IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

DAPP to Store Electronic Medical Health Records on Ethereum Blockchain and IPFS

D. B. Khadse[1], Uddesh Nikam[2], Nisha Mate[3]
Assistant Professor, Department of Computer Science and Engineering[1]
UG Students, Department of Computer Science and Engineering[2,3]
Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
dipakhadse@gmail.com[1], uddesh.nikam100@gmail.com[2], nishamate12@gmail.com[3]

Abstract: *In this digital world, information technology is growing day by day. Due to this, a large amount of data is generated every day from various domains, and one of the domains is medical health records. A large amount of medical data is generated every day. Such as electronic medical records, medical images, diagnostic reports, X-rays, MRI scans, etc. These medical records can help in treating a patient when needed and can be shared with different medical institutions. There are systems built that are used to store all the medical records of patients. But they are centralized and may not be secured, and a user may not know how and where these records are shared. However, if these medical records are leaked or shared with a third party, the owner of that medical record may not know how and where these medical records are used, thus sabotaging the patient's privacy. Therefore, controlling the access rights to medical data is an urgent issue. On the other hand, patients do not have any proper application that will help them store and view their history of medical records and have control over them. This project aims to build a decentralized application to store the medical records of patients on the Ethereum Blockchain and Inter Planetary File System (IPFS). This app will help users to keep electronic medical records in one place, and the user will have full control over their data. This app will help doctors diagnose the patients by seeing their medical history. This will also help researchers to research various diseases. This app will store the data of patients from doctors and pathology labs. Users will be able to control who can add the medical details and see them. They can give access and revoke it. This application will store the file in DICOM, JPEG, JPG, PNG, and PDF format. In this application, there is no centralized authority. This application is secured because of peer-to-peer and distributed networks, it is tamper-proof. User has control over their data. They can choose whom to share their data with, and blockchain is reliable.*

Keywords: Blockchain, IPFS, Electronic Medical Health Records, Decentralized Application

I. INTRODUCTION

1.1 Importance of Medical Health Records

The rapid development in the fields of information technology and medical science has made electronic medical records widely used for medical treatment and research purposes. A large amount of medical data is generated every day such as electronic medical images, diagnostic reports, X-rays, MRI scans, CT scans, etc. Medical data can be used to reflect the treatment situation of patients and share the treatment experience with other doctors, laboratories, and medical institutions. Electronic medical records or electronic health records are the digital collection of a patient's medical history, including diagnostic reports, medications, allergy reports, treatment plans, and lab test reports. EMRs typically contains medical images and patient information, such as physician name, personal statistics (e.g., age and weight), home monitoring device data, and other data processed by practitioners in a text format. Medical images and patient data are stored and maintained by different medical institutions, even when being related to the same patient.

1.2 Drawbacks of Centralized EMR Systems

Most medical institutions and hospitals store their patient's data locally in their data centres which require engineering, maintenance, and high security of data centre is very costly, and some of them do not have any backup storage system in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

case of system failures. It poses a threat of data loss, data corruption or stealing of data. Although many hospitals are migrating to cloud storage, the clouds have their threat vectors. In the past f years, many health care providers were hit by various ransomware attacks and DDoS attacks during the time of the COVID-19 pandemic. Due to these attacks, many healthcare services were halted, affecting many medical institutions and patients. There are such systems built that are used to store all the medical records of patients. But they are centralized and may not be secured, and the user may not know how and where the records are shared. However, once the shared medical data are leaked, the patient's privacy will be sabotaged. Therefore, controlling the access rights of patients' medical data is an urgent issue. On the other hand, patients do not have any proper application that will help them store and view their history of medical records and have control over them.

1.3 Damages due to Centralized EMR Systems

In the year 2015, an NPR report stated that organized criminals and their networks have a way of selling EMRs in the black market illegally. The cost of these records in the black market could go up to USD$40-50 per record. Between 2009 and 2020, nearly 3705 health care data breaches have been reported to HHS' Office for Civil Rights. Those breaches have resulted in theft, exposure, and disclosure of 268,189,693 healthcare records, which is equivalent to 81.72% of the population of the USA. In December 2020, these numbers nearly doubled. The below table shows some major medical data breach incidents recorded in the year 2020.

