Blockchain based Health Care Protocol

Kaviyaraj R[*,2]
Department of Computational Intelligence,
SRM Institute of Science and Technology,
Kattankulathur, India.
https://orcid.org/0000-0002-1858-1582

Akshat Singh
Undergraduate
Department of Computational Intelligence,
SRM Institute of Science and Technology,
Kattankulathur, India.

***Abstract*— Healthcare data digitalization has completely changed how electronic health records (EHRs) are managed, providing previously unheard-of prospects for process optimization and patient care improvement. But these developments also bring with them serious problems with access control and data security. In order to overcome these obstacles, this research study suggests a revolutionary framework that makes use of blockchain technology. Through the use of off-chain storage and granular access constraints, the framework seeks to offer a dependable, secure, and comprehensive approach to EHR management. In order to further improve the confidentiality and integrity of healthcare data, the article also investigates the integration of sophisticated security features like role-based access control, two-factor authentication, and time-limited access rights.**

Keywords*— *Electronic Health Systems, Data Security, Privacy Concerns, Role Based Access, Time Based Access, Two-Factor Authentication

I. Introduction

A new era in medical record administration has begun with the digitization of healthcare data, offering previously unheard-of accessibility and efficiency. Modern healthcare systems are built around Electronic Health Records (EHRs), which allow for seamless communication between healthcare providers and tailored patient treatment. But even with the quick digitization of medical records, issues with access control and data security remain significant. Because medical data is sensitive and cyber threats are becoming more sophisticated, strong security measures are desperately needed to protect patient confidentiality and privacy.

This research study presents a ground-breaking approach that uses blockchain technology's revolutionary potential to improve healthcare data security and access management in response to these issues. Through the utilization of cryptographic principles and blockchain's decentralized architecture, the framework aims to provide an architecture for handling electronic health records that is safe from tampering. The framework seeks to ensure the confidentiality and integrity of healthcare data while resolving scalability challenges associated with traditional blockchain solutions through the use of off-chain storage techniques and granular access rules.

.

II. Background

An important turning point in the global modernization of healthcare systems has been reached with the widespread use of electronic health records, or EHRs. Electronic Health Records (EHRs) provide a digital archive for keeping all patient data, including diagnosis, treatment plans, lab results, and medical history. The shift from paper-based to electronic records has simplified the healthcare industry's operations, allowing for more effective information retrieval and real-time provider communication. But this digital shift has also made healthcare companies more vulnerable to never-before-seen cybersecurity risks, which calls for the deployment of strong data security protocols.

In the healthcare sector, worries about data security and privacy endure despite the advantages of electronic health records. Medical data is particularly vulnerable to cyberattacks due to its sensitive nature. These assaults can take many different forms, from ransomware attacks and identity theft to illegal access and data breaches. Healthcare data management is further complicated by the need to adhere to strict regulations like the Health Insurance Portability and Accountability Act (HIPAA). Consequently, healthcare institutions are under tremendous pressure to protect patient information while adhering to legal requirements.

Access controls and encryption, two common security methods, have proved crucial in defending healthcare data against outside attacks. But frequently, these precautions don't have the level of detail needed to impose stringent access control guidelines and stop illegal access. Furthermore, because traditional data storage systems are centralized, they come with inherent risks because centralized servers are single points of failure that can be targeted by hackers. A rising number of people are interested in investigating cutting-edge technologies that can improve the security posture of healthcare systems and solve the drawbacks of conventional security approaches in response to these constraints.

Blockchain technology has shown promise in resolving the privacy and security issues that healthcare data management is now confronting. Blockchain is a distributed network of nodes that records transactions in a decentralized, unchangeable ledger. It was first made popular as the technology underpinning cryptocurrencies like Bitcoin. Because it does not require a central authority, its decentralized architecture is intrinsically resistant to tampering and unauthorized modifications, hence lowering the danger of single points of failure. Blockchain technology can offer an open, transparent, and safe platform for EHR management that guarantees data integrity, confidentiality, and authenticity by utilizing cryptographic techniques.

