A Decentralized Medical Record Storage System Using Blockchain

Adithya Shenoy
Student
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
vu1f2021005@pvppcoe.ac.in

Ashif M.
Student
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
vu1f2021011@pvppcoe.ac.in

Sonali Kharat
Student
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
vu1f2021018@pvppcoe.ac.in

Nikita Domale
Student
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
vu1f2021034@pvppcoe.ac.in

Asharani Shinde
Professor
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
ajshinde@pvppcoe.ac.in

Priya Gupta
Professor
Vasantdada Patil Pratishthan's College of Engineering
Mumbai, India
pmgupta@pvppcoe.ac.in

***Abstract*—Hospitals and health systems still have numerous difficulties in setting up, maintaining, and modernizing their electronic health record systems today. The numerous problems with using EHRs are covered in this study along with potential fixes. Maintaining a single version of the truth and safely storing medical records are the goals. Using blockchain is a likely solution. A patient's data may be accessed by various organizations, including hospitals, clinics, labs, and other health insurers, in order to document transactions and fulfill their mandates on the distributed ledger. By leveraging the blockchain to provide a distributed access and validation system, a platform for safely storing and exchanging electronic health records can be developed, helping to fully replace the present centralized middlemen. Consequently, the issues with today's health records are resolved.**

Keywords—Electronic Health Record, Distributed ledger, Blockchain, IPFS, BigchainDB.

I. INTRODUCTION

The way medical records are kept is one of the clearest issues facing the medical industry. The complexity of managing medical records that span many institutions and lifetimes was never intended for electronic health records, or EHRs.The goals of the recent large expenditures in Electronic Health Records (EHRs) were to reduce costs, increase research capacity, and improve patient safety. The majority of these health systems and health records are dispersed across several organizations and do not share patient information, but the EHRs have failed to do this. The system's security has been called into question due to recent security breach reports. Blockchain technology can be used to safely store medical records in order to prevent this. With the consent of the patient, several organizations, including physicians, hospitals, labs, and other health insurers, can add and see patient records on a distributed ledger. Numerous industrial issues can be solved by empowering users and digitizing health records.

II. PROBLEM STATEMENT

The issue concerns limitations in current medical record management systems. Patients still struggle to securely and efficiently share their records, while healthcare providers face interoperability and data security problems in centralized systems. A new solution is needed to address the demand for decentralized control, increased security, and transparent, auditable records that benefit both patients and healthcare providers. Our mission is to use blockchain technology to secure, trace, and transparently store and access medical records, altering the landscape of record management.

III. EXISTING SYSTEM

The degree of care that physicians, nurses, and other health professionals can offer has decreased during the last few years. This results from not being able to view the accurate and full health record. Each hospital has its own software for managing records. Some employ cloud service providers, some keep data locally in their databases, while yet others store data in a format that complies with insurance companies. The majority of the time, the hospital owns or rents a server on which the user's data is stored.The major problems that this model causes are,

- Fragmentation of patient data across medical facilities, independent practitioners, and other m-health apps. Patients who switch providers no longer have simple access to previous records since their data is dispersed among several institutions.

- Complete access to medical records is not given to patients. As a result, individuals must have numerous tests conducted repeatedly at various establishments.

- Inability to access vital medical information in case of emergencies.

- Manipulation of data by hospital authorities.

DOI: 10.55041/IJSREM33975

- Unauthorized access to private medical data.

Without a question, data will be the future economy's most important resource. Large corporations require more data as machine learning algorithms become more sophisticated. The controversy around the sale of user data is already plaguing social media sites like Facebook. Data has intrinsic value, and in the future, large corporations and businesses might potentially pay people for their data. Therefore, data needs to be protected in the same way as other assets like gold, cash, or cryptocurrency because information has equal value in both cases. information about medical data, perhaps more so.

IV. LITERATURE REVIEW

DD-Locker: Blockchain-based Decentralized Personal Document Locker

This paper is about a blockchain-based digital locker system. [1] It discusses the problems with centralized digital lockers. These systems are vulnerable to security breaches and privacy concerns. The authors propose a system that uses blockchain technology to store documents securely. The system would also allow for easy verification of documents.