1.4 Decentralized EMR Systems

To overcome the drawbacks of traditional centralized electronic medical record systems and to assure interoperability by providing access to EMRs, while still protecting the data privacy, keeping the data anonymous and avoiding any kind of data misuse, Decentralized Electronic Medical Record System was developed. All the issues that are mentioned above concerning centralized EMR systems can be overcome by Blockchain technology along with the Inter Planetary File System (IPFS), which allows sharing the data in a decentralized manner, thus maintaining the privacy and accessibility of EMRs. These systems store the data by breaking it into smaller pieces and scattering those pieces of data across the entire decentralized network so that even if the data from one server is hacked, the hacker cannot read or steal the data. It also has a bigger advantage in that, even if one server is down, the other servers in the network will be continuously running, and data can be accessed any time, thus having no downtime. But still, systems that are built have some limitations.

II. AIM AND OBJECTIVES

2.1 Aim of the Project

The Aim of this project is to build a Decentralized Application to store the medical records of patients on the Ethereum Blockchain and IPFS. This app will help user to keep electronic medical records in one place and user will have full control over their data.

2.2 Objectives of the Project

The objective of the project is to build a web app (for doctor/pathology labs) and an android app (for patients) and store the medical records on the Ethereum blockchain and IPFS. Both applications will be connected to the IPFS and smart contract which will run on the Ethereum blockchain. With the help of the Ethereum blockchain and IPFS, healthcare data can be stored in a decentralized manner, and it will be immutable. With this, there will be no single point of entry for hackers to hack the data. This app will help doctors diagnose the patients by seeing their medical history. This will also help researchers research various diseases. This app will store the data of patients from doctors and pathology labs. Users will be able to control who can add the medical details and see them. They can give access and revoke it. This application will store the file in DICOM, JPEG, JPG, PNG, and PDF format. In this application, there is no centralized authority. Secured through a peer-to-peer and distributed network. It is tamper-proof. User has control over their data. They can choose whom to share their data with, and the blockchain is reliable.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

III. Literature Survey

In recent years, researchers have been developing a reliable and feasible solution for storing medical images in the field of health care. Current systems are deployed in the cloud and are centralized, which increases maintenance costs, storage space and also raises privacy concerns about sharing data over the public network. Therefore, it is important to develop a system to enable the storing and sharing of a large amount of medical data efficiently within a trustless environment. In the past few years, many doctors and health professionals have been unable to provide the level of care that they can provide. This is due to the unavailability of the history of medical records.

Recently, a platform for patient's medical care was introduced known as Personal Health Records (PHR). It enables the self-management of medical records. PHRs are the online system used by patients online. Patients can keep track of their medical records and can share them with anyone. PHR and EMR can reside on different platforms under various technologies and standards.

EMRs are the digital version of physical medical records. An EMR can contain the medical and treatment history of the patients in one practice. EMRs are much better than paper records like tracking data over time, easily identifying which patients are due for preventive screenings or check-ups. Checking how the patients are doing in their recovery periods such as keeping track of blood pressure readings or vaccinations, etc. Send data to experts for more clarity of the patient's situation. The data gathered by the healthcare providers tell the clinicians about the patient's life-threatening allergy so that it can be treated or prevented before it gets worse. The patient can log in to their records and see the lab reports over the last year, which can motivate them to take their medication and various precautions and keep up with a healthy lifestyle. It can also avoid duplicate tests. It enables a patient to move from one healthcare setting to another smoothly.

Data breaches and exposing patients' data in the healthcare sector needs a better platform that they can rely on. A study was conducted to analyse the data breaches in EHR systems and the conclusion came that over 173 million data entries have been exposed or compromised in these systems since 2009. Another study conducted by Argaw et al states that hospitals and other healthcare institutions have become targets of cyber-attacks, which is why a lot of research work has been done in this domain. But still, many EMR systems are not designed to fulfil the requirements of the patient and face the issues related to inefficiency and poor adaptation of these systems. These problems make it reasonable, and we need to find a platform that would help make the healthcare sector more patient-centred.

