2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) | 979-8-3503-4842-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICETET-SIP58143.2023.10151658

2023 11th International Conference on Emerging Trends in Engineering &
Technology - Signal and Information Processing (ICETET - SIP)

Decentralized Medical Healthcare Record Management System Using Blockchain

Bhavik Bhandari[1]
Information Technology
G H Raisoni College of Engineering
Nagpur, India
bhandari_bhavik.it@ghrce.raisoni.net

Prof.Rupali Vairagade[2]
Assistant Professor
G H Raisoni College of Engineering
Nagpur, India
rupali.vairagade@raisoni.net

Himanshu Trivedi[3]
Information Technology
G H Raisoni College of Engineering
Nagpur, India
trivedi_himanshu.it@ghrce.raisoni.net

Harshal Thakre[4]
Information Technology
G H Raisoni College of Engineering
Nagpur, India
thakre_harshal.it@ghrce.raisoni.net

Gunjan Indurkar[5]
Information Technology
G H Raisoni College of Engineering
Nagpur, India
indurkar_gunjan.it@ghrce.raisoni.net

Ajit Yadav[6]
Information Technology
G H Raisoni College of Engineering
Nagpur, India
yadav_ajit.it@ghrce.raisoni.net

Abstract The possibilities and benefit of using distributed ledger technology for storing and protecting patient medical information is greatest in the health care industry, which is one of the primary industries in this regard. Blockchain technology is being used by several companies. Inorder to protect the security and privacy of its people' personally identifiable information and to promote the use of blockchain technology, the Government of India (GoI) is eager to digitize. Using the Ethereum blockchain, we provide a solution in this study for the safe keeping of patient medical records (PMR).Our solution provides secure and hasslefree access, storage, and patient medical record sharing. We have developed the front end as well as the back end of our project using TypeScript and Next UI. Users need to register themselves if they are visiting for the first time. The information shared by the user will be stored entirely in our backend applications. We have used the IPFS file system for storing and accessing files on the internet. IPFS is a file system that helps to create a permanent and decentralized method for storing and accessing files. First, a user will upload his or her document, and the document will be uploaded to the Inter Planetary File System (IPFS). Once the document is uploaded, a unique hash is returned, which is also known as a CID (content identifier). This is used to uniquely identify the uploaded file on IPFS. Then, that CID is stored in the blockchain as a private variable, so not everyone can access it. When someone can access it, we will specify the conditions.

Keywords: PMR, IPFS, and Patient Medical Record

1. INTRODUCTION

Including a patient's medical history, clinical findings, diagnostic test results, pre- and post- operative care, health improvement, and prescriptions, a patient's medical record (PMR) is a historical record of their health information. Using the details in a patient's medical record, a medical professional may comprehend the patient's current status and offer effective therapy. Healthcare providers or other medical experts are [9-10] responsible for creating, updating, and maintaining these records. The patient's medical treatment is at its most crucial point during this time. Patient monitoring, medical research and audit, statistical analysis, insurance claims, and criminal proceedings are a few instances when it's important to retain accurate medical records. The PMR is crucial for determining the patient's health status, but it also contains a ton of sensitive personal information that needs to be kept secret and discreet. Due to storage problems, access restrictions, privacy difficulties, and security challenges, managing medical records can be difficult. Hospitals that use manual and paper-based medical record systems commonly run into issues with managing active and inactive records, deleting data, and other issues. The Online Registration System (ORS), a cloud-based program, and the nation's inhabitants of the e-hospital were established [12-14]. As part of the MeitY's Digital India project to deliver healthcare services to all of the people of India.

This demonstrates the importance of, the need for, and the lack of a system for digitizing medical records and healthcare services among healthcare providers. Even though a copy of the record should be provided to the patient upon request, the healthcare provider is typically in responsible of maintaining the record. Different laws apply differently in different nations to the ownership and upkeep of PMRs. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, a federal legislation in the United States, was created to secure sensitive patient health information, even though the information in a medical record belongs to the patient.

