Secure Blockchain Based Health Care Data Management System

Abdul Rahoof T P
Guided By
Asst. Prof Deepthi V R

College Of Engineering Trivandrum

May 19, 2019

Schedule

Introduction

Introduction

- Health care data security is an important element of Health Insurance Portability and Accountability Act Rules (HIPAA).
- As patient moves from one hospital to other, the patient needs to bring his/her own records and submits to the newly assigned doctor.
- Some cryptographic schemes have been proposed to solve the problems about medical data sharing. But they are insufficient, the disadvantages still exist.
- This paper focuses on a secure medical data sharing using a decentralized distributed technology, Blockchain.

Motivation

Motivation

- Reduced risk of patient record keeping.
- Blockchain guarantee medical data cannot be altered by anybody including Physicians and patients himself.
- Patient becomes the owning and controlling access to their health data.
- Records can only be accessed by intended users.
- Records are signed by source, allows legitimacy of records to be verified.

Literature Review

Literature Review

Title	Procedure	Issues
Medical Infromation Exchange System[1]	■ Central registry server: It stores patient's information and generate an index for that patient. ■ CDA transfer server: Using the index of patient, It extract relevant CDA documents from the CDA Repository.	■ Hospital Authority can edit or remove the patient record. ■ Administrator can change the permission on records. ■ Lack of scalabilty.
federated interoperability architecture[2]	■ It connects inter-regional medical institutions.	■ Hospital Authority can edit or remove the patient record.

Literature Review

Title	Procedure	Issues
	■ In each hospital, Document manager allows storing and retrieving documents created by an authorized user. ■ Regional registry in the regional server enable to localize the data archived in the repositories within the region.	■ Administrator can change the permission on records.
Medrec[3]	■ A decentralized record management system.	

Literature Review

Title	Procedure	Issues
	■ MedRec utilizes Ethereum's smart contract.	■ Hospital Authority can remove the patient record. ■ Medical records are not protected. ■ The system is vulnerable to intrusion. ■ Lack of scalabilty
Ancile[4]	■ Based on the Ethereum Blockchain.	■ Hospital Authority can remove the patient record.

Literature Review

Title	Procedure	Issues
	■ Ancile utilizes the technique proxy re-encryption for transferring encrypted records	■ The system is vulnerable to intrusion. ■ Lack of scalabilty
BSPP[5]	■ Private Blockchain: It is responsible for storing the personal health information (PHI). ■ Consortium Blockchain: It keeps index of PHI.	■ Ground level replacement of the existing system. ■ Require large storage space and time.

Problem Statement

Problem Statement

- To design and implement a secure blockchain based health care management system using multiple blockchains with scalabilty and low execution time and storage space.

Objectives

Objectives

Implement smart contract for intra-regional medical record sharing and add critical functions

Use cryptographic operations for protecting the record

Deploy the contract in the blockchain and test the web application

Implement smart contract for inter-regional medical record sharing

Deploy the contract in the blockchain and connect to the web application

Design

Blockchain

- It is a decentralized database.
- It maintains a distributed shared ledger which contains details of each transaction happened during a time interval.
- Each member in the blockchain have an address(Ethereum-20 bytes address).
- Each block have a previous block hash, current transaction details and a nonce for mining.
- Permissioned Blockchain:
  - The block can be created by the authorized person only.
  - Users are not freely able to join the network, see the history or issuing transactions of their own.
- Inter Blockchain technique:
  - To enable users to transfer valuable assets between different blockchain.
  - Reduce the global users and the size of distributed shared ledger.

Blockchain

- Smart contracts:
  - Also known as a cryptocontract , is a computer program that directly controls the transfer of digital currencies or assets between parties under certain conditions.
  - Smart contract helps to solve the issue of mistrust between parties and business partners.
- web3.js:
  - It enables to develop website or client that will interact with the blockchain.
  - It helps to write code which can read and write data from the blockchain with smart contract.
  - It talks to the Ethereum blockchain with JSON RPC, a "Remote Procedural Call" protocol.

InterPlanetary File System (IPFS)

- It is a peer to peer distributed file system.
- Also known as content addressed block storage model.
- It emerges as a stack of sub protocols,
  - Identities: Nodes are identified by a NodeId, cryptographic hash of public key.
  - Network: Manages connection to other peers.
  - Routing: Maintains information to locate other peers and objects.
  - Block Exchange - BitSwap protocol: Data distribution occurs by exchanging blocks with peers using a BitTorrent inspired protocol BitSwap.
  - Object Merkle DAG: IPFS builds a Merkle DAG, a Directed Acyclic Graph where links between objects are cryptographic hashes.
  - Files: Protocol for version control file system.
  - Naming:Protocol for self-certifying mutable name system.

