International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Electronic Health Records (EHR) storage using blockchain

Jintal Roy[1], Devesh Salke[2], Sudarshan Sangale[3], Prof. Deepali Maste [4]

[1,2,3]*Students, Dept of Information Technology Engineering, Atharva College of Engineering*
[4]*Prof, Dept of Information Technology Engineering, Atharva College of Engineering*

Abstract - *This paper discusses electronic health record (EHR) systems for storing patient information, which includes medical reports. Electronic health records (EHRs) are patient health records that are saved digitally and shared across a network. EHR systems have proven to be quite advantageous in the healthcare sector since they allow for the effective storage of patient data without the use of pen and paper. Although EHR systems have proven extremely valuable, the methods for storing records have been extremely insecure. Hospitals and other organizations, rather than patients, have complete control over electronic health record (EHR) systems, which makes seeking medical advice from other hospitals or doctors more difficult. The current mechanism for keeping patient information is extremely reliant on the organization's servers. The data can be easily hacked, and the central authority in charge of such systems could misuse it. Furthermore, patients don't even have ready access to the data, and sharing it with other healthcare practitioners is challenging. As a result, EHR systems encounter challenges in terms of data security, integrity, and administration. However, blockchain has the potential to solve these problems. Several industries have taken advantage of blockchain's capabilities. Similarly, blockchain's security, privacy, confidentiality, and decentralization can tremendously help the healthcare sector. We offer a solution that could be used to integrate blockchain technology into healthcare systems to store electronic health records (EHRs). Furthermore, our approach addresses the scalability issue that blockchain technology has in general through the use of off-chain storage. This system provides the EHR system with the advantages of a blockchain-based solution that is scalable, secure, and integrated.*

Key Words: **Electronic Health Record (EHR), Blockchain, Off-chain storage, Security, Decentralization**

1. INTRODUCTION

EHR (Electronic Health Record) systems offer several benefits. They are concerned, however, about the security of medical records, user data ownership, data integrity, and other issues. Implementing a game-changing technology such as blockchain could be the answer to these problems. This technology offers the ability to create a secure and safe platform for keeping medical records and other health-related information. Before the emergence of contemporary technology, the healthcare business relied on a paper-based approach to retain medical records, namely handwritten processes. This inefficient, insecure, and unorganized paper-based medical record system had to go. Because all of the facilities where patients visited had several copies of their medical information, it also had to cope with data duplication and redundancy. In the healthcare industry, EHR systems, which were designed to combine paper-based and electronic medical records, gained popularity. EHR systems have been placed in several hospitals throughout the world due to the benefits they provide, including better security and cost-effectiveness. They are regarded as a crucial part of the healthcare business because they provide a great deal of functionality [1]. Although the purpose of EHR systems in hospitals and healthcare was to improve care quality, these systems had several flaws and fell short of expectations [2]. EHR systems were found to have difficulties such as being unreliable and lacking in user-friendliness in research conducted in Finland to learn about nursing staff's experiences with EHRs [3]. The EHR system faces difficulties such as interoperability, information asymmetry, and data breaches. This paper proposes a system for developing a decentralized platform that would store patients' medical records and provide access to clinicians and other interested parties, such as patients. We also wish to address the blockchain's scalability problem, as storage of enormous amounts of data are not in the blockchain's architecture. As a result, we'd use an off-chain scaling approach by storing the data on the underlying medium to solve the scalability problem. Furthermore, our proposed research intends to address the above-mentioned information asymmetry and data breach vulnerabilities in the EHR system.

2. TECHNICAL DEFINITION

2.1 Blockchain

It's a distributed ledger system that can record transactions between two parties efficiently and decisively [4]. Each transaction is saved on a record called a block, and these blocks are then linked together using cryptography to form a list or blockchain [5]. Each block in a blockchain network comprises transaction data, a cryptographic hash, the hash of the preceding block, and a timestamp. The blockchain is built in such a way that it cannot be tampered with [6]. There has been a boom in interest in blockchain technology and its possible uses since the technology's inception in 2008. The lack of centralized authority in Blockchain technology provides security, transparency, and data integrity without intervention from third-party organizations overseeing

