IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

MedDoc : Secured Medical Document Storing And Exchange Using Blockchain

Pranay Nimsatkar
Department Of Computer Engineering, Jayawantrao Sawant College Of Engineering,Pune,India
pranaynimsatkar16@gmail.com

Prathamesh Padalkar
Department Of Computer Engineering, Jayawantrao Sawant College Of Engineering,Pune,India
padalkarprathamesh00@gmail.com

Darshan Pardeshi
Department Of Computer Engineering, Jayawantrao Sawant College Of Engineering,Pune,India
gauravpardeshi05022003@gmail.com

Sangram Ranshing
Department Of Computer Engineering, Jayawantrao Sawant College Of Engineering,Pune,India
sangramranshing57@gmail.com

Dr. Mansi Bhonsle
Department Of Computer Engineering, Jayawantrao Sawant College Of Engineering,Pune,India
mansibhonsle@jspmjscoe.edu.in

Abstract— This paper explores how blockchain can revolutionize the healthcare industry, addressing the limitations of current Electronic Health Records (EHRs). EHRs offer opportunities for better patient care and clinical research, but they lack sufficient security, leading to data breaches and restricted access for patients and caregivers. Blockchain's decentralized nature and cryptographic features provide a solution to these issues, ensuring data integrity, privacy, and secure data access. By replacing traditional methods, blockchain can significantly improve health data sharing, reducing delays in patient treatment.

Keywords — Healthcare, medical documents, blockchain, decentralized , secure exchange, privacy

1. Introduction

An electronic health record is a digital document that contains details of the patient's medical history. It includes very highly sensitive information such as medical history, diagnosis and treatment. Many other details are also stored on EHR's such as appointments, accounts and medical bills.

There are various advantages of using EHR's for the storage of medical records such as EHR's enhances the security of the medical records. With the help of EHR's we can enhance the security and integrity of the data of the patient. [1] EHR's can be used to reduce the redundancy in the medical records. The various problems that we face during the storage of data in the traditional paper records can be solved using EHR's.

In the current scenario, EHR's can be considered as an important part of the medical industry but still different issues such as interoperability and privacy issues remain which can be solved.

Interoperability refers to the sharing of data between different programs and devices which are used by different healthcare systems.

Privacy refers to another issue within the EHR systems. As the information is stored digitally, it can be hacked and misused for any purpose.

Blockchain is a database storage using encrypted data blocks organized in the form of chains. All the users participating in the blockchain decide which block is validly accessed by different users with the help of various consensus algorithms.

2. Literature Review

The various existing blockchain based EHR systems and their standards are discussed below:

OmniPHR is a decentralized peer-to-peer (P2P) network that integrates Electronic Health Records (EHRs) using a variety of technologies, including blockchain, routing overlay (a method for decentralizing data, locating nodes, and managing their positions in the P2P network), and the Chord algorithm. This system provides [2] consumers with a consolidated picture of their health records while also allowing healthcare providers to receive up-to-date information about their patients, even if the data is spread across multiple healthcare facilities.

FHIRChain, designed to meet the criteria set by the Office of the National Coordinator (ONC), adheres to Health Level 7 (HL7) and Fast Health Interoperability Resource (FHIR) standards. This framework [3] ensures decentralized storage and preserves data ownership rights. FHIRChain utilizes trustless decentralized storage for metadata, facilitating data exchange without the need for data downloads or uploads. Identity and authentication are secured through encrypted reference pointers.

The blockchain-based approach to Health Information Exchange (HIE) focuses on enabling secure data sharing through blockchain technology, aiming to replace centralized trust mechanisms with network consensus. This methodology utilizes blockchain to [4] facilitate data sharing, with a consensus algorithm ensuring interoperability. Additional security measures are implemented using smart contracts and network-wide keys to enhance data integrity and access control.

Ancile, operating on the Ethereum blockchain, aims to provide secure interoperability and controlled access to health records by patients, third parties, and healthcare providers. Employing innovative security measures, Ancile utilizes smart contracts on Ethereum to enforce access control and ensure data integrity. Advanced cryptographic techniques further enhance security, making Ancile a robust solution for secure health record management and interoperability.

Challenges and Issues in implementation of blockchain in healthcare:

The healthcare industry's use of blockchain technology is progressing, but it faces significant challenges, including scalability, privacy concerns, and regulatory complexity.

