A Framework for Secure Storage and Sharing of Electronic Health Records using Blockchain Technology

Anurag Gharat[1,*], *Pratik* Aher[2,**], *Punit* Chaudhari[3,***], and *Bhavana* Alte[4,****]

[1]Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India

Abstract. Public Healthcare issues have been the main focus of any governing body for the last decade. Each day a large amount of Healthcare data is generated by individual and Medical Organizations. This information is considered highly sensitive and private, which needed to be securely stored and protected against unauthorized access. In a traditional system, all the data is stored in a centralized system which comes with lots of drawbacks. This where blockchain technology comes in because of its Peer-To-Peer nature and Security. Several studies highlight the importance of blockchain and how it can be implemented in Electronic Medical Record(EMR) systems which face problems regarding privacy,security,decentralization and confidentiality.In this paper, We explain how blockchain technology may be utilised to improve EMR systems and how it could be a solution to these problems. We offer a framework for implementing blockchain technology in the healthcare industry for EMR.The aim of our proposed framework is first to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover,this framework provides the EHR system with the benefits of a blockchain-based solution that is scalable, secure, and integrated.

1 Introduction

The worldwide Electronic Wellbeing Record (EHR) market is developing drastically and expected to reach ""39.7 billion by 2022[8]. To shield the security and protection of EHR, access control is a fundamental instrument for overseeing EHR information. Electronic clinical records (EMRs) are computerized records of patient's clinical history, medicines, actual assessments, medical problems, and so forth This data is viewed as profoundly delicate and private, which should be safely put away and secured against unapproved access. The medical care area confronted a pattern shift towards moving the current paper and archive based wellbeing record the board framework to advanced EHR frameworks that were intended to oversee electronic clinical records (EMR)[9]. These frameworks were utilized to store clinical notes and the research facility brings about its various parts. They were proposed to upgrade the well-being part of the patients by forestalling mistakes and expanding data access. The objective of EHR frameworks was to take care of the issues looked at by the paper-based medical care records and to give a productive framework that would change the condition of the medical care area. Even though utilization of EHR frameworks in the medical clinics or medical services was to improve the nature of medical services, these frameworks dealt with specific issues and didn't meet the assumptions related to them. These frameworks were hackable, information from such unified frameworks was effortlessly spilt and altered. Additionally, while this happened the proprietor had no admittance to it likewise had no clue about where his information is shared and who is utilizing it. Such frameworks couldn't give the proprietor the force and control to deal with his records. Utilizing a Blockchain controlled HIE can beat every one of the disadvantages of conventional HIE frameworks. While electronic health information exchange cannot replace provider-patient communication, it can greatly improve the completeness of patient's records, (which can have a big effect on care), as past history, current medications and other information is jointly reviewed during visits[11]. Also, appropriate and timely sharing of medical records will improve the decision-making process of Healthcare workers and also result in 1. Proper Medication 2. Avoid Medication Errors 3. Improved Security 4.Quality of Treatment. Such a system will benefit the patients by providing them with complete control of their data. He can add his records, update them and can grant access to anyone he wants to. He will have no limitation on the kind of data that has to be submitted. He can upload any format of data, whether an image, scanned prescription or a text-based brief history. Research and Analysis is another sector that can make use of such a platform effectively. They can request access for data from the owner through classified ways and as the data is always maintained by users themselves, the Analyst will always get true data that is always up to date. As all these transactions related to data will be logged directly on Blockchain,