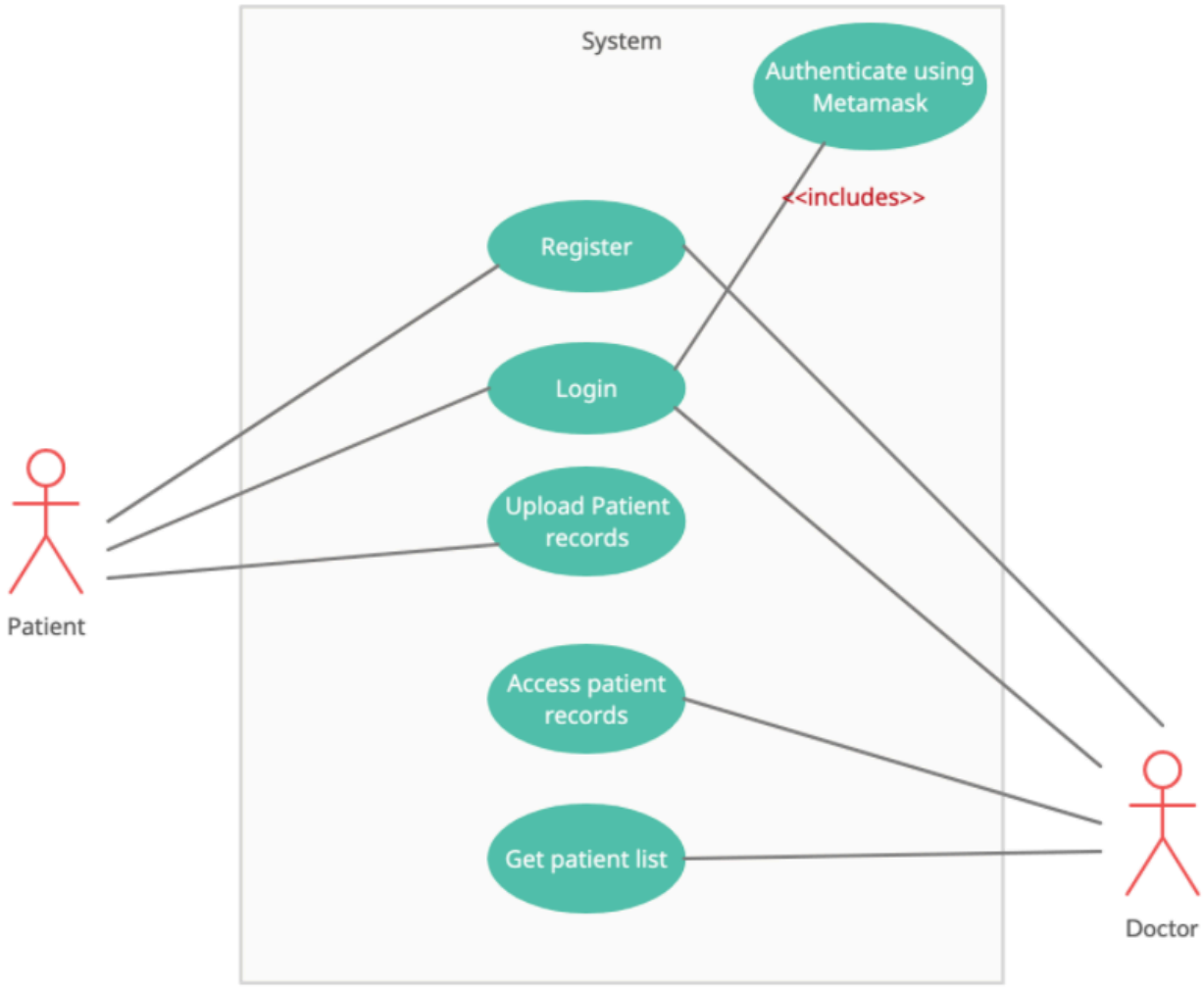


Fig 1: System Flow Diagram

III. Proposed System

Using blockchain technology, the suggested system provides a novel approach to maintaining electronic health records (EHRs). Fundamentally, the system makes use of the decentralized ledger of blockchain technology to offer a safe and unchangeable platform for handling and storing medical data. The system reduces the possibility of unauthorized access and tampering by distributing data throughout a network of nodes and using cryptographic techniques to guarantee the integrity and confidentiality of EHRs.

The incorporation of off-chain storage technologies to overcome scalability issues with conventional blockchain systems is a crucial component of the suggested approach. Large amounts of data, including as medical records and diagnostic pictures, can be safely saved off the blockchain using off-chain storage while still retaining cryptographic assurances of their integrity. This method maximizes storage effectiveness and speeds up data retrieval, improving the system's overall performance. The system has granular access restrictions in addition to off-chain storage to control user access to EHRs and safeguard patient privacy. Users are given particular roles and permissions according to their organizational functions and responsibilities through the use of role-based access control (RBAC) systems. This reduces the possibility of data breaches and unauthorized disclosures by guaranteeing that only those with permission can access the information necessary for them to perform their jobs.

In addition, the system places a high priority on data security by enforcing strong encryption methods to protect private data kept on the blockchain. The technology makes sure that patient data is private and safe even in the case of a security breach or unwanted access attempt by encrypting EHRs while they are in transit and at rest. This increases the confidence and trust of patients in the security of their medical records.

All things considered, the suggested system offers a complete approach to healthcare data management by fusing cutting-edge access control methods with the security and transparency of blockchain technology. The system's objective is to solve the changing difficulties facing the healthcare industry and encourage the use of safe digital healthcare solutions by offering a scalable, secure, and privacy-centric platform for managing electronic health records.

IV. RELATED WORK

A.