transactions, and so gives motivating options for doing research in a range of sectors [7]. Because the blockchain is a decentralized, distributed ledger system that keeps track of transactions across several computers, any changes to the data will influence all following blocks. This allows the blockchain's participants to authenticate transactions independently and fairly. A blockchain database is created independently via a peer-to-peer network. The majority of the network's consensus confirms them. The blockchain could be built in such a way that it facilitates processing. With the use of a blockchain, double-spending is also eliminated. Blockchains were formerly largely utilized as a distributed ledger for cryptocurrencies, but the technology has since grown and is now employed across a wide range of businesses [8]. Blockchain technology is used to record transactions in the majority of cryptocurrencies, including bitcoin. Furthermore, smart contracts based on the blockchain can be constructed that can be performed or enforced partially or completely without the need for human interaction. The engineers who design a blockchain network build smart contracts for that blockchain network [9]. When a set of specified requirements and conditions are met, these programs are automatically launched. They're useful in business partnerships, where they're used to impose a contract between the participants so that the network's members may be confident in the conclusion without the involvement of a third party. Blockchain technology is known for its security, decentralization, and transparency. This is what sets it apart as a cutting-edge solution for completing transaction activities safely and easily.

2.2 Consensus Algorithm

Each block added to the blockchain goes through a process of obtaining confirmation from all other nodes on the network that the node being added is authorized. A consensus algorithm is used to complete this operation. They aid in the development of participant trust and network reliability. PoW (Proof of Work), PBFT (Practical Byzantine Fault Tolerance), and PoS (Proof of Stake) are some of the most commonly used consensus algorithms.

2.3 Block

Blockchains are decentralized applications made up of a number of blocks connected in a peer-to-peer network. In the headers of these blocks, there are hashes of previous blocks. Data, the current block's hash, and the previous block's hash make up a block. Depending on the blockchain type, the data could be anything. The SHA-256 cryptographic technique is used to uniquely identify each block on the chain in the hashes of these blocks.

2.4 Interplanetary File System (IPFS)

IPFS is a data storage protocol that employs a peer-to-peer network. It provides secure data storage since IPFS data is shielded from tampering. It employs a cryptographic identification to safeguard data from tampering, as any effort to alter data saved on IPFS can only be accomplished by changing the identifier. A cryptographically generated hash value is included in every data file stored on IPFS. It is one-of-a-kind and is used to identify IPFS-stored data files. IPFS protocol's safe storage technique makes it a good alternative for storing crucial and sensitive data. To reduce the computing processes on the blockchain, the created cryptographic hash could be stored on the decentralized application. Thus, the IPFS protocol functions as follows:

- IPFS files have a unique cryptographic hash allocated to them.
- On the IPFS network, duplicate files are not permitted.
- A network node stores the node's content and index information.

3. FEATURES OF BLOCKCHAIN TECHNOLOGY

3.1 Privacy and Security

Cryptographic functions are used by blockchain technology to provide security to the nodes connected to its network. The hashes stored on the blocks are hashed using the SHA-256 cryptographic algorithm. The Secure Hashing Algorithm (SHA) creates hashes that provide security to the blockchain by ensuring data integrity.

Cryptographic hashes are one-way strong functions that generate checksums for digital data that can't be extracted. As a result, blockchain is a decentralized platform secured by cryptographic approaches, making it a viable option for protecting the privacy of certain applications.

3.2 Decentralization

Information in a blockchain system is spread across the network rather than being stored in a single location. This also allows for information control to be spread and handled by consensus obtained through shared input from the network's nodes. This makes a blockchain system decentralized.

3.3 Transparency

A trust-based connection between entities is required to achieve data transparency in any system. The data or record in question needs to be safe and secure. Any data recorded on the blockchain is spread across the network

rather than being concentrated in a single location and controlled by a single node. Data ownership has now been shared, making it more transparent and secure against third-party interference.

4. DRAWBACKS OF BLOCKCHAIN TECHNOLOGY

4.1 Scalability and Confidentiality

Confidentiality and scalability are two major issues that arise when data is stored on the blockchain. The data on the blockchain is exposed to everyone on the network, making it susceptible, which is not what a decentralized platform should be. Patient medical history, records, lab results, X-ray reports, MRI results, and many other reports would be maintained on the blockchain, and this enormous data would have a significant impact on the blockchain's storage capacity as all the nodes have a copy of the data.

