Grenze International Journal of Engineering and Technology, June Issue

A Blockchain-Based Approach to Eliminating Fraudulent Healthcare Record Activities

Megha Jain[1], Yogita Sharma[2], Omveer Yadav[3] and Smriti[4]
[1-4]JSS Academy of Technical Education, Noida
Email: meghajain12@gmail.com,sharmayogita962@gmail.com, omyadav16081999@gmail.com,22smriti05@gmail.com

***Abstract*— The Electronic Health Record (EHR) systems provide health information about patients. Data security, integrity, and management of EHR are a crucial problem. Records can be modified and altered by different stockholders as the different users may be using it in more than one form. Medical records management is a suitable application for blockchain-enabled records that can be stored, track, and manage all the transactions to prevent fraudulent activities. A novel framework has been presented here in the healthcare sector by using the blockchain concept. The major goal of this article is to implement Blockchain for electronic health records (EHR) and its decentralized approach eliminated the chance of a single point of failure which in turn makes the system robust. The Proposed work also covers the extensible problem faced by Blockchain in common with the help of an off-chain repository of the data. The results indicate the computing much more secure and free from a scam in comparison to the traditional health record system. Finally, the proposed approach suggests scenarios such as in EHR where the introduced approach should prove adequate.**

***Keywords*: Blockchain, decentralization, consensus, scalability, smart contract, Firebase,Solidity and Ethereum**

I. INTRODUCTION

The Blockchain technology was basically tailor-made for keeping a distributive financial ledger but the Blockchain paradigm can be generalized to make a decentralized ledger to store information of any specific domain. The transactions between what is referred as the singleton state-machine are secured by cryptography. Whenever a new data entry is made the node encodes the logic thus, validating it before uploading it to the Blockchain. The Blockchain technology-based ledgers used for storing data is primarily based on the use of "smart contracts" which allows automation and tracking of data related characteristics such as, Viewership Records new data entries[1].

The viewership and ownership permissions are shared through the peer-to-peer network, accessible to the private members. The smart contracts available on the Ethereum framework for Blockchain, we define the relationships between two entities and also formulate the viewing instructions and data retrieval permissions for them to be available for external databases. Through this system patients can choose and allow the sharing of their medical data among trusted providers, whereas providers are capable of adding new entries related to patient. All these data transactions are secured by adding a cryptographic hash of the record on the blockchain ensuring data integrity. Thus, validating and keeping the users indulged in the evolution of the data making it more secure[2] The traditional patient records require a large number of human work-hours. For instance, suppose a patient

Grenze ID: 01.GIJET.9.2.377

visits a clinic or a hospital, now his/her documents must be found and then transported to the required department, and then the actual examination of the patient can start. Besides, the high chances of mishandling of the patient record files also exist. Fig1 shows the traditional medical record system.

Fig 1: Traditional Medical Record System

The medical care industry, specifically, frequently has been a significant objective for data robbery as prosperity records consistently contain private information like the names, government upheld retirement numbers, and addresses of patients. Through blockchain, everyrecord is protected with a unique blockchain ID that not only protects the records but also makes them easily accessible to the authorized personnel only. In the healthcare industry, doctors and their helpers receive with decentralized blockchain system, they have control over their patients' credentials and can simply check their histories.

II. Related Study

To make the foundation frameworks straightforward, a systematic literature review has been done in many areas. A summary of a detailed review of major research works in direction of various approaches toward health care management is presented below.

A. Health Care Approach

Various approaches toward health care management have been suggested by researchers. Uddin *et al.* discuss the increased usage of the Internet of Things (IoT) in the day-to-day life of human beings has also led to the concept of Remote Patient Monitoring, a Patient- Centric Agent using the blockchain technology is commendable.

Agbo *et al.*[3] worked extensively on the research paper Blockchain Technology in Healthcare: security because the data of healthcare of a patient not only contains the records of his or her health and treatments but also personal information like contact address, contact number, and other sensitive information such as social security number.

Matthias Mettler and MA [4]studied the different areas and various fields where Blockchain can be used and how it can be used in other non-financial sectors. The major areas in which Blockchain can be implemented successfully are the areas of Smart Healthcare Systems, to fight the counterfeit drugs in pharmaceutical companies, for digitally signing of emails as well as contracts of legal purposes. The use of Blockchain helped the companies which were already existed in storing and transferring the data more quickly and securely without any third-party intervention.

Ramani *et al.* [5]discussed in the field of healthcare record Securing and efficient data accessibility by using blockchain technology. Blockchain as a decentralized and circulated innovation can assume a key function in giving such medical care administrations. Smart contract and ethereum platform maintain authenticity, security, and prevent data alteration.