aims to revolutionize access control by enabling access to data based on user attributes rather than a predetermined identity. This granular approach increases security, simplifies permissions management, and facilitates secure data exchange in scenarios with specific access requirements. However, ABE introduces key management complexity and potential performance overhead due to additional cryptographic operations. Although these challenges must be carefully considered, ABE's ability to provide granular control over sensitive data makes it a promising solution for a variety of security-conscious applications.

B.

aims to simplify key management by eliminating the need for pre-distributed public keys.Instead, users' public keys are derived from their unique identities, such as their email addresses. This simplified approach is convenient and potentially reduces administrative burden. However, the BIE raises concerns about its vulnerability to blocking attacks, where a compromised identity can be used to gain unauthorized access. In addition, the security of the entire system depends heavily on a trusted authority that is responsible for issuing keys. It is therefore extremely important to ensure the integrity and robustness of this central authority.

C.

leverages the power of blockchain technology to provide transparent and tamper-proof access records.This immutability promotes trust and facilitates auditability by providing an immutable record of all connection attempts. However, the inherent characteristics of blockchain technology, such as its distributed nature and consensus mechanisms, can lead to scalability issues and potential performance limitations, especially in the case of large numbers of access requests.

D.

aims to bridge the gap between data sharing and privacy in healthcare. They allow authorized healthcare facility personnel to access critical patient data while maintaining the security of the original data at the source facility. This approach improves collaboration and facilitates effective care.However, implementing federated access control requires defining complex interoperability standards and supporting close collaboration between participating healthcare organizations, which can be difficult to achieve in practice.

E.

emphasizes flexibility and allows you to create access control policies based on a variety of attributes and conditions. This allows for detailed control and customization to the specific needs of your business. However, the complexity of managing complex policies can be challenging. Establishing clear, consistent and complete policies often requires expertise, and any inconsistency can create security gaps or hinder effective access management.

