Storing Medical Records Securely with Blockchain

Shradha Sehgal
Roll No. 2018101071

Sravani Boinepelli
Roll No. 20171050

Mohammad Shahbaz S Shaik
Roll No. 2018111025

I. Problem Statement

Electronic Health Record (EHR) systems face problems related to data security, data ownership, integrity, and management. We propose a framework involving blockchain technology for EHR. We provide secure storage of electronic records by defining granular access rules for the users (i.e. patients, doctors, & hospital staff). Overall, using blockchain's decentralized principles, we improve the accessibility and security of patient information, whilst also tackling issues of scalability with off-chain storage of encrypted records.

A. Motivation

EHR systems are used to store medical records, clinical notes, and laboratory results. However, they face multiple problems [1] that we need to tackle:

1) **Data Security**: EHR systems lack a secure structure and often result in data breaches. [2] Unauthorized access attempts from inside the network or ecosystem (e.g. employee of the healthcare provider, or cloud service provider) can also take place in conventional systems.

2) **Data ownership**: Patients are currently unable to have ownership of their medical data. EHR systems and the general healthcare sector are centralized as doctors and hospitals have monopoly over patient's records. If a patient wants to access their medical records, they have to follow a long and tedious process to access them.

3) **Interoperability**: Interoperability is how different information systems exchange information between them. Health Information Exchange (HIE) is an important aspect of EHRs, but with a number systems being deployed in various hospitals they have a varying level of terminologies, technical and functional capabilities which makes it to have no universally defined standard. [3] This makes a patient's medical information fragmented across hospitals and it becomes a tedious process to transfer records from one hospital or application to another. Using blockchain and IPFS system (explained later), this information can be transferred seamlessly and speedily.

B. Beneficiaries

1) **Patients**: The proposed framework is patient-centered as the data is accessible and controlled by the patients. They can grant access to other healthcare providers. Records can also not be altered without both the doctor and the patient's signatures so healthcare providers cannot deny accountability in case of an incorrect diagnoses.

2) **Doctors**: Multiple doctors working on a case can stay updated with the records. This also makes cross-hospital consultancies easier. A doctor can be sure that the record has not been tampered with, and patients can also not generate false prescriptions under their name.

3) **Healthcare providers**: Universal access to records can actually save healthcare providers money related to administration costs of the upkeep and transfer of records and also from reduced liability from data breaches, staff misdoings, etc.

C. Impact

In 2018, the Department of Health and Human Services' Office for Civil Rights (OCR) in the U.S. received notifications of many data breaches that resulted in the exposure of 13 million total healthcare records! [4]. Argaw et al. [5], explain that hospitals have become a target of cyber-attacks and an increasing trend is being observed (2019 study).
Our framework successfully tackles such issues of data security as blockchain technology relies on a distributed network where there is no one point of failure. It is not possible for hackers to simply find a security flaw and gain access to the entire data. Although 51% attacks are possible, the probability of a successful attack is extremely low as the attacker would need enormous computing power or hashing power. The IPFS protocol also provides secure data storage as it uses cryptographic identifiers to protect data from alteration.
This lack of interoperability in a conventional EHR system can lead not only to clinical errors but administrative ones, such as the National Health Service's (NHS's) recent failure to invite 50,000 women for a cervical screening test [6]. Furthermore, patients must recount their history multiple times, a process found to be inefficient as well as tiresome, and which can lead to confusion as well as clinical errors because of incomplete information [7]. Our framework tackles these issues by enabling seamless, effective, and speedy interoperability, on a large scale. The patient can just grant access of their medical records to a doctor, without going through elaborate administration.

Overall, using Blockchain for medical records facilitates the shift to patient-centered interoperability and enables us to fully enjoy the benefits of data liquidity by eliminating challenges surrounding security and privacy, incentives, and governance that must be addressed for this type of data sharing to succeed at scale.

II. Solution

In order the solve some of the problems facing the current EHR systems, and we use a combination of Ethereum and IPFS (Inter Planetary File System) to create a scaleable alternative to the EHR system. We use off-chain storage in conjunction with blockchain to create a decentralized platform that allows creation and sharing of records, with concerned individuals or healthcare providers. The usage of Ethereum enables the usage of smart contracts, which is simply code running on Ethereum, that eases development of the proposed solution. We discuss the architecture of the proposed solution in detail below.