IV. Related Work

Blockchain-Based Distributed Patient-Centric Image Management System: In this, they have used Ethereum blockchain and IPFS system. They have implemented an Ethereum smart contract called the patient-centric access control protocol to enable a distributed, decentralized and trustworthy access control policy. But it is noticed that, due to the decentralized nature of the system, losing private keys and files connected to them is the limitation of the system. Furthermore, the medical images and data stored in the system are not protected once the data is decrypted. They have difficulty in authorization and authentication of the recipients who attempt to tamper or manipulate the decrypted medical image also data hiding techniques have not yet been clinically employed. [1]

Hyperledger Health chain: Patient-Centric IPFS-Based Storage of Health Records: This system is an innovative solution called Patient-Centric Healthcare Data Management (PCHDM). This project implements an on-chain health record database, which stores the hashes of the medical records in Hyperledger fabric and in off-chain it encrypts the actual data and stores it in the distributed network of IPFS. There are some limitations to this research that need to be addressed, multi-blockchain systems require a tremendous number of resources to be implemented. One of the drawbacks of this project is that it uses a hyper ledger fabric which is not an efficient way to store hashes.[2]

Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS: In this, they have constructed an attribute-based encryption scheme for storing and sharing electronic medical records securely and efficiently in the IPFS storage environment. It is based on cipher-text policy attribute encryption. It controls the access of EMRs without affecting the performance of retrieval of data. It stores any kind of medical records like X-rays, diagnostic reports, CT scans etc. in a decentralized manner. [3]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

In an existing system [3],[4] some issues have been found like, it is not secure because the data of the patient is accessible to everyone. Anyone can add and update the medical records. No authority is given to the user to allow only selected people to change their data. There is no proper application is implemented to store the medical records of a user inefficient manner and provide them security.

V. Software and Hardware Requirements

- Solidity programming language and Truffle framework for creating Smart Contracts.
- Moralis IPFS and MongoDB for storing data.
- Javascript ES6 (React.js for frontend, Express.js for backend, web3js for connecting smart contract and application)
- Java 8 and Android SDK for making android app.
- Ganache for creating local Ethereum test network.
- Metamask wallet for transactions.
- Any computer or laptop with Windows10/Ubuntu 18.0 OS, Intel i3 processor, 4GB DDR4 RAM, 500GB HDD.
- Android smart phone with android version 5.0 or up.
- Stable internet connection

VI. Project Design and Methodology

6.1 Blockchain Technology

As the name suggests, A Blockchain is a technology that is made up of record blocks that are linked together like a linked list using cryptographic hashes. Each block contains a cryptographic hash of a previous block, a timestamp, and all the transactional data. The Blockchain can store all the transactional data of the cryptocurrency and it can be verified by the public. Blockchain technology provides some major security advantages such as integrity of the transactions, strong authentication, and immutability of data. Blockchain is like a distributed database maintained by the nodes in the Blockchain network. Block records several transactions in a specific data structure. The data stored in the block can vary in size. Blockchain works on a decentralized network, therefore it is more reliable and there is no single point of failure. Also, decentralization enables direct peer-to-peer transactions without the need for third-party exchanges or middlemen, thus eliminating the extra fee and charges. [5]

6.2 Distributed File System – IPFS (Inter Planetary File System)

IPFS stands for Inter-Planetary File System. In IPFS a cryptographic hash is used to represent a unique fingerprint for each file within IPFS. It is a peer-to-peer(P2P) protocol. In this, rather than relying on location-based addressing IPFS uses content-based addressing. Due to IPFS, the cost of bandwidth can be reduced and download speed can be enhanced, and a large amount of data can be shared without duplication which can save storage space. The hash value of an IPFS file cannot be changed or tampered so IPFS is an immutable storage mechanism. When a file is added to IPFS it is broken down into smaller pieces and each piece is hashed cryptographically, and a unique fingerprint is given called content identifier (CID). These pieces are then scattered across the network, thus making it decentralized, hack-proof and tamper-proof. [6]

6.3 Smart Contracts

A smart contract is a program that runs on the "Ethereum Virtual Machine (EVM)", which is distributed network consisting of many nodes, and each node is running its EVM. The smart contract is executed automatically when the condition mentioned in the program are met. The smart contract is like an agreement between two parties to which they can agree on without any third-party involvement. It can be developed by using the Solidity programming language. The advantages of smart contracts are speed, efficiency, accuracy, trustability, transparency and security. [7][8]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

