Patient-Centric and Scalable Electronic Health Record System Using Blockchain And Interplanetary File System

Akash Savle[1], Gaurav Ghadge[2], Tanmay Sankpal[3], Vishwajit Sayambar[4], Prof.Sana Shaikh[5]
[1, 2, 3, 4, 5] Dept of Information Technology Engineering
[1, 2, 3, 4 5] Genba Sopanrao Moze College of Engineering,Balewadi

Abstract- *Electronic Health Records are gaining popularity all around the world. However, their security and privacy concerns have become a concern for most of the users. This paper proposes a mechanism that enables patients to control their records and revoke their access to them.*

Blockchain technology can improve the capability of electronic medical records systems by storing large amounts of data. This framework proposes a way to implement blockchain in the healthcare industry by storing patient records in an on-chain database and implementing off-chain solutions on ipfs that secure the data using cryptography.

Keywords- blockchain, IPFS, Electronic Health Records, Decentralise, Scalable.

I. INTRODUCTION

Despite the rise of EHR, many hospitals in developing nations still lack the necessary facilities to implement it. The main challenge that they face is the security and privacy concerns related to their data. Due to the sensitive nature of the data that it contains, medical records are regularly attacked by hackers. They usually install malware on the server and then release it once their demands are met. The records are managed by the hospitals that created them. If the facilities fail to implement adequate security measures, the data could be easily manipulated. There is also a lack of uniformity in the way the records are stored.

In India, a government agency known as the National eHealth Authority is working to establish regulations for the use of e-health records. These regulations would help ensure that the records are secure and are not prone to abuse. The new user's metamask ID is stored in the blockchain as well as their Ether account. This is done through the use of the InterPlanetary File System. Ganache is a Chrome Plugin that gives access to a website through Ethereum. The goal of this project is to provide patients with complete control over their data.

Related Works

The study that is focused on the principles and techniques of different development, this system will be able to provide them with the necessary information. Such papers are being reviewed and studied as part of the project's study Survey EC is one of the earliest suggested models for a blockchain-based medical record management system. The Medchain is a blockchain the based application that allows hospitals, patients, and pharmacies to share healthcare data. Data is stored on- chain, but they suffer from privacy and scalability problems.

It uses the Smart Contracts and Ethereum Blockchain to store accessibility details of the health record. But the actual health record is not stored on the Blockchain system, it is stored on the Healthcare Providers database which is operated by a third party. Hence these records are still vulnerable to attack or misuse. The primary difference between MedRec and our approach is that we store the health records in a distributed manner and do not rely on a third-party service provider. Also, we do the use hashes in IPFS which guarantees the immutability of records.

In Blockchain for Healthcare, the patient data is stored on the blockchain and after being encrypted with the patient's private key. This data can be decrypted by using the patient's public key which is provided to users such as Pathology labs and hospitals to whom the patient has given permission. This is in contrast to our approach in which the patients have complete control over who can view their data. In our Framework, the patient's private key is required to decrypt the health data instead of encrypting it. Also, we do not save the data over the blockchain but instead, w use IPFS for the same.

Requirement And Preliminary

The important requirements that need to have happened in an electronic health record management system are-

- The patient records once stored must be immutable and changing them should be infeasible.
- The patient must be able to grant or remove the access of his/her records as and when he/she wants.
- The patient should have complete control over who can view his/her records.

Required Tools

A. **Ganache**: Ganache is part of the Truffle Suite Ecosystem as well as Truffle is a development environment, asset pipeline, and testing framework using the Ethereum Virtual Machine. On the other hand, Ganache is a high-end development tool it is used to run your own local Ethereum blockchain. Ganache is helpful in every aspect of the development process. The local chain allows you to deploy, develop and test your projects and smart contracts in a deterministic and safe environment. It is a personal blockchain for rapid Ethereum and to Make D-Apps development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your decentralized Apps in a safe and deterministic environment. Ganache is used for setting up a Private Ethereum Blockchain System for testing your Solidity contracts.

B. **Metamask**: MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It Permissions users to obtain their Ethereum wallet through a mobile app as well as a browser extension, which can then be used to interact with decentralized applications. MetaMask is a browser plugin that Provides an Ethereum wallet. Users can store Ether and other ERC-20 tokens in the MetaMask wallet. The wallet can alsobe used to connect with decentralized applications or apps.

C. **IPFS**: The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to particularly identify each and every file in a global namespace connecting all computing devices.

