International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. 09 Issue 02 | 2025

Blockchain Enabled Secure Transactions of Electronic Health Records for Modern Healthcare

[1]Prof. M. S. Chinchamalatpure [2]S. B. Pundkar
Department of Computer Science & Engineering Dr. Sau. Kamaltai Gawai Institute of Engineering and Technology

DOI: 10.5281/zenodo.15422234

ABSTRACT

Health record maintenance and sharing are one of essential tasks in the healthcare system. In this system, loss of confidentiality leads to a passive impact on the security of health records, whereas loss of integrity can have a serious impact, such as loss of a patient's life. Therefore, it is of prime importance to secure electronic health records. In recent years, blockchain technology has been considered as adaptable compared to other techniques. But, in existing methods, when data is stored on outside servers, it might be stolen or legitimate. In addition, the trustworthiness of a storage server highly depends on a single server provider. In order to maintain access control and record transaction authentications without anonymous interruptions, the existing techniques have failed. In this research proposal, an effective secure blockchain technology-based homomorphic encryption technique is developed to address the health record information transaction between the patient, doctor, service providers, and institutions in a privacy-preserving way. In a secure manner, the patients can be enabled to control and share their health records in cloud storage without violating any privacy in healthcare. Moreover, the patient data is privately stored in intelligent health care systems that are effectively provided by the research study.

1. INTRODUCTION

Electronic Health Records (EHRs) contain sensitive patient information related to diagnosis and treatment, making their secure handling a critical concern. However, the existing healthcare data systems are fragmented, with inconsistent data standards and limited interoperability among institutions. Access to medical records is often restricted, and sharing beyond the originating institution is typically not allowed, leading to inefficiencies in care coordination and data usage.

Most medical data is stored centrally, making it vulnerable to threats such as data breaches, unauthorized access, and tampering. The current institution-centric model lacks mechanisms to ensure the integrity, reliability, and privacy of patient records. These challenges highlight the need for a more secure and transparent method for managing EHRs.

Blockchain technology offers a promising solution due to its decentralized, tamper-proof, and transparent nature. It enables secure data sharing across healthcare providers while allowing patients to retain control over their records. Unlike public blockchains, permissioned healthcare blockchains restrict access to authorized users only, ensuring data confidentiality and compliance.

This research proposes a blockchain-based system integrated with homomorphic encryption to enhance the privacy and security of EHRs. The system ensures data integrity, reduces computational overhead, and provides a scalable, distributed access control framework. By leveraging blockchain's strengths, this approach addresses critical challenges in health data management and improves patient care through secure and efficient information exchange.

2. LITERATURE REVIEW

In this section, the survey of recent techniques that are developed for secure healthcare record transaction using block chain technology. In addition, the advantages of the existing techniques with limitation are also presented.

A. D. Dwivedi et al. (2019) proposed a novel framework for modified blockchain models that are suitable for IoT devices, taking into account their distributed nature. This architecture addresses many security and privacy concerns while considering the resource constraints of IoT; however, it remains vulnerable to attacks such as modification, dropping, and denial of service (DoS). H. A. El Zouka and M. M. Hosni (2019) developed a lightweight authentication scheme for protecting personal health data and ensuring secure communication. While their scheme achieved fast key generation and reduced access time overhead, it was limited in managing vast amounts of data. A. Mubarakali et al. (2019) implemented the SEHRTB algorithm to enable secure health record transactions. This method allowed patients to control their data privately on the cloud but lacked the ability to measure the interest factor between patients and

insurance agents. C. Qu et al. (2018) designed a layered, self-organized Blockchain Structure (BCS) for device credibility verification, which improved storage and response times but failed to ensure node credibility if the Manage Server was attacked.

