Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-B, pp. 1977–1988
DOI : 10.47974/JIOS-2289

An approach to secure medical data through blockchain technology

Ravi Saharan
Department of Computer Science and Engineering
Central University of Rajasthan
Ajmer 305817
Rajasthan
India

Abstract

As we know that healthcare contains sensitive information of human health history. Privacy and security are main concern. By internet enables sharing information of those record possible. It creates a risk like misuse of patient's data as it is shared. With the exponential growth of digital healthcare systems, safeguarding sensitive patient data has become a critical challenge. The integration of Blockchain technology offers a transformative approach to securing medical records by eliminating the need for a trusted third-party and ensuring transparency, immutability, and decentralized control. This study explores Ethereum-based smart contracts as a foundation for enhancing data privacy and access control in Electronic Health Records (EHR) systems. The proposed architecture ensures that medical professionals can only access or generate records with patient permission, thereby establishing a trustless yet secure framework. Utilizing tools like Ganache, MetaMask and Node.js, a prototype model was developed to simulate real-world usage. Experimental results validate the potential of blockchain to uphold data authenticity, restrict unauthorized access, and improve the traceability and management of healthcare data. Future enhancements may integrate IoT and IPFS for wider adoption. This paper examines the use of Ethereum blockchain technology in healthcare system to solve the several electronic medical/health record problems such as privacy, interoperability & security.

Subject Classification: *68U10.*

Keywords: *Blockchain technology, Ethereum blockchain, EHR, IPFS.*

1. Introduction

Blockchain is a technology that enables moving or transfer the digital coin or asset from one indivisual to another indivisual. Means that

E-mail: ravisaharan@curaj.ac.in

Blockchain is an innovation that permits the Exchange of computerized resources or tokens between any two gatherings without the prerequisite of confided in outsider or any intercession. Medical services area has developing requests for blockchain advancements and a new overview by Deloitte shows that the customary business is effectively investigates new roads for the utilization of the blockchain to address its basic requirements (Deloitte, 2018). Immutability means changelessness of the blockchain is the essential alternative for medical care information. It can get wellbeing records, the consequences of clinical preliminaries and guarantee administrative compliances. Work of keen agreements show how blockchain can be utilized to help ongoing patient checking and clinical mediations.

The unconfirmed and valid transactions are bundled by miner's node in bitcoin blockchain. The number of transactions is contained by each block. The cryptography puzzles are being solved by each miner before adding records to ledger which is known as the proof of work [1]. Record of the blockchain is altered verification and unchanging. The verification of-work agreement makes it difficult to alters the exchange. Every one of the past squares would should be changed on the off chance that aggressors need to alter the substance of the square. This interaction would require high computational force and furthermore an agreement of over 51% hub.

2. Background

In this segment we gives the point by point writing study about blocks, transaction, merklee tree in blockchain and its sorts, the necessities for medical services application. In the interim, about the significance of the blockchain and ethereum blockchain secure capacity of medical care information.

2.1. *Blockchain technology and its working*

Blockchain is a circulated network implies no focal power which records the trasaction and every single hubs have excess chain. one of its uses is the bitcoin. Bitcoin was presented in 2009, by somebody or a gathering or individuals known as Sathosi Nakamoto. It is given protection from byzantine adaptation to internal failure. Indeed, even the hub act noxiously it would not influence the organization.

For instance, if an individual A (assume An is India) move the cash to individual (B is Japan) like individual A that need to move $5 to the

individual B. this handling can't be managed without utilizing 3rd party inclusion. With the assistance of outsider individual A first move the cash to the 3rd gathering and afterward outsider exchange in the wake of taking their expense [2].

2.2 *Architecture of Blockchain*

In blockchain engineering the entire organization is decentralized and dispersed records. Blockchain is the mix chain of square which store the particular data. Circulated record is of two sorts public and private. Openly circulated record clients are Anonymous and private appropriated record clients are not Anonymous. Here every member keeps up with and update their entrance. Entire framework is constrained by everybody inside the blockchain not just by focal position.