4.2 Lack of universal standards

There is no established standard for this technology because it is still in its early stages and is constantly evolving. As a result, using this technology in the healthcare sector will take longer and require more effort. As recognized standards from international agencies who oversee the standardization process of any technology would be required. These uniform standards will aid in determining the size, format, and type of data that can be kept on the blockchain. Furthermore, the stated standards would make it easier to adopt this technology because they could be easily enforced within enterprises.

5. PROPOSED SOLUTION

As we saw above, traditional Electronic Health Record (EHR) systems have their fair share of flaws. To encounter these issues, we will build a web-based application that can be used by both doctors and patients to safely and effectively store all the patient's past ailments and diagnoses without the fear of data tampering or data loss. Also, the data won't be stored directly on the blockchain, instead whenever the doctor will put any ailment and it's the diagnosis the data will be stored on the IPFS network which is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. The hash that will be unique to that data will be stored on the blockchain so we can easily scale our blockchain system. We will use solidity to write the smart contracts for our application and also make use of different JavaScript libraries like web3.js and jQuery in our application. So, our application will have these features as follows:

It is a blockchain-based web app for doctors and patients.

- The patient can register using their name and age along with their metamask wallet which acts as their identifier. Once registered the patient can see their previous health records, share them and also choose from all the doctors to permit them to edit new records.

- The doctor can register using their name along with their metamask wallet which acts as their identifier. Once registered the doctor will be able to edit new records of the patient that has permitted them to edit their profile.

- Once the doctor edits a record their permission will be revoked, also the patient can manually revoke permission to access.

6. WORKFLOW OF THE SYSTEM

So, we will use Ganache (Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development) which acts as a local blockchain network on our computer. So, we code our application using Solidity for smart contracts and JavaScript for the core logic of the application. The code for connecting to the IPFS network, and sending and receiving data is all written in these files. After completing our application, we need to compile our smart contracts and then deploy them on our local blockchain network i.e., Ganache. We then start our application; we have already imported ganache accounts in our metamask wallet which will be used to mimic 'Patients' and 'Doctors' of our application. So, we select an account and name that 'Patient1' and we register our account on the application, similarly we register another account and name that 'Doctor1'.

- **Patient**: - So as soon as the patient opens their profile, they can see a dashboard where they can request for their old medical records to be shown (which uses IPFS behind the scenes). They can select from all the list of doctors registered on the application from whom they want to get a treatment and then allow them access to edit their profile i.e., edit the ailment and its diagnosis. They can also see the list of doctors they have already given permission to and if needed can revoke their permission.

- **Doctor**: -When a doctor opens their account, they will be able to see all the patients that have given them access to their profile, the doctors can see the past medical records of the patient to better diagnose the patients and then edit the current disease and diagnosis. As soon as they submit the data their access will be revoked.

7. USER INTERFACE

The user interface has mainly three pages

- **Home Page**: - This is the landing page from which users can log in/register to their respective accounts.
- **Patient Page**: - The patient will have a dashboard at the top from which they will be able to get their records from the IPFS network. The second dashboard will help them to choose from all the lists of doctors to permit them to edit their records. The third dashboard allows them to see the list of doctors to whom they have already given permission.
- **Doctor Page**: - The doctor will be able to see the list of patients that have allowed them to view and edit their profiles. The doctor can click from the patient list and view their past record and then edit more new records.