J. H. Ryu et al. (2019) used blockchain to enhance data integrity by storing all IoT communications as transactions, though it increased execution time and complexity due to IoT heterogeneity. P. Tasatanattakool and C. Techapanupreeda (2018) provided an overview of blockchain technology and bitcoin, discussing its healthcare challenges, but they didn't address how third-party stakeholders could access patient records without breaching privacy. S. Wang et al. (2018) proposed a Parallel Healthcare System (PHS) using ACP and a consortium blockchain for better scalability and integrity. However, despite its security, it lacked data recovery in case of system failure. L. A. Linn et al. (2016) developed a blockchain-based access control system to manage health records securely, yet it didn't address common data security threats.

G. G. Dagher et al. (2018) developed the Ancile framework to securely access medical records while preserving patient privacy. Although it tracked usage and allowed secure data transfer, its search efficiency declined as the system scaled. D. J. Skiba (2017) highlighted blockchain's importance in healthcare and education but failed to delve into its security for large-scale patient data. W. J. Gordon and Christian Catalini (2018) proposed a blockchain solution to facilitate secure health record transitions through mechanisms such as data liquidity and identity, although it didn't effectively minimize public data exposure. X. Yue et al. (2016) designed the Healthcare Data Gateway (HDG) based on blockchain, empowering patients to control and monitor data access. Despite its privacy advantages, HDG removed identifiable information for memory optimization, potentially losing data granularity.

I. Radanovic and Robert Likic (2018) examined the challenges of using blockchain in healthcare and its potential to support public health and personalized medicine, though it remains unfit for broad adoption. K. N. Griggs et al. (2018) used smart contracts for real-time analysis of medical sensors. While the method enhanced data reliability, key management became complex at scale, and delays limited emergency response use. S. Rathore et al. (2019) combined blockchain with a decentralized security architecture for software-defined networks, offering real-time threat detection. However, it added overhead on fog nodes. A. Dorri et al. (2019) introduced the Memory Optimized and Flexible Blockchain (MOF-BC), reducing memory use and supporting transaction removal, but processing overhead increased as blocks accumulated.

Q. Xia et al. (2017) built a blockchain-based framework for secure data sharing in the cloud, ensuring data access only after identity and key verification. R. Guo et al. (2018) proposed an Attribute-Based Signature Scheme with multiple authorities, which resisted collusion but lacked support for non-monotone predicates. A. Zhang and X. Lin (2018) developed the BSPP scheme for secure personal health information sharing, offering security and revocation controls, yet its performance depended on optimal keyword set size. Y. Chen et al. (2019) created a blockchain-cloud storage scheme for personal medical data that reduced device and backup costs but increased energy consumption.

G. Nagasubramanian et al. (2020) introduced a Keyless Signature Infrastructure using Blockchain (KSIBC), enhancing signature secrecy and authentication. Nonetheless, users had to pay fees to miners and providers. G. Rathee et al. (2019) designed a blockchain-based healthcare framework addressing multimedia data in IoT. While it traced communication anomalies, its transaction time and cost were high. L. Chen et al. (2019) proposed a searchable encryption scheme for EHRs using blockchain, offering index integrity and traceability, though search time increased with more transactions. A. Al Omar et al. (2019) created a privacy-preserving platform for healthcare data on the cloud, ensuring pseudonymity through encryption but lacking in interoperability and key management. E. Y. Daraghmi et al. (2019) implemented MedChain, using time-based smart contracts to manage EMRs securely. Although feature-rich, balancing on-chain and off-chain operations posed challenges. Lastly, A. Shahnaz et al. (2019) developed a blockchain system combining secure storage and granular access, using off-chain mechanisms to handle medical records, but the system lacked well-defined compliance policies.

2.1 Problem Definition

The current healthcare systems store Electronic Health Records (EHRs) in centralized databases that lack interoperability, making data sharing between institutions insecure and inefficient. These systems are vulnerable to data breaches, unauthorized access, and tampering. There is a need for a secure, decentralized solution that ensures data integrity, privacy, and patient control over health records. Blockchain technology offers a promising approach to address these challenges.

2.2 Objective of the Research Study

The objective of the research proposal is presented in the following statement:

Design an effective block-chain technology to support a general non-monotone predicate, which is used in many distributed system applications.