979-8-3503-4842-2/23/$31.00 ©2023 IEEE

The organization in charge of keeping the record is the one that legally owns the physical version of it. Patients can ask the healthcare practitioner to update inaccurate information if they discover any errors in the record. According to the Indian Medical Council (IMC) Regulations, 2002, medical professionals are obligated to keep patient medical records for at least three years. Details about the patient must also be kept private, particularly information about their personal and family situations. Medical professionals are required to offer access to medical records within 72 hours after receiving a request from a patient or authorized legal personnel.

If a doctor is determined to have committed professional fraud, their name may be temporarily or permanently deleted from the list of practitioners with licenses.

In a blockchain ledger, each block is a container that is cryptographically linked to every other block, much like a linked list in a data structure.

Blockchain technology is a distributed ledger and decentralized computing platform that enables rational decision- making among many actors in an open and public system to successfully maintain transactions in an immutable method. Digital rights management (DRM), the Internet of Things (IoT), supply chain management, identity management, and even the healthcare industry for insurance coverage and securely storing medical information have all found considerable usage of blockchain, the primary technology behind cryptocurrencies, By implementing blockchain technology for healthcare record keeping, it may be possible to distribute PMR data more easily and avoid purposeful and inadvertent manipulation with PMR data. Similar to a distributed healthcare blockchain network, accessing, retrieving and updating the independent private medical record (also known as PMR) at actual time requires the permission, understanding and his/her sanction of the individual candidate (patient/person) [9-13].

2. RELATED WORKS

In this part, we make references to and give an overview of works on the management of medical records using blockchain technology.

The majority of the study focuses on defining patient data accessibility and hospital-to-hospital communication of medical records. The patient's medical records are readily accessible to both the patient and the treating physician thanks to MedRec, which is a very significant and robust electronic medical record storage system that is ultimately powered by the Ethereum blockchain. By granting access to aggregate and anonymized medical data, it encourages medical researchers and healthcare professionals.

The Proof of Authority (PoA)-based incentive model put forth by Medchain encourages generic practitioners and healthcare professionals to build, validate, and attach new blocks with timedbased smart contracts to regulate transactions and restrict access to patient records. Smart contracts and proxy re-encryption are used in Anclie, a privacy- preserving and interoperable healthcare record solution built on Ethereum, allowing for greater access control, data obscuration, and security. Similar to this, the MedBloc project makes use of a smart contract and a permissioned blockchain to offer an access control system and privacy-preserving scheme design. Madine et al. suggested using smart contracts built on the Ethereum blockchain to offer patients control over their PHR. It also makes use of Inter Planetary File Systems (IPFS), which use trustworthy reputation-based re-encryption oracles, to store and distribute patient medical records in a secure manner.

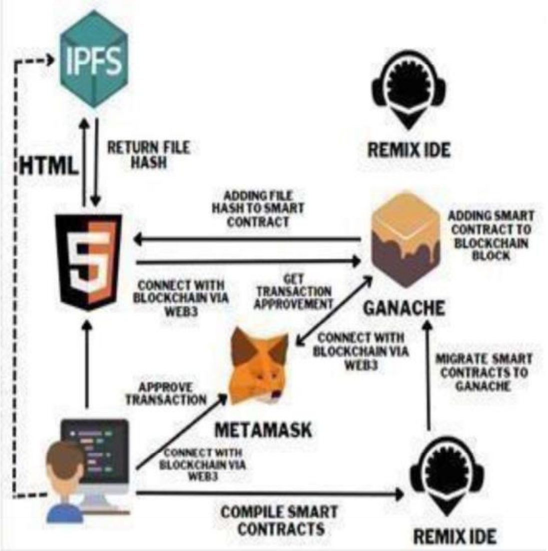
IPFS
HTML
RETURN FILE HASH
REMIX IDE
ADDING FILE HASH TO SMART CONTRACT
ADDING SMART CONTRACT TO BLOCKCHAIN BLOCK
5
CONNECT WITH BLOCKCHAIN VIA WEB3
GET TRANSACTION APPROVEMENT
GANACHE
CONNECT WITH BLOCKCHAIN VIA WEB3
MIGRATE SMART CONTRACTS TO GANACHE
APPROVE TRANSACTION
METAMASK
CONNECT WITH BLOCKCHAIN VIA WEB3
COMPILE SMART CONTRACTS
REMIX IDE

Figure 1: Software requirement of Proposed System

Blockchain: A distributed ledger can execute smart contract. They record references for health transactions like examination, appointment and medications. This is also used in crypto currency transfer. We have a block that contains private information. This block has a reference pointer to the complete health information about the patient. Assume we have some patient A, and he is examined by some doctor B. So the things will go like, some transaction will be sent to B from A after which B can see the information from A. This information would be easily accessible by B. This information can also be stored on cloud services like Dropbox, Amazon Cloud (AWS), Heroku, Google Cloud but as we are using blockchain technology, so we will use the IPFS.

