Healthcare Record Management System

Meghana Bhandari[#1] ,Prarthana Y Aradhya[#2] , Rakshitha G K[#3] , Sagar M[#4], Chethan H S[#5]
[#1234]Student , Department of CSE , Bangalore Institute of Technology , Bangalore , India
#5Professor , Department of CSE , Bangalore Institute of Technology , Bangalore , India

***Abstract* - Blockchain technology has emerged as a transformative tool for ensuring security, transparency, and immutability in various domains, including healthcare. This paper introduces a Healthcare Record Management System (HRMS) built on blockchain, designed to address the challenges of data integrity, security, and accessibility in patient record management. The system empowers authorized doctors to edit patient records while maintaining a transparent log of changes using timestamps. By leveraging the decentralized nature of blockchain, the proposed system ensures that patient data remains tamper-proof, enhancing trust among stakeholders. Additionally, the timestamp functionality provides users, including patients and healthcare providers, with a detailed history of record modifications, fostering accountability and facilitating better decision-making. This study explores the design, implementation, and evaluation of the system, highlighting its potential to revolutionise healthcare data management by offering a secure, transparent, and efficient solution.**

Keywords: Blockchain , Timestamps , Transparency , Decentralized , Tamper-proof.

I. INTRODUCTION

Healthcare systems are increasingly reliant on digital record-keeping for improved patient care and operational efficiency. However, these systems often grapple with critical challenges, including data security, patient privacy, and controlled access to sensitive medical records. Traditional centralized healthcare databases are vulnerable to breaches, unauthorized access, and single points of failure, raising concerns about the integrity and confidentiality of patient data.

To address these issues, blockchain technology emerges as a transformative solution.Blockchain's decentralized, immutable, and secure architecture ensures that healthcare records are resistant to tampering and unauthorized modifications. Furthermore, its ability to maintain a transparent and verifiable audit trail fosters accountability among all stakeholders.

We propose a (HRMS) leveraging blockchain to revolutionize the management of patient records. This system places patients at the center of data control, enabling them to selectively grant access to authorized users, such as doctors, nurses, or researchers. Additionally, timestamps are incorporated to log and track all interactions with patient records, providing an exhaustive history of access and edits.

The system also addresses critical scenarios, such as medical emergencies, by allowing a designated relative to manage access on behalf of the patient. This feature ensures seamless continuity of care while preserving the core principles of privacy and security. By integrating blockchain with user-centric access control mechanisms, the proposed HRMS aims to enhance data integrity, trust, and efficiency in healthcare systems.

We delve into the design,implementation and potential applications of the system, highlighting its contributions to addressing existing gaps in healthcare record management.

II. RELATED WORKS

The integration of blockchain in healthcare has gained significant attention in recent years, with numerous studies exploring its potential to enhance data security, accessibility, and privacy.

Studies such as Xia et al. (2017) have demonstrated blockchain's capability to secure healthcare data exchange between stakeholders. These works highlight blockchain's decentralized architecture, which eliminates single points of failure and ensures the integrity of medical records. However, many of these solutions lack

mechanisms for granular access control, leaving room for improvement in patient-centric data governance.

Azaria et al. 2016 proposed MedRec, a blockchain-based system focusing on access control and interoperability in electronic health records. MedRec introduced the concept of patient-centric control, allowing patients to determine who can access their data. While foundational, this work did not address emergency scenarios where patients are incapacitated, a gap our system aims to bridge.

Research by Roehrs et al. (2019) emphasized the use of timestamps in blockchain-based systems to provide a transparent audit trail. These timestamps ensure accountability and traceability of data access and edits.

Few studies have addressed the need for emergency access mechanisms in healthcare systems. Ekblaw et al. (2018) briefly touched on granting proxy access to relatives in emergencies, but the approach lacked detailed implementation guidelines. Our system builds on this concept by implementing a structured mechanism where designated relatives can act on behalf of patients during emergencies.

III. PROPOSED SYSTEM

The proposed Healthcare Record Management System (HRMS) utilizes blockchain technology to overcome the challenges of managing, securing, and sharing patient medical records in a transparent and efficient manner. The system adopts a decentralized approach to store patient records on a blockchain network, ensuring that the data remains immutable and protected against unauthorized access or tampering. Patients are given primary control over their medical data, enabling them to grant or revoke access to specific users, such as doctors, nurses, or researchers, through smart contracts that automate these processes securely and transparently. Authorized doctors can edit patient records only when access is explicitly provided by the patient, ensuring patient consent is at the forefront of the system′s design.

To enhance accountability, all interactions with the patient records, including viewing, editing, or granting permissions, are logged with timestamps. This timestamped audit trail provides a comprehensive history of all activities, fostering trust among stakeholders and facilitating regulatory compliance. The system also addresses critical emergency scenarios by introducing a mechanism where a designated relative can temporarily grant access to healthcare professionals when a patient is incapacitated and unable to provide consent. This feature ensures timely and uninterrupted access to critical medical data during emergencies, improving patient outcomes.

The system incorporates role-based access control to distinguish between different categories of users, such as doctors, nurses, and researchers. For instance, researchers are limited to viewing anonymized data, while doctors may have permissions to view and edit patient records based on granted access. To further enhance privacy, patient records are encrypted, ensuring that only authorized users can decrypt and access sensitive information. Even in a public blockchain environment, this encryption guarantees the confidentiality of patient data.

Designed with scalability and interoperability in mind, the proposed system seamlessly integrates with existing healthcare infrastructures, ensuring it can support a growing number of users and records. By leveraging blockchain's inherent strengths—security, transparency, and decentralization—combined with user-centric access control mechanisms, the proposed HRMS offers a robust, efficient, and secure solution to modernize healthcare record management while empowering patients and maintaining their privacy.