In order to minimize the energy consumption and high processing time, a privacy-preserving based blockchain technology must be designed and developed.
Develop an optimization based blockchain technology to reduce the queuing time for encryption and decryption phase.
In order to provide the data integrity and maintain access control for anonymous interruptions, a secure block chain algorithm is implemented.

2.3 Objective of the Research Study

The objective of the research proposal is presented in the following statement:
Design an effective block-chain technology to support a general non-monotone predicate, which is used in many distributed system applications.
In order to minimize the energy consumption and high processing time, a privacy-preserving based blockchain technology must be designed and developed.
Develop an optimization based blockchain technology to reduce the queuing time for encryption and decryption phase.
In order to provide the data integrity and maintain access control for anonymous interruptions, a secure block chain algorithm is implemented.

3. STRUCTURE OF BLOCKCHAIN

Blockchain technology was originally used as a decentralized and de-trusted infrastructure for encrypting digital currency. Blockchain is linked together by hash values on the block. This kind of chain structure is usually used to verify and store data. It can be said that blockchain uses distributed consensus algorithms to generate and update data, uses cryptography to ensure data transfer and access security, and uses smart contracts consisting of automated scripting code to program and operate data. The data in blockchain ledger has the characteristics of non-tampering and publicly verifiable. The blockchain can be classified as public blockchain, consortium blockchain and private blockchain. Public blockchain, just as its name implies, is public to all users in system. The data stored in ledger is visible to all nodes. The private blockchain is used only by private organizations. Similarly, the accounting, reading and writing permissions of the blockchain are specified by organization rules called as consortium blockchain. Figure 1 [23] shows the basic diagram of block chain technology.

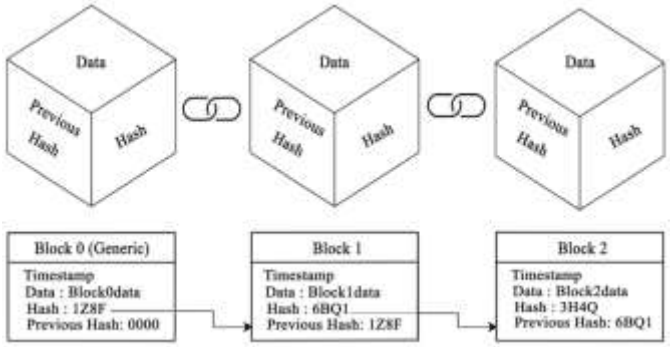

Figure 1: Structure of Block-chain

The first block is called generic block, and some extraordinary block in the network named miners try to solve a cryptographic puzzle named Proof of Works. Thus, participating nodes build a trusted network over untrusted participants in the network. New transactions are verified by all participating nodes that omit the necessity of the central dependency and propose a distributed management system. Each block contains the hash of its previous block which ensures the constancy of the transaction; thus, alternation of any block from the network is unattainable. If one transaction is valid, then the transaction is continuously stored in the public unchanging blockchain network that can be accessed by any node. All transactions among this network are signature using public-key cryptography; thus, their authenticity nature is accomplished. Therefore, this research work studied the public block-chain.

4. PROPOSED METHODOLOGY

The system architecture of the proposed healthcare framework is represented in the Figure 2 which requires a web-based application consisting of two ends such as front end that attaches with patients and back end which provides the internal communication using block chain. The particular request acts as a link among these ends. The proposed healthcare framework is understandable by presenting a web-based communication among the patients and vendors. During the execution of back end where block chain communication process occurs, there are the entities that linked together as a system of nodes.