F.

aims to dynamically adjust access permissions based on a real-time assessment of potential threats. This approach can increase security in environments where threats are constantly evolving. By considering factors such as user behavior, device location and access times, RBAC can limit access in high-risk situations and enable broader access in low-risk times. However, implementing an effective RBAC system requires the development of accurate risk assessment models and continuous monitoring of these

factors, which can require intensive resource deployment and constant maintenance.

G.

prioritizes patient autonomy and gives them control over their health data. This approach allows patients to set access permissions and manage who can access their information, increasing transparency and increasing trust in the healthcare system. However, this emphasis on user control also has a potential downside. If patients do not have sufficient knowledge of the complexities and implications of access control, they may inadvertently grant inappropriate access or make decisions that jeopardize the privacy of their data. Therefore, effective implementation requires educational initiatives that ensure patients are well prepared to make informed decisions regarding data sharing.

H.

takes access control to an even higher level. The data is encrypted using specific access policies so that only users whose attributes match those policies can decrypt the information. This enables very detailed control based on complex criteria, which is a significant advantage. However, this increased control introduces greater complexity in key management and encryption/decryption processes compared to standard ABE, which may potentially impact the performance and scalability.

I.

allows authorized users to perform calculations directly on encrypted data, eliminating the need to decrypt it.This offers a significant advantage in terms of data protection as

sensitive information remains encrypted throughout the analysis or processing phase. However, current homomorphic encryption schemes have limitations. Their computational complexity can have a significant impact on processing speed, making their use potentially difficult in resource-limited environments. In addition, the scope of supported operations may be limited compared to traditional encryption methods, so their suitability for specific tasks must be carefully considered.

J.

provides users with a unique mechanism to demonstrate that they have certain qualities or knowledge without revealing the underlying details.This proves beneficial in access control scenarios where users need to prove their permissions without compromising sensitive information. However, the ZKP also faces challenges. Generating and reviewing complex evidence can be computationally intensive and impact performance. Furthermore, the security of FPC systems largely depends on fundamental cryptographic assumptions. Any gaps in these assumptions could potentially compromise the effectiveness of the entire system.

V. Methodology

The proposed system was developed using a methodical approach that guarantees the security, dependability, and efficacy of the healthcare data management solution. To ensure the smooth integration of crucial features and the validation of the system's functionality, the technique comprises multiple crucial phases, such as assessment, implementation, and testing.

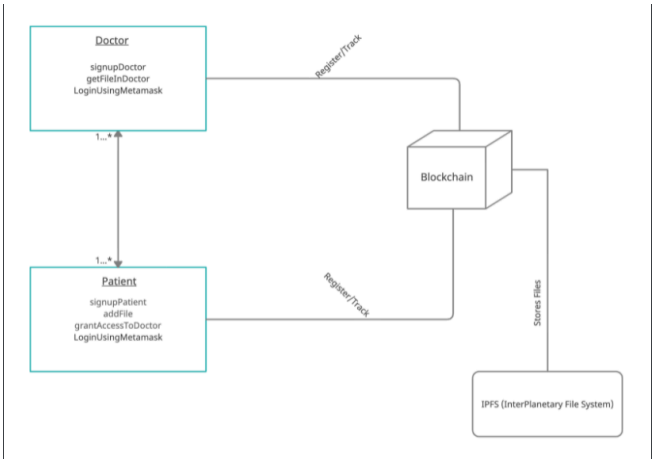
The methodology's initial step entails analyzing potential system vulnerabilities, identifying current issues, and reviewing the state of healthcare data management practices. The assessment phase lays the groundwork for further development efforts by providing a thorough understanding of the limitations and requirements related to healthcare data security and access control.

The implementation step, which comes after the assessment phase, concentrates on incorporating crucial components into the system architecture to improve security and access control capabilities. To address identified security risks and guarantee regulatory compliance, this entails designing and implementing crucial elements such off-chain storage solutions, encryption methods, and role-based access control (RBAC) systems.