Vora *et al.*[6] proposed BHEEM: A Blockchain approach-based system for Securingmedical records in 2018. Blockchain innovation settles the plans dealing with the security of EHRs which have brought about information being commonly unavailable to patients. They have proposed a Blockchain framework gives secure and data access to health records by patients, doctors, and outsiders while securing the patient private data.

B. Healthcare Care Information System

Electronic medical records (EMRs) meet the opposition to converse patient’s privacy and share healthcare medical records among researchers when they need it. El-Yafouri and Klieb [7]discussed the software

technologies in the medical sector using EMRAM, a HIMSS modelfor considerate the effect on organizations approving HIS and explain different types oflevels of adoption. Saranummi[8] explains the Electronic Health Record (EHR) and the Personal Health Record (PHR). The information within a health Care Delivery Organization (CDO), the second recording the medical record of an individual, is owned by the patients themselves. Swan discusses safety and security features. The power to ensure identity develops opportunities for holding abstract assets such as medical records. This opens theway for the user to declare data stored within the system. Data transformation from Computerized Patient Records (CPR) to CPR across many CDOs to the Personal Health Record (PHR) where an identity would be used to get health records for patients from the system. HIPAA use as a standard for security measures in place for the storage and use of the medical record. Blockchain, together with current control systems, databases, and security enables us to build next-generation information systems that can securely manage health records across the network while ensuring transparency and scalability of the medical records[9].

III. Proposed Methodology

The most prominent things to be kept in mind while designing and developing new technologies to carry out the same task is evidently, transparency and accessibility of medicalhistory data to the patients while keeping the economic feasibility in mind. Moreover, patients will have to be convinced about the confidentiality of their information which is mandatory for them to indulge in the process with full disclosure[10].
The new technology should definitely consider adding exceptions cases while providing information to the patients as not every data can be transferred to patients, for example psychotherapy notes or therapist's personal information. Not only maintenance of these records will be time consuming, the patients involved hardly care enough to take out their time to indulge in the process. These sections, when combined, would keep our structure running. Fig.2 shows the Blockchain-based Medical Service System Framework.

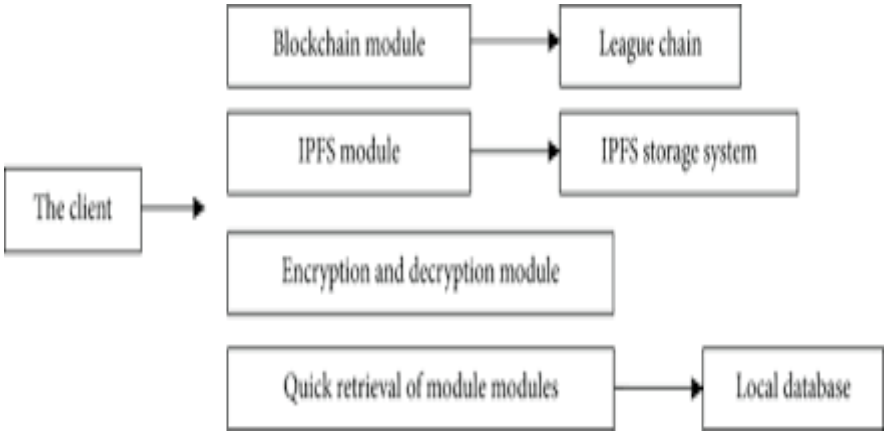

Fig. 2: System Design of Blockchain-based Medical Service Framework

A. Client

Doctors, users, and staff are examples of users. A user has many features and tasks on the system, such as interacting with the system and performing simple task operations such as create, read, delete, update, and so on, which allows him to be identified on the system. Users can access system functions via the GUI (Graphical User Interface), and they can communicate with the blockchain layer via the GUI[11].

B. Blockchain Module

The blockchain layer is the next layer on the framework; this is the middle layer of the framework that contains code for user communication with DApps that are running on the blockchain. This layer contains three modules.

1. *Ethereum***:** Ethereum was officially presented in 2015 and Ethereum is to make a smart contracts platform that could hold the component of software systems. This framework utilizes its own digital money known as Ethers. Digital money could be utilized for accessing it between accounts associated with Ethereum. Ethereum gives the software engineers a language where they make the blockchain system, thislanguage is Solidity
2. *Ethereum Virtual Machine (EVM):* Ethereum systems offer to incorporate the programming in the blockchain. It gives the user to make their applications working on Ethereum. The applications

manufactured utilizing this system is known as Distributed Applications (DApps). They contain various rules that make a system for Distributed Applications (DApps). The applications based on smart contracts areexecuted on EVM[12].