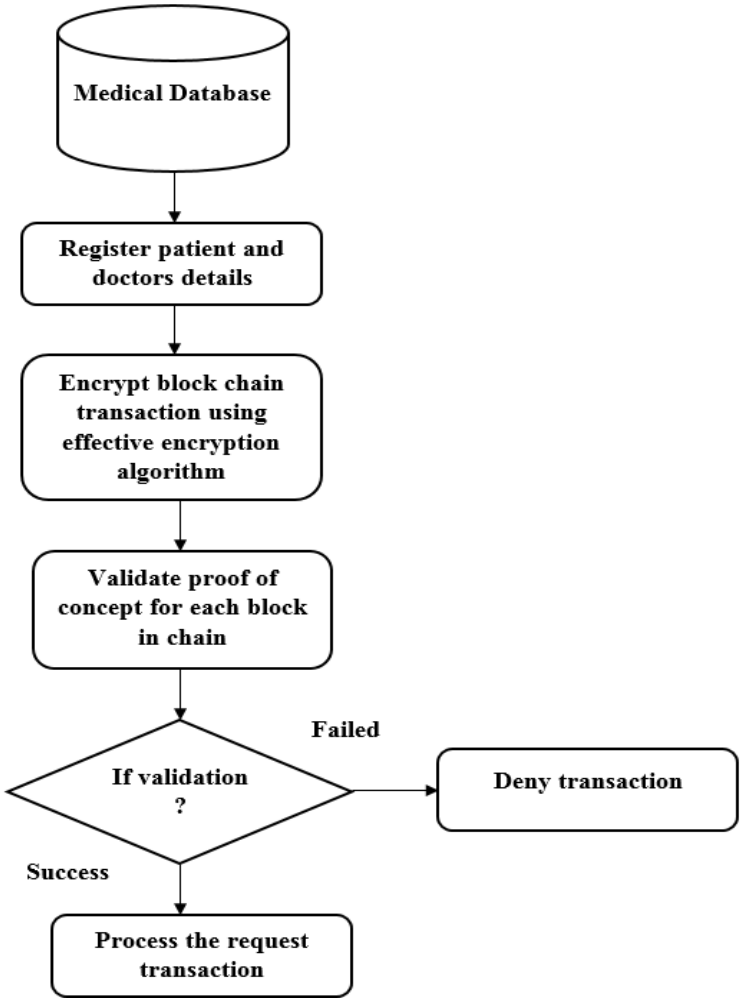

Figure 2: Block Diagram of Proposed Study

The medical database collected from standard database called University of California, Irvine (UCI) machine learning repository (https://archive.ics.uci.edu/ml/datasets.php). The next step is to register the patients and doctor details in a secure lightweight authentication and key agreement protocol. There are three phases presented in this proposed protocol such as registration phase, login phase and authentication phase.

4.1 Registration Phase

In this phase, the medical information of the patients including age, gender, general health, family history, and current sensors readings are assumed to be stored in a separate secure database. Only the authorized doctors and medical staff should be allowed to access these patients' medical information. Therefore, the basic purpose of this phase is to provide strong authentication between the patient and the provider within a strong policy framework. The patient will communicate with the provider through a fine-grained privacy and security protocol which will automatically provide both authentication and access control.

4.2 Login Phase

In this phase, the following calculations are made such as the patient/doctor chooses an identity and a private password. Then, an arbitrary random number is chosen by patient/doctor to calculate dynamic password. Then, the dynamic password is sent along with the patient/doctor to the cloud healthcare server through a secure channel. Then, the cloud server will query and update the table of the registered patients. The server will then calculate the one-time password (OTP) every time when it receives a registration request from a patient/doctor. Then, the server chooses a random number and computes a session key by using private encryption algorithm. Finally, the server stores all the patient/doctor information on a table, and sends the session key via a secure channel to the patient. When the session key is received by the patient/doctor, he will use that key to encrypt all communication transactions in the current network connection using a symmetric algorithm.

4.3 Authentication Phase

After the key agreement and login processes are completed, the patient/doctor and the server will be able to authenticate communications. The patient/doctor can change the dynamic password at any time if the session key and time stamp are all bundled in a request. The healthcare server will then be able to verify the new password by matching the authentication against the verification key. Otherwise, the connection is denied. If an intruder tries to impersonate a legal patient/doctor by copying some messages/transactions that are sent by the patient/doctor and resending them to the server in the same time, the applied timestamp along with the random number will prevent such an attack from happening

4.4 Encryption phase

In order to secure the healthcare blockchain process, the research proposal uses the fully homomorphic encryption algorithm [24]. There are two keys required for communication: one is a public key and the other is a private key. Furthermore, the crypto system is a one-way process, i.e., the public key is used only for encryption, and the private key is used only for decryption.

