International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 12 | December - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A REVIEW: AN ENHANCED E-HEALTH SYSTEM USING PERMISSIONED BLOCKCHAIN-BASED IDENTITY MANAGEMENT AND USER AUTHENTICATION SCHEME

Prof. Sangeeta Alagi, Sakshi Gawali, Sanjana Godse, Aakanksha Kate, Bhagyashree Jadhav, Nikita Dhanage

Genba Sopanrao Moze College of Engineering, Savitribai Phule Pune University, Pune, India

Abstract

The health problems of this world's population are universal. Everyone nowadays values protecting their personal health information. No one likes to let people in on their vulnerabilities. Electronic Health Records (EHR) were developed as a solution to this issue. However, several writers have pointed out that there are drawbacks with EHR, including as costs, data loss, security threats, and others. In this study, we will explore how blockchain may replace EHR and other healthcare record keeping methods. Blockchain is a distributed ledger that records and verifies all transactions via the use of hash values and referencing of prior blocks. Since blockchain is becoming more popular in the medical industry. Blockchain ensures the confidentiality, availability, auditability, and manageability of health records conveniently.

Keyword Blockchain, Smart contracts, PHR (Personal Health Records), healthcare, access control.

Introduction

Cloud computing or fog networking, also known as fogging, and is pushing frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge. A blockchain system can be considered as a virtually incorruptible cryptographic database where critical medical information could be recorded. The system is maintained by a network of computers, which is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has still privacy issue since all transactions are exposed to the public, even though it is tamper-proof in the sense of data-integrity. The access control of heterogeneous patients' healthcare records across multiple health institutions and devices needed to be carefully designed. Blockchain itself is not designed as the large-scale storage system. In the context healthcare, a decentralized storage solution would greatly complement the weakness of blockchain in the perspective. Focuses on the applicability of Blockchain technology in healthcare. A network topology inference method has been proposed along with a proof of concept in real network. Blockchain might replace conventional methods of keeping track of valuable information such as contracts, intellectual-property rights, and corporate accountings. A blockchain system can be considered a virtually incorruptible cryptographic database where critical medical information can be recorded. The blockchain network as a decentralized system is more resilient in that there is no single point attack or failure compare to centralized systems. Personal Health Records (PHRs) have played a key role in enabling safer, more efficient, and consumer-driven health-care systems. Personal Health Records (PHRs) are valuable assets to individuals because they enable them to integrate and manage their medical data. A PHR is an electronic application through which patients can manage their health information.

Literature Review

Patients have authority over their medical records thanks to blockchain [1]. Smart contracts based on the Ethereum blockchain allow patients control over their data in a decentralized, immutable, transparent, traceable, trustworthy, and safe way. To securely collect, store, and exchange patients' medical data, the proposed solution uses decentralized storage of Interplanetary File Systems (IPFS) and trusted reputation-based re-encryption oracles. Algorithms are presented together with complete implementation information. We assess the suggested smart contracts based on two key performance indicators: cost and accuracy. We also explore the generalisation elements of our technique and give security analysis. The suggested approach's drawbacks are outlined. On Github, we make the smart contract source code openly accessible.

IPFS [2] provides a blockchain-based secure storage and access solution for electronic medical data. We built an attribute-based encryption scheme for safe storage and efficient exchange of electronic medical records in IPFS storage environment based on the ciphertext policy attribute-based encryption system and IPFS storage environment, paired with blockchain technology. Our method is based on ciphertext policy attribute encryption, which effectively regulates access to electronic medical data while maintaining retrieval efficiency. Meanwhile, we store encrypted electronic medical data in the decentralized Interplanetary File System (IPFS), which not only provides storage platform security but also eliminates the single point of failure concern. Furthermore, we use blockchain technology's non-tampering and traceable characteristics to

enable safe storage and search for medical data. Our approach delivers selective security for pick keyword assaults, according to the security proof. Our approach is efficient and viable, according to performance analysis and actual data set simulation studies.