Scalability remains a big barrier to blockchain adoption. Blockchains handle a finite number of transactions every block, with set block sizes and formation durations. While these constraints preserve important features such as immutability and decentralized verification, they also cause sluggish transaction processing. [5] For example, Ethereum, a well-known blockchain platform, processes around 15 transactions per second. Furthermore, blockchains constantly add data, with the ledger growing from the genesis block onward. As a result, network nodes must commit significant storage and processing resources to support Ethereum's increasing ledger, which now exceeds one terabyte.

Privacy arises as another significant concern, particularly in permissionless blockchain systems. In these systems, the ledger is publicly distributed among network participants, allowing everyone to see transactions. This transparency exposes users to possible privacy violations, since attackers can use the ledger to follow user activity and extract sensitive information via a variety of ways, including graph analysis and transaction linking. The public nature of blockchain databases exacerbates these problems, especially in healthcare applications where data security is critical. As a result, privacy concerns restrict the widespread use of blockchain in healthcare, limiting its potential utility in delicate medical settings.

Furthermore, healthcare systems are often distributed across many places, with hospitals located in different geographic areas. This distributed nature presents a substantial hurdle for building and sustaining a blockchain infrastructure. Without a centralized system, combining all medical records becomes a difficult operation, impeding the widespread implementation of blockchain technology.

The speed of blockchain transactions creates another barrier. Processing speed can be slow, especially in big networks, causing confirmation delays and eventually slowing down information sharing. This slowness in transaction processing might prevent the timely sharing of critical medical data, jeopardizing the efficiency and efficacy of healthcare operations.

3. RELATED WORK

A blockchain is a decentralized and distributed ledger technology that allows transactions to be recorded in a secure and immutable manner.

A blockchain network consists of multiple nodes (computers) spread across the globe. These nodes work together to maintain the blockchain. When a transaction occurs, such as the transfer of digital assets like cryptocurrency or recording data, it is broadcasted to the network.

The nodes on the network verify the validity of the transaction using consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms. The verification process ensures that the transaction is legitimate and conforms to the rules of the network. Verified transactions [6] are grouped together into blocks. Each block contains a certain number of transactions, along with a timestamp and a reference to the previous block, forming a chain of blocks - the blockchain. Each block is secured using cryptographic hash functions. This ensures the integrity of the data within the block and makes it nearly impossible to alter or tamper with the information stored in previous blocks.

Once a block is created, it is added to the blockchain through a consensus mechanism agreed upon by the network. This process may vary depending on the blockchain protocol being used. Once a block is added to the blockchain, it becomes a permanent part of the ledger. This immutability ensures that the data recorded on the blockchain cannot be altered or deleted, providing a transparent and tamper-proof record of transactions. Every node on the network maintains a copy of the entire blockchain. This distributed nature ensures that no single entity has control over the data, making the blockchain resistant to censorship and single points of failure.

Depending on the blockchain protocol, nodes may receive rewards, such as cryptocurrency, for their contributions to the network, such as validating transactions or mining new blocks. A blockchain operates as a transparent, secure, and decentralized system for recording transactions and maintaining a tamper-proof ledger of digital assets or information.

4. PROPOSED SYSTEM

In the current system of healthcare the documents of the patients such as prescriptions, health reports, insurance, test reports are stored on a centralized server or in the databases of specific organization such as hospitals or insurance companies etc. Due to the storing process of the documents is centralized and the authority is present at single organization or a person the risk of tampering, misuse of documents and the permanent deletion of document is possible and can hamper the life of patient who has the real need of documents at the present time or in condition where he need to give proof of his health record.

To overcome the problem of tampering and misuse of healthcare documents of patients we designed a system where the documents can be stored directly on the blockchain. And also we can share the access of our documents to any doctor , person or authority which can lead to easy exchange of documents. Due to the system is implemented on blockchain there is no central authority which is controlling over the documents it is present on the largely spreaded decentralized network.

