Project Report On

Secure Electronic Medical Record Management System using Blockchain Technology

Under the guidance of Asst. Prof. Dr. S Venkatesan

Indian Institute of Information Technology, Allahabad
January – May 2018

Submitted By :-
1. Sagar Kumar (IIT2015020)
2. Tushar Murarka (IIT2015091)
3. Aditya Dewan (IIT2015097)
4. Deepak Yadav (IIT2015124)

Candidates' Declaration

We hereby declare that the work presented in this project report entitled "Secure Electronic Medical Records Management System Using The Blockchain Technology", submitted as end-semester report of 6th Semester report of B.Tech. (IT) at Indian Institute of Information Technology, Allahabad, is an authenticated record of our original work carried out from January 2018 to May 2018 under the guidance of Asst. Prof. Dr. S Venkatesan. Due acknowledgements have been made in the text to all other materials used. The project was done in full compliance with the requirements and constraints of the prescribed curriculum.

Place: IIIT Allahabad
Date: 26 - 04 - 2018

Sagar Kumar (IIT2015020)
Tushar Murarka (IIT2015091)
Aditya Dewan (IIT2015097)
Deepak Yadav (IIT2015124)

Certificate

This is to certify that the project work “Secure Electronic Medical Record Management System using Blockchain Technology” is a bonafide work of Sagar Kumar (IIT2015020), Tushar Murarka (IIT2015091), Aditya Dewan (IIT2015097) and Deepak Yadav (IIT2015124) who carried out the project work under my supervision.

Place: Allahabad
Date: 26 - 04 - 2018

Asst. Prof. Dr. S Venkatesan

Abstract

Electronic medical records (EMRs) are critical, highly sensitive private information in healthcare, and need to be frequently shared among peers in particular between healthcare providers and researchers. Blockchain is a continuously growing list of records known as blocks which are securely connected like a linked list using cryptographic techniques. A typical block in a block chain contains data, hash value of the previous block and timestamp. Blockchain is a digital public ledger which secures the data stored in it using cryptographic techniques. There are multiple nodes which are the server computers and each node contains the whole blockchain. New blocks are mined and broadcasted into the network by a particular node and then verified and accepted or rejected by other nodes. Blockchain has found many applications since its first use in 2008 [1]. It is used in many cryptocurrencies. The biggest constraint that the blockchain imposes is storage space. The complete blockchain has to be stored on each and every node which make it very difficult and expensive to maintain large block chains. This can be tackled by keeping a centralized data store and only saving the metadata of the records in the blockchain.

We propose a model where we implement our own blockchain with a predefined block structure that suits our purpose the best. The proposed blockchain based model can significantly reduce the turnaround time for EMR sharing and access where the patients are owners of their own data. It provides an efficient access control management framework for a patient to grant/revoke access to/from different hospitals and also reduces the overall cost.

Table of contents

1. Introduction

Electronic medical records (EMRs) are critical but highly sensitive private information for diagnosis and treatment in healthcare, which need to be frequently distributed and shared among peers such as healthcare providers, insurance companies, pharmacies, researchers, patients families, among others. This poses a major challenge on keeping a patient's medical history up-to-date. Storing and sharing data between multiple entities, maintaining access control through numerous consents only complicate the process of a patient's treatment. A patient suffering from some serious disease has to maintain a complete history of all treatment process. Having access to a complete history may be crucial for his treatment: for instance, knowing the delivered radiation doses or laboratory results is necessary for continuing the treatment.

A patient may visit multiple medical institutions for a consultation, or may be transferred from one hospital to another. A patient has complete right over his health information and may set rules and limits on who can look at and receive his health information. If a patient needs to share his clinical data for the research purposes, or transfer them from one hospital to another, he may be required to sign a consent that specifies what type of data will be shared, the information about the recipient, and the period during which the data can be accessed by the recipient. This may be extremely difficult to coordinate, especially when a patient is moving to another city, region, or country and may not know in advance the caregiver or hospital where he will be receiving care later on.

Having access to a ledger - shared, immutable, and transparent history of all the actions that have happened to all the participants of the network (such as a patient modifying permissions, a doctor, accessing or uploading new data, or sharing them for research) overcome the issues presented above. By providing the tool to achieve consensus among distributed entities without relying on a single trusted party, blockchain technology will guarantee data security, control over sensitive data, and will facilitate healthcare data management for the patient and different actors in medical domain.