*e-mail: anuraggharat55@gmail.com
**e-mail: ahe.pratik.17ce1014@gmail.com
***e-mail: punit.chau20@gmail.com
****e-mail: bhavana.alte@rait.ac.in

they will serve as hard and solid proof in future operations. A D-app (Decentralized App) based interface is implemented which utilizes Ethereum based blockchain. The addition of a new user to the Blockchain takes place through met mask ID. The user and doctor authentication along with other non-sensitive data are stored on a MongoDB cloud database. The D-app interacts with the Blockchain by adding a new Patient record, adding a new Healthcare worker in the access list and revoking access from the healthcare worker when the user wants. For the scope of our project, the Blockchain is tested on a local test net and the patient's medical records are stored on secure off-chain storage. In our case, we use InterPlanetary File System which is a peer-to-peer network for storing and sharing data in a distributed file system. Ganache is used to get Ethereum accounts pre-funded with ether for testing purposes. Metamask is a Chrome Plugin used to access the D-app. Ganache, Metamask and Ethereum are integrated using Truffle Framework. Proof of Work (POW) is a consensus algorithm used and SHA-256 hashing is used for creating transaction hashes. The Blockchain logic is written in Solidity programming language and tested on Remix IDE.

The remainder of this paper is arranged as follows. Section 2 will highlight our motivation while working on this project. We present related work and blockchain-based EHR studies in section 3. Section 4 is subdivided into our proposed work and the methodology we have used. In section 5, we present our system design. Results and the final output is described in section 6. In section 7, we have mentioned the conclusion and future work. Finally, we added the references in the last section.

2 MOTIVATION

Improve Transferability: Many patients have to change their doctors frequently due to conflicting schedules and high demand for doctors. Thus if all patients previous EMR are available his transfer from one doctor to another becomes easier.

Help Genuine Patients: Many impersonators use EMR records of unsuspecting patients for insurance frauds. This leads to genuine people not benefiting from insurance policies. Thus it will ensure that genuine people get benefits.

Improve Security: Blockchain renders records untameable due to hashing and thus it increases the security of records.

Ownership: The Healthcare provider can only access a patient's medical data with his consent. Hence the patient can be assured that his sensitive information cannot be accessed by any unknown entity.

Improve Healthcare: There have been so many cases where a patient receives an improper treatment, because of the old stale data that resides on a database which no one cares to update. In our approach, the healthcare worker will get a complete updated copy of data along with medical history.

3 RELATED WORK

The study of literature contains different principles and techniques from research papers that are used in system development. The study undertaken for the implementation of the intended framework involves an overview of different current applications and research papers. Such papers are being reviewed and analysed as part of the project's study survey.

3.1 A. Existing Systems

Zhang et al.[1] have given an analysis about which metrics and parameters should be considered while developing Blockchain Healthcare based Decentralized apps. They evaluated these metrics based on domain and technical perspectives.

Kumar et al.[2] mentioned the key requirements and challenges faced by Healthcare systems having Blockchains. They have also listed the applications in which Blockchain could be used.

Faisal Jamil et al.[3] proposed a way to store data on blocks for monitoring purpose. Data is directly stored in blocks in this approach.

Shahnaz et al.[4] mentions usage of IPFS in blockchain for maintaining records. Their proposed system works on role based architecture where a administrator assigns roles to users.

Vora et al.[5] have proposed system with combination of privacy preserving schemes. Here encryption of patients private data stored on Blockchain.

S. Ali et al.[6] proposed work is on permissioned blockchain . The paper highlights various areas in healthcare that can be benefitted with the use of Blockchain. The proposed methodology used DHT (Distributed Hash Tables) for access stored records on Blockchain.

Ehab Zaghoul et al.[7] has listed all the use cases of Blockchain in Healthcare. The paper presents ideas how using an offchain storage can be cost efficient. The paper compares all approaches in designing blockchain on cost basis.