4.4.1 Key Generation

The process for generate the private key and public key, the following equation should be calculated,

$$\beta = r\, w_i \; mod \; q$$

where r is a random integer, such that gcd (r,q) = 1 (i.e. r and q are coprime)

To encrypt n-bit messages, $w = (w_1, w_2, \ldots . w_n)$ of n natural nonzero natural numbers and a random integer q,

$$q > \sum_{i=1}^{n} w_i$$

4.4.2 Encryption

The process of encrypting the public key, the following equation are calculated as,

To encrypt an n-bit message

$$\alpha = (\alpha_1, \alpha_2, \ldots . \alpha_n)$$

where α_i is the *i*-th bit of the message, $\alpha_i \in \{0,1\}$, calculate

$$c = \sum_{i=1}^{n} \alpha_i \beta_i$$

The ciphertext is then *c*.

4.4.3 Decryption

In order to decrypt a ciphertext *c* a receiver has to find the message. The following equations are calculated as,

$$c' = \sum_{i=1}^{n} \alpha_i w_i$$

After this process, the validation of each blockchain are carried out by Proof of Concept (POC) or Proof of Work. The POC steps include:

- Check whether the patient is valid or not.
- Check whether the doctor is valid to retrieve the patient data or not.
- Suppose, if the patient had guardian, whether he/she can able to access the sensitivity of patient's information.
- Check whether the lab technician's data are related to patient's lab report.

If the request transaction is successful, then that transaction are proceeded to further process. Otherwise, the transaction is denied.

5. SUMMARY

Data leakage in EHR could result in the compromise of patient privacy (e.g. health conditions). Generally, data in EHRs remain unchanged once they are uploaded to the system, and thus, blockchain based homomorphic encryption algorithm can be potentially used to facilitate the sharing of such data. Different participating medical organizations and individuals (e.g. medical practitioners, hospitals, medical labs and insurance companies) can then access EHRs stored on the blockchain with a higher level of confidence. The algorithm provides a proof-of-concept based framework, shows how standards of decentralization and could achieve security, interoperable health records frameworks. It accomplishes confidentiality and protection among the health record distribution.

6. REFERENCES

[1] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT". *Sensors*, vol. 19, no. 2, pp. 326, 2019.
[2] H. A. El Zouka, and M. M. Hosni. "Secure IoT communications for smart healthcare monitoring system." *Internet of Things*, pp. 100036, 2019.
[3] A. Mubarakali, S. C. Bose, K. Srinivasan, A. Elsir, and O. Elsier, "Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain". *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-9, 2019.
[4] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities". *Security and Communication Networks*, 2018.
[5] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A block chain-based decentralized efficient investigation framework for IoT digital forensics". *The Journal of Supercomputing*, pp. 1-16, 2019.
[6] P. Tasatanattakool, and C. Techapanupreeda. "Blockchain: Challenges and applications." *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2018.
[7] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, and F. Y. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach". *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942-950, 2018.
[8] L. A. Linn, and Martha B. Koo. "Blockchain for health data and its potential use in health it and health care related research." *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*. 2016.
[9] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology". *Sustainable cities and society*, vol. 39, pp. 283-297, 2018.
[10] D. J. Skiba, "The potential of Blockchain in education and health care." *Nursing education perspectives* vol. 38, no. 4, pp. 220-221, 2017.
[11] W. J. Gordon, and Christian Catalini. "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability." *Computational and structural biotechnology journal* vol. 16, pp. 224-230, 2018.
[12] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control". *Journal of medical systems*, vol. 40, no. 10, pp. 218, 2016.
[13] I. Radanovic, and Robert Likic. "Opportunities for use of blockchain technology in medicine." *Applied health economics and health policy* vol. 16, no. 5, pp. 583-590, 2018.