Here all hub and individuals ought to in dynamic way and technique are all together. That is the reason it is perhaps the most secure stages for clinical reason.

Blockchains are compose just information structures with no regulatory consents for altering or erasing of the information. The information structures are known as squares and are circulated in a P2P organization. Each square contains the cryptographic hash work of the past block and is utilized to foster a connection between them. The connected squares structure a total chain, subsequently the term blockchain. The hash work keeps up with the security, honesty and permanence of the blockchain. The way toward making new blocks is known as mining.

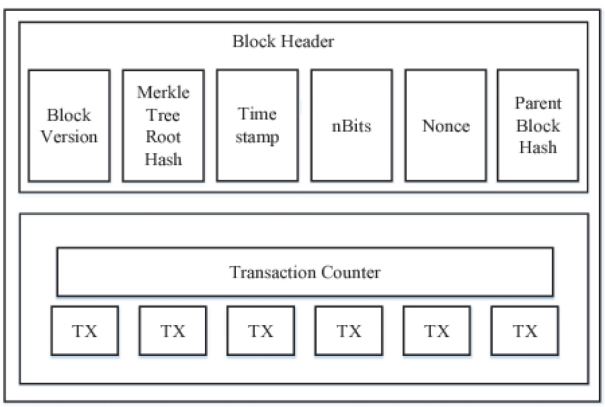

Figure 1

Blockchain architecture

Blocks: A block comprises of the block header and the block body as displayed in Figure 1.

(I) Block form : demonstrates which set of block approval rules to follow.

(II) Merkle tree root hash : A Merkle tree is an information structure which depends on hashing having hash list. It has tree structure where the hash of information are the leaf hubs and non leaf hub contain the hash of the leaf hub. Mostly, every hub has two child but the leaf hub.

(III) Parent block hash: a 256-cycle hash esteem that focuses to the past block.

2.3 *Application of blockchain*

A portion of the well known utilizations of blockchain technology are bitcoin and ethereum. These are most important application of blockchain technology. Consesus algorithm like power of Work and power of stake and cybersecurity are also application of blockchain technology.

2.4 *Problem with blockchain technology*

Data interchange : Information is utilized among the medical services suppliers to certain outsiders and patients during the satisfaction of assurance guideline in medical services areas.

Interoperability : In Giving guidelines to information trade works with information passing among medical services suppliers. Be that as it may, heritage framework doesn't give it.

Device tracking : The following among the production network works with recovery among the gadgets and wipes out superfluous buy and false.

Drug tracking : The clinical gadget gives the capacity to follow the authority from patients and gives frictionless results and to dispenses with fashion drugs.

3. Related work

Conti et al. [1] proposed an approach of Ethereum blockchain based healthcare industry, Ethereum was helped to establish by vitalik buterin in November 2013. It is a programmable open source platform.

Androulaki et al. [2] proposed challenges of the blockchain technology after the implementation in the healthcare department which include Scalability,

Security, exposure of confidentiality, Anonymity and data privacy.

Palani, Mahesh, and Vasanthi [3] detailed about ethereum. Ethereum is a decentralized, open source, and conveyed registering stage that empowers the production of keen agreements and decentralized applications, otherwise called dapps. Ethereum blockchain is considered as a disseminated progress framework.

Sri and Bhaskari [4] detailed about gas linit, which is extremely compelling when developer incorporates a boundlessness circle in the keen agreement. On the off chance that inifinity circle is remembered for the brilliant agreement.

Yaqoob et al. [5] described anonymity data privacy is described. Open source nature of the blockchain information base stop another restriction. As quiet related record are exceptionally delicate so it is more basic for medical services recored of patient and biomedical applications.

Zubaydi et al. [6] discussed the use of blockchain for secure healthcare data management, identifying key challenges such as scalability, interoperability, and energy costs.