4 PROPOSED APPROACH

4.1 Proposed Work

The Electronic Medical Records Management System will be built on public Blockchain platform Ethereum. It will be built with Truffle web framework which compiles the smart contracts and injects them into the Web App. All the users would necessarily have a Metamask account, which can be created using a installable chrome plugin. The Metamask plugin will allow us to connect to local Ethereum network and provide us account address to sign transactions. All the transaction fees will be paid using Metamask account. As our system is developed on a local test network it uses ganache for users account prefunded with 100 ethers. A New user can sign up on the blockchain using his Metamask Account. The D-APP is built on

MERN Stack. The entire front-end is developed using React and Backend is managed by Node-Express server. All the profile details which are non-sensitive will be stored on a MongoDB database. Once the successfully logs inside the D-APP he can upload his/her medical records in form of images. During upload process he will be needed to sign the transactions using his private key. The user documents are uploaded on an Off-chain storage securely. IPFS (Inter Planetary File System), a distributed file system, is used as an Off-chain storage. Once the records are uploaded on IPFS we store the hash of address of the stored documents on blocks of blockchain. So every time a new block is added on the blockchain, the IPFS hash of the record will be stored on the blockchain rather than the data. Hence, using this technique we reduce the space needed on blocks, which ultimately reduces the cost of every transaction.

4.2 Proposed Methodology

The EMR management system consists of three main parts:

1. IPFS (Inter Planetary File System): IPFS is a distributed system for storing and accessing files, websites, applications, and data. IPFS is a file sharing system that can be leveraged to more efficiently store and share large files. It relies on cryptographic hashes that can easily be stored on a blockchain. In IPFS, instead of addressing the content by the server it is stored on, it is address by the content itself from the nearby peer. This is necessary, if sensitive or personal data needs to be shared.

2. Smart Contracts: Smart contracts are actually similar to business contracts, all things considered. From Blockchain viewpoint, They add rationale to the Blockchain. Smart contracts are self-executing contracts containing the terms and states of an understanding among peers. The terms and states of the understanding are composed into code. The Smart contracts executes on the Ethereum blockchain's decentralized stage. The arrangements work with the trading of cash, offers, property, or any resource. In Layman terms, Smart contract is basically a program that runs on the Ethereum blockchain. It's an assortment of code (its capacities) and information (its express) that dwells at a particular location on the Ethereum blockchain. In our proposed procedure, Smart contract are utilized to transfer records, award admittance to medical care specialist to see your records just as repudiate access from medical care laborer..

3. Proof of Work (PoW): Proof of Work is a kind of consensus algorithm. As the name says for approving/validating an exchange a node ought to openly demonstrate that it did a specific measure of work. In Blockchain, this calculation is utilized to affirm exchanges and produce new squares to the chain. With POW, excavators go up against one another to finish exchanges on the arrange and get remunerated. Ethereum, as Bitcoin, at present uses an agreement convention called Proof-of-work (POW). This permits the hubs of the Ethereum organization to concede to the condition of all data recorded on the Ethereum blockchain, and forestalls specific sorts of financial attacks.

5 SYSTEM DESIGN

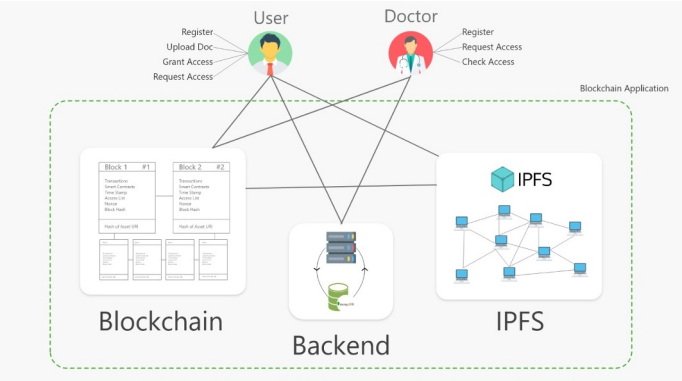

Figure 1. System Design

As shown in figure 1, doctors and patients act as entities or nodes in this blockchain network. Both the entities have their own login and signup pages. All their authentication details are processed on Node-Express server and then sent to MongoDB Cloud Database. Figure 2, shows the flow diagram for user and Figure 3 shows the flow diagram for doctors.

• The Patient User will need a Ethereum account using Metamask plugin to be a part of the Blockchain.

• Once done he can visit the signup page and enter his personal details and credentials. After passing all the authentication checks he must login into his profile.

