IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134170

ELECTRONIC HEALTH REPORT SYSTEM USING BLOCKCHAIN TECHNOLOGY

Ms. Manjula K,A R Amrutha,Satvik B Metri,G R Aishwarya

Assistant Professor,Department of Computer Science & Engineering (CSE),

Ballari Institute of Technology and Management,Ballari, India

8th Semester Bachelor of Engineering (CSE),Department of Computer Science & Engineering (CSE),Ballari Institute of Technology and Management,Ballari, India

Abstract: The healthcare industry has witnessed a rapid transformation in last few years, with the digitalization of patient health records playing a pivotal role. Electronic Health Records (EHRs) have become the standard for storing and managing patient information, offering convenience and accuracy in healthcare delivery. However, concerns regarding the integrity of EHRs persist. To tackle these issues, this project implements blockchain-based system for the private management of electronic health reports. This project will involve the enhancement of a blockchain network, a user-friendly front-end application for medical care providers and patients, and integration with EHRs.

Keywords: blockchain technology, health report, electronic health report, EHR.

I. INTRODUCTION

The advancement of Information tech within the healthcare field has brought forth a integration of electronic data systems, including diagnostic reports, and medical images. This surge in data availability holds immense potential for predicting and managing infectious diseases, bolstering defense preparedness, and serving as crucial evidence in medical disputes. However, alongside these opportunities come significant challenges concerning patient privacy.

Addressing the above challenges needs immediate attention to develop robust solutions for managing access rights while ensuring the assured future of medical data. One proposed solution entails the combination of attribute-based encryption (ABE) and block-chain technology within the Inter Planetary File System (IPFS) storage environment. By leveraging ABE to encrypt medical data based on specific attributes and utilizing the distributed storage capabilities of IPFS, this system targets to provide secure content storage, verifiable keyword search functionalities, and robust access control mechanisms. Additionally, this technology in recording and verifying the entire data access and manipulation process offers an immutable ledger for tracking medical data interactions, thereby enhancing transparency and accountability.

Furthermore, the enhancement of healthcare through the combining of medical devices, sensors, cloud computing, and the IoT has made way to the the adoption of EHRs. However, safeguarding the solidness of EHRs, especially during data-sharing processes involving semi-trusted cloud servers, necessitates the deployment of advanced cryptographic techniques like CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and block-chain technology.

Moreover, the positive growth in healthcare data generation and distribution has prompted exploration into blockchain technology as a means to facilitate secure data transfer. With the advent of remote health monitoring and the proliferation of IoT (internet of things) devices, ensuring the safe storage of medical data has come out as a crucial priority. A view of literature in this area underscores, emphasizing its potential benefits and associated challenges. The decentralized, transparent, and programmable nature of this technology positions it as a promising technology for safeguarding the solidness of health data.

In conclusion, the versatile combining of blockchain technology into various sectors of the healthcare industry underscores its revolutionary potential in providing secure, efficient, and transparent solutions for managing and sharing medical information.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134170

II. LITERATURE REVIEW

The accelerated development of the IoT (internet of things) has gained more attention to the safety of personal data, making electronic health reports (EHR) a key element of modern medical services [2]. However, EHRs, considered a powerful tool to enhance the quality of medical services and accelerate biomedical discoveries, struggle with confidentiality problems inherent in their information systems. In EHRs, current storage methods have a low level of security, making them vulnerable to potential data leaks [2].

The growth of cloud technology has greatly improved EHR storage methods, but they still are challenged by security issues, especially with cloud service providers. Various attribute-based encryption (ABE) schemes have been proposed to address these issues, including encryption-based attribute-based encryption (CP-ABE), fine-grained flexible access control, and secure attribute-based signatures [2]. The purpose of these technology is to make sure that EHRs are encrypted, allowing only users with certain qualities to decrypt.[2].

[4] Governments in some countries, including Chile, Germany, and the UK, to issue immunity certificates via blockchain networks to people who recovered from corona virus so they can return to work and school. This approach explains the confounds of faking and engaging in social activities [4]. Blockchain networks play a vital role in securely storing and authenticating information related to COVID-19 through distributed ledgers and smart contracts. Biometric authentication and contact tracing are facilitated by smart devices connected to blockchain networks, which improve privacy and help detect potential exposure to a virus [4].