2. Motivation

Blockchain technology has been at the center of media attention due largely to bitcoin, an upcoming digital currency that uses blockchain technology, increasing in value, netting investors unheard of returns. While blockchain is being considered for many uses, its potential to revolutionize healthcare is evident. Having an open blockchain for medical data can prove useful as most healthcare data now is segregated amongst different providers, who often use different database systems. But by this approach crucial information is often scattered and inaccessible, which is very dangerous in a medical industry where even a few extra seconds or minutes to obtain critical information could be the difference between life or death for a patient. By having blockchain systems built for healthcare, important healthcare-related data can be more easily accessible amongst healthcare providers, which can lead to better and faster treatment.

But storing the entire records into the blockchain isn't a good idea either! In a blockchain like Ethereum, storing 1KB of data costs around 0.032 eth i.e. nearly 30 USD according to the current ethereum data storage costs. And therefore we proposed a model that stores the metadata of the records instead of the original records which reduce the amount of memory consumed by a considerable amount.

3. Problem Statement

Implement a light-weight blockchain to store Electronic Medical Records (EMR) in which only the metadata of the records are saved and the actual records are saved in a centralized data store/cloud in an encrypted format.

Develop a web/mobile decentralized application (DApp) for easy accessibility along with permission control, secure management and efficient sharing of medical records.

4. Literature Review

King yip et al [2] supports the use of blockchain in a positive way. He encourages the use of private blockchain that are accessible only to the hospitals that exchange data(medical records) with real time update facility . This can cut down many false claims and makes sure the final bill is correct.

Ariel Ekblaw [3] proposed Medrec, a novel system which give patients a comprehensive, immutable log and easy access to their medical information across different providers and hospitals using blockchain's unique property they provides confidentiality and authentication. They incentivized medical stakeholders to participate in the network as blockchain "miners". However maintaining record can be a major challenge as most patients are not interested in reviewing their own record and this reflects the nature of how these records are managed.

Kenneth D [4] showed consent towards present electronic medical record system that records fragmented medical records by adopting unreliable means to store and communicate data. Record systems should accept data from different sources including personal computer as well as doctor's hospital.However they are still configuring the loopholes of their system before universally deploying them.

Allison Ackerman Shrier [5] reviewed the threat to the security,confidentiality of public medical information these challenges can be overcome through their system which creates peer to peer network that enables parties to store and analyse data jointly.Use of permissioned blockchain to access controls through smart contracts and digital identities.

5. Methodology

5.1 Blockchain based proposed model :-

In the proposed model, we use a light-weight blockchain to store the metadata of electronic medical records(EMR) of a patient. The blockchain provides a secure, self-controlled way to store the medical records of patients where the patients have the control over who can see their records. Other than this, the blockchain implementation as per our proposed model has an efficient way to look at medical history of a patient, so the patient need not maintain all the previous records all the time he/she visits a hospital for treatment. As the hospitals act as the nodes in the blockchain, their connectivity will facilitate in quicker and better access control management of the records. This connectivity can also serve as a great source to updated and recent medical data for medical research purposes.

Whenever a patient visits a hospital, medical record(s) corresponding to the patient will be generated at the hospital. The hospital will encrypt this record with the public encryption key $PE_{patient}$ of the patient and will store the record in the cloud/ data store. After this, the hospital will generate metadata of this record and will initiate a transaction and broadcast the metadata to the network. This transaction will go to the transaction pool of each of the nodes which will be included in the blocks once miners start mining.

The patient's meta-data is stored in the blockchain using merkle patricia tree. The implemented patricia merkle tree is similar to one present in ethereum blockchain, but the main difference is in the data stored in leaf nodes in the tree. In the proposed method, nodes of patricia tree will have meta-data corresponding of patients. The block will have the following attributes :-

```
Block : {
        index,
        timestamp,
        nonce,
        Transactions,
        hash,
        previousHash,
        merkleRootHash,
        patientStateTrieHash,
        hospitalStateTrieHash
    }
```

- Index: Index will have the sequence number starting with 0. Genesis block has index 0.
- Timestamp: Each block is assigned a timestamp when that block is mined.
- Nonce: Nonce here is similar to one present in bitcoin and ethereum. Nonce is a 32 bit arbitrary random number that is typically used once. In mining process, the goal is to find a hash below a target number which is calculated based on the difficulty.
- Transactions: Transactions will have all the transactions mined and verified by the miner.
- Hash: Hash contains a 32 byte hex representation of the block.
- previousHash: Hash of the previous block mainly used for the validation of the block.
- MerkleRootHash: As mentioned previously all the transactions are stored in merkle tree and therefore this attribute will have the hash of merkle tree root.
- PatientStateTrieHash: We are using state trie to maintain all the information of the patient in the latest block. And this attribute has the hash to the state trie root.
- HospitalStateTrieHash: This attribute contains the hash of the state trie root that is used to store information corresponding to a particular hospital.