• Once logged in he can upload his records in image format to the blockchain. For uploading he must pay some ethers in order to complete the transaction.

• There are several subpages created in user profile such as:

Dashboard: The dashboard will display all the records the user has uploaded till now.

Profile page: This page shows all his personal details mentioned during signup process.

Doctors Page: This page displays a list of all doctors who are a part of Blockchain. Here he can grant access to anyone after checking his profile.

Requests Page: This page has all the requests sent by doctors to access his medical records. He can either delete these requests or accept them.

Access List Page: This page mentions the list of all the Doctors that have access to view his records. He can revoke their access from here.

• When the user uploads his record, the record is sent to IPFS network which in turn returns us hash of the uploaded asset. We store this hash on the blockchain along

with other necessary details.

• The doctor needs to go through the same procedure of signup and then signin, once he enters in his profile he will be able to see the records if the user has granted him the permission. Else the dashboard will be empty.

• He can go to users page and find the user whose records he wants to check. He can request a grant access from the user, his request will go through the server and will be sent to the specific users dashboard.

• If he has access he can view the records from his dashboard.

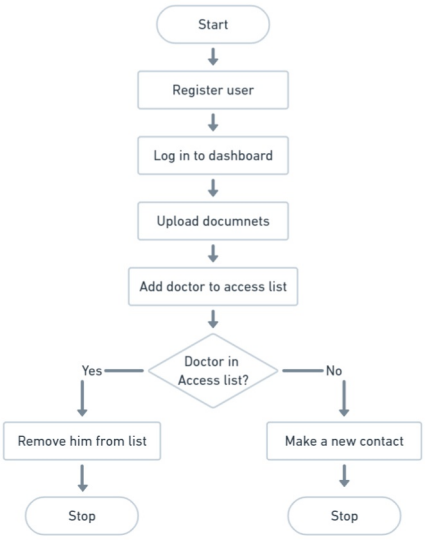

Figure 2. Flow Diagram for user

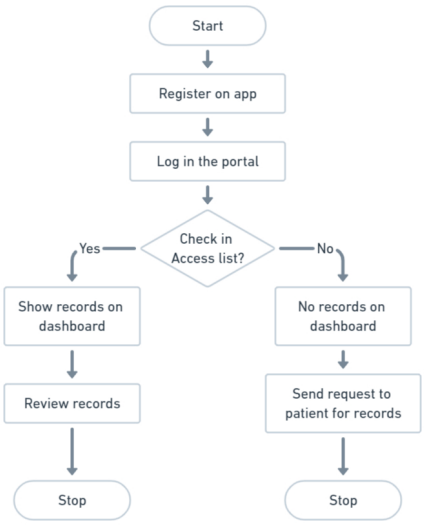

Figure 3. Flow Diagram for doctor

6 RESULTS

Figure 4 shows user dashboard where he can upload his reports as well as visit various sub-pages

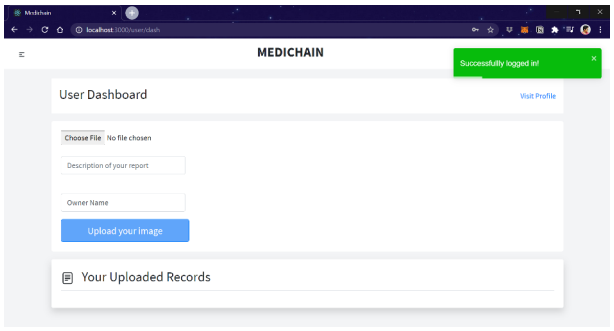

Figure 4. User Dashboard

User is uploading his record to IPFS and Blockchain is verifying the user by requesting his digital signature figure 5. The user pays some ethers to mine the block and save his record.