Along with government initiatives, private blockchains have found applications in healthcare information management. Platforms like BlocHIE use loosely coupled chains for electronic medical records (EMR) and personal health records (PHD) that use transaction compression algorithms to improve fairness and eliminate retention issues. It ensures secure data storage in health sector of the system [4]. Combining blockchain and cloud storage offers a promising opportunity to address issues regarding the information security, patient access, and efficiency of information sharing in healthcare systems [4].

In summary, the evolving healthcare landscape requires innovative solutions to meet the targets and effective data sharing. EHRs are a critical component of modern medical services and require sophisticated cryptographic mechanisms, including attribute-based encryption systems, to ensure secure access and prevent unauthorized disclosure [2]. [4].These advances underscore the transformative potential of emerging technologies to shape the future of healthcare by providing solutions that maintains patient data privacy, security, and effective information exchange.

III. PROPOSED SYSTEM

Enhancing Healthcare Information Security with Advanced Blockchain Technologies

Amid mounting concerns surrounding the security of healthcare data, our proposed system offers innovative solutions to fortify patient data protection. We employ a strategic amalgamation of cutting-edge technologies, including private blockchain implementation, interoperability-driven consensus algorithms, and multi-factor authentication.

1. Private Blockchain Implementation:
Our primary objective is to present a secluded enclave for health information within a private blockchain network. This implementation guarantees stringent control over data access, permitting entry solely to authorized individuals. By utilizing a centrally stored private blockchain, we mitigate potential security risks associated with broader data dissemination.

2. Interoperability-Focused Consensus Algorithm:
Our proposed consensus algorithm is designed to enhance the transactional efficiency of healthcare applications by prioritizing interoperability among participants. Operating on a three-tier architecture, comprising an online platform for patient communication, a cloud-based middleware for data management, and a blockchain management node. By segmenting blockchain functionality into distinct layers, we aim to streamline data flow and provide seamless interoperability across the healthcare ecosystem.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

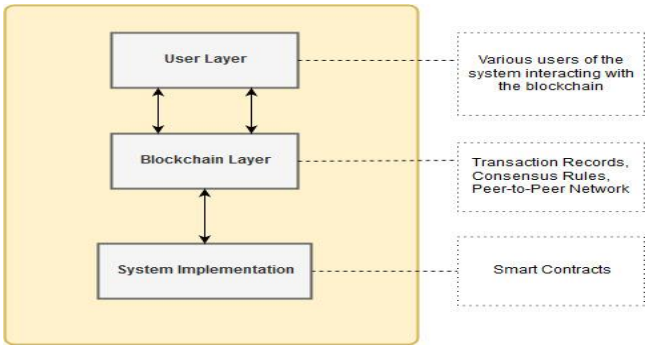
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134170

3. Multi-Factor Authentication:
To bolster participant authentication of fraudulent activity, our system incorporates multi-factor authentication measures. This ensures that any additions to blockchain data necessitate authentication by a majority (51%) of participants. Through the execution of robust user control mechanisms, our system guards against potential fraudulent activities and upholds the confidentiality of health data.

In summary, our comprehensive system endeavors to establish a flexible and privacy-centric information management environment. By utilising the plus points of private blockchain technology, cloud storage infrastructure, interoperability-driven consensus algorithms, and multi-factor authentication, we aim to address existing vulnerabilities and elevate security standards within healthcare information systems. This approach secures sensitive patient data and facilitates efficient and secure data exchange throughout the healthcare landscape.

IV. SYSTEM ARCHITECTURE



In the above figure, the framework or system has three modules.

