International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 01 | Jan – 2026 DOI:10.55041/ISJEM03386
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A Sensor-Based Data Analytics for Patient Monitoring in Connected Healthcare Applications

Dr.Majidha Fathima K M
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology Coimbatore, India
majidhafathimakm@skcet.ac.in

Ajaynavaneeth G R
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology Coimbatore, India
727721eucs010@skcet.ac.in

Bhuvaneshwari R
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology Coimbatore, India
727721eucs021@skcet.ac.in

Deepika T
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology Coimbatore, India 727721eucs023@skcet.ac.in

ABSTRACT

Wireless sensor networks have been increasingly popular in healthcare applications in recent years, including patient monitoring in hospitals and at home. Compared to wired networks, wireless medical sensor networks are more susceptible to eavesdropping, alteration, impersonation, and replaying assaults. The security of wireless medical sensor networks has been the subject of extensive research. Although the current solutions can shield patient data while it is being transmitted, they are unable to stop insider assaults, in which a patient database administrator divulges private information. In this research, we use numerous data servers for dispersed patient data storage as a workable solution to counter insider threats. To improve data security and integrity, our suggested method makes use of the SHA-256 algorithm in conjunction with the CUNA framework. Without jeopardizing patient privacy, this method permits statistical analysis while guaranteeing safe patient data release. EHR systems and wireless medical sensor networks greatly enhance patient care without compromising patient 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 Mala mas [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

Wireless sensor networks have been increasingly popular in healthcare applications in recent years, including patient monitoring in hospitals and at home. Compared to wired networks, wireless medical sensor networks are more susceptible to eavesdropping, alteration, impersonation, and replaying assaults. The security of wireless medical sensor networks has been the subject of extensive research. Although the current solutions can shield patient data while it is being transmitted, they are unable to stop insider assaults, in which a patient database administrator divulges private information. In order to mitigate the risk of unauthorized access, we suggest a secure data distribution system that stores patient data across many data servers. Our solution combines the SHA-256 algorithm with the CUNA framework to improve data security, confidentiality, and integrity. The use of SHA-256 for cryptographic hashing keeps patient data safe from tampering, while CUNA guarantees strong access control. This method preserves patient privacy while enabling safe data storage and statistical analysis. EHR systems and wireless medical sensor networks greatly enhance patient care without compromising patient comfort.

1. The Doctor Module

Authorised medical practitioners can securely access and manage encrypted patient data using the Doctor Module, which acts as their main interface. It incorporates cutting-edge cryptographic methods to guarantee the integrity and secrecy of data.

SHA-256 and CUNA

To improve security, this submodule uses the SHA-256 hashing method in conjunction with the CUNA framework. While SHA-256 protects data integrity by producing cryptographic hashes that are impenetrable, CUNA controls access and ensures safe data delivery.

View Server Details

Doctors can use this tool to access and review server-related data, such as storage status, data encryption information, and security measures put in place inside the system.

View Sensor Details

Numerous wireless medical sensor nodes placed in patient homes or healthcare institutions provide real-time data to doctors. This submodule offers information on connectivity status, data transfer, and sensor performance.

Uploaded Files

This submodule enables physicians to access and control securely uploaded encrypted patient records on dispersed servers. It guarantees privacy and adherence to healthcare security standards by limiting access to patient data to authorised persons only.

2. SENSOR NODE MODULE

The task of gathering, encrypting, and sending patient data to safe storage places falls to the Sensor Node Module. In order to guarantee the safe and smooth transfer of medical data, it is essential.

Connect

Between the sensor node and the system servers, this submodule creates a secure connection. It guarantees that the sensor can follow security procedures and send data effectively.

Server Details

Before uploading data, the sensor node requests and confirms server information. This phase guards against unwanted access and guarantees that data is sent to the right place.

Encrypt and Upload

To improve security, the sensor node uses SHA-256 hashing to encrypt patient data prior to transmission.

The data is uploaded to dispersed servers once it has been encrypted, guaranteeing that it is safe from unwanted changes or breaches.

3. SERVER MODULE

The Server Module oversees the safe processing, retrieval, and storage of data received from sensor nodes. It serves as a focal point for preserving patient records' availability and integrity.

Connect

This submodule enables encrypted data transmission by facilitating secure connections between servers and sensor nodes. It guarantees that the system can only receive data from authenticated sensor nodes.

Sensor Nodes Details

This feature shows the status, activity logs, and data transmitted by each of the connected sensor nodes. It aids in tracking sensor performance and identifying irregularities.

Upload Details

Each uploaded file's details are logged and stored by the system, guaranteeing accountability and traceability. Authorised users can monitor data integrity over time by using the timestamps, encryption status, and file metadata recorded by this submodule.