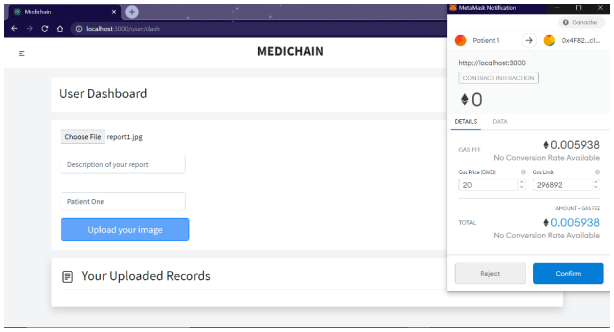

Figure 5. Transaction

Figure 6 shows how user provides Access to Doctor by checking his profile. While providing access he must sign the transaction using his private key for authenticity. Once done the doctors address will be added to user's access list.

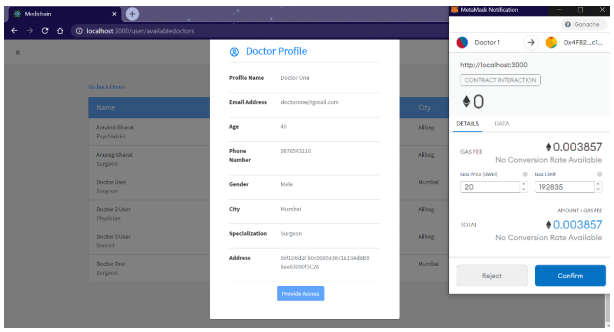

Figure 6. Providing Access to Doctor

On Figure 7 the user will have record of all the access provided by him along with timestamp. He can revoke access from any Doctor from here.

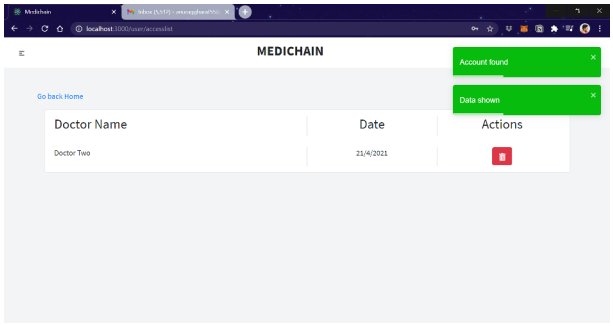

Figure 7. Access list

Figure 8 shows doctors dashboard where all the available records will be present. If he has no access, no records will be displayed.

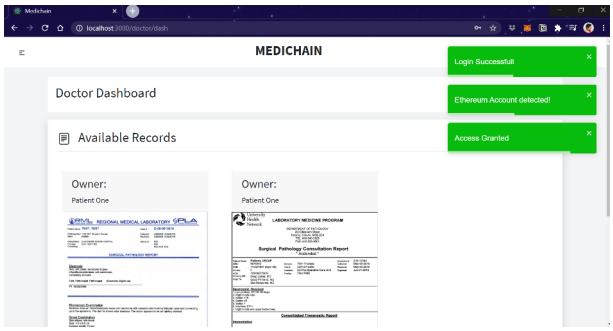

Figure 8. Doctors dashboard

The Doctor from his profile can visit user's profile and send him a request to access his records figure 9. These requests will be displayed on User's Dashboard which user can either accept or reject.

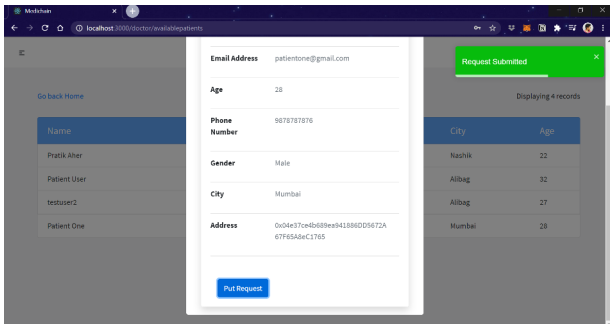

Figure 9. Patient's List

6.1 Result Analysis

Monetary Benefits: The cost of mining each block on a Blockchain is directly proportional to the content or variable data added on the block. Using the off-chain storage functionality to store images we were able to reduce the size of data added on blocks drastically, hence reducing the cost to mine each block.