IV. EXISTING DRAWBACKS

While blockchain technology has shown immense potential in revolutionizing healthcare record management, existing systems face several challenges and limitations that hinder their widespread adoption and efficacy:

Scalability Issues: As blockchain networks grow, they face performance issues, such as slower

transaction speeds and increased latency, limiting their efficiency in large-scale healthcare applications.

Data Privacy Concerns: Storing sensitive data on a blockchain, even with encryption, can pose privacy risks, particularly if key management or data sharing isn't properly secured.

High Energy Consumption: Some blockchain systems, especially those using proof-of-work, require a lot of energy, raising both cost and environmental concerns.

Interoperability Challenges: Blockchain struggles to integrate with existing healthcare systems, which use different standards, making data exchange difficult and reducing system efficiency.

Cost of Implementation: The cost of deploying and maintaining blockchain systems, including infrastructure and training, can be prohibitively high,especially for smaller healthcare organizations.

Regulatory and Legal Barriers: The evolving regulatory landscape around blockchain, including compliance with data protection laws like GDPR and HIPAA, poses legal challenges for widespread adoption in healthcare.

V. ALGORITHM-AES(ADVANCED ENCRYPTION STANDARD)

The **Advanced Encryption Standard (AES)** is a widely used symmetric encryption algorithm known for its efficiency and robust security. In the context of your Healthcare Record Management System (HRMS), AES plays a pivotal role in ensuring the confidentiality and integrity of sensitive patient data stored on the blockchain. AES works by encrypting data in fixed-size blocks (128 bits) using a secret key, with key sizes of 128, 192, or 256 bits. The encryption process involves multiple rounds of transformation,including substitution,permutation, and mixing, which make it highly resistant to cryptographic attacks. Decryption is the reverse process, using the same key to recover the original plaintext from the encrypted data.

In our project, AES is used to encrypt patient records before they are stored on the blockchain, ensuring that even if the blockchain is publicly accessible, unauthorized users cannot access or tamper with sensitive information. Only authorized users with the correct decryption key—such as the patient or healthcare providers—can decrypt and view the records. This enhances the overall security of the system by ensuring data privacy. AES offers strong security with proven resilience against attacks, while also being computationally efficient enough to handle large volumes of healthcare data. Furthermore, AES is certified under FIPS 140-2, a U.S. government standard for cryptographic algorithms, making it a reliable choice for securing sensitive healthcare data. Through the integration of AES encryption, your system effectively meets privacy and security requirements, safeguarding patient records in a blockchain-based environment.

VI. CONCLUSION

The integration of blockchain technology with AES encryption in the Healthcare Record Management System (HRMS) presents a powerful solution to address the critical challenges of data security, privacy, and access control in healthcare. By leveraging blockchain′s decentralized, immutable structure and AES′s strong encryption capabilities, the system ensures that patient records are securely stored and only accessible by authorized individuals. The patient-centric access control model, along with timestamped audit logs, provides transparency, accountability, and robust tracking of interactions with sensitive data. Furthermore, the inclusion of emergency access protocols ensures timely medical interventions while preserving patient privacy.

This system not only enhances the security of healthcare records but also offers a scalable, interoperable solution that can integrate with existing healthcare infrastructures. It addresses gaps in current healthcare systems by offering a secure, efficient, and user-friendly platform for managing patient data. The proposed HRMS contributes to improving healthcare delivery by empowering patients with control over their own

medical records while ensuring that healthcare professionals have the necessary access to provide timely care.

In conclusion, the proposed system sets a new benchmark for secure, patient-centric healthcare record management, offering a practical application of blockchain and AES encryption that aligns with modern healthcare needs and regulatory standards.

VII. REFERENCES

[1].T.-Y. Ou and W.-L. Tsai, "Designing a Flow-Based Mechanism for Accessing Electronic Health Records on a Cloud Environment," IEEE, 2022.

[2]. C. Taramosco, D. Rivera, C. Guerrero, and G. Márquez, "Design of an Electronic Health Record for Treating and Monitoring Oncology Patients in Chile," IEEE Access, 2023.

[3]. R. Tertulino, N. Ivaki, and H. Morais, "Design a Software Reference Architecture to Enhance Privacy and Security in Electronic Health Records," IEEE, 2024.

[4]. A. Koren and R. Prasad, "IoT Health Data in Electronic Health Records (EHR): Security and Privacy Issues in Era of 6G," Journal of ICT Standardization, 2022.

[5]. M. M. Sravani and S. A. Durai, "Bio-Hash Secured Hardware e-Health Record System," IEEE, 2023.

[6]. A. U. R. Butt, T. Mahmood, T. Saba, and S. A. O. Bahaj, "An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment," IEEE Access, 2023.

[7]. A. Sahi, D. Lai, and Y. Li, "A Review of the State of the Art in Privacy and Security in the eHealth Cloud," IEEE Access, 2021.

[8]. V. Usha Rani and G. Attigeri, "Secure EMR Classification and Deduplication Using MapReduce," IEEE, 2024.

[9]. J. Zhao, P. Zeng, and K.-K. R. Choo, "An Efficient Access Control Scheme with Outsourcing and Attribute Revocation for Fog-Enabled E-Health," IEEE Access, 2021.

[10]. K. Edemacu, B. Jang, and J. W. Kim, "Efficient and Expressive Access Control with Revocation for Privacy of PHR Based on OBDD Access Structure," IEEE Access, 2020.