IPFS

- Life time of a peer connection:
  1. Open: Peers send **ledgers** Until they agree.
  2. Sending: Peers exchange **want-lists** and **blocks**.
  3. Close: Peers deactivate a connection.
  4. Ignored: (special) a peer is ignored(for the duration of a timeout) if a node's strategy avoids sending.

Cryptography

- AES Encryption:
  - Key size: 256 bit key.
  - Padding: Pkcs7.
  - Mode: CBC.
- SHA256 Hashing:
  - Digest size: 256 bit.
- RSA Encryption:
  - Key size: 1024 bit modulus.

Smart contracts

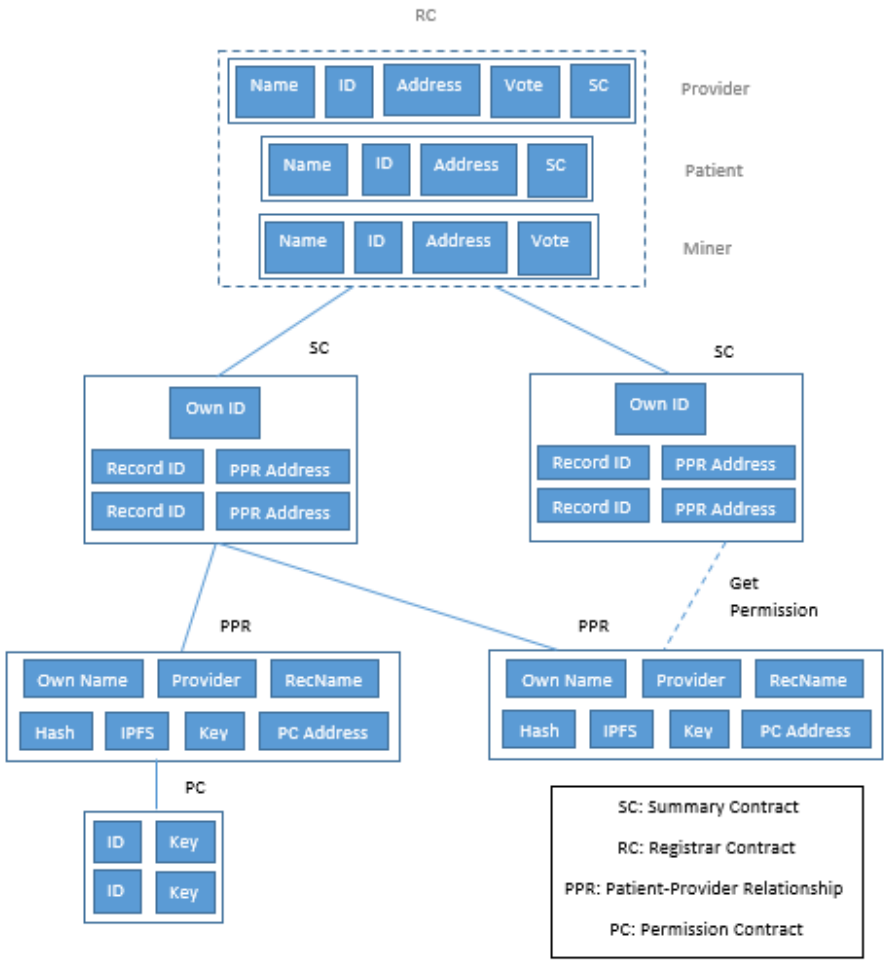

Figure: Intra-regional blockchain

Smart contracts

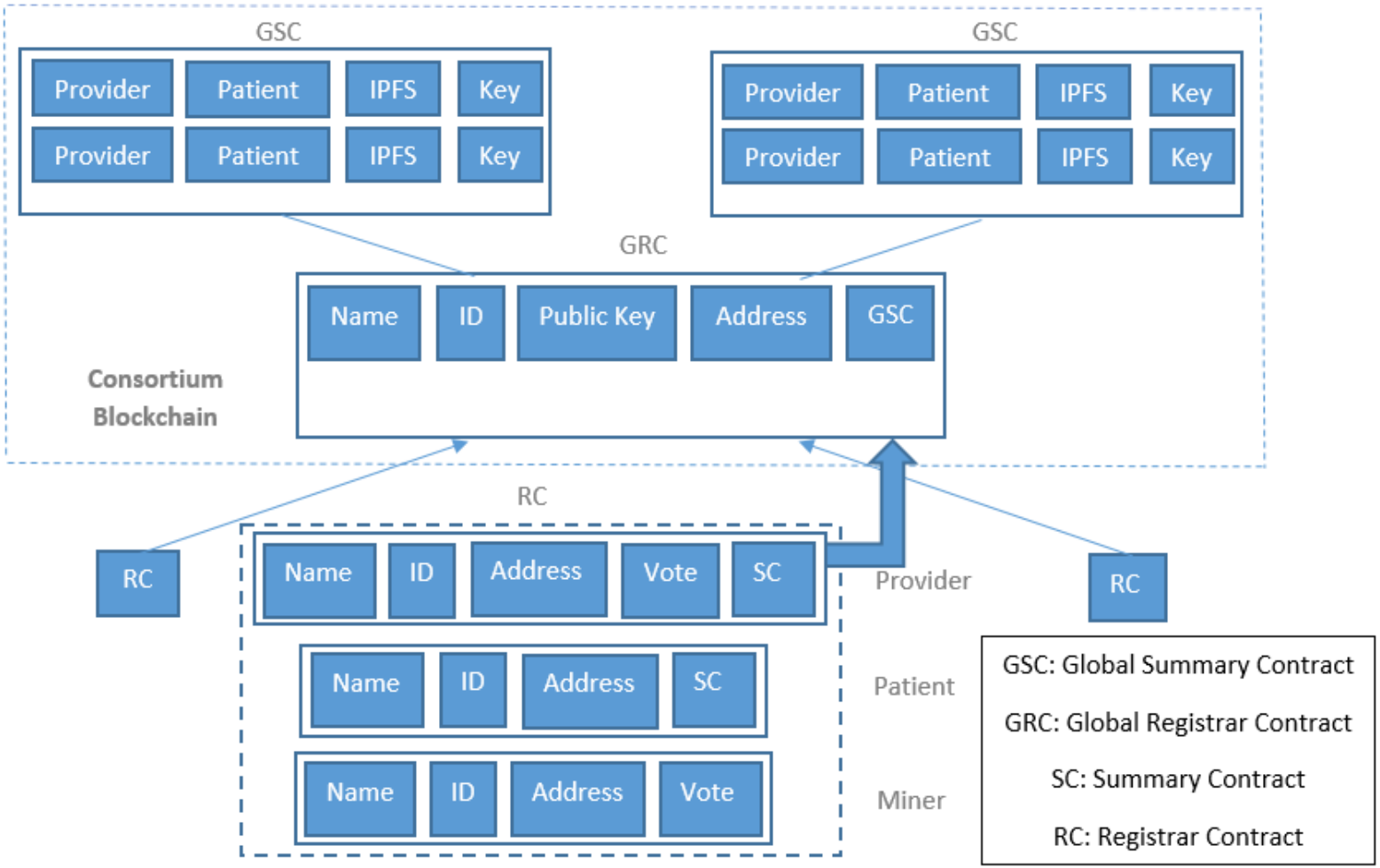

Figure: Inter-regional blockchain

Initial Process

- Users register into the blockchain with Name, Id and with their public key.
- For patient, the unique Id is generated at the time of registration.
- For Providers, the unique id is their Unique Physician Identification Number(UPIN).
- Providers must be verified by miners to add a medical record to the blockchain, using consensus mechanism.
- Providers must register into the consortium blockchain for accessing inter-regional medical records.

1. Storing an EMR record

Require: Register Provider and Patient to the blockchain.

1. Let the *emrrec* be the EMR record.
2. Find cryptographic hash of *emrrec*,

$$emrhash = sha256(emrrec) \tag{1}$$

3. Encrypt *emrrec* using AES algorithm with random key, k

$$encrec = E_k(emrrec) \tag{2}$$

4. Get the public key of provider and patient from blockchain.
5. Encrypt key using RSA algorithm

$$enckeypat = E_{PatKey}(k) \tag{3}$$

$$enckeypro = E_{ProKey}(k) \tag{4}$$

1. Storing an EMR record

6. Store the *encrec* into the **IPFS** and get the *ipfs-link*.

7. Store the *recname*,*recid*,*ownname*,*provname*,*enckeypat*,*enckeypro* and *ipfs-link* to the blockchain.

2. Retrieving EMR record

Require: Register Provider and Patient to the blockchain.