The functionality, performance, and security of the suggested solution are rigorously tested after the key components have been incorporated into the system. This testing phase includes a range of scenarios and use cases to evaluate how well the system protects patient information, upholds access control guidelines, and reduces possible security threats. Prior to deployment, thorough testing helps find and fix any problems or vulnerabilities, guaranteeing the system's robustness and dependability.

Following industry norms and best practices at every stage of the development process is essential to guaranteeing the viability and efficacy of the suggested solution. To spot new threats and vulnerabilities and put prompt corrective action in place, the system's performance and security posture must be continuously monitored and evaluated.

Fig 2. Class Diagram



In summary, a methodical approach to healthcare data management with an emphasis on security, dependability, and regulatory compliance was emphasized in the creation of the suggested system. The proposed solution seeks to meet the changing difficulties facing the healthcare business and encourage the use of safe and effective digital healthcare solutions by incorporating necessary features, carrying out thorough testing, and abiding by industry norms.

VI. Result and Analysis

Fig 3. The main landing page.

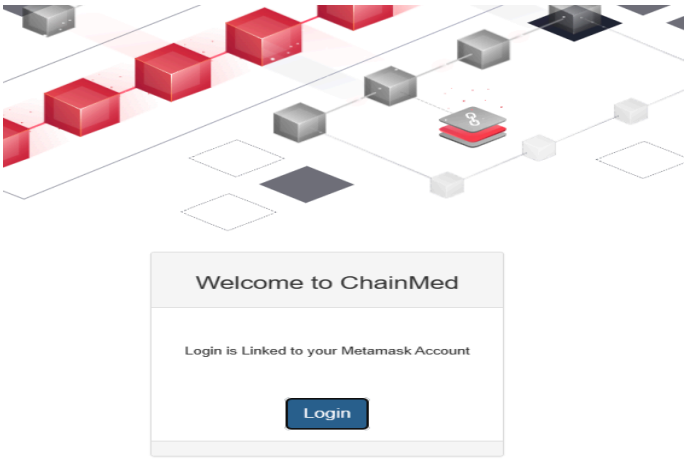


Fig 4. Screenshot of the Compiled Contracts

Fig 5. Screenshot of Contract Migrations

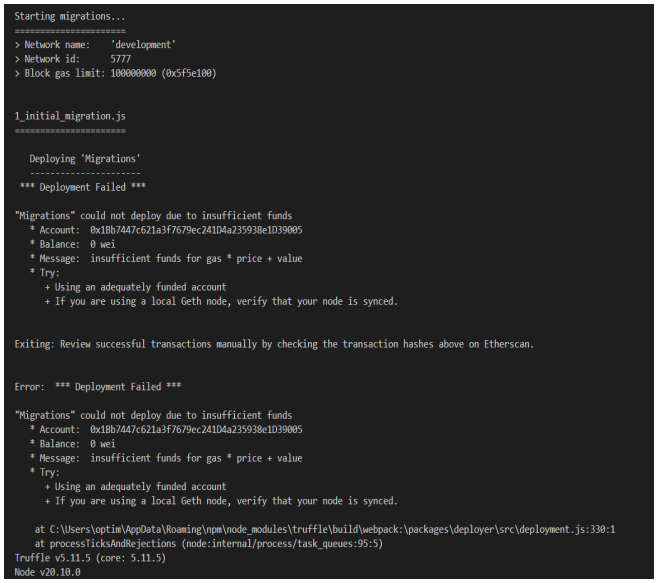


Fig 6. Local Ganache Server

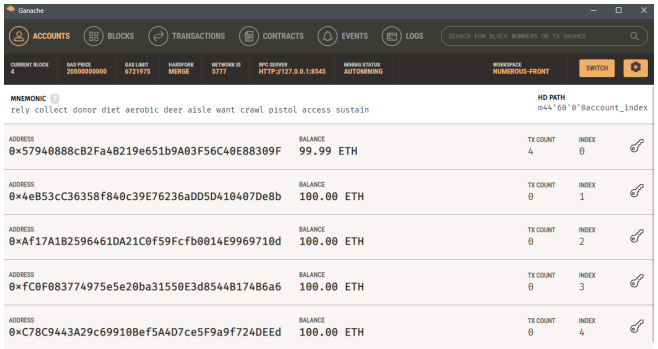
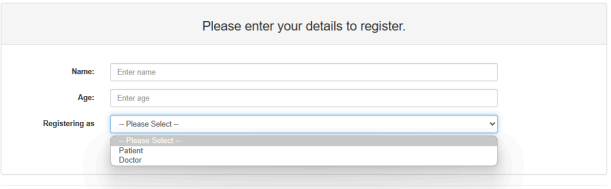


Fig 7. User Registration Page



VII. FUTURE WORK

There are great prospects to grow and enhance the healthcare data management system in the future. Investigating how artificial intelligence might assist in forecasting health trends and offering individualized treatment regimens is one direction for future research. This has the potential to completely change the way we provide patient care by making it more proactive and individualized. We may also concentrate on improving the system's interoperability with other medical technology, such as wearables, which could offer real-time health data for improved monitoring and decision-making. Finally, in order to improve the security and effectiveness of the system and guarantee that patient data is kept safe and available, we might look into recent advancements in blockchain technology. The efficacy and accessibility of healthcare services could be significantly impacted by these next initiatives.

