International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390250

Healthcare Data Management System Using Blockchain

Prerna Rajeev Ranjan, Anand Sagar Yadav, Aanchal Ramkaran Verma, Aabha Patil, Devanand Parmanand Gupta

Department of Computer Engineering, Shree LR Tiwari College of Engineering, Mumbai, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 01 April 2023
Published: 15 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
382-387

ABSTRACT

The healthcare industry generates vast amounts of data that must be managed and stored securely. Blockchain technology has the potential to revolutionize healthcare data management by providing a secure, decentralized, and tamper-proof way to store and share data. Today's medical data management systems require data transparency, traceability, Immutability, auditing, lineage, flexible access, trust, privacy, and security. Also, most of the existing Healthcare systems used to manage data are centralized and pose potential risks in the event of a single point of failure Natural disaster. Blockchain is an emerging and disruptive decentralized technology that has the potential to become an important technology. This research will show you the use of blockchain for medical data management systems can stimulate innovation and make great strides in improvement. It also describes the key benefits of hiring Opportunities in blockchain technology and the healthcare industry. The purpose of this research is to explore the implementation of blockchain technology in health data management and identify related challenges.

Keywords— Peer-to-Peer, Trustworthy, Decentralization

I. INTRODUCTION

Several hospitals and clinics are providing healthcare services due to the increasing specialty in healthcare services and the mobility of patients. Doctors who have accurate information about a patient's medical history can make a precise decision regarding the patient's medical condition and treatment. It is a major problem for healthcare services now to share clinical data with other hospitals while maintaining patient confidentiality, data integrity, and patient privacy.

An electronic platform known as an electronic health record (EHR) is used to maintain a patient's medical data, including their diagnoses, treatment plans, allergies, lab results, and medical history. Healthcare professionals from different hospitals, clinics, and other medical facilities can access it as an electronic version of a patient's medical records. EHR use has grown in popularity in recent years since it provides a more effective and practical means of exchanging patient medical records. EHRs give healthcare professionals quick and simple access to a patient's

medical history as opposed to depending on paper-based data. No matter where they receive treatment, patients will always receive the best care thanks to this. The Electronic Medical Record (EMR), which includes comprehensive data about a patient's health status, is one of the most important elements of an EHR. This includes details regarding their medical conditions, diagnosis, prognoses, and tests. EMRs are essential in ensuring that healthcare professionals have access to the most recent medical data about a patient, which can enhance the caliber of treatment given.

Human resources (HR) can be utilized in machine learning and data analysis. Electronic health records (EHRs) use healthcare IT standards such as Fast Healthcare Interoperability Resources (FHIR)and Health Level 7 (HL7) to transfer clinical data between different healthcare providers. There are three models for sharing medical data between healthcare providers: push, pull, and view.

In the push model, medical information is sent from one healthcare provider to another, and only the sender and receiver can access the information. A protected email standard called Direct is used for encrypted transfer between sender and receiver. However, there is no guarantee of data integrity from creation to use, and there is no standard audit trail.
In the pull model, one healthcare provider can query medical information from another healthcare provider. In the view model, one healthcare organization can view a patient's medical data from another healthcare organization's record.

II. PROBLEM STATEMENT

“In the current era, the maintenance of each healthcare document can be challenging and sometimes it gets lost, which leads to the issue of losing valuable documents. However, developing a web application for storing important documents of people required for healthcare use for easy and efficient access and secure storage using blockchain technology can lead to a great solution.”

Systems for the storage and exchange of medical data are essential. Sharing personal information among numerous individuals across unsafe channels, however, can result in the leakage of crucial data. Additionally, the absence of client control over their personal information has negative effects, such as unauthorized identities having access to or the ability to modify their sensitive medical information. Furthermore, there may be even greater hazards when exchanging patient information. Blockchain for healthcare can ensure the security of the personal and medical information of the patients and can make sure that only authorized identities can access/edit the data using smart contracts which enable specific features among various identities in the system.

Therefore, there is a clear need for a distributed way of sharing and storing data where patients are more sure about their data security and privacy, and in addition, all the involved identities can see the holistic view of overall transactions and interactions.