1. Get *enckeypat* or *enckeypro* and *ipfs-link* from blockchain.
2. Get *encrec* from **IPFS** using *ipfs-link*.
3. Decrypt the record key using private key of user,

$$k = D_{Patpriv}(enckeypro) \tag{5}$$

or

$$k = D_{Propriv}(enckeypat) \tag{6}$$

4. Decryt the EMR record,

$$emrrec = D_k(encrec)) \tag{7}$$

3. Adding Permission(by patient)

Require: Register Provider and Patient to the blockchain.

1. Get the public key of third party say *ThirdKey* from blockchain.
2. Get *enckeypat* from the blockchain.
3. Decrypt the record key using private key of patient,

$$k = D_{Patpriv}(enckeypat) \tag{8}$$

4. Ecrypt k with public key *ThirdKey*,

$$enckeythird = E_{ThirdKey}(k)) \tag{9}$$

5. Add *enckeythird* in the blockchain.

4. Interchain Permission

Require 1: Register Provider and Patient to the blockchain.
Require 2: Register Providers to the consortium blockchain.

Patient Side:

1. Get the public key of third party say *ThirdKey* from provider.
2. Get *enckeypat* from the blockchain.
3. Decrypt the record key using private key of patient,

$$k = D_{Patpriv}(enckeypat) \tag{10}$$

4. Ecrypt k with public key *ThirdKey*,

$$enckeythird = E_{ThirdKey}(k)) \tag{11}$$

5. Add *enckeythird* in the blockchain.

Provider Side:

1. Get *enckeythird* from the blockchain.
2. Add *enckeythird* in the consortium blockchain.

Software Requirements

- Ganache-cli: Ganache CLI is the latest version of TestRPC, a fast and customizable blockchain emulator. It allows to make calls to the blockchain without the overheads of running an actual Ethereum node.
- Remix Ethereium Online Compiler: To complile the Solidity Code.
- Web3: It is a collection of libraries, allow to interact with a local or remort Ethereum node, using an HTTP connection.
- IPFS node: For interacting with IPFS network.

Project Status

- Implemented smart contract for intra-regional medical record sharing.
- Protected record using cryptographic operations.
- Implemented smart contracts for inter-regional medical record sharing.
- Deployed and tested the whole system with sample users.

Contribution

Contribution

- Reduced Block creation time(Regional-blockchain)
- Reduced ledger memory(Regional-blockchain)
- Enhanced scalability(Inter-regional concept)
- Secured the EMR record(AES Encryption)
- Restricted fake providers(mining)
- Records cannot be altered(Blockchain: immutability)
- Records cannot be deleted(IPFS)
- No need of hostname or database port address, preventing intruders(IPFS)

Future Work

- Re-encryption: Proxy re-encryption (PRE) schemes are crypto-systems which allow third parties (proxies) to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another.

Conclusion

Conclusion

- Centralized health care systems are easy vulnerable to attacks like medical records have been changed by authorized or unauthorized users.
- Blockchain based ideas overcome these issues by keeping metadata of records immutable. But they need high time and storage requirments.
- To avoid these barriers, this paper proposes an inter blockchain concept.
- Also the proposed system prevents intruders which was an issue in the existing blockchain based ideas.

References

References

[1] Soon Hwa Han, Min Ho Lee, Sang Guk Kim, Jun Yong Jeong, Bi Na Lee, Myeong Seon Choi,Il Kon Kim, Woo Sung Park, Kyooseob Ha, Eunyoung Cho, Yoon Kim and Jae Bong Bae, "Implementation of Medical Information Exchange System Based on EHR Standard," IEEE Health Information research article 2010, Volume:16, pages 281-289.

[2] Mario Ciampi, Giuseppe De Pietro, Christian Esposito and Mario Sicuranza, "A federated inter-operability architecture for health information systems," IEEE international journal internet protocol technology 2013. Proceedings,volume: 07.

[3] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," International Conference on Open and Big Data 2016.

[4] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, Praneesh Babu Marella, "Ancile: Privacy Preserving Framework for access control and interoperability of electronic health records using blockchain technology", Elsevier International Journal 2018, volume:39, pages 283-297.

[5] Aiqing Zhang1 and Xiaodong Lin2, "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain", Springer International Journal 2018.