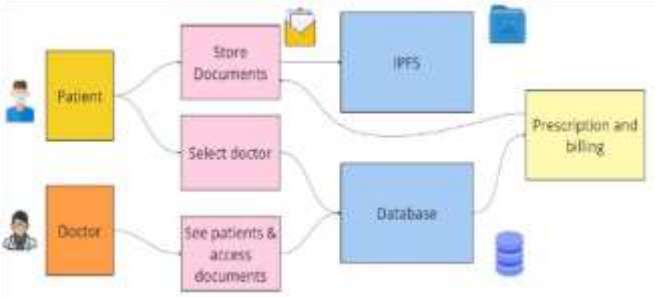

Fig. 1. Proposed System

As the features of blockchain like immutability, decentralized, encrypted data is collinear with the need of improvement in the existing system of storing health care documents, we can use it perfectly for the new proposed system which can give the user assurance that the documents are safe enough.

The paper signifies that there are two main entities present as patient and the doctor. The patient and doctor both can register on the platform as patient and doctor category with their own metamask wallet. Then the patients can store their documents on platform easily just by uploading the documents manually. Also the patient can see the different doctors which are registered on the platform and can give access to the specific doctor easily by taking their metamask wallet id. And the doctors can see on their side who has given the access to the documents and can easily check the previous documents of the patient and can give proper advise to the patient. If the patient feels like now there is no need of access to specific person or doctor he can easily remove the access of that person.

By implementing this system we can easily store the documents on non tamperable system and also provide paperless treatments or paperless visit to the doctor.

5. METHODOLOGY

For the implementation of MedDoc platform there are two essential things which are frontend by using which the user can interact with the platform and the backend in which the business logic is written we can call it the brain of the MedDoc platform.

5.1 Frontend Development With ReactJs :

To build the frontend part of the platform we are using HTML,CSS and ReactJs. ReactJs is an open – source javascript library primarily used for building user interfaces (UI's) and single page application. We are using ReactJs because it provides efficiency, flexibility, and performance to web based platform. To store the information of user such as name and metamask id we are storing this information on MySql database.

5.2 Simplifying User Access with Database :

We are using database here because if user want to give access to somebody then the other person has to give his metamask id physically and it becomes little difficult so to make it simplified, the user can simply search the other person name and if he is registered on the platform it is very easy to retrieve his id and give access to him.

5.3 Backend Development With Solidity Smart Contract:

To build the backend part of the platform we are using smart contract which is written using the programming language known as Solidity. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

5.4. Connecting Frontend And Backend With Web3.js :

To connect the frontend and the backend we are using the Web3Js library. This library provide interfaces for interacting with the Ethereum blockchain, which is where most smart contracts are deployed. They allow you to interact with smart contracts by sending transactions, reading data from the blockchain, and listening to events emitted by smart contracts. It provides a collection of APIs that allow developers to interact with Ethereum nodes, smart contracts, and the Ethereum blockchain. With web3.js, you can deploy contracts, send transactions, query contract state, and more.

5.5 Smart Contract Deployment And Testing With Hardhat :

To deploy and test the smart contract we are using Hardhat. Hardhat is a development environment and tool suite for Ethereum smart contract development. It provides a set of tools and tasks to compile, test, deploy, and interact with Ethereum smart contracts and decentralized applications (dApps). Hardhat is designed [7] to streamline the smart contract development process and improve developer productivity. Hardhat includes a built-in Solidity compiler, allowing developers to compile their smart contracts with ease. It allows developers to write deployment scripts to automate the deployment of smart contracts to various Ethereum networks. Developers can write custom scripts in JavaScript to automate tasks such as interacting with contracts, querying blockchain data, or performing other actions.

5.6 For the storing of medical documents we are using Pinata. Pinata is a platform and service for storing, managing, and distributing digital assets on the Inter Planetary File System (IPFS) and other decentralized storage networks. IPFS is a protocol and peer-to-peer network for storing and sharing hypermedia in a distributed file system, making it a decentralized alternative to traditional web hosting. This enables users to store their files

in a decentralized manner, ensuring data integrity and availability. Pinata integrates with blockchain platforms such as Ethereum, enabling developers to store and retrieve data from IPFS directly within their blockchain applications and smart contracts. How IPFS works? IPFS takes image and converts it to hash or a Image URL. To convert the image into URL the IPFS uses algorithms like SHA-256 etc. After fetching this URL from IPFS we store it on a blockchain through smart contract to maintain the transparency and we can easily fetch images that we uploaded on IPFS easily using the smart contract.

