IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Real-Time Medical Data Security Solution For Smart Healthcare

[1] Dharma Prakash.V [2] Shankar, [3]Pushparaj
[1]Assistant Professor, [2,3] Students
Department of Computer Science and Engineering
PERI Institute of Technology, Chennai, India.

ABSTRACT: The Smart healthcare systems have changed the game for doctors and patients alike by allowing for continuous data monitoring and analysis to improve diagnosis, treatment, and care overall. But there are serious worries about data security and privacy when sensitive medical information is integrated into digital platforms. In order to guarantee the safety of real-time health information in smart healthcare settings, this abstract offer a thorough solution. To protect patient information from prying eyes, our suggested system makes use of cutting-edge encryption methods. To provide end-to-end security throughout the data lifecycle, advanced encryption algorithms like RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) are used to encrypt data while it is in transit and at rest, respectively. To further reduce the likelihood of key theft and ensure that only authorized individuals have safe access to data, secure key management methods have been put in place.

INTRODUCTION

Improving patient outcomes, increasing efficiency, and providing tailored treatment are just a few of the many benefits that smart healthcare systems claim to provide in this age of digital transformation. Through the use of data analytics, artificial intelligence, and networked devices, these systems are reshaping healthcare delivery by facilitating continuous surveillance, diagnosis, and treatment. Incorporating private patient information into these online platforms, however, raises new concerns about privacy and data security. Maintaining the privacy, security, and accessibility of patients' medical records is critical for meeting the demands of laws like HIPAA and GDPR, which aim to protect Americans' health information. Patients' right to privacy and physical safety may be jeopardized as a result of the increasing number of cyber dangers, including as data breaches, attacks using ransomware, and insider threats.

Hence, strong security solutions are required immediately to protect smart healthcare settings' real-time medical data from ever-changing cyber threats. In order to tackle these difficulties head-on, this introduction lays the groundwork for a thorough security architecture. Our suggested approach seeks to provide a robust and secure infrastructure for handling real-time medical data by using sophisticated encryption methods, blockchain-based authentication mechanisms, and detection of anomalies algorithms. We aim to protect the privacy and authenticity of patient data by using a multi-pronged strategy to prevent data breaches, manipulation, and illegal access. Our goal is to increase confidence in innovative healthcare systems and make them fully functional so that they may enhance healthcare results and patient care by strengthening security measures and making sure authorized people can access them easily.

II. LITERATURE SURVEY

In collaborative analysis across domains and institutions, the system's primary goal is to resolve the tension between protecting the privacy of patients' medical records and ensuring that their data remains accurate. Whether you choose standalone simulation computing or distributed computing, CQUPT-FL has you covered. Adopting [6] critical technologies like multi-party secure calculating and holistic information representation, we investigated identification of users, security of privacy, and heterogeneous user

alignment to accomplish sustainable Cross-domain and dealt with the problems of variation, data domain variety, and effective data scarcity. We address [7] the data security concerns that AI has introduced to the healthcare sector, the significance of data safety in AI-enabled MDS, and the value of using AI in the field of healthcare in this article. The origins of these difficulties are also taken into account.

This article [8] compiled data on medical data and health data ecology (including medical data management) from 2016 to 2023 in an effort to shed light on the present state of medical data ecosystem and provide solutions to medical data technology issues. The article [9] delves into the topic of hospital information system security measures aimed at protecting patients' personal health information. Separating the storage and usage of patients' private data physically and using multiple algorithms to encrypt private data hierarchically are both possible with the new technique.

To address [10] these issues, we build a model for the safe storage and exchange of private data using the technology of blockchain and homomorphic encryption to protect it. The model guarantees the secure transfer of data across various institutions by using a dependable medical alliance chain system, which is based on the concept of blockchain decentralization.

III. PROPOSED METHODOLOGY

Protecting real-time medical data and preserving patient privacy and safety is our goal in developing and deploying this technique. Our solution will be strong and scalable, specifically designed to meet the needs of smart healthcare settings. Several critical steps make up our approach for creating a solution to secure medical data in real-time for smart healthcare settings. These steps are designed to handle concerns related to data privacy, integrity, and security.