Blockchain Private File Storage-Sharing Method Based on IPFS

This paper is about a blockchain private file storage-sharing method based on IPFS. It discusses the problems of current data storage methods, including lack of security and transparency. The authors propose a method that uses a combination of technologies including NDN, blockchain, and IPFS. This method is designed to address the security and confidentiality concerns of data storage.

MediChainTM: A Secure Decentralized Medical Data Asset Management System

This research paper is about a secure decentralized medical data asset management system called MediChainTM. It discusses blockchain technology and its limitations in the financial services industry. The paper proposes a permissioned blockchain system that uses off-chain storage and standard interfaces. This system could be used for patient-centered health data management.

HealChain: A Decentralized Data Management System for Mobile Healthcare Using Consortium Blockchain

This research paper is about a decentralized data management system for mobile healthcare called HealChain. It discusses the security risks of centralized data management systems and proposes a solution using consortium blockchain. The system consists of three layers: data collection, verification, and storage. Consortium blockchain is used to ensure authorized data validation and legal transaction auditing.

V. PROPOSED SYSTEM

Blockchain technology has already secured billions of dollars worldwide. Thus, it might also be applied to safeguard health records for medical purposes. With the robust security of blockchain technology, the current EHR system may be put to the test. This presents a more advanced, yet economically viable, alternative. The suggested remedy is to totally replace the existing centralized middlemen by building a distributed access and validation system on the blockchain.

This allows anyone to add the patient's medical records to a database that is accessible to the public. But unless the patient expressly grants consent, nothing will make sense to anyone. Every record that is made will be kept on a public blockchain and will not be subject to arbitrary manipulation. The following is a list of the technologies that can be used and how our solution can leverage them.

A. IPFS—The Interplanetary File System

The HTTP protocol is built on a client-server architecture, wherein any content that a client requests is stored on a server, and the client initiates contact with the server to request the content. The requested content is subsequently provided to the client by the server in response.

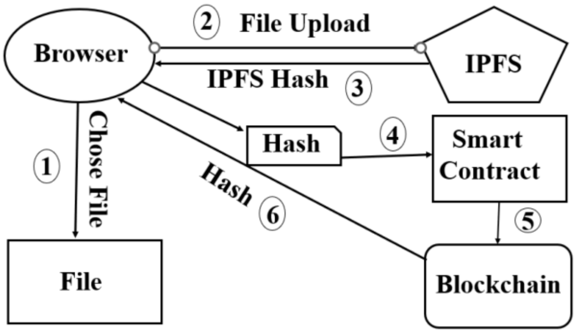

Figure 1 *- Working of IPFS*

In the case of medical records, one of the main disadvantages is the fragmentation of data among several servers. The data is stored on each hospital's own server, which must be contacted in order to obtain the data. The server could occasionally even be unreachable or private. So, IPFS can be used in its place. Here's how IPFS functions: Each file and every block contained in it receives a distinct fingerprint upon addition to IPFS, which is known as a cryptographic hash. Next, duplicates are eliminated throughout the network using the IPFS. Only stuff that it finds interesting is stored on each network node, together with some indexing data that aids in identifying which users are saving what. The user asks the network to locate nodes storing the information behind a distinct hash while searching for files. Through the use of a decentralized naming system known as IPNS, each file may be located using human-readable names.

The basic idea is to address content by its hash, or more precisely by the content itself, rather than by the server it is stored on. And the closest computer will be used to retrieve this content. Data will be stored here using IPFS. This means that if a patient only stays at one hospital, their records will also remain there. However, the records will simply accompany the patient if they relocate to a different hospital and ask to see them there. Anytime, anywhere, as long as someone with access to the data is operating an IPFS node, that data is always accessible.

B. Symmetric And Asymmetric Encryption

We must employ encryption in order to protect our records so that only those with permission can access them. A key, also known as a cypher, is used in symmetric encryption to encode a document into a disorganized mess. The original document needs to be decrypted using the same key in order to be retrieved. AES, often known as the Advanced Encryption Standard, is a widely used symmetric algorithm nowadays.