III. LITERATURE REVIEW

Several works have been done in the field of Blockchain for Healthcare Data Management System:
Ibrar Yaqoob
1
Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, "Blockchain for Health Data Management: Opportunities, Challenges, and Future Directions" [1] proposes a comprehensive overview of blockchain technology and its potential applications in healthcare data management. It discusses the opportunities that blockchain offers, such as improved data interoperability, enhanced data security and privacy, and increased patient empowerment. It also highlights the challenges and limitations of implementing blockchain in healthcare,

including scalability, regulatory concerns, and technical complexities.

Jingwei Liu, Xiaolu Li, Lin Ye, Hongli Zhang, Xiaojiang Du, Mohsen Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records" [2] have proposed that blockchain based privacy-preserving data sharing for EMRs, called BPDS. In BPDS, the original EMRs are stored securely in the cloud and the indexes are reserved in a tamper-proof consortium blockchain. By this means, the risk of the medical data leakage could be greatly reduced, and at the same time, the indexes in blockchain ensure that the EMRs cannot be modified arbitrarily. Secure data sharing can be accomplished automatically according to the predefined access permissions of patients through the smart contracts of blockchain.

Chitra Karunakaran, Kavitha Ganesh, Sonya Ansar, and Rohitha Subramani, "A Privacy Preserving Framework for Health Records using Blockchain" [3] proposed that a privacy-preserving framework for electronic health records using blockchain technology is implemented to address these issues. The patient has complete control over the EHR, and the patient can share their health records with doctors of various medical institutions. The privacy and security of the patient's EHR are guaranteed by the verifiability and immutability property of the blockchain technology. The doctor uploads the EHR, and it is encrypted using the SHA256 hashing algorithm and stored as a separate block. The patient shares the EHR with the doctor of any medical institution through the unique key shared via the doctor's email. The doctor can access and update the EHR using the shared key. The block validation is done using Delegated Proof of Stake (DPoS) consensus algorithm, which guarantees the privacy of the patient's data.

Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid [4] suggest that a new architecture that takes advantage of decentralized databases to avoid centralized storage issues. The decentralized used database for storing patient electronic health records is the OrbitDB with Interplanetary File System (IPFS). Besides, we have deployed a blockchain network built on Hyperledger fabric by using Hyperledger composer to save hashes of stored data and control access when retrieving it. The proposed Blockchain-based architecture is designed to contribute to the healthcare management systems' robustness and to avoid recorded security limitations in commonly used systems for smart healthcare.

IV. METHODOLOGY

Healthcare data management system using blockchain technology involves utilizing the distributed, transparent, and secure nature of blockchain to manage sensitive healthcare data. Its development process include the following steps:

Following the identification of specific use case and the stakeholders who will be involved in the data management process, a suitable blockchain platform is chosen, considering factors such as scalability, security, privacy and consensus mechanism.

Thereafter, a smart contract was created. Smart contracts are self-executing agreements with pre-defined rules, to govern the interactions and transactions on the blockchain. It can automate processes such as consent management, data sharing, and data access control. A web-application based interface was designed that allow stakeholders to interact with the blockchain-based system, such as patients, healthcare providers, and other relevant parties to manage data, view transactions, and provide consent.

After that, a blockchain network was set up and smart contracts were deployed on blockchain platform. Data ingestion and validation was done to ensure data accuracy, integrity and consistency. Blockchain's transparency and immutability was used to track and audit data transactions. Compliance was ensured with relevant healthcare regulations, such as HIPAA, GDPR, and other data protection laws. Henceforth,

testing and deployment was done to monitor its performance, security, and effectiveness.

Implementing healthcare data management using blockchain requires careful planning, design, and implementation to ensure the privacy, security, and integrity of sensitive healthcare data. Collaboration among stakeholders, compliance with regulations, and robust testing and maintenance are crucial for successful implementation.

V. IMPLEMENTATION

The Blockchain technology has the potential to revolutionize healthcare data management by providing a secure, transparent, and decentralized system for storing and sharing sensitive patient information.

1. Patient data creation:
Healthcare data, such as electronic health records (EHRs), are created when a patient visits a healthcare provider. This data can include patient demographics, medical history, diagnoses, treatments, and other relevant information.