6. RESULTS AND DISCUSSIONS

Earlier, there were various existing storage systems that are centralized for the storage of medical records. The issues that we face in the existing systems were security and privacy. The document are stored in centralized databases of specific hospitals or organizations. So there is a single point of failure and the data breach becomes easier. Also anyone can tamper the documents in a centralized system easily and no one can know who changed the documents or what changes are done to the documents. Also the whole system is under the control of a single authority. The patients need to visit the organization to take the copy of the documents and they have to store it in a physical format for their reference.

On the other hand, MedDoc provides a lot of features that overcome the flaws of existing centralized system of different organizations. MedDoc is a fully decentralized DAPP which helps users to store their medical records in a secure way. It overcomes the main flaw of the existing storage system i.e security, ownership and ease of use.

The first disadvantage of an existing system which stores documents in a centralized manner that is overcome by using blockchain which is fully decentralized system and has no single point of failure. As the data is lost when a centralized system fails , MedDoc stores the data using multiple nodes making the system more stable and resilent.

Another problem we face in a centralized system is the ownership of documents. In a centralized system, the documents are stored under the control of a single user and he has the ability to decide who can access the documents.

The existing system have a lot of cost to upgrade to store more data on the system and it is very expensive and time consuming while MedDoc can naturally expand its nodes for more storage of data and is comparatively less expensive and less time consuming as compared to the existing sytems.

The platform of MedDoc is well designed such that a new user can use the platform in a first go. It is as simple as a google drive that everyone access in daily life. On the other hand the existing system that store the documents has a very different user architecture and the users face a lot of problem for the storage and retrieval of the documents.

The main feature of MedDoc is the data backup and recovery. In the existing system , the users can face a problem of data loss. As the documents stores are under a single authority it can happen that once the data is lost, it cannot be recovered while in MedDoc as we use a decentralized storage system the data is stored in a decentralized way and if a system goes down the user can still have access to the documents.

Another problem that exist in a centralized system is a lack of transparency. The data that is stored on a centralized system is much less accessible to the users and the users face a lot of problems while accessing the data. MedDoc provides users with a feature of transparency , like we can see who has accessed the documents in the entire time period.

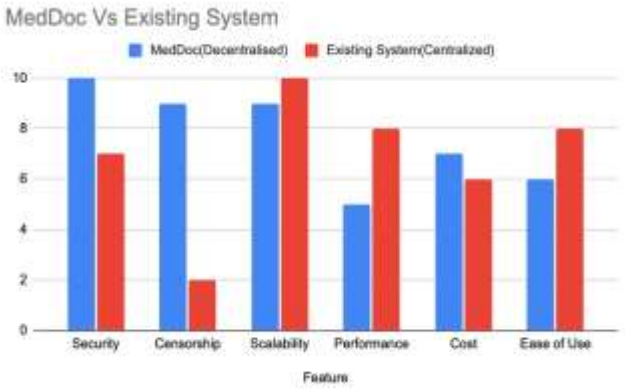

Fig.2. Comparison between MedDoc and Existing System

7. CONCLUSION

This paper signifies the implementation of MedDoc, it marks a significant advancement in healthcare technology, offering a secure and efficient solution for electronic health record storage and retrieval. By addressing the challenges associated with medical record management, MedDoc empowers individuals to take control of their health information and facilitates proactive healthcare practices. Through its user-friendly interface and robust blockchain technology, MedDoc enhances prescription accuracy, prevents fraud, and promotes preventive healthcare measures. Looking ahead, the integration of various security features and interoperability standards presents promising avenues for further enhancement. Overall, MedDoc represents a pivotal step towards a patient-centric healthcare ecosystem, where accessibility, security, and informed decision-making converge to redefine the future of healthcare delivery.

REFERENCES

[1] Peng Xi , Xinglong Zhang, Lian Wang, Wenjuan Liu and Shaoliang Peng (2022). A Review of Blockchain-Based Secure Sharing of Healthcare Data

[2] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi. (2017). OmniPHR: A distributed architecture model to integrate personal health records

[3] Zhang, P., White, J., Schmidt, D. C., Lenz, G., Rosenbloom, S. T., FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal (2019).

[4] Cornelius C. Agbo, Qusay H. Mahmoud OR CID and J. Mikael Eklund (2019) Blockchain Technology in Healthcare: A Systematic Review.