II. PROPOSED APPROACH

Proposed Work - The EHR Management System will be built on the public Blockchain platform Ethereum. It will be built with the Truffle web framework which compiles the smart contracts and injects them into the Web App. All the users would compulsorily have a Metamask account, which can be created using an installable chrome plugin. The Metamask plugin will allow us to connect to the local Ethereum network and provide us account address to sign transactions. All the transaction fees or Gas fees will be paid using the Metamask account. As our system is developed on a local test network it uses ganache for users' accounts which are funded 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 the Backend is managed by a 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 the upload process, he will be needed to sign the transactions using his private key. The user documents are uploaded on Off-chain storage securely.

IPFS (InterPlanetary File System), a distributed file system, is used as Off-chain storage. Once the records are uploaded on IPFS we store the hash of the address of the stored documents on blocks of the blockchain. So every time a new block is added to 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.

III. SYSTEM DESIGN

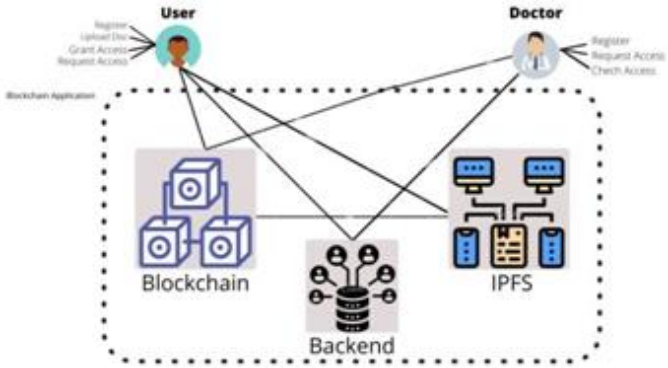

Diagram 1

As shown in Diagram 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 the Node-Express server and then sent to MongoDB Cloud Database.

Diagram 2, shows the flow diagram for users, and Diagram 3 displays the flow diagram for doctors.

- The Patient User will require an Ethereum account using Metamask Extention to be a part of the Blockchain.

- Once complete he can visit the signup page and enter his personal details and credentials. After passing all the authentication checks he must log in to his profile.
- Once logged in he can upload his records in an image format to the blockchain. For uploading, he must pay some others in order to complete the transaction.
- There are discrete subpages created in the user profile such as:

    - Dashboard: The dashboard will show all the records the user has uploaded till now.
    - Profile page: This page shows all his personal details mentioned during the signup process.
    - Doctors Page: This page shows 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 queue 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 transferred to the IPFS network which in turn returns us the hash of the uploaded asset. We collect this hash on the blockchain along with other necessary details.
- The doctor requires to go through the same procedure of signup and then sign in, once he enters his account he will be able to see the records if the user has verified the permission. Else the dashboard will be empty.
- he could go to the user's page and explore the user whose records he wants to check. He can request a verify access from the patient-user, his request will go through the server and will be sent to the specific user's dashboard.
- If he has access he can view the records from his dashboard.

Diagram 2

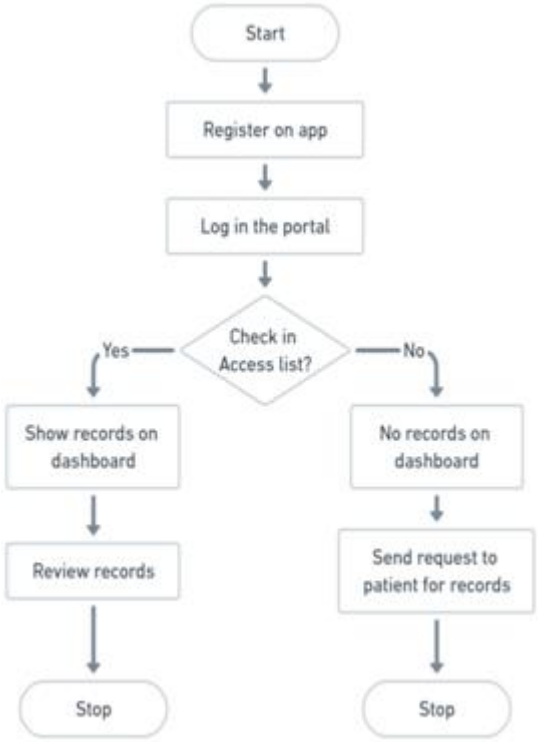

Diagram 3