3. *IPFS Interplanetary File System (IPFS):* IPFS gives secure information stored on IPFS and is secure from any modification. All the medical records on IPFS contain a hashing value that is produced cryptographically. It is utilized for an ID to store information on the IPFS. The working of IPFS protocol is done in a simpler manner first file record on IPFS is allocated hash, replication of documents does not permit to exist on the IPFS, and a block of the system record index and file data of the block.

IV. IMPLEMENTATION

After the system has been planned in detail, the next stage is to move the system into a functioning one. For this, various interfaces can be created which will then be linked with the backend. On the backend there can be numerous tools used so as to ensure maximum correctness as well as enhanced security[13].

The new technology should definitely consider adding exceptions cases while providing information to the patients as not every data can be transferred to patients, for example psychotherapy notes or therapist's personal information. The updating and removal of erroneously added data hence becomes impossible. This causes both patients and medical institutions to deal with compromised data and in a fractured manner. The health records need to be cohesive, whereas this method of data storing results in fragmented manner. One major cause can be the strategically barriers between the various medical institutions and Healthcare centers. Thus, a patient trying to retrieve his/her past medical treatment data is often hurdled by the economic incentive involved. Recent investigation shows that IT developers providing information exchanging interface charge exorbitant prices making it even more impractical as shown in FIG 3.

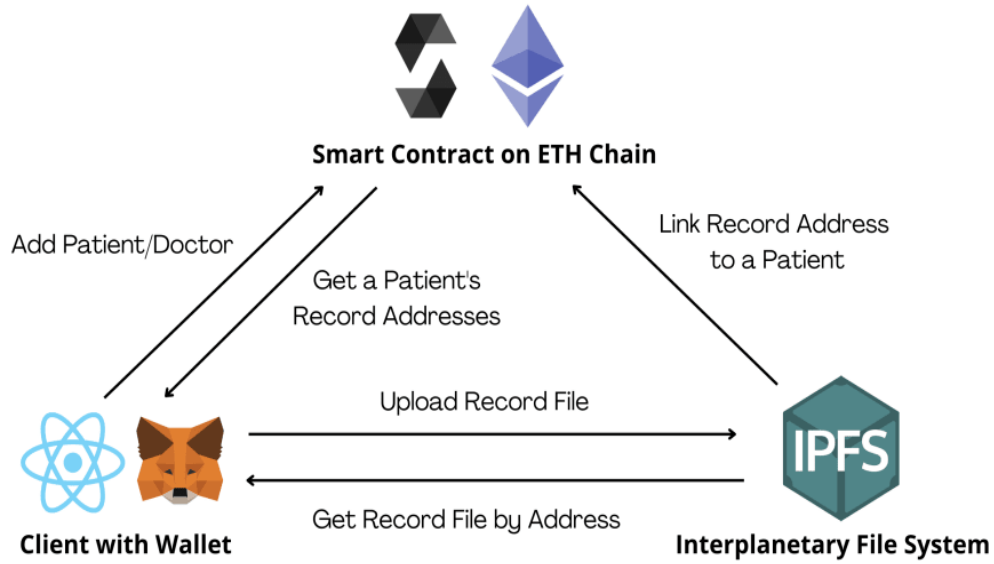

FIG 3: Admin and User Interaction with DApp

The doctor generates a request to acquire a medical-health-record of a patient, through which the doctor requests to fetch information about the patient's medical record from the database. After generating the request, we verify the doctor's identity. User being authenticated is referred to as requester and the user whose authentication is being conducted is referred to as verifier. Acquiring the patient record according to the doctor's request is the phase during which the patient's record is retrieved from the database[14]. The next step is to generate new diagnosis data to be shown to the doctor. Encryption of the medical-health-record is the final phase where the medical-health-record which will be sent is encrypted[15].

The patient then verifies the credibility of the Doctor and also gets access to the previous feedbacks from other patients for the same doctor to make an informed decision. The newly created user can also create a password to prevent unauthorized access to his/her data as well as the Blockchain in general through his/her user interface. The encryption for the newly created record is carried out[16].

V. PERFORMANCE EVALUATION

Here ethereum is used to implement purposed framework and the time between block is 10- 19 seconds. Block time means the time to generate a new Block. In Ethereum we have a gas limit instead of the block size. The add user record function takes around one or two minutes and it depends on the size of the data and the show user record function takes 50 sec approximately and the time taken for a transaction to be confirmed is 38 sec[17].
Working of the algorithm in terms of size of transactions is described below.