2. Data encryption:
The patient data is encrypted to ensure its confidentiality and security. Encryption converts the data into a code that can only be accessed by authorized parties with the correct decryption key.

3. Data hashing:
The encrypted patient data is then hashed, which is a process that generates a fixed-size unique code (hash) that represents the data. Hashing ensures data integrity, as any changes to the data will result in a different hash.

4. Blockchain network setup:
A blockchain network is set up, which includes multiple nodes (computers) that participate in the network. These nodes validate and record transactions (in this case, patient data) on the blockchain.

5. Data transaction:
The hashed patient data is then sent as a transaction to the blockchain network. The transaction includes the hash of the patient data, a timestamp, and other relevant information.

6. Consensus mechanism:
The blockchain network uses a consensus mechanism, such as proof-of-work or proof-of-stake, to verify the transaction and ensure that all nodes agree on the validity of the transaction.

7. Block formation:
Once the transaction is verified, it is combined with other transactions into a block. The block is then added to the existing chain of blocks, creating an immutable record of transactions.

8. Data access and permissions:
Access to the patient data on the blockchain is controlled through smart contracts, which are self-executing contracts that define the rules and permissions for accessing the data. Patients and authorized healthcare providers can access the data based on their permissions.

9. Data auditing and traceability:
The blockchain provides transparency and traceability, allowing for auditing of patient data transactions. Any changes or updates to the data are recorded as new transactions on the blockchain, creating an audit trail of all activities related to the data.

10. Data privacy and security:
Blockchain technology provides enhanced data privacy and security through encryption, hashing, consensus mechanisms, and smart contracts. This

ensures that patient data is secure, tamper-proof, and only accessible to authorized parties.

VI. CONCLUSION AND FUTURE WORK

In conclusion, the integration of blockchain technology in healthcare data management has the potential to bring about transformative changes. With its enhanced security, interoperability, consent management, streamlined data exchange, research capabilities, trust, transparency, and compliance with data regulations, blockchain can address many of the challenges associated with managing healthcare data. By providing a decentralized, transparent, and secure framework for data management, blockchain can facilitate efficient and secure data sharing, promote patient privacy and consent, accelerate research, and ultimately improve patient care and outcomes.

However, it is important to acknowledge that implementing blockchain in healthcare data management requires careful planning, consideration of regulatory requirements, and addressing technical, organizational, and ethical challenges. Blockchain is not a one-size-fits-all solution, and its adoption should be evaluated based on the specific needs, requirements, and context of each healthcare organization or system.

There are several areas of future work and potential developments for healthcare data management using blockchain technology. Some of the key areas include:

- Scalability and Performance: Further research and development efforts can focus on improving the scalability and performance of blockchain networks for handling large volumes of healthcare data. This can involve exploring new consensus mechanisms, data compression techniques, and optimization strategies to enhance transaction speed, data storage capacity, and overall system performance.
- Patient Identity Management: Blockchain can provide a secure and decentralized way of managing patient identities, ensuring accurate patient identification, and reducing medical errors. This can enhance patient safety and improve care quality.
- Disaster Recovery and Health Information Exchange: Blockchain can provide a resilient and decentralized infrastructure for disaster recovery and health information exchange during emergencies or natural disasters. This can ensure continuity of care and enable rapid response in crisis situations.
- Personalized Medicine: Blockchain can enable secure and transparent sharing of genomic data for personalized medicine applications, such as precision diagnostics and targeted therapies. This can accelerate research, enable personalized treatment plans, and improve patient outcomes.