[5] Abdurrashid Ibrahim Sanka, Ray C.C. Cheung (2020). A systematic review of blockchain scalability: Issues, solutions, analysis and future research

[6] Gautami Tripathi , Mohd Abdul Ahad , Gabriella Casalino (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges

[7] Khaled Shuaib , Juhar Abdella , Farag Sallabi , Mohamed Adel Serhani (2021). Secure decentralized electronic health records sharing system based on blockchains

[8] E. Chukwu and L. Garg, ‘‘A systematic review of blockchain in health- care: Frameworks, prototypes, and implementations,’’ IEEE Access, vol. 8, 2020

[9] Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado (2017). Blockchain distributed ledger technologies for biomedical and health care applications.

[10] André Henrique Mayer Cristiano André Da Costa Rodrigo Da Rosa Righi (2019). Electronic health records in a Blockchain: A systematic review.

[11] Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang & Zhongdai Wu (2022). A blockchain-based secure storage scheme for medical information.

[12] Faheem Ahmad Reegu, Yonis Gulzar, Qin Xin, Ali A. Alwan, Abdoh Jabbari, Rahul Ganpatrao Sonkamble and Rudzidatul Akmam Dziyauddin (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System.

[13] Halima Mhamdi, Manel Ayadi, Amel Ksibi, Amal Al-Rasheed ,Ben Othman Soufiene and Sakli Hedi. (2022). SEMRAchain: A Secure Electronic Medical Record Based on Blockchain Technology

[14] Ebtisam Ali Abdullah, Anwar Al Shamiri, Abdualmajed A. G. Al-Khulaidi (2024). Encrypting the Electronic Health Record using the Cloud Computing and Blockchain Technologies.

[15] Abdullah Al Mamun; Sami Azam; Clementine Gritti (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction.

[16] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, ‘‘A patient-centric interoperable framework for health information exchange via blockchain,’’ in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019.

[17] S. Wu and J. Du, ‘‘Electronic medical record security sharing model based on blockchain,’’ in Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy (ICCSP), 2019.

[18] A. Fernandes, V. Rocha, A. F. D. Conceicao, and F. Horita, ‘‘Scalable architecture for sharing EHR using the hyperledger blockchain,’’ in Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C), Mar. 2020.

[19] K. T. Win, ‘‘A review of security of electronic health records,’’ Health Inf. Manage., vol. 34, no. 1 Mar. 2005.

[20] M. Al Baqari and E. Barka, ‘‘Biometric-based blockchain EHR system (BBEHR),’’ in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020.

[21] L. Ismail and H. Materwala, ‘‘BlockHR: A blockchain-based framework for health records management,’’ in Proc. 12th Int. Conf. Comput. Mod- eling Simulation, 2020.

[22] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, ‘‘A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud,’’ IEEE Access, vol. 8, 2020.

[23] G. S. Reen, M. Mohandas, and S. Venkatesan, ‘‘Decentralized patient centric e-health record management system using blockchain and IPFS,’’ in Proc. IEEE Conf. Inf. Commun. Technol., Dec. 2019.

[24] T. A. Rahoof and V. Deepthi, ‘‘HealthChain: A secure scalable health care data management system using blockchain,’’ in Proc. Int. Conf. Distrib. Comput. Internet Technol. Bhubaneswar, India: Springer, 2020.

[25] M. Shah, C. Li, M. Sheng, Y. Zhang, and C. Xing, ‘‘CrowdMed: A blockchain-based approach to consent management for health data sharing,’’ in Proc. Int. Conf. Smart Health. Shenzhen, China: Springer, 2019.

[26] S. Rahmadika and K.-H. Rhee, ‘‘Blockchain technology for providing an architecture model of decentralized personal health information,’’ Int. J. Eng. Bus. Manage., vol. 10, Jul. 2018.

[27] G. Carter, H. Shahriar, and S. Sneha, ‘‘Blockchain-based interoperable electronic health record sharing framework,’’ in Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jul. 2019.

[28] H. Guo, W. Li, M. Nejad, and C.-C. Shen, ‘‘Access control for electronic health records with hybrid blockchain-edge architecture,’’ in Proc. IEEE Int. Conf. Blockchain (Blockchain), Jul. 2019.