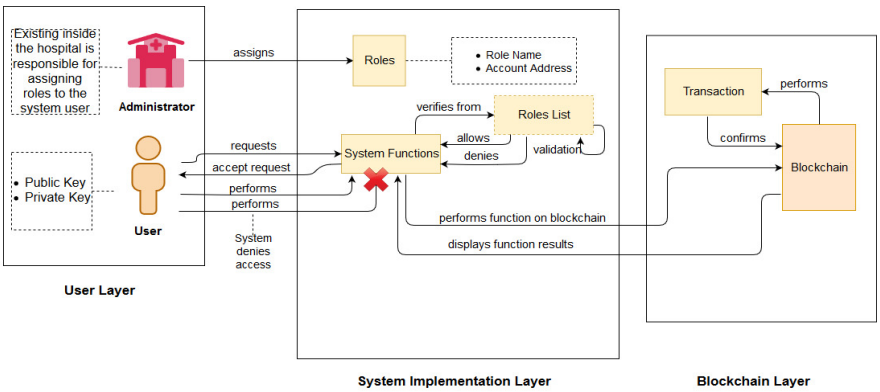
1. USER LAYER
A user is defined as an individual who makes efficient use of system and its resources. A user has multiple roles and use cases on the system, making them identifiable on the system. The users of this system could be patients or doctors.

2. BLOCKCHAIN LAYER
It contains the code for the communication of the user with the DApp which is working on the block-chain. The layer contains 3 elements in it. They are:

- Blockchain Assets
- Governance Rules
- Network

3. SYSTEM IMPLEMENTATION
As previously explained, the system was deployed by using Ethereum and its dependencies.

V. IMPLEMENTATION OF MODULES



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134170

VI. FEASIBILITY STUDY

Feasibility Study:

1. Technical Feasibility:
This technology is technically feasible for implementation in healthcare systems. There are existing frameworks and platforms tailored for healthcare data management using blockchain.
The integration of attribute-based encryption, blockchain, and IPFS storage is technically viable, as demonstrated by various proof-of-concept implementations and pilot projects in the healthcare system.
However, technical challenges may include scalability issues, interoperability with existing healthcare IT infrastructure, and ensuring data integrity and privacy in a distributed environment.

2. Financial Feasibility:
Initial investment for developing and deploying the proposed system, including software development, hardware infrastructure, and personnel training, can be substantial.
However, long-term cost savings can be realized through enhanced security, reduced administrative overhead, and streamlined data exchange processes.

3. Legal and Regulatory Feasibility:
Legal considerations regarding patient consent, data ownership, and liability in data breaches or disputes must be addressed.

4. Operational Feasibility:
User acceptance and adoption of the blockchain-based system among healthcare professionals, administrators, and patients are critical for its success.
Training programs and user-friendly interfaces should be provided to facilitate a smooth transition and utilization of the new system.

VII. CONCLUSION

The blockchain technology into healthcare systems presents a robust solution to critical challenges concerning data privacy and efficient data exchange. This proposal introduces a comprehensive encryption system that combines attribute-based encryption, blockchain technology, and IPFS storage to ensure protected storage and controlled access to electronic medical records (EMRs). While there may be perceived shortcomings such as access rights management and data timeliness, future enhancements, including attribute recall mechanisms and smart contracts, are poised to bolster the system's efficacy.

The transformative impression of blockchain on health information management is profound. Historically, healthcare applications have grappled with various security threats, but blockchain, along with innovative security methodologies, has majorly improved data security against breaches, theft, and tampering.

Furthermore, the significance of electronic health records (EHR) sharing systems in advancing accurate and comprehensive patient care cannot be overstated. The given system adopts a hybrid approach, leveraging both on-chain and off-chain platforms to ensure data authenticity and integrity. Incorporating a multi-keyword searchable cryptosystem bolsters efficiency, while an enhanced “Practical Byzantine Fault Tolerance” consensus algorithm adeptly handles Byzantine failures of nodes. Additionally, ongoing research into advanced cryptographic techniques, including proof-of-null and homomorphic encryption, ensures for further improvements in patient identity protection and EHR privacy. In essence, the overarching impact lies in its capacity to augment security, enhance information exchange, and revolutionize conventional healthcare applications.

REFERENCES

[1] Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access, 8, 59389-59401.
[2] Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. IEEE Access, 10,87803-87815.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134170

[3] Kassab, M., DeFranco, J., Malas, T., Laplante, P. Destefanis, G.& Neto, V. V. G. (2019). Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing, 9(4), 1835-1852.

[4] Kaur, M., Murtaza, M., & Habbal, M. (2020, November). Post study of Blockchain in a smart health environment. In 2020 5th International Conference on Innovative Technologies in Intelligence Systems and Industrial Applications (CITISIA) (pp. 1-4). IEEE.