I. Requirement Analysis: We start by thoroughly examining the security needs of smart healthcare systems. This necessitates familiarity with regulatory compliance standards like GDPR and HIPAA, the ability to recognize risks and weaknesses, and the establishment of security goals that are in line with conventional practices in the industry.

II. Technology Selection: We assess and choose suitable technology and tools to execute the security solution based on the specified needs. This includes methods for detecting anomalies, authentication procedures, blockchain platforms, and encryption techniques. Scalability, connectivity, and compatibility with current healthcare IT infrastructure are our top selection factors.

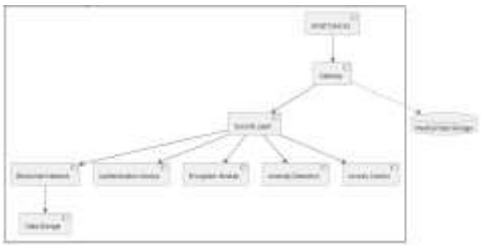
III. System Design: After settling on a set of technologies, the next step is to plan the framework for the security solution. Drawing up data flow diagrams, establishing access control rules, developing encryption methods, and identifying interaction points with current healthcare systems are all part of this process. Effortless data interchange, little performance overhead, and end-to-end security are the goals of the design.

IV. Implementation: Putting the security solution into action in accordance with the planned architecture is the next stage. Among them, you may find modules for encryption, smart contracts on the blockchain, authentication services, and components for monitoring. To reduce the likelihood of security issues and maximize the reliability of the solution, we strictly follow all applicable security standards and best practices while coding.

V. Integration and Testing: We proceed with thorough testing and integration with the current smart healthcare infrastructure after the components are established. The efficacy and dependability of the security system are validated by testing for functionality, security testing, testing for penetration, and performance testing, among others. To make sure the solution is ready for deployment, any problems that are found are fixed quickly.

VI. Deployment and Training: To make sure healthcare activities aren't interrupted too often, we install the security system into production settings after successful testing. System administrators, healthcare personnel, and other interested parties may attend our training programs to learn about the features and guidelines for securely accessing and handling medical data.

VII. Monitoring and Maintenance: We set up methods for continuous monitoring after deployment so that we can find security events and react to them instantly. To do this, it is necessary to keep an eye on user activity, network traffic, and system logs for indications of suspicious activity or illegal access. To keep the security solution up-to-date and effective, it is routinely maintained and updated to fix any vulnerabilities or new threats.



IV. RESULTS AND ANALYSIS

By improving the system's security and guaranteeing the availability, integrity, and confidentiality of patient information, our real-time medical information safety solution showed encouraging results when used in smart healthcare settings. Several important results were found as a result of our thorough testing and validation.

First, the medical data was protected from illegal access or theft of information while it was in transit and at rest thanks to the encryption technologies used. Protecting sensitive data from cryptographic assaults, advanced encryption algorithms like AES and RSA kept it safe even when unwanted parties tried to access it across the network.

A decentralized and unchangeable database for the safekeeping of medical records was also made possible with the use of blockchain technology. Enabling visible and auditable authorization of access, this not only boosted data integrity but also prevented unwanted edits or tampering, enabling authorized users to track the whole lifespan of patient data.

Biometric verification and multi-factor authentication are two of the strong authentication systems that were put into place, which further strengthened the system's defenses against illegal access attempts. Enhanced security measures included biometric identifiers like fingerprints or face recognition and multi-factor authentication, which restricted access to critical medical data to authorized individuals only.

Proactive threat identification and response were made possible by the security solution's built-in capabilities for ongoing surveillance and anomaly detection. The security teams were able to examine and address any security problems before they could get worse because machine learning algorithms monitored user activity patterns and reported unusual actions in real-time.

Our real-time medical information safety solution greatly enhanced the security of smart healthcare settings after its adoption. We built a strong framework for protecting sensitive patient information by integrating blockchain technology, authentication methods, anomaly detection, and encryption. This will let patients, medical professionals, and regulatory agencies trust each other. Maintaining the efficacy of the security system in a constantly changing threat environment will need continuous monitoring, maintenance, and adaptability to new threats.