Decentralization: The proposed Decentralized system has the power to overcome all the drawbacks that the traditional Centralized system possesses. Using Decentralization we are removing a central governing authority and distributing the trust among the peers of the network. Due to the secure nature of Blockchain, the chances of hacking or tampering is almost negligible.

Data Assets Sharing: Previously proposed systems displayed the sharing of only text-based data among the Blockchain peers. Whereas this implemented system allows to share and store asset-based records and data among peers. More types of data assets can be added in further versions.

User Authentication and other functionalities: All the studied Blockchain systems were more inclined towards using Blockchain and did not focus on other important aspects like - How will user Login to Portal?, How will the System flow work? How can he find suitable doctors? , How will the doctors request data? All these important aspects were studied and a suitable backend was added which would do all such tasks with ease. The Backend works as a supporting system to the Blockchain.

Record Ownership: One of the most important drawbacks of the Traditional System is handling the ownership of records. The proposed system provides the ownership of data in the hands of the user. The user himself is responsible to handle his data and maintain it instead of any other third party. Hence, reducing the risk of Illegal data leaks and sharing.

7 Conclusion and Future Work

Our current EMR management systems fails to maintain the secrecy and confidentiality of sensitive reports. With Blockchain based EMRs patients can play a more active role in the healthcare, and managing their medical and health data. This systems give individuals the complete control and hold on his/her personal data. As he no longer has to trust his Healthcare providers for keeping his data and there will be reduce in risk of sharing of data to untrusted parties. The proposed system succeeds in providing the power in the hands of the owner itself. Hence he can use, share and maintain his/her records as per his needs. It provides a far more superior ability to share and manage personal healthcare records than any traditional system. This system is scalable, hence adding new entities to the system is possible. Currently the system is deployed on localhost network using Ganache and Metamask. This is because our scope is limited to making a prototype of the real world system as deploying on the main Ethereum network requires real monetary transactions. But the system can be deployed on main network in future.

In future works we plan to add even more functionalities in the smart contracts like an Access Timer, Control on which documents to share, Edit/Update control to Doctors. Also the current system is limited to two entities namely Patients and Doctors. We plan to add more

entities like Pharmacist, Insurance Providers and Medical Researchers. The release of Hyperledger Fabric v.2.0 has opened a new scope for us to try similar approach using a Private Blockchain.

References

[1] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., Lenz, Metrics for assessing blockchain-based healthcare decentralized apps, (2017)

[2] Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M., Blockchain Utilization in Healthcare: Key Requirements and Challenges, (2018)

[3] Faisal Jamil, Shabir Ahmad , Naeem Iqbal and Do-Hyeun Kim, Towards a Remote Monitoring of Patient Vital Signs Based on IoTBased Blockchain Integrity Management Platforms in Smart Hospitals, (2020)

[4] Shahnaz, A., Qamar, U., Khalid, A.,Using Blockchain for Electronic Health Records., (2019)

[5] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat,S., Rodrigues, J.A blockchain-based framework for securing electronic health records., (2018)

[6] S. Ali, G. Wang, B. White and R. L. Cottrell, A Blockchain-Based Decentralized Data Storage and Access Framework for PingER, (2018)

[7] E. Zaghloul, T. Li, M. Mutka and J. Ren, d-MABE: Distributed Multilevel Attribute-Based EMR Management and Applications, (2020)

[8] TechSci Research, Global Electronic Health Records (EHR) Market (2020 to 2025), (2020)

[9] Peter Garrett, Joshua Seidman, EMR vs EHR – What is the Difference?, (2011)

[10] Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K, Security Aspects of Blockchain Technology Intended for Industrial Applications, (2021)

[11] Professor Wilkins, Electronic health information exchange, (2019)