A. Architecture

This section details the architecture of the system that is proposed, and details the various individual components that make up the entire system. As shown below, the architecture of the system consists of multiple layers interacting with each other. The interaction of these layers ensures the working of the entire system.

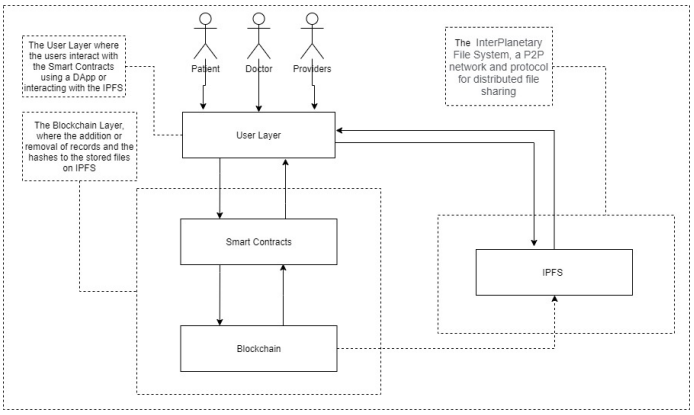

Fig. 1. Overview of the proposed model

1) User Layer: This is the layer that interacts with the users. The users of the system can be patients, doctors, or other hospital staff. These users would need to interact with the system and perform CRUD operations on the records. The interface for these users would be a DApp, with the functions that can be accessed by a particular user being shown. This layer is used by the user to interact with the blockchain layer.

2) Blockchain Layer: The blockchain layer contains the mechanisms for interaction of the user with the blockchain, and also contains the blockchain itself. This layer also contains the mechanisms for creation, updation (essentially adding new records), viewing, deletion of records, and access control to the records. The records are private, and each patient can only view his or her own patient records. The doctors can view the patients medical records. Only the basic information of the student is stored on the blockchain, with the detailed information as well as the results of various tests or scans being stored on IPFS. The IPFS hash is also stored along with the basic patient information on the blockchain. The system uses public account addresses and other methods to ensure that a patients records do not fall into the wrong hands.

3) IPFS Layer: IPFS (Inter Planetary File System) is a protocol that makes uses of peer-to-peer network for storing data. Data stored on IPFS is protected from alteration, and any alteration made to the files stored can only be done by changing the cryptographic identifier that protects the data. The files stored on IPFS contain a hash that is generated cryptographically, and this hash assists in identification of stored data files, since it is unique. [8] [9]

By storing the IPFS hash on the blockchain, the number of operations that need to be done over the blockchain are reduced, and the storage requirements also decrease.

B. Smart Contracts

In the proposed system, we use two contracts, *Patient Records* and *Roles*. These contracts fulfill the following purposes:

- CRUD Operations on patient records
- Assigning roles

The *Patient Records* contract takes care of the CRUD operations of the patient records. The pseudocode for the *Patient Records* is as follows:

1) Patient Records Pseudocode: Add Data:

```
function Add Patient Record(data)
    if(msg.sender==doctor) then
        add data to patient's record
    else Abort
    end if
end function
```

Retrieve Data:

```
function View Patient Record( patient id )
    if(msg.sender==doctor||patient) then
        if(patient id) == true then
            retrieve data from patient(id)
            return(patient record)
                to msg.sender
        else Abort
        end if
    end if
end function
```

Update Data:

```
function Update Patient Record(data)
    if(msg.sender == doctor) then
        if(id == patient id ) then
            if(patientsign)
                update data to patient(id)
                return success
        else return fail
        end if
    else Abort
    end if
end function
```

Delete Data:

```
function Delete Patient Record
                        ( patient id )
    if(msg.sender == doctor) then
        if(id == patient id) then
            delete patient (id)
            return success
        else return fail
        end if
    else Abort
    end if
end function
```

Share Record:

```
function Share Patient Record(patient id)
    if(msg.sender == patient) then
        if(msg.sender == patient id)
            share record(id)
            return success
        else Abort
        end if
    else Abort
    end if
end function
```