6.4 Flowcharts

Figure 1: Use-case diagram of the project

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

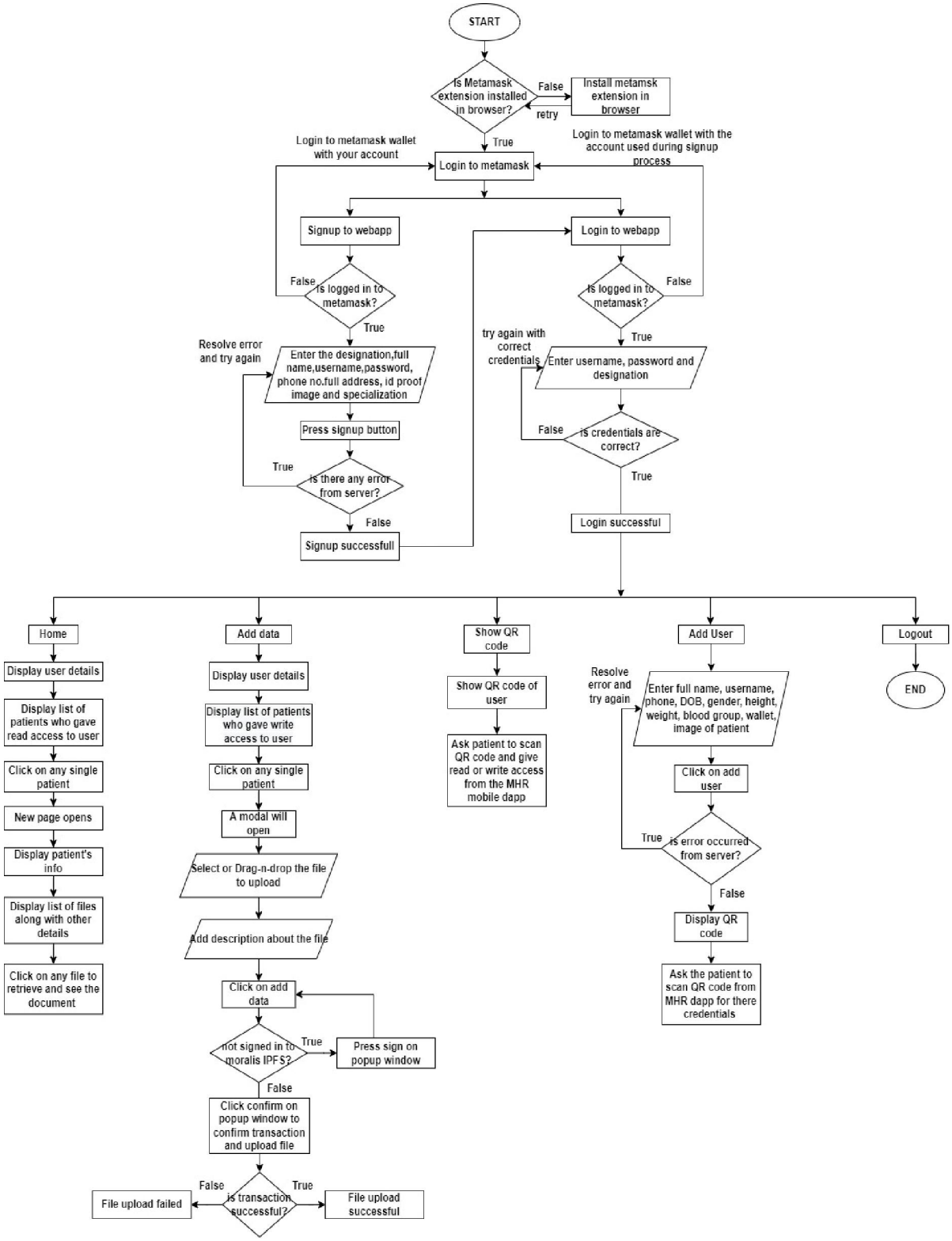

Figure 2: Working of medical health records web-application

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

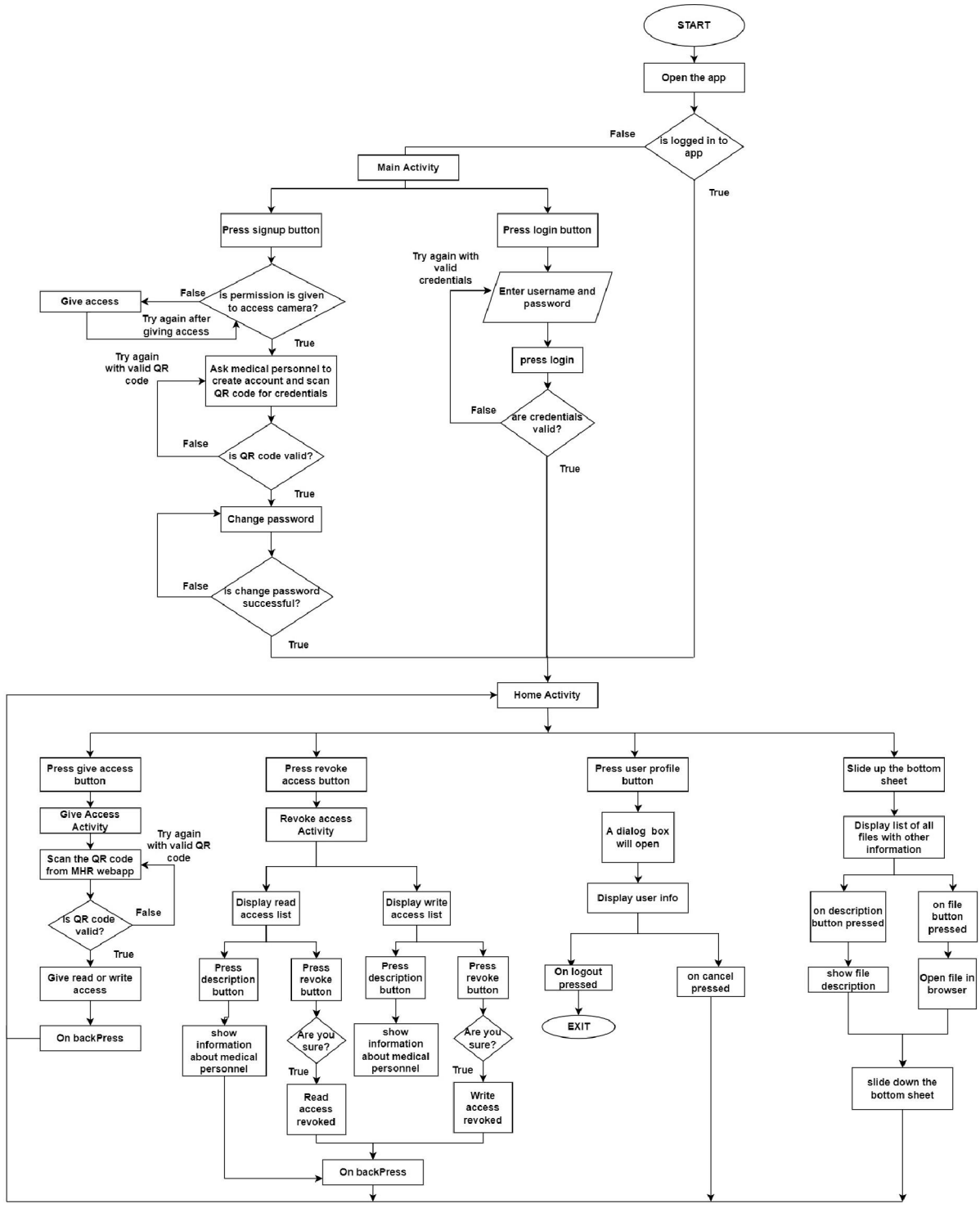

Figure 3: Working of medical health records mobile app

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

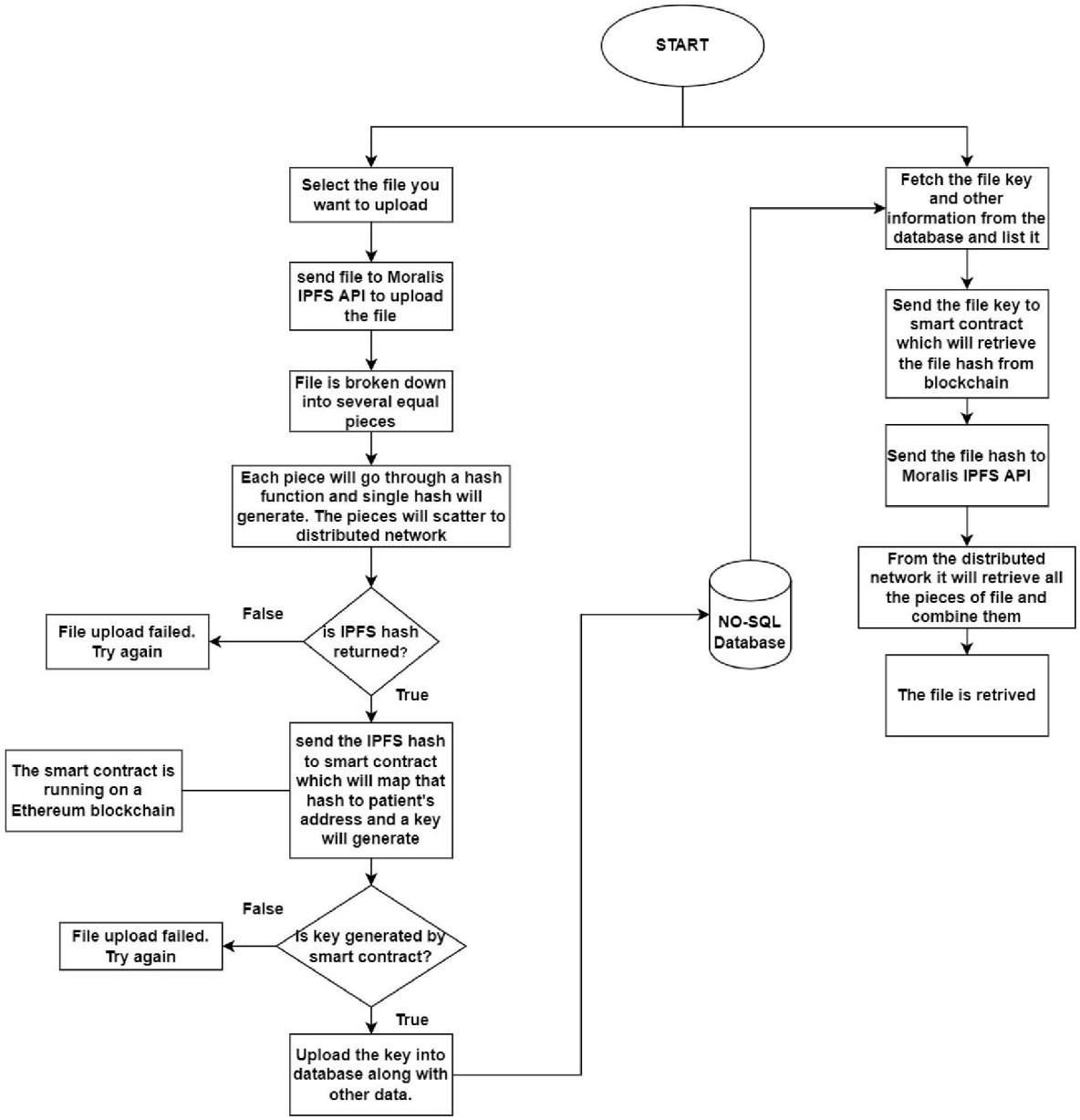

Figure 4: Working of Blockchain and IPFS

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

VII. Experimental Result

Fig. 5 Home page of MHR Web-application

Fig. 6 Patient details page

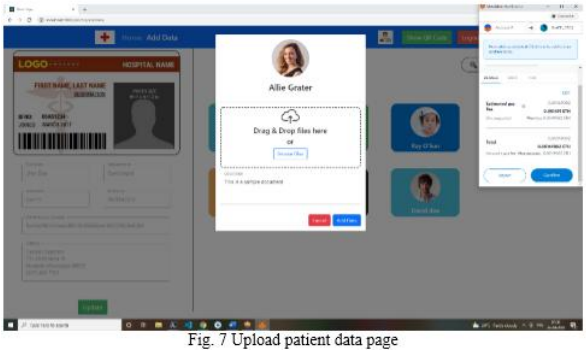

Fig. 7 Upload patient data page


Fig. 8 Data retrieved from IPFS

Fig. 9 MHR mobile app home activity

Fig. 10 Patient data activity

Fig. 11 Give access using QR code

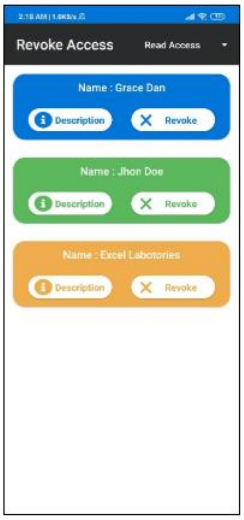

Fig. 12 Revoke access activity

VIII. Conclusion and Future Work

8.1 Conclusion

It is a blockchain-based approach to give patients control over their medical records in a decentralized, traceable, reliable, trustful, and secure manner. This decentralized app will help not only storing Electronic medical record securely into