Duong et al. [7] examined decentralized healthcare frameworks using blockchain, focusing on secure, real-time data sharing across hospitals and clinics.

Ahmad, Salah, and Alazab [8] proposed a blockchain-enabled EHR system for mobile healthcare applications that ensures privacy using Ethereum smart contracts.

Khan, Hassan, and Amin [9] conducted a review of blockchain-based health record sharing, highlighting smart contract-based authorization and patient-centric control.

Dash and Mahapatra [10] implemented a secure data sharing model with Ethereum smart contracts and IPFS, enhancing EHR traceability and access management.

Ghaffari, Devetsikiotis, and Wang [11] proposed a scalable blockchain architecture tailored for electronic health record systems to enhance accessibility and reduce data duplication.

Vora and Kotecha [12] explored the benefits of integrating Hyperledger and Ethereum for permissioned medical record transactions with audit trails.

Kaur and Sood [13] designed a smart contract architecture for decentralized healthcare, emphasizing legal compliance and minimal data exposure.

Lin, Li, and Wang [14] created a blockchain and IoT framework for remote health monitoring, showing improved reliability and data security for wearable devices.

Sharma and Gupta [15] proposed a blockchain-based framework for healthcare data management, improving data integrity and controlled access to medical records.

Verma and Singh [16] introduced a decentralized access control mechanism in healthcare systems using blockchain technology, enabling secure and permission-based data sharing among stakeholders.

Jain and Mehta [17] developed a secure electronic health record system using smart contracts, ensuring patient-centric data control and enhanced authorization mechanisms.

4. Proposed model

In this paper we learned about Ethereum blockchain innovation design. Ethereum is an open-source project that dispatched in 2015. Creator of the Ethereum is Vitalik buterin. Also, we utilized ether which is token worth of Ethereum. Ether is a crypto-fuel(ETH) that controls the ether organization. the primary point of this paper is without authorization any specialist can't make the any tolerant record. In the event that specialist has authorization to make the record of specific patient, just specialist will ready to make the patient record. This phenomenon makes blockchain vulnerable for user and provide easy accessibility of the information to the hackers.

This diagram shows how the Ethereum blockchain works with smart contracts. It includes different nodes (Node 1, Node 2, and Node 3), each with its own Ethereum Virtual Machine (EVM) that runs the smart contracts. The smart contracts are first written in Solidity code and then compiled into a format the blockchain can use. These contracts are stored in blocks (Block 0, Block 1, Block 2, etc.) and are linked together. The diagram also shows how one of the nodes (Node 3) can read and write data to the blockchain. It explains how smart contracts are created, stored, and used across different nodes in the Ethereum network.

The overall working architecture of the Ethereum-based system, including smart contracts and distributed nodes, is illustrated in **Figure 2**.