Future research will also look into improving accessibility and user experience. The need to improve the accessibility and usability of healthcare systems is becoming more pressing as technology advances. To better understand the requirements and preferences of various user groups, including as patients, healthcare professionals, and administrators, future development may involve performing user studies. These findings could be used to improve data visualization, simplify navigation, and increase general usability in user interface designs. Furthermore, it should be a top priority to guarantee accessibility for people with disabilities by integrating features like screen reader compatibility and alternate input ways into the system. Future versions of the healthcare data management system can enable users to better utilize its potential by emphasizing accessibility and user experience.

References

[A] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In EUROCRYPT 2005, pp. 412-428. Springer, Berlin, Heidelberg, 2005.

[B] Beguelin, Jean-Luc, Jean-Marc Robert, and Michel Yung. "Filtered-IBE: Efficient revocation in identity-based encryption." In International Conference on Cryptology and Information Security in Latin America, pp. 107-120. Springer, Berlin, Heidelberg, 2007.

[C] Azab, Mohamed, et al. "Blockchain-based access control for secure e-health records." Journal of Medical Systems 43.2 (2019): 29.

[D] Yu, Yu, et al. "Federated access control for healthcare data in cloud computing." IEEE Transactions on Information Technology in Biomedicine 17.8 (2013): 1714-1723.

[E] Sandhu, Ravi S., Edward J. Coyne, and Haleh Nissenbaum. "Federated access control using role-based access control (RBAC)." In Proceedings of the National Computer Security Conference, vol. 95, pp. 169-180. 1995.

[F] Sandhu, Ravi S., and Qi Li. "Role-based access control models." IEEE Computer 39.9 (2006): 34-40.

[G] Ienca, Maria Alexandra, et al. "Patient-centric access control in healthcare information systems: A systematic review." Journal of biomedical informatics 49 (2014): 124-133.

[H] Amit, and Brent Waters. "Fuzzy identity-based encryption." In EUROCRYPT 2005, pp. 412-428. Springer, Berlin, Heidelberg, 2005.

[I] Gentry, Craig. "Computing arbitrary functions of encrypted data." In Communications of the ACM, vol. 51, no. 12, pp. 39-47. ACM, 2008.

[J] Goldreich, Oded, Silvio Micali, and Ronald L. Rivest. "A digital signature scheme secure against adaptive chosen-message attacks." SIAM Journal on Computing 17.2 (1988): 285-308.