Asymmetric Encryption is an additional encryption method. This technique uses two keys. There are two keys: a public key and a private key, which is a secret key. Using the public key, a communication can be encrypted. On the other hand, the secret key is required to decode it. This implies that the message cannot be decrypted, not even by the one who encrypted it. Although there is a mathematical relationship between the public and secret keys, the secret key cannot be obtained from the public key. Modern computers use the widely used RSA asymmetric encryption method to encode and decrypt messages.

C. A Public Immutable Database

A public database that many people have access to, meaning that it can be trusted by all. Important data about our patients, physicians, and data will be stored here; however, the actual data will not be stored here; IPFS will be used for that.

VI. BLOCKCHAIN

An unidentified writer by the name of Satoshi Nakamoto originally discussed and developed blockchain technology in 2009. It has been the foundation for thousands of cryptocurrencies worldwide since its release, including Bitcoin, Litecoin, Ethereum, Ripple, and many more. Furthermore, it has been widely acknowledged as the safest online database management solution accessible. Blockchain technology is a decentralized data storage system that maintains a transaction ledger open to the public. This ledger can document a variety of transactions, including the storing of ballots and the transfer of real estate. All transactions that take place on a typical Blockchain are encrypted and validated using cryptography to guarantee security and anonymity. By utilizing elliptic curve cryptography, this system's security is substantially enhanced. Put simply, the system's security and privacy are provided by the encryption, while openness and accountability are increased by the public ledger.

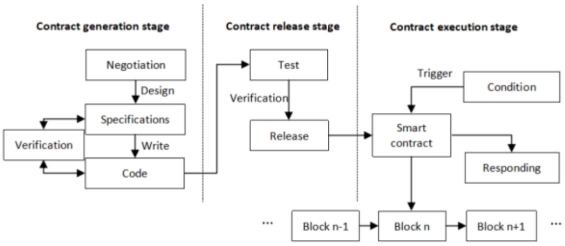

Figure 2 *- Working of Ethereum Blockchain*

Decentralization is one of the key features of blockchain technology. It is possible to build a blockchain that supports the safe storage of medical records and the upkeep of a single version of the truth. In order to document transactions and fulfill their purposes, many organizations, including physicians' offices, hospitals, labs, and other health insurance companies, may seek access to a patient's record on the distributed ledger.

VII. METHODOLOGY

A. User Registration:

Patients and doctors register on the platform. Users provide necessary details such as name, contact information, and identification documents. Doctors submit additional credentials for verification by government authorities.

B. Doctor Verification:

Government authorities verify the credentials of doctors registered on the platform. Verified doctors receive authorization to access patient records.

C. Patient Visit:

When a patient visits a doctor, the doctor creates a request for access to the patient's medical records. The request includes the patient's unique identifier (e.g., patient ID).

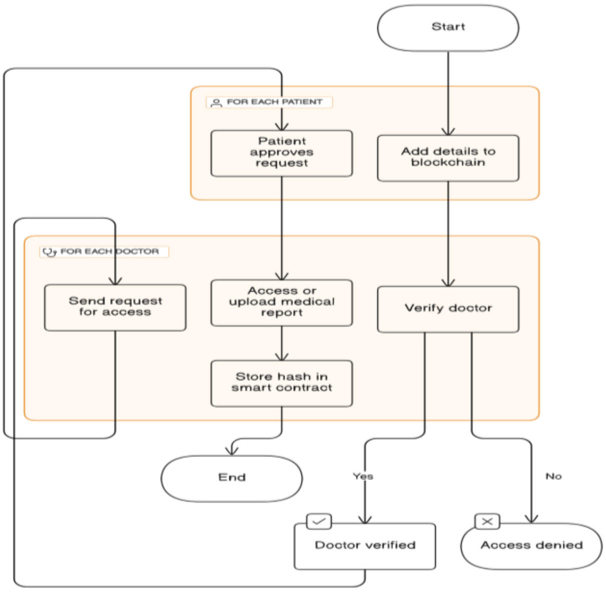

Figure 3 *- Healthcare Blockchain System*

D. Patient Approval:

The patient receives a notification of the access request. The patient reviews the request and decides whether to approve or deny if approved, the doctor gains access to the patient's medical records.

E. Medical Record Access:

Upon approval, the doctor accesses the patient's medical records stored on IPFS. The doctor can view existing records or upload new medical reports.