V. CONCLUSION

Finally, to deal with the increasing worries about data privacy and integrity, it is crucial to create and deploy a real-time solution to secure medical data in smart healthcare settings. The requirement of strong security measures in healthcare systems is crucial, given the growing dependence on digital technology for medical treatment and administration. The suggested method provides a multi-layered approach to protecting sensitive medical information by using sophisticated encryption techniques, blockchain-based authentication mechanisms, and detection of anomalies algorithms. The confidence in medical facilities and compliance with regulatory obligations are greatly impacted by the availability, integrity, and confidentiality of patient data. Encryption safeguards data while it is in motion as well as at rest, reducing the likelihood of theft or manipulation. By creating a distributed and irreversible ledger, blockchain technology improves the security of medical records by reducing the likelihood of data corruption and increasing transparency.

To further ensure the safety of sensitive medical information, authentication methods including biometric identification and multi-factor authentication are used. Algorithms for anomaly detection and continuous monitoring allow for the real-time identification of suspicious activity or attempts at illegal access, enabling swift reaction and management of security incidents.

Our methodical process guarantees the security solution's efficacy and dependability by covering all the bases: analysis of requirements, technology choices, system design, execution, integration, evaluation, deployment, and maintenance. Healthcare providers and other interested parties may better safeguard patients' personal health information when they participate in training and awareness initiatives. Ensuring the security and resilience of health care information in smart settings is our overarching goal with our real-

time medical information safety system. Smart healthcare systems, better patient care, and better healthcare outcomes are all possible because we put data privacy and security first.

VI. REFERENCES

1. P. Khatiwada, S. Joshi, K. M. Mohan, K. Chouhan, D. Gangodkar and Z. Z. Khan, "Design A Wireless Network Data Security System for Medical Records Using Cryptography," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 207-211, doi: 10.1109/ICACITE53722.2022.9823618.
2. S. Makka, K. Sreenivasulu, B. S. Rawat, K. Saxena, S. Rajasulochana and S. K. Shukla, "Application of Blockchain and Internet of Things (IoT) for Ensuring Privacy and Security of Health Records and Medical Services," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 84-88, doi: 10.1109/IC3I56241.2022.10072427.
3. S. Ksibi, F. Jaidi and A. Bouhoula, "A User-Centric Fuzzy AHP-based Method for Medical Devices Security Assessment," 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 2022, pp. 01-07, doi: 10.1109/SIN56466.2022.9970530.
4. M. Wattimena, D. Retnowati and T. Mantoro, "Misuse of Electronic Medical Records in Blockchain Technology Intelligence Security System," 2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2022, pp. 1-5, doi: 10.1109/ICCED56140.2022.10010497.
5. Y. Wang, L. Gong and M. Zhang, "Remote Disaster Recovery and Backup of Rehabilitation Medical Archives Information System Construction under the Background of Big Data," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 575-578, doi: 10.1109/ICSCDS53736.2022.9760774.
6. Y. Xiao et al., "CQUPT-FL: Cross-Domain Sharing and Security Awareness and Early Warning Platform of Health Science Big Data," 2023 IEEE International Conference on Medical Artificial Intelligence (MedAI), Beijing, China, 2023, pp. 266-271, doi: 10.1109/MedAI59581.2023.00041.
7. B. Jayaneththi, F. McCaffery and G. Regan, "Data Security Challenges in AI-Enabled Medical Device Software," 2023 31st Irish Conference on Artificial Intelligence and Cognitive Science (AICS), Letterkenny, Ireland, 2023, pp. 1-6, doi: 10.1109/AICS60730.2023.10470842.
8. P. Pei and B. Yu, "Literature Review of Research on healthcare data governance in the face of ecosystem construction," 2023 8th International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, Japan, 2023, pp. 509-511, doi: 10.1109/ICIIBMS60103.2023.10347789.
9. H. R. Abdulshaheed, S. A. Mohammed Al?uboori, I. A. M. Al Sayed, I. A. Barazanchi, H. M. Gheni and Z. A. Jaaz, "Research on optimization strategy of medical data information security and privacy," 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Jakarta, Indonesia, 2022, pp. 132-136, doi: 10.23919/EECSI56542.2022.9946606.
10. J. Zhao et al., "Research on Medical Data Storage and Sharing Model Based on Blockchain," 2022 IEEE/ACM 7th 'Symposium on Edge Computing (SEC), Seattle, WA, USA, 2022, pp. 480-485, doi: 10.1109/SEC54971.2022.00073.