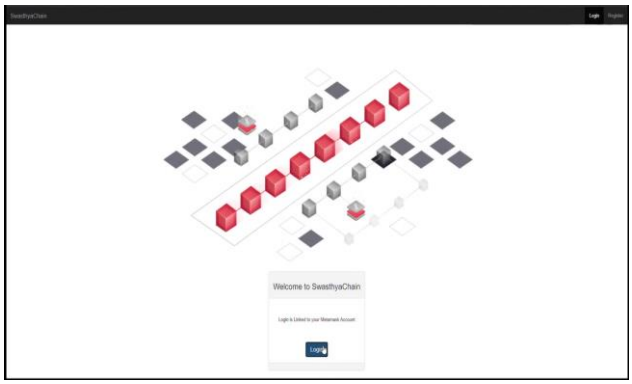

Figure 1: Front-End UI

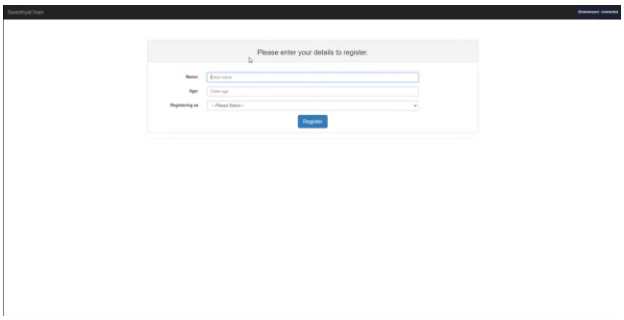

Figure 2: Register

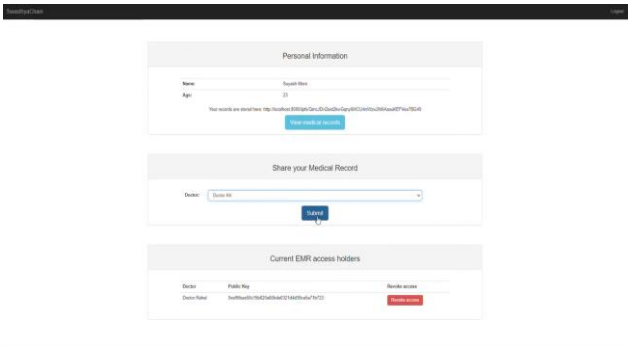

Figure 2: Patient Dashboard

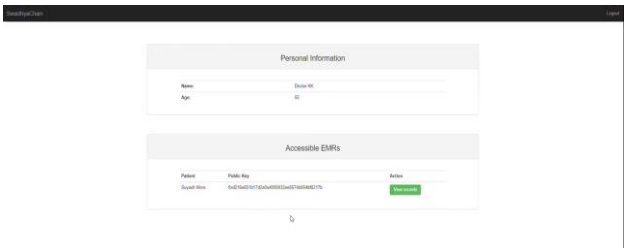

Figure 2: Doctor Dashboard

VII. REFERENCES

[1]. S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri Blockchain technology in healthcare: a comprehensive review and directions for future research.

[2]. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila Blockchain utilization in healthcare: key requirements and challenges 2018 IEEE 20th International Conference on E-Health Networking, Applications, and Services (Healthcom), IEEE (2018 Sep 17)

[3]. Khatoon A (2020) A blockchain-based smart contract system for healthcare management.

[4]. Jamil F, Hang L, Kim KH, Kim DH (2019) A novel medical blockchain model for drug supply chain integrity management in a smart hospital.

[5]. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila. "Blockchain Utilization in Healthcare: Key Requirements and Challenges." In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). 2018.

[6]. Roman Beck. "Beyond Bitcoin: The Rise of Blockchain World." In: Computer 51 (Feb. 2018), pp. 54–58.

[7]. Neeraj Kumar Muhammad Khurram Khan Shuyun Shi Debiao He and Kim-Kwang Raymond Choof. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." In: NCBI. 2020.

[8]. Mazlan AA, Daud SM, Sam SM, Abas H, Rasid SZA, Yusof MF (2020) Scalability challenges in healthcare blockchain system—a systematic review. IEEE Access 8:23663–23673.

[9]. Florian, G. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis. In Proceedings of the Hawaii International Conference on System Sciences, Puako, HI, USA, 4–7 January 2017.

Cite this article as :

Prerna Rajeev Ranjan, Anand Sagar Yadav, Aanchal Ramkaran Verma, Aabha Patil, Devanand Parmanand Gupta, "Healthcare Data Management System Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.382-387, March-April-2023. Available at doi : https://doi.org/10.32628/CSEIT2390250
Journal URL : https://ijsrcseit.com/CSEIT2390250