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 ()

decrypt And StoreData (encrypted Data)

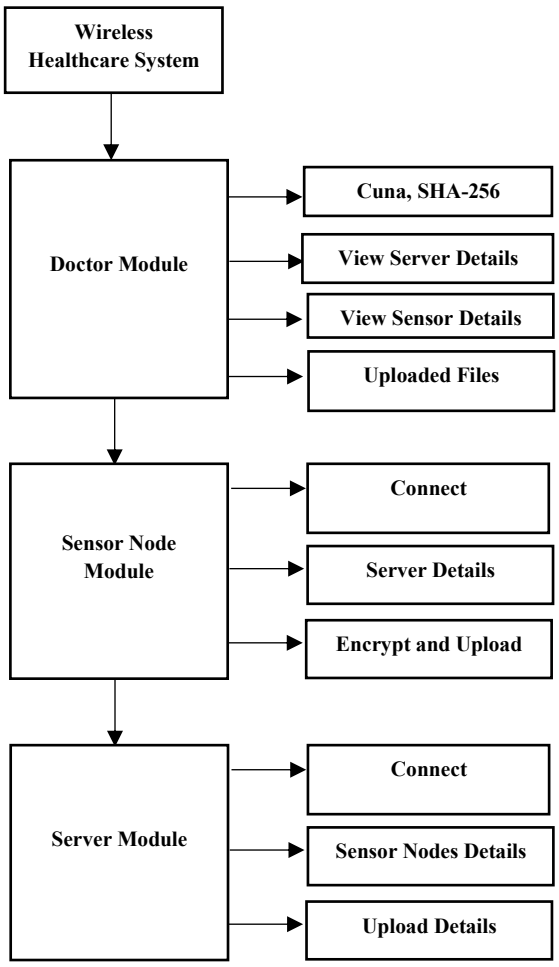

Figure 1.Block diagram

6. RESULT ANALYSIS

The study of the results assesses the system's performance across many modules in terms of security, effectiveness, and usability. The CUNA framework efficiently controls access control, lowering the possibility of insider attacks, while the use of SHA-256 encryption guarantees data integrity by prohibiting

unwanted changes. The sensor node module ensures real-time data security by properly encrypting and uploading patient data to dispersed servers. The server module manages the storage and retrieval of encrypted data effectively while preserving smooth connectivity with authorized users and sensor nodes. Only authorized experts are able to retrieve and analyze patient data thanks to the doctor module's protected access. Performance testing verifies that the system can manage large data loads with low latency and continue to operate at its best in a variety of scenarios. Security testing verifies that the system is impervious to dangers like replay assaults and eavesdropping. The results of user acceptance testing show that the system is easy to use and satisfies the requirements of medical professionals. All things considered, the findings show that the system effectively guarantees the safe, effective, and private handling of patient data while upholding adherence to healthcare security regulations.

ALGORITHM	ACCURACY
Lstm	75
Cuna, sha 256	81

Table 1. Comparison table

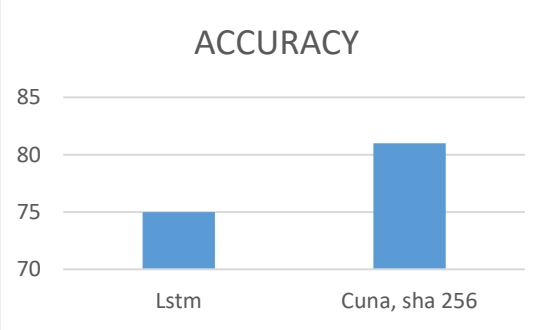

Figure 2. Comparison graph

7. CONCLUSION

By combining SHA-256 encryption with the CUNA framework for safe data storage and access management, the solution effectively improves the security and privacy of patient data in wireless medical sensor networks. The approach reduces the possibility of insider threats and illegal access by spreading encrypted data among several servers. Secure connection between sensor nodes, servers, and physicians guarantees patient data protection while facilitating quick access by authorized personnel. Evaluations of the system's performance and security show that it is resilient to possible attacks and can manage the transmission and retrieval of encrypted data without sacrificing efficiency or speed. Healthcare workers can deal with encrypted medical data with ease because to the system's user-friendly interface. All things considered, the suggested approach successfully strikes a balance between security, effectiveness, and usability, making it a solid framework for protecting patient data in contemporary healthcare settings.

8. FUTURE WORK

Future research could examine how to improve the security and transparency of the wireless medical sensor network by integrating cutting-edge technology like blockchain. Further study can also concentrate on improving 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 to cryptographic methods 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. Udaya sankaran, 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.