5.2 Types of Transactions :-

In our implementation of the blockchain, we have defined four different types of transactions, each of which facilitates a certain utility to the network. The types of transactions are as follows :-

5.2.1 Submit Record Transaction :-

In this transaction the hospital will submit the metadata of the medical record(s) into the blockchain network. This transaction will be initiated by the hospital towards the patient and will contain all the metadata of the record(s) that is to be entered into a block of the blockchain. This transaction will have the following fields :-

Transaction : {
Type = 0,
Patient ID,
Hospital ID,
Disease ID,
Link to the record,
Description of the record,
Hash of the record,
Permissions List [ ],
Signature
}

5.2.2 Grant Access Transaction :-

This transaction is meant for granting access of a previously generated record of a patient to a hospital. The transaction will be initiated by the patient towards the hospital to which he/she wants to grant access. Once this transaction gets mined into a block, the public-key of the hospital to whom the access is granted will be included in the list of permissions of the corresponding record whose access was requested by the hospital. Once this is done, the hospital can download the record from the cloud/ data store and can decrypt it. This transaction will have the following fields:-

Transaction : {

Type = 1,
Patient ID,
Service Requester ID,
Service Provider ID,
Disease ID,
Signature

}

5.2.3 Revoke Access Transaction :-

This transaction is similar to the Grant Access Transaction but . This transaction is for revoking the access to see/download/decrypt a certain medical record of a patient. The transaction will be initiated by the patient towards the hospital from which he/she wants to revoke the access. Once this transaction gets mined into a block, the public-key of the hospital from which the access needs to be revoked will be removed from the list of permissions of the corresponding record. After this, the hospital won't be able to see/download the contents of the record. This transaction will have the following fields :-

Transaction : {

Type = 2,
Patient ID,
Service Requester ID,
Service Provider ID,
Disease ID,
Signature

}

5.2.4 Request Decryption Key Transaction :-

Once a hospital gets access to see/download a certain record, it won't be able to decrypt the record as it was encrypted using the public encryption key of the patient who owns the record. So the hospital makes a transaction to the hospital-A (where this record was generated) to re-encrypt the data so that it can decrypt it by its own private key. The hospital-A applies proxy re-encryption algorithm on the encrypted record, re-encrypts the record and after this the hospital can decrypt it easily. This transaction will have the following fields :-

Transaction : {
Type = 3,
Requester Hospital ID,
Provider Hospital ID,
Hospital ID (where the record was generated),
Signature
}

6. Software requirements

6.1 Flask Server :-

The implementation requires a flask server which will serve the API endpoints that will fetch data from the blockchain and serve this data to the frontend where a user (hospital/patient) can see their data.

6.2 File Server :-

A file server is required to store the records (encrypted) generated during a patient's to a certain hospital.

6.3 User Interface :-

A user interface is required for the users to interact with the blockchain. The user interface will facilitate the users to easily carry out transactions, mine new blocks, see their medical history or to see contents of the blockchain.

7. Conclusion :-

As discussed in the above sections, the blockchain technology has made significant impact in various applications and can make a tremendous amount of improvement in the current healthcare systems. The model that we proposed discusses various issues present in the current healthcare scenario and provides a cost-efficient, secure and easy-to-implement solution. The model facilitates the user to control their own data with an efficient access control management framework. The model has hospitals as nodes which facilitates data availability all the time even in case of failures at certain nodes in the network. The connectivity in the hospitals also provides better healthcare opportunities and access to recent data for medical research purposes.

8. References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Whitepaper 2008 https://bitcoin.org/bitcoin.pdf Accessed 14 February 2018.

[2] King Yip, “BlockChain and alternative payment models,” White paper, 2016.

[3] A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data by *MIT Media Lab, †Beth Israel Deaconess Medical Center August 2016..

[4] Public standards and patients’ control: how to keep electronic medical records accessible but private by Kenneth D Mandl, Peter Szolovits, Isaac S Kohane.

[5] Blockchain and Health IT: Algorithms, Privacy, and Data. Prepared by: Allison Ackerman Shrier, Anne Chang, Nadia Diakun-thibault, Luca Forni, Fernando Landa, Jerry Mayo, Raul van Riezen .