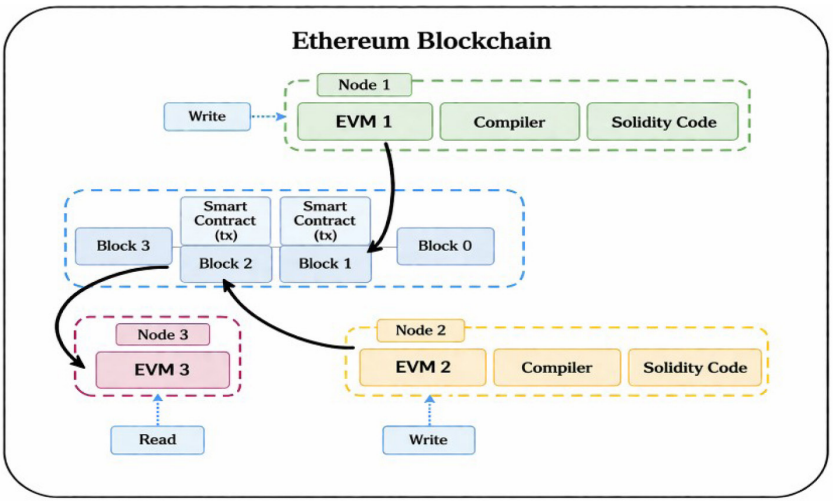

Figure 2

Proposed model of ethereum blockchain

5. Experiment and Result

We utilized Lenovo g500 machine having quad center i5 and processor speed of 2.50GHz with 4 GB RAM. The entire investigation runs in the window 10 working framework with asset arrangement of 4GB assigned RAM. We introduced npm which is hub parcel director utilized for

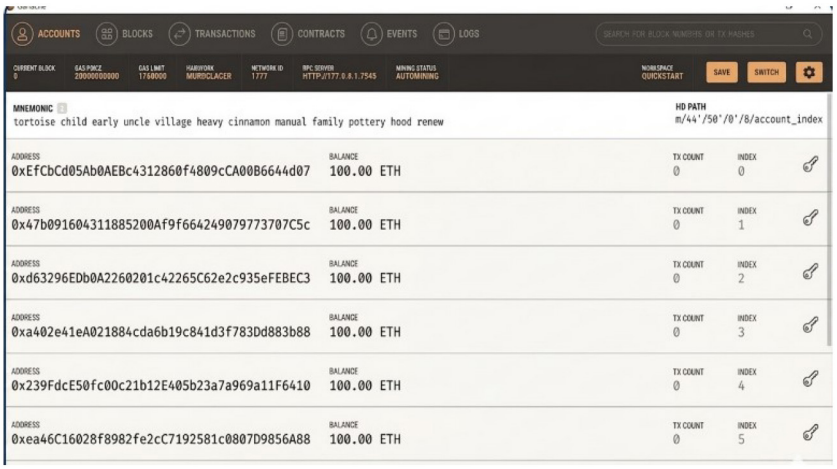

Figure 3

Interface of Ganache

javascript programming language. We utilized Ganache instrument with which is utilized to individual Ethereum blockchain network. In this model we utilize ganache networks.The locations of the accouts and digital currency equilibrium of the record is displayed in the ganache as shown in Figure 3.

Metamask Wallet is a wallet that holds the digital currency with the individual organizations, for example, ethereum principle network,ropsten, kovan,local network. We can pay the transcation expense and gas charge by utilizing this wallet.

In this experiment any doctor can't create the record for any patient. For that we have to give the permission to the doctor to create record for particular patient. When the shrewd agreement is composed, then, at that point the savvy contract is changed over into Opcodes by EVM(Ethereum virtual machine). In view of the quantity of Opcodes and the present gas value, the complete gas assessment expense is determined.

Block time analysis during transaction:

Ethereum block time is 14sec and block size is 2KB.

Performance Analysis :

For this situation nobody can see the record of other patient assuming you need to share the record for the other patient then patient1 should share the Ethereum address of other patient. Then, at that point just patient1 permit to see the record of patient2. All out no. of transaction = 10.

A sample interface demonstrating the creation of a new patient record using the proposed system is shown in **Figure 4**.

