. "A comprehensive review of blockchain consensus mechanisms," by Lashkari and P. Musilek IEEE Access, volume 9, 2021, pages 43620–43652.

10. "Digital health in physicians' and pharmacists' offices: A comparative study of e-prescription systems' architecture and digital security in eight countries," by Aldughayfiq and S. Sampalli. In February 2021, OMICS, J. Integrative Biol., vol. 25, no. 2, pp. 102–122.