blockchain but it will also help doctors to diagnose patients by seeing their medical history and treat them accordingly and warn them about diseases that they can prevent. The patient's application can give and revoke access to medical

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

personnel any-time and anywhere. It will also help researchers to research on various diseases. This app can also be used as the medical evidences that can be used by law. The data stored in this system is immutable which means no one can change the medical records. Since entire system is built on Ethereum blockchain and IPFS so it is tamper-proof and it cannot be hacked and use the data illegally.

8.2 Future Work

In this system, there is room for lots of improvement, like adding functionalities like online payment for doctors using cryptocurrency, online booking and scheduling of appointments, and online consulting with doctors. On the Ethereum blockchain, there is one big problem, and that is high gas fees. So, in the future, it can be reduced by migrating the smart contract to the Solana blockchain, which has very few gas fees and can be affordable for most users. The user interface of the mobile application and web application can be improved. Currently, the patient's mobile app is only available for Android, so support for iOS can be implemented. The application supports the Metamask wallet, so other crypto wallets can be integrated with it.

ACKNOWLEDGMENT

Many people have contributed in bringing this report to its present form. We are the presenter ascribe our success in this venture to our guide Mr. D. B. Khadse, Asst. Professor of Computer Science & Engineering Department, P.B.C.O.E. Their endeavour for perfection, indefatigable zeal, enthusiasm, foresight and innovation contributed in a big way in completing this report with considerable ease in the stipulated time.

We are also grateful to Mr. K. N. Hande, H.O.D. of Computer Science & Engineering Department, P.B.C.O.E. The enthusiastic feedback from him was instrumental improving the presentation and in establishing our confidence in the structuring of the material. Our sincere thanks are extended to Dr. N. K. Choudhari, Principal, P.B.C.O E. for constantly encouraging and helping us during the course.

REFERENCES

[1]. Jabarulla, M.Y.; Lee, H.-N. Blockchain-Based Distributed Patient-Centric Image Management System. Appl. Sci. 2021, 11, 196.

[2]. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Health chain: Patient-Centric IPFS-Based Storage of Health Records. Electronics 2021, 10, 3003. https://doi.org/10.3390/electronics10233003.

[3]. Jin Sun, Xiomin Yao, Shangping Wang, and Ying Wu. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS (School of Science, Xi'an University of Technology, Xi' an 710054, China) Digital Object Identifier 10.1109/ACCESS.2020.2982964.

[4]. Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid. Using Blockchain for Electronic Health Records. Computer Science Department, National University of Science and Technology (NUST), Islamabad, Pakistan 2Computer Science Department, National University of Science and Technology (NUST), Islamabad, Pakistan 3Centre for Secure Information Technologies (CSIT), ECIT Institute, Queen's University of Belfast, UK. DOI 10.1109/ACCESS.2019.2946373, IEEE Access.

[5]. Blockchain Whitepaper. https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf

[6]. IPFS - Content Addressed, Versioned, P2P File System, Juan Benet https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[7]. Smart Contracts. https://www.howtogeek.com/350322/what-is-ethereum-and-what-are-smart-contracts/

[8]. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014.