- No. of node/ hour (average) = 31473 and No. of transactions/hour (average) = 269
- Mean transaction per node = (No. of node/ hour (average)) / No.of transactions/hour(average) =31473/269 =117
- Mean transaction size = node size/mean transaction per node =21.6 KB/117 =0.19KB

So, calculations show that Average transaction size is approximately 0.2KB.
Configuration used for testing the performance is mainly in a system consisting of 8 GB memory with 64-bit Windows OS version 10 along with Intel Core i7-6498DU CPU @ 2.50 GHz processor. The programming language used by Ethereum is Solidity which encapsulates JavaScript and python.
The framework was put under test for performance mitigation on by using the followingconfigurations:

- Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHz processor
- And 8.00 GB of memory with Windows 64-bit OS (version 10)

For the evaluation process, the transaction data was collected in two forms mainly, i.e. transaction deployment time and transaction completion time. Thereafter the metrics was used which involved entities such as execution time, throughput and latency.
Latency is the delay in the time taken by the system for execution. Mainly latency period is the difference between the time of deployment and completion.

VI. CONCLUSION

During the transfer of information between various parties, the design of the security of medical records for any EHR system remains a significant issue. A new extension that uses the blockchain approach to protect medical records is described in this chapter. EHR plan andassurance of the integrity of all records are provided by this new strategy. Using Blockchain, a framework has been developed to create a secure, distributed, and decentralized platform for medical records. This method helps to monitor medical professionals' lack of transparencyand restricts access to the EHR system to the appropriate number of users. We focused on making the data in health records more secure, which opens up new research avenues for meeting other security requirements. For critical application deployment for any medical purpose, other security models that are more general, cater to the need for health datasecurity, and identify the untrusted hosts will be useful in future work. This would help us avoid fraudulent activities as well as save time when computing. The proposed work will be beneficial to a number of new application areas for implementing transparency toward patients, medical professionals, and related fields.

REFERENCE

[1] "Xtelligent Media Editorial Approach."
[2] M. Jain, D. Pandey, and K. K. Sharma, "A Granular Approach to Secure the Privacy of electronic Health Records Through Blockchain Technology," Int. J. Distrib. Syst. Technol., vol. 13, no. 8, 2022, doi: 10.4018/IJDST.307899.
[3] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," Healthcare, vol. 7, no. 2, p. 56, 2019, doi: 10.3390/healthcare7020056.
[4] R. Tonelli, IEEE Computer Society, Institute of Electrical and Electronics Engineers, and E. IEEE International Conference on Software Analysis, IWBOSE '19 : 2019 IEEE 2nd International Workshop on Blockchain Oriented Software Engineering (IWBOSE '19) : February 24, 2019, Hangzhou, China. .
[5] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," 2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018, pp. 1–7, 2018, doi: 10.1109/HealthCom.2018.8531136.
[6] 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," Sustain. Cities Soc., vol. 39, pp. 283–297, May 2018, doi: 10.1016/j.scs.2018.02.014.
[7] R. El-Yafouri and L. Klieb, "Electronic medical records adoption and use: Understanding the barriers and the levels of adoption for physicians in the USA," 2014 IEEE 16th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2014, pp. 506–512, 2014, doi: 10.1109/HealthCom.2014.7001894.

[8] N. Saranummi, “In the Spotlight: Health Information Systems,” IEEE Rev. Biomed. Eng., vol. 1, pp. 15–17, 2008, doi: 10.1109/RBME.2008.2008217.
[9] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135. Academic Press, pp. 62–75, Jun. 01, 2019, doi: 10.1016/j.jnca.2019.02.027.
[10] M. Jain, D. Pandey, and K. K. Sharma, “A Granular Access-Based Blockchain System to Prevent Fraudulent Activities in Medical Health Records,” Lect. Notes Data Eng. Commun. Technol., vol. 106, pp. 635–645, 2022, doi: 10.1007/978-981-16-8403-6_58.
[11] M. Jain, D. Pandey, and K. K. Sharma, “A blockchain approach on security of health records for children suffering from dyslexia during pandemic COVID-19,” Artif. Intell. Mach. Learn. Ment. Heal. Pandemics A Comput. Approach, pp. 343–363, 2022, doi: 10.1016/B978-0-323-91196-2.00004-1.
[12] M. jain, S. Kaswan, and D. Pandey, “A Blockchain based Fund Management Scheme for Financial Transactions in NGOs,” Recent Patents Eng., vol. 16, no. 2, pp. 1–14, 2021, doi: 10.2174/1872212115666210615155447.
[13] “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.”
[14] A. A. Monrat, O. Schelén, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” IEEE Access, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.
[15] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” Futur. Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.
[16] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, “Blockchain Technology Use Cases in Healthcare,” in Advances in Computers, vol. 111, Academic Press Inc., 2018, pp. 1–41.
[17] A. Shahnaz, U. Qamar, and A. Khalid, “Using Blockchain for Electronic Health Records,” IEEE Access, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.