Blockchain technology is being used to handle health records [3]. a patient-centered, entirely decentralized strategy that can detect data theft, prevent data modification, and gives patients control over access. Blockchain technology is the most effective way to solve all issues and meet all demands. As a decentralized and distributed ledger, blockchain has the potential to affect billing, record sharing, medical research, identity theft, and financial data crimes in the future. Smart contracts in health care may help to simplify things even further. On the Blockchain, invocation, record generation, and validation will all take place. on a patient-driven model of record maintenance based on Blockchain technology, with smart contracts to be added in the future, allowing for more data sharing possibilities. Finding its vast reach, I hope that additional study will be conducted and actual applications will be realized.

A medical data exchange and protection method based on blockchain[4]. To enhance the hospital's electronic health system, a medical data exchange and protection strategy based on the hospital's private blockchain was developed. For starters, the system may meet a variety of security requirements, including decentralization, openness, and tamper resistance. Doctors will be able to retain medical data or retrieve patient history data via a secure approach that respects their privacy. A symptom-matching technique is also provided between patients. It enables patients who have the same symptoms to complete mutual authentication and generate a session key for future disease communication. PBC and OpenSSL libraries are used to implement the suggested approach.

Healthy Block is a blockchain-based IT architecture for electronic medical records that is resistant to network outages. [5]. a patient, posing a direct danger to the person and resulting in large public health expenses for governments. The creation of electronic medical record (EMR) systems using blockchain networks is one of the proposed solutions to this problem; however, most of them fail to account for the occurrence of connectivity failures, such as those found in various developing countries, which can lead to data integrity failures. To address these issues, Healthy Block is described in this paper as a blockchain-based architecture that proposes a unified electronic medical record system that takes into account multiple clinical providers, has data integrity resilience during connectivity failure, and has usability, security, and privacy characteristics. A prototype for patient care in a network of hospitals was developed based on the Healthy Block architecture. The evaluation's findings revealed a high level of efficiency in maintaining patients' EMRs unified, updated, and secure, regardless of which network healthcare provider they contact.

[6] A blockchain-based personal health record sharing system with certified data integrity. A novel blockchain-based personal health record sharing system with certified data integrity. The new scheme uses searchable symmetric encryption and attribute-based encryption techniques to achieve privacy protection, keyword search, and fine-grained access control in the process of personal health record sharing, addressing the problems of privacy disclosure, limited keyword search ability, and loss of control rights. In comparison to other comparable methods, the new approach enables patients to give attribute private keys to users, eliminating many of the security issues that the scheme's attribute authority causes. Furthermore, the new scheme manages keys in the scheme using blockchain, reducing the single point of failure concern associated with centralized key management. The new technique, in particular, maintains the hash values of encrypted personal health information in blockchain and the corresponding index set in a smart contract, which may boost data integrity verification efficiency even further.

An efficient consortium blockchain for the exchange of medical data [7]. a new business approach for exchanging medical data and a blockchain-based platform Our solution takes use of the benefits of blockchain in the recording and exchange of medical data. The distributed network's participants may store, exchange, and reliably verify information. A novel consensus method and a universal anonymous sharing mechanism are also proposed. These techniques improve the efficiency and security of medical data exchange among users. To avoid manipulation and fraud, both the information and the traces of the transaction may be maintained in a dispersed manner in this fashion.

For improved privacy, scalability, and availability, blockchain is being used to retain patient information in electronic health records [8]. consortium blockchain to create a distributed system using existing EHRs utilizing Hyper ledger Fabric. The address of a patient record in an EHR is recorded on the same ledger held by peer nodes. Individual patients are recognized by one-of-a-kind certificates issued by local certificate authorities who operate together in a network channel. When transferring data, we employ a proxy re-encryption mechanism to preserve a patient's privacy. We created and implemented a number of chain codes to handle business logic that was agreed upon by the network's member organizations.