Wallets: Wallets are the software which usually store the keys of users. This contains public and private keys. Wallets are required to transfer minimum gas fees to smart contracts so that contracts can be deployed on test networks. This is capable enough to show user information after getting deployed. This is capable of listing all the services offered to patient X in the listing format. IPFS can be used for implementing this. Services offered by ledger includes the following: Storing a transaction, Accessing and processing requests and Registration of all transactions for which access is granted.

Smart contracts: A smart contract is a code fragment deployed on the blockchain that need the consent of multiple parties basically two or more parties. They we recreated and are conducted outon top of the blockchain.If the prerequisites are satisfied, they run automatically. To construct smart contracts, we used the Solidity programming language. Each stakeholder is recognized, as well as a specific smart contract governs how they allcommunicate with one another. Smart contracts are supported only on the Ethereum blockchain. Smart contract codes are translated into EVM (Ethereum Virtual Machine) byte code and then deployed to EVM.

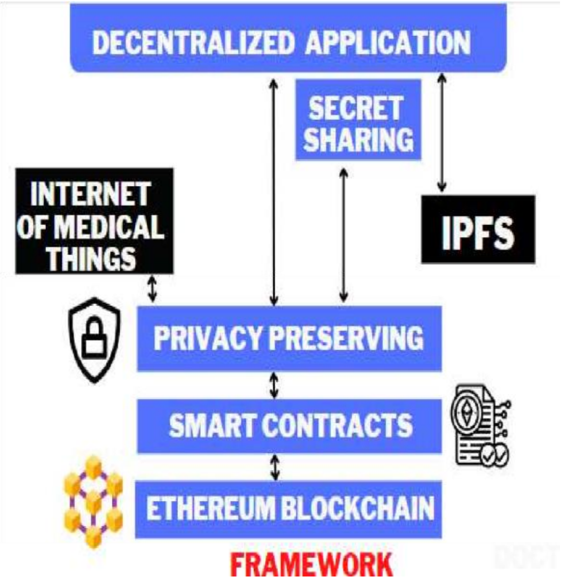

Figure 2: Blockchain Framework

The components listed below are used in the framework mentioned above:

Decentralized Applications: Dapps are applications that are built on distributed platforms with trust distributed among their users and are completely open-source. This means that they are designed to avoid single points of failure and are also more transparent and accountable than existing applications. And further, simply because atraditional app runs on a single network of computers and a dApp runs on top of a decentralized peer-to- peer network, over which no single entity has complete control, it will perform its function even if a single node is online in the network. (D-Apps) are applications with smart contracts built into the user interface.

They are used by hospital medical personnel to register patients and note their medical conditions, and by patients to evaluate their healthcare data. D-Apps are developed using the Ethereum blockchain, Solidity, and JavaScript.

Inter Planetary File System (IPFS): The Inter Planetary File System (IPFS), a distributed file system with content addressing, can be used to store and exchange data. Each file that is saved is given a distinct identifier using a cryptographic hash value [14]. On the blockchain, the hash value of large medical records like lab and diagnostic reports is utilised to refer to them. These documents are securely kept in a private IPFS.

Ethereum: A second-generation blockchain platform called Ethereum uses a special Virtual Machine called the EVM to execute blockchain transactions and enables smart contracts. ETH stands for the Ethereum blockchain's native currency. There is a cost associated with every activity, which is measured in terms of gas. We created our proposed framework and implemented it on the Ethereum-Ropsten
Testnet.

The main requirement for this project is user should have a metamask account and should have crypto in the account. This model only works when the crypto are sent to the account.

Also user must be familiar with web3 working though it's safe but user need to have proper understanding of the model because small mistake in private key can cause transferring crypto in wrong account which may result in financial loss.