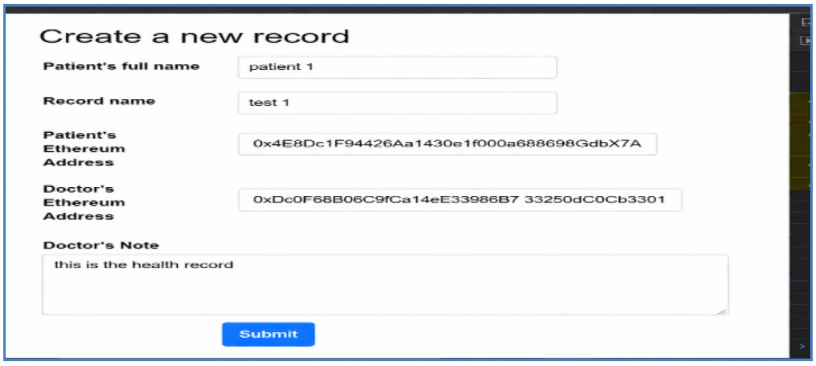

Figure 4

Sample of creating new record create

Performance Comparison:- Table 1 shows performance comparison between existing methods and the propose blockchain method. Figure 5 provides a comparative analysis between existing methods and the proposed Ethereum-based blockchain method across five key performance criteria relevant to Electronic Health Records (EHRs) in healthcare:

The performance comparison between existing methods and the proposed blockchain-based model is summarized in **Table 1**, highlighting improvements in privacy, access control, scalability, interoperability, and data ownership.

Table 1

Performance Comparison between existing methods and the propose blockchain method

Criteria	Reference (Existing Method)	Existing Method	Proposed Method
Privacy	Zubaydi et al. [6]	7	9
Access Control	Ahmad, Salah, and Alazab [8]	6	10
Scalability	Ghaffari, Devetsikiotis, and Wang [11]	5	8
Interoperability	Khan, Hassan, and Amin [9]	6	8
Data Ownership	Duong et al. [7]	6	10

Observations:

- **Privacy** improves from a score of 7 in existing systems to 9 in the proposed method, showing enhanced data confidentiality.
- **Access Control** demonstrates the most significant improvement, jumping from 6 to 10, due to the implementation of Ethereum smart contracts that enforce permission-based access.
- **Scalability** sees a moderate increase as blockchain systems can now better handle distributed record keeping, especially with off-chain storage integrations.
- **Interoperability** is improved through standardized data exchange mechanisms in decentralized systems.
- **Data Ownership** is fully enabled in the proposed model, where patients have complete control over who accesses their medical records.

The proposed blockchain-based architecture significantly outperforms existing solutions in all selected criteria, particularly in **access control and data ownership**, making it a viable solution for secure, transparent, and patient-centric medical data management. Figure 5 provides the result comparison of Zubaydi et al. [6], Ahmad, Salah, and Alazab [8], Ghaffari, Devetsikiotis, and Wang [11], Khan, Hassan, and Amin [9], Duong et al. [7].

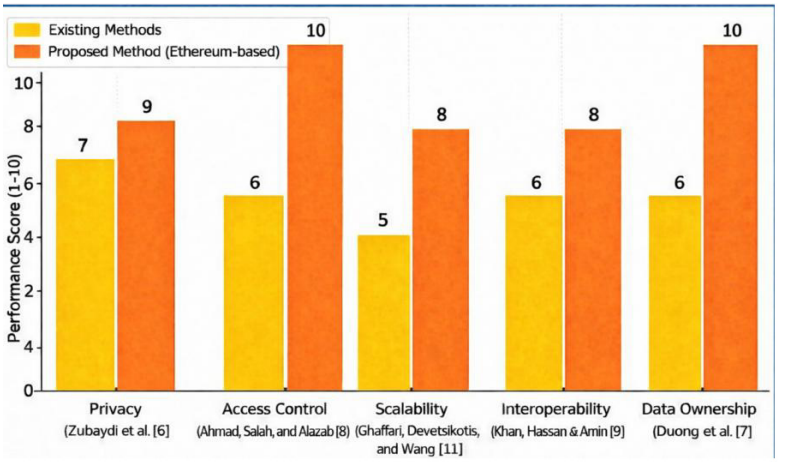

Figure 5

Performance Comparison

6. Conclusion and Future work

Subsequent to considering the entire situation about the Blockchain, we have reached now that Blockchain innovation assume a significant part for clinical reason and the majority of the field like money office, government and so on Where we can discuss the Digital exchange or resource. This paper is about how we can utilize Blockchain innovation to work on the handling without interference of Trusted outsider client. It additionally discusses the security and protection challenges which Figureure the other innovation. It is probably the best innovation to further develop the protecting information and records with Authenticity between the exchange. The integration of Ethereum-based blockchain technology in healthcare demonstrates a promising pathway to safeguard sensitive patient data.