In healthcare, a poll on blockchain-based self-sovereign patient identification [9]. Blockchain (BC)-based self-sovereignty and patient data records in healthcare are at the cutting edge. Our objective is to look into the possibilities of using BC technology in patient data and identity management. BC may be particularly advantageous as a distributed decentralized technology, providing patients ownership over their own data and self-sovereign identification. To the best of our knowledge, no literature exists that addresses the same issues. More particular, solutions aimed at realizing comprehensive BC-based Electronic Health Records (EHR) and Patient Health

Records are the emphasis (PHR). EHR and PHR are used to keep track of patient information such as doctor's notes and radiological pictures. As a result, they include crucial information on the patient's privacy and identity. As a result, in terms of architectural and technological framework, developing pure decentralized Healthcare Information Systems (HIS) is a significant problem. Designing a strong and dependable EHR and PHR, which serve as the basis for a variety of other healthcare services, requires carefully balancing a number of aspects, including decentralization, privacy, scalability, and data throughput.

Using blockchain to protect the privacy of electronic health records [10]. a way to use blockchain technology to build EHRs and make them more safe and private. Using cryptographic methods and decentralization, blockchain technology will maintain control over information access. It will also strike a balance between data security and data accessibility. This project's major goal is to frame data privacy and security challenges in electronic healthcare.

Table 1: Literature Review

Sr. No.	Name of Paper	Authors	Publication Name	Approaches
11.	"Using Blockchain for Electronic Health Records."	Ayesha Shahnaz 1 , Dr. Usman Qamar2 and Dr. Ayesha Khalid.	March 27 2021 IEEE	In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues.
12.	"eHealth Chain—a blockchain-based personal health information management system".	Pravin Pawar1 ·Neeraj Parolia2 · Sameer Shinde3 · Thierry Oscar Edoh 4 · Madhusudan Singh	March 5-7, 2021 IEEE	The Personal Health Information Management System (PHIMS) supports activities such as acquisition, storage, organization, integration, and privacysensitive retrieval of consumer's health information.
13.	"Research on the Application of Blockchain inSmart Healthcare: Constructing a Hierarchical Framework"	Xiamen Du , 1 Beibei Chen , 2 Ming Ma,2 and Yanjiao Zhang 3.	December 31 2020 IEEE	Constructed a development application system of smart healthcare under the blockchain based on stakeholder theory.
14.	"Application of Blockchain in the Hospital management system"	ZEQI leng.	July 3 2020 IEEE	Compared to existing systems, eHealth Chain provides complete control to the user in terms of personal health data acquisition, sharing, and self-management.

Existing Technology

Infrastructure (both technical and social) that enables data to move electronically between institutions. Depending on the system and health care settings, mobile devices like tablets and smartphones with handwriting capabilities may also be used to access and update patient records in an electronic medical record (EMR). Individual notes from an electronic medical record (EMR) might be linked to a

patient's private health record (PHR), making this information readily available to patients.

Limitations of Existing System

- There are significant differences in how each care environment operates. In the realm of electronic health records, it's challenging to create a "one-size-fits-all" solution.
- The possibility that electronic health records may one day be utilized longitudinally and linked across locations of treatment further complicates the challenges surrounding their long-term preservation. Multiple independent parties may generate, access, and make changes to records.
- Doctors, hospitals, insurance companies, and patients are all part of the healthcare ecosystem.
- Users' data may be compromised.

System Architecture

System must validate the previous block before commit block. User can access the data over the internet 24*7. If any block has changed by third party attacker or unauthorized user, it must show during transaction current blockchain is invalid. It can recover the invalid blockchain using other data nodes, with the help of majority of trustiness. The node or user who wants to initiate a transaction would record and broadcasts the data to the network. The node or user who receives the data verifies the authenticity of the data received in the network. Then the verified data is stored to a block. All nodes or users in the network validate the transaction by executing either the proof of work algorithm or the proof of stake algorithm to the block that needs validation. Consensus algorithm used by the network will store the data to the block that is added to blockchain. And all nodes in the network admit the respective block and extend the chain base on the block.