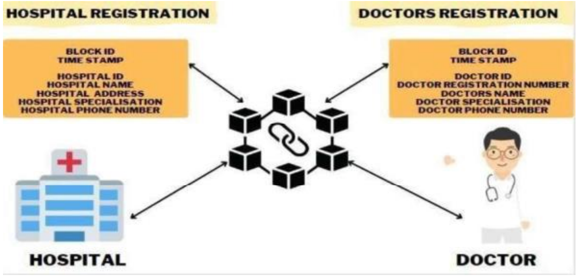

Figure 3: Blockchain Proposed system Architecture

In this project we have used Ganache to carry out the transactions. Ganache provides ten accounts with fake ethers which can be used for development and testing projects.

This is our proposed system in which we will have two entities hospital and doctor. A user needs to register himself on the portal then there will be admin and patient. User can access the name of hospital by using hospital id. Also the name, address of hospital would be present. Doctor can have its own unique id along with registration number, name, specialization and phone no. The user need to have a metamask account from which the ethers can be shared to portal so that the records can be saved and accesed from the portal.

3. WORKING OF SYSTEM

The system is a distributed, decentralized, blockchain-based system for managing medical records. The system is based on securely and efficiently storing the patients' electronic health records, giving them better access to and control over their records, and enabling simple and secure sharing of the records with physicians, clinics, hospitals, or insurance companies. The website consists of vivid sections for signing in or signing up for new users (patients) as well as doctors. In blockchain, the information is stored in the form of blocks, where each block has its own hash (the hash of the forward block) and a particular set of distinct data stored in it. In simple terms, all the blocks are connected with each other, and they together form a chain-like structure. So once the user (patient) or doctor is finished with finishing the prequisites, the information of that individual is stored in a specific distinct block. The first block that is created is called the Genesis Block. Once the first person deploys the smart contract, that information will go into the genesis block. The data that is stored in the blocks will be reflected (updated) in all the peer-to- peer connected networks in the IPFS data storage, and the peers will validate whether the information is all correct and ethically moral or not to add (update) into the blockchain.

Once the validation is done, the changes will be reflected on all the peer networks. The record will be stored in an encrypted format, and the hash of the record has been returned by the IPFS database. Once the hash of the record is returned, we store that particular hash in an encrypted format on the blockchain contract using the SHA (Secure Hash Algorithm) 256 encryption method.SHA-256 uses a cryptographic (one-way) hash function.

We are using our project on the Goerli test net. It isa test network on the Ethereum blockchain, which will ultimately allow us to test our smart contracts on the Ethereum blockchain by using the test ethers. After this step, the next thing is to connect the smart contracts with the Metamask wallet. In order to run our smart contracts, we need a minimum amount of gas, which we transfer from our Metamask to smart contracts. All this transaction will be registered on the ether scan.

Key management helps to protect the records and can also be used to back them up, store them, organise them, and limit their access by third parties. Keys fall under cryptography. This involves encryption and decryption of public and private keys. Public key can be shared with everyone in order to grant access or receive crypto whereas private keys should be only known by account holder because if the private key is known to any unauthorized person then he can easily transfer the ethers. So this technique is used in our project. When the user will login he would be having his public key to login. This will be checked by server and when validated then he can login.

This all things are done in Remix Ide. Remix Ide supports the Solidity programming language to write smart contracts and deploy them on the test net. We have two options for connecting our smart contracts to the blockchain network in order to deploy them. First is metamask and another is Ganache. Ganache is specially used for testing projects by transferring test ethers. Same things can be done metamask but in order to transfer ether in metamask we need to mine them and it takes hours to mine. So we have kept both options. In our project, patients can interact with multiple doctors, i.e., records can be shared with multiple doctors, and it helps patients manage their time.