2) Roles Pseudocode: Add Role:

```
function Assign Role(Role, Account)
    add role and account in roles mapping
end function
```

III. Need for a Blockchain

Central data storage of medical data has led to cyberattacks and data leaks in the past. Blockchain circumvents this issue by distributing the medical data over a network and making it persistent (as there is no one-point failure). Hackers cannot just get access and corrupt the data. Due to consensus and the digital record, blockchain transactions can't catch fire, be misplaced, or become damaged by water. In order to give the patient true ownership of their health records, we need to eliminate the requirement of a Trusted Third Party as they can tamper with the data and also leak records of important personnel. In a universal system, hospitals cannot deny accountability in case of an incorrect diagnosis as they do not have monopoly over records. A blockchain also ensures that user-information is accessible immediately, rather than being fragmented across different hospitals and medicine practitioners.

IV. Analysis

Blockchains innately do not offer suffer sufficient storage as they are not designed to store huge volumes of data, so we store the encrypted medical records off-chain using an IPFS mechanism. As we store the IPFS hash and not the entire medical record, the storage requirements of the system are greatly relieved. The transaction size is also reduced due to the limited information being stored on the blockchain itself. This results in transactions being performed faster as well.

Transactions are only made when a new patient comes to the hospital, an existing patient's records are updated, or when a patients records are being shared. When a transaction is requested, the user must pay for the computation. In the Ethereum network, the payment is calculated in "gas" and the gas is paid in "ETH". As the blockchain stores much lesser data than the IPFS system, the gas required is not that high. Even if the number of transactions increase, the use of a blockchain system would replace current storage systems (electronic health records (EHRs), personal medical records, disease registries, and other databases. It will also eliminate costly data breaches and other errors, ultimately rendering the system cost-efficient.

There does exist the possibility of storing data in smart contracts, but the risk with such an approach is that the gas cost soon starts to grow too large for the system to be viable. Hence, our proposed system offers a more scalable solution. Furthermore, due to the IPFS hash being stored on the blockchain, it is possible to mark certain patients as deleted, making it so that their IPFS records cannot be accessed, allowing for a method of deletion (requires authorization from both patient and doctor).

Considering the aspect of security, only encrypted patient files are stored on IPFS, and any changes to the files also changes the cryptographic indentifier. Due to this, the IPFS files are stored securely. The smart contract, by checking the public addresses of the various people making transactions or requests, ensures that no one without the authority is able to access the records. Even in case of the patients, their public address is checked and the smart contract ensures that they can only access their own records.

V. Future Work

For future work, we can develop our platform to store records of mobile health applications and monitoring devices like Fitbits. Some challenges with these are that this information must be updated in real-time and also the vast amounts of data generated with these apps - monitoring devices produce data-points more frequently than hospital visits. The relevance of personalized medicine and wearables is on the rise and the 'ownership' of this data belonging with large corporations has raised several concerns. Thus, mobile app records storage becomes an important problem to solve. [10]

Future work also includes scaling the application to operate in multiple hospitals across cities and states. Due to the scalable combination of IPFS and blockchain, the extension should be relatively easy to perform.

REFERENCES

[1] M. Hochman, ""electronic health records: a "quadruple win," a "quadruple failure," or simply time for a reboot?"."

[2] G. Jetley and H. Zhang, "Electronic health records in IS research: Quality issues, essential thresholds and remedial actions, decis. support syst." pp. 113–137, 2019.

[3] M. Reisman, "Ehrs: The challenge of making electronic data usable and interoperable," pp. 572–575, 2017.

[4] J. H. (2018), "Largest healthcare data breaches of 2018," hIPAA Journal.

[5] N. E. B. S. T. Argaw, "The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review," pp. 1–11, 2019.

[6] Iacobucci, "G. cervical screening: Gp leaders slam capita over failure to send up to 48 500 letters."

[7] C. Strategies., "Malpractice risks in communication failures."

[8] Authors, "The frobnicatable foo filter," 2014, face and Gesture submission ID 324. Supplied as additional material `fg324.pdf`.

[9] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative ipfs-based storage model for blockchain," pp. 704–708, 12 2018.

[10] [Online], "Interplanatery file system, https://www.ipfs.io," (accessed November 2, 2020). [Online]. Available: https://www.ipfs.io/.