Fig 1: - Login Page

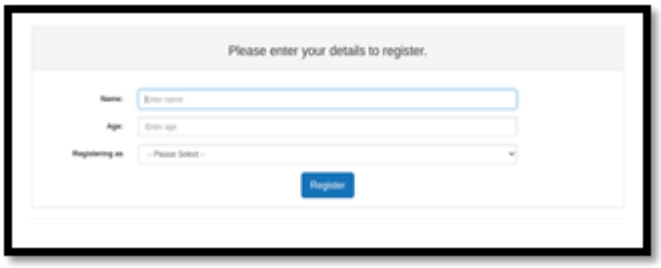

Fig 2: - Registration Page

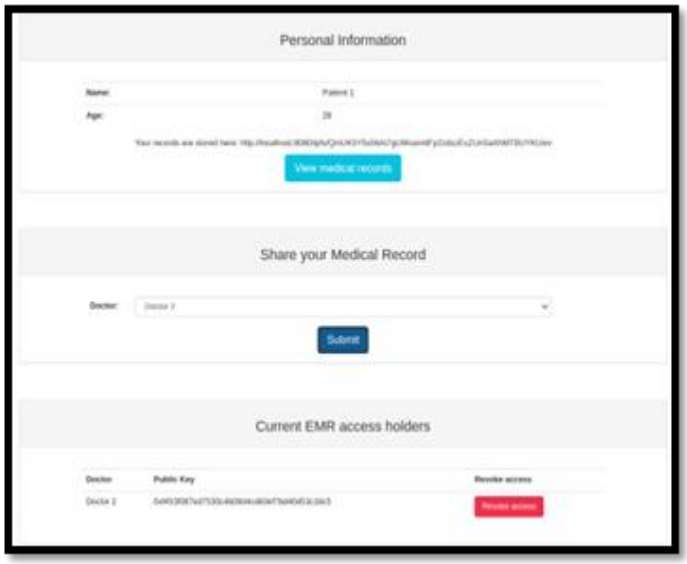

Fig 3: -Patient UI

Fig 4: - Patient's Past Records

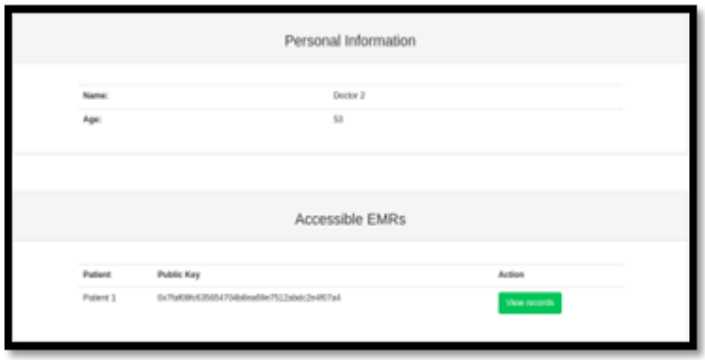

Fig 5: - Doctor UI

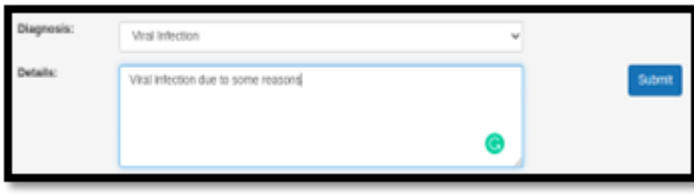

Fig 6: - Doctor editing patient's diagnosis

8. CONCLUSIONS & FUTURE SCOPE

So, we created a blockchain-based application that can be used by doctors, patients, and other organizations to safely store patients' health data without the fear of data loss or tampering. We also tackled the problems of scalability by using off-chain storage making our application much more scalable. Even though we have quite a lot of advantages of this it can still be improved a lot in the future. We can add support for different types of files like PDFs, X-Ray images, etc. We can encrypt the data so that even if someone gets hold of that data, they won't be able to use it or decrypt it.

REFERENCES

1. Q. Gan and Q. Cao, "Adoption of electronic health record system: Multiple theoretical perspectives", *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, pp. 2716-2724, Jan. 2014. [1]
2. M. Hochman, "Electronic health records: A "Quadruple win" a "quadruple failure", *J. Gen. Int. Med.*, vol. 33, pp. 397-399, Apr. 2018. [2]
3. T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen, et al., "Experienced time pressure and stress: Electronic health records usability and information technology competence play a role", *BMC Med. Inform. Decis. Making*, vol. 19, no. 1, pp. 160, Aug. 2019. [3]
4. "The great chain of being sure about things", *The Economist*, 2019. [4]
5. M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaram, *Blockchain Technology*. 2019. [5]
6. G. Karame, S. Capkun, Blockchain Security and Privacy, IEEE Security & Privacy, 16 (4) (2018), pp. 11-12. [6]
7. J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where Is Current Research on Blockchain Technology? —A Systematic Review, PLOS ONE, 11 (10) (2016), p. e0163477. [7]
8. Aoyagi and D. Adachi, "Fundamental Values of Cryptocurrencies and Blockchain Technology", *SSRN Electronic Journal*, 2018. [8]
9. "Smart contract", *En.wikipedia.org*, 2019. [9]