4. RESULT

We've spoken about how secure management of electronic health records is essential, as well as how blockchain technology could be able to help with the current problems. We also studied the different blockchain-based frameworks and solutions. We have presented a framework built on the Ethereum Blockchain that would allow patients to manage and own their medical information while preserving their privacy. This framework would do this through anonymous sharing and effective storage using distributed storage systems like IPFS. The accuracy, consistency, completeness, and non-redundancy of PMR data will be ensured by the suggested design, in our opinion, over the course of the data's life cycle. We are able to prevent data leaks and safeguard user records thanks to this effort. Additionally, the items are centralized, making it easier for both patients and hospitals to operate. The solution may be improved ina variety of ways to produce an application that is suitable for production. There are still issues to be resolved before medical records can be adequately secured, despite the fact that blockchain and fabric currently offer a lot of protection by design. Despite the fact that the fabric framework is already extensively pluggable, the source code may be changed to make the solution more adaptable when adding more hospitals and their peers. In order to accommodate the amount of new peers and organizations joining the channel as the network expands, transaction requests and approvals, numerous ordering peers are required.

5. CONCLUSION

In this project, we looked at the need for efficient administration of electronic health records and the potential applications of blockchain technology to some of the problems that are currently being encountered. We also looked at more blockchain- based frameworks and solutions. In our architecture, which is built on the Ethereum Blockchain, patients will be able to own and own their medical records while maintaining their privacy through anonymous sharing and practical storage using distributed storage systems like IPFS.The proposed design, in our opinion, will make surethat PMR data is reliable, consistent, comprehensive, and nonredundant over its entire life cycle.

6. REFERENCES

1. Minu M. and Ramaguru R.Terminologies used in blockchain. Lab for the NamChain Open Initiative (2021). https://github.com/NamChain-Open-Initiative-Research-Lab/Blockchain-Terminologies
2. Samal D. and Arul R. (2020) A Creative Blockchain-Based Scheme for Internet of Things Privacy Preservation. International Conference on Communication, Computing, and Electronics Systems, edited by Bindhu, Chen, and Tavares. Vol. 637 of Lecture Notes in Electrical Engineering Singapore's Springer. https://doi.org/10.1007/978-981-15-2612-1 66
3. Blockchain Framework for Social Media DRM Based on Secret Sharing, by Kripa M., Nidhin Mahesh A., Ramaguru R., and Amritha P.P., 2021. In: Joshi A., Senjyu T., Mahalle P.N., Perumal T. (eds) Technology for Information and Communication for Intelligent Systems. ICTIS 2020. Systems and Technologies for Smart Innovation, volume 195. Singapore's Springer. https://doi.org/10.1007/978-981-15-7078-0 43.
4. "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25–30;

Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Using Blockchain for Medical Data Access and Permission Management.", doi: 10.1109/OBD.2016.11.

5. Alex Roehrs, Cristiano André da Costa, and Rodrigo da Rosa Righi, "OmniPHR: A distributed architectural paradigm to integrate personal health data," Journal of Biomedical Informatics, volume 71, issue 1, pages 70–81, ISSN 1532-0464, doi:10.1016/j.jbi.2017.05.012
6. Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella, and Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities and Society, Volume 39, 2018; Pages 283-297; ISSN 2210-6707; DOI: 10.1016/j.scs.2018.02.014.
7. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, pp. 594-601, doi: 10.1109/TrustCom/BigDataSE.2019.00085. J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. Tu, "MedBloc: A Blockchain-.
8. "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," E. Daraghmi, Y. Daraghmi, and S. Yuan, IEEE Access, vol. 7, no. 16, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.
9. Rupali Vairagade: Vairagade, R.S. and SH, powered IoT networks. Transactions on Emerging Telecommunications Technologies, 33(4), p.e4.
10. Rupali Vairagade: Vairagade, R.S. and Savadatti Hanumantha, B., 2022. Secure Concurrency and Computation: Practice and Experience, 34(21), p.e7057.
11. Rupali Vairagade: Vairagade, R., Bitla, L., Judge, H.H., Dharpude, S.D. and Kekatpure, S.S., 2022, April. Proposal on NFT Minter for Blockchain-based Art-Work Trading System. In 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 571-576). IEEE.
12. Rupali Vairagade: Vairagade, R.S. and Brahmananda, S.H., 2020, April. Secured Multi-Tier Mutual Authentication Protocol for Secure IoT System. In 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 195-200). IEEE.
13. Rupali Vairagade: Prof. Dr. Brahmananda S H, R. S. V. (2020). A Comprehensive Analysis of the significance of Blockchain and AI for IoT Security. International Journal of Advanced Science and Technology, 29(3), 5542-5553.Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/6 120