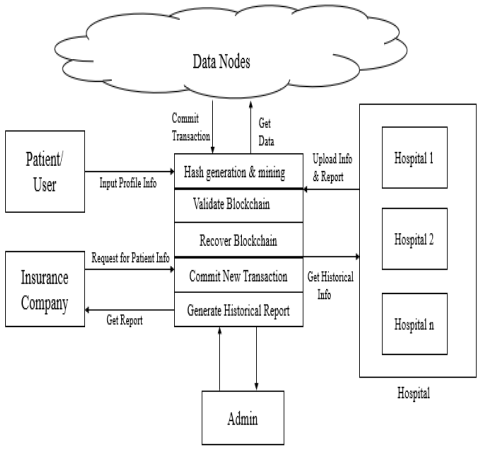

Figure 1: System Architecture

Methodology

The system contains following modules:
Hospital: An entity that communicates with the patient to generate a symmetric data to each medical record. An entity that requests medical record locally.
Patient: Patients are responsible for registering themselves into the system, deploying their uploading and submitting the medical records, and responding to data queries from doctors (requests to share medical records).
Insurance Company: Upload Policy details and show patient history.
Distributed Block chain: The Blockchain is the distributed ledger used to represent the current state of delegated access rights in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities

Conclusion

There are many research directions in applying Blockchain technology to the healthcare industry due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many healthcare use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating an interoperable ecosystem using the Blockchain technology while balancing critical security and confidentiality concerns in healthcare. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in healthcare is also needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility). In some cases, a new Blockchain network may be more suitable than the existing Blockchain; therefore, another direction may be investigating extensions of an existing Blockchain or creating a healthcare Blockchain that exclusively provides health-related services.

References

[1] Madine, Mohammad Moussa, et al. "Blockchain for giving patients control over their medical records." IEEE Access 8 (2020): 193102-193115.

[2]Sun, Jin, et al. "Blockchain-based secure storage and access scheme for electronic medical records in IPFS." IEEE Access 8 (2020): 59389-59401.

[3]Harshini, V. M., et al. "Health record management through blockchain technology." 2019 3rd International

Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019.

[4] Liu, Xiaoguang, et al. "A blockchain-based medical data sharing and protection scheme." *IEEE* Access 7 (2019): 118943-118953.

[5] Gutiérrez, Omar, et al. "Healthy Block: Blockchain-Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures." International Journal of Environmental Research and Public Health 17.19 (2020): 7132.

[6] Wang, Shangping, Dan Zhang, and Yaling Zhang. "Blockchain-based Personal Health Records sharing scheme with data integrity verifiable." *IEEE Access* 7 (2019): 102887-102901.

[7] Du, Mingxiao, et al. "An optimized consortium blockchain for medical information sharing." *IEEE Transactions on Engineering Management* (2020).

[8] Tith, Dara, et al. "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability." *Healthcare informatics research* 26.1 (2020): 3-12.

[9] Houtan, Bahar, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. "A survey on blockchain-based self-sovereign patient identity in healthcare." *IEEE Access* 8 (2020): 90478-90494.

[10] Sharma, Yogesh, and B. Balamurugan. "Preserving the privacy of electronic health records using blockchain." *Procedia Computer Science* 173 (2020): 171-180.

[11] J. S. Ancker, M. Silver, and R. Kaushal, “Rapid growth in use of Personal Health Records in newyork, 2020–2021,” J. Gen. Internal Med., vol. 29, no. 6, pp. 850–854, Jun. 2019.EHRs Have Made it Easy for Cardiologists to Treat Their Patients. Accessed: Jul. 8, 2020. [Online]. Available: http://tbrcinfo.blogspot.com/ 2018/12/ehrs-have-made-it-easy-for.html

[12] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, “Penetration testing framework for smart contract blockchain,” Peer-to-Peer Netw. Appl., pp. 1–16, Sep.2020, doi: 10.1007/s12083-020-00991-6.

[13] Y. Sharma and B. Balamurugan, “Preserving the privacy of electronic health records using blockchain,” Procedia Comput. Sci., vol. 173, pp. 171–180, Jan. 2020.

[14] M. Qazi, D. Kulkarni, and M. Nagori, “Proof of authenticity-based electronic medical records storage on blockchain,” in Smart Trends in Computing and Communications. Singapore: Springer,2019, pp. 297–306.