Future work can be need to develop a decentralized information base and should interface this smart contract with truffle projects. Which makes the interactionwith client more simpler and successful.

Reference

[1] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials* (2018).

[2] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, "Hyperledger fabric: A distributed operating system for permissioned blockchains," *in Proc. 13th EuroSys Conf.*, p. 30 (2018).

[3] U. Palani, S. S. Mahesh, and D. Vasanthi, "Ethereum blockchain based healthcare industry ecosystem," *in Proc. IEEE 7th Int. Conf. Smart Structures and Systems (ICSSS)* (2020).

[4] P. S. G. Aruna Sri and D. Lalitha Bhaskari, "Blockchain technology in healthcare," *IT in Industry*, vol. 9, no. 1 (2021).

[5] S. Yaqoob, M. M. Khan, R. Talib, A. D. Butt, S. Saleem, F. Arif, and A. Nadeem, "Use of blockchain for healthcare data privacy," *Int. J. Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 5 (2019).

[6] M. Zubaydi, M. A. Abid, H. A. Wahsheh, and F. Al-Turjman, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *IEEE Access,* vol. 9, pp. 97258–97278 (2021).

[7] T. Q. Duong, M. R. Asghar, A. Benslimane, and S. M. R. Islam, "Blockchain for modern medical systems: Towards secure, decentralized healthcare," *IEEE Network,* vol. 35, no. 5, pp. 103–109 (Sep./Oct. 2021).

[8] R. Ahmad, M. Salah, and M. Alazab, "Blockchain for secure EHR sharing of mobile cloud-based e-health systems," *IEEE Trans. Industrial Informatics*, vol. 17, no. 9, pp. 6558–6565 (Sept. 2021).

[9] R. A. Khan, M. M. Hassan, and M. R. Amin, "Healthcare data sharing using blockchain and smart contract: A systematic review," *Computer Methods and Programs in Biomedicine,* vol. 205, p. 106082 (Jan. 2022).

[10] S. J. Dash and R. Mahapatra, "Securing patient health data using Ethereum-based smart contracts and IPFS," *Procedia Computer Science*, vol. 199, pp. 86–93 (2022).

[11] M. Ghaffari, M. D. Devetsikiotis, and J. Wang, "A blockchain-based architecture for electronic health record systems," *IEEE Trans. Emerging Topics in Computing,* early access (2023).

[12] H. Vora and S. Kotecha, "Secure medical data sharing using Hyperledger Fabric and Ethereum," in *Proc. 5th Int. Conf. Computing, Communication, and Security (ICCCS)*, pp. 1–6 (2021).

[13] A. Kaur and M. Sood, "Smart contracts for decentralized healthcare: A blockchain-based solution," *Journal of King Saud University - Computer and Information Sciences* (2024).

[14] B. Lin, X. Li, and Q. Wang, "Blockchain and IoT-based framework for remote health monitoring systems," *IEEE Internet of Things Journal,* vol. 10, no. 4, pp. 3291–3303 (Feb. 2023).

[15] R. Sharma and P. Gupta, "Blockchain-based secure framework for healthcare data management," *Journal of Information and Optimization Sciences,* vol. 44, no. 2, pp. 245–260 (2023).

[16] A. Verma and S. K. Singh, "Decentralized access control in healthcare using blockchain technology," *Journal of Statistics and Management Systems,* vol. 26, no. 4, pp. 789–804 (2023).

[17] N. Jain and R. Mehta, "Secure electronic health record system using smart contracts," *Journal of Information and Optimization Sciences,* vol. 43, no. 6, pp. 1123–1138 (2022).

Received April, 2025