F. Hash Calculation and Storage:

After accessing or uploading medical records, the system calculates the hash value of the records. The hash value is stored in a smart contract on the blockchain in an encrypted form.

G. Confirmation:

Both the doctor and the patient receive confirmation of the successful access/upload of medical records. Any changes to the records trigger a new hash calculation and update in the smart contract.

H. End of Session:

Once the doctor completes the medical examination or consultation, the session ends.The doctor no longer has access to the patient's records unless a new access request is made for future visits.

VIII. CONCLUSION

With this approach, the robust security of blockchain technology can be used to challenge the present EHR system, providing a more advanced, yet economically viable, option. Patients will be able to access and manage their data completely, and they will also be able to provide access to several individuals, which will enhance data security. The existing centralized middlemen can be totally replaced by a distributed access and validation system that is created using blockchain technology and a platform designed to securely store and exchange electronic health records. This will solve numerous issues with the present Electronic Health Record (EHR) systems, including data leaks, data fragmentation, and unauthorized access to patient information. Many business issues can be solved by empowering users and digitizing health records.

ACKNOWLEDGMENT

The completion of this work has been made possible through the concerted efforts of many individuals and organizations to whom we extend our heartfelt gratitude. First and foremost, we would like to express our deepest appreciation to our supervisors whose guidance, encouragement, and invaluable insights have been instrumental in shaping this research endeavor. Their expertise and unwavering support have been a constant source of inspiration throughout this project. We are indebted to the faculty of Computer Engineering Department of Vasantdada Patil Pratishthan's College of Engineering, whose contributions and dedication to academic excellence have provided us with a conducive learning environment and ample resources to pursue our research goals. Our sincere thanks go to all participants and volunteers who generously contributed their time and expertise to this study, without whom this research would not have been possible.

REFERENCES

[1] DD-Locker: Blockchain-based Decentralized Personal Document Locker Jai Singhal, et. al. International Conference on Information Networking (ICOIN), 2022.

[2] Blockchain Private File Storage-Sharing Method Based on IPFS. Peng Kang, et. al. Italian National Conference on Sensors, 2022.

[3] HealChain: A Decentralized Data Management System for Mobile Healthcare Using Consortium Blockchain Weiquan Ni, et. al. Chinese Control Conference (CCC), 2019

[4] MediChain: A Secure Decentralized Medical Data Asset Management System Sara Rouhani, et. al. IEEE International Conference on Internet of Things, 2018

[5] Yujin Han, Yawei Zhang, Sten H. Vermund, ”Blockchain Technology for Electronic Health Records”, November 2022.

[6] Liat Wasserman, Yair Wasserman,”Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)”, August 2022.

[7] Shivansh Kumar, Aman Kumar Bharti, Ruhul Amin, “Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions”, April 2021.

[8] Deven McGraw,Kenneth D. Mandl, “Privacy protections to encourage use of health-relevant digital data in a learning health system”, January 2021.

[9] Yuxin Huang, Ben Wang and Yinggui Wang, “Research and Application of Smart Contract Based on Ethereum Blockchain”, IOP Publishing Ltd, November 2020.

[10] Rizwan Majeed, Nurul Azma Abdullah, Imran Ashraf, Yousaf BinZikria, Muhammad Faheem Mushtaq, Muhammad Umer, “An Intelligent, Secure, and Smart Home Automation System”, Research Gate, October 2020.

[11] Kumar R, Tripathi R., “A secure and distributed framework for sharing COVID-19 patient reports using consortium Blockchain and IPFS.”, IEEE, 2020.

[12] Kadam S, Motwani D., “Blockchain Based e-Healthcare Record System. International Conference on Image Processing and CapsuleNetworks”, Springer, Cham, 2020.

[13] Ni W. et al., “HealChain: a decentralized data management system for Mobile healthcare using consortium Blockchain”, IEEE, 2019.

[14] Vitalik Buterin, “Ethereum: A Next-Generation Smart Contract andDecentralized Application Platform”, Google Scholar, January 2014. Catherine Quantin, Gouenou Coatrieux, Maniane Fassa, Vincent Breton, David-Olivier Jaquet-Chiffelle, “Centralised versus Decentralised Management of Patients’ Medical Records”, Google scholar, 2009.