ISBN 978-9937-0-4872-9
September 27, 2018

ELECTRONIC HEALTH RECORD USING BLOCKCHAINTECHNOLOGY

Raj Prasad Shrestha
Department of Computer and Electronics Engineering
Kantipur Engineering College, T.U.
Lalitpur, Nepal
rajpsdshrest@gmail.com

Sushant Shrestha
Department of Computer and Electronics Engineering
Kantipur Engineering College, T.U.
Lalitpur, Nepal
yala.sushantshrestha@gmail.com

Suresh Gautam
Department of Research and Development
Extenso Data
Kathmandu, Nepal
suresh.gautam@extensodata.com

***Abstract*—The current existing electronic health records systems have many challenges like the patients are restricted to access their medical records and providing their essential medical data to the healthcare providers is quite difficult. In addition, the sensitive data(medical data) stored in the existing centralized systems are most likely to get hacked (by hackers), making it less secure. To address these challenges, electronic health record using the blockchain technology is the key solution. In this paper, it discusses how the blockchain technology solves the problem of a single point of failure and making the system more secure. Moreover, how this technology gives patient the full access to his/her medical data and also how it provides the authorization schemes to provide his/her available medical data to healthcare organizations or biomedical researchers.**

***Index Terms*—Electronic health record,Challenges,Blockchain technology**

I. Introduction

Electronic Health Record(EHR) simply means patients health record in the digital form. The health record contains two types of data they are administrative and clinical data. The administrative data are the patient's personal information like name, address, age, sex, phone no etc. And the clinical data are the patient's diagnosis summaries, lab reports and so on. The traditional paper-based health records have many disadvantages. Some disadvantages are handwritten or printed paper-based the record may get lost or stolen. Furthermore, other many factors like accessibility, availability, and maintainability of health data in a paper-based record system are quite difficult to achieve. EHR was designed and developed especially to address these problems of the paper-based system. Talking about the capabilities of EHR, the sensitive health data are stored in a manageable way. For the better health care service, health record data is very crucial considering this EHR gives the better availability of such data in a real time. EHR is also capable of maintaining each patients health record providing features like showing the doctor sessions date, statistics of health record and so on. Even though EHR has tremendous capabilities, it fails in providing privacy to the patient.

> EHR data contains the most value- able information like home addresses, personal mobile number, and patient health histories, making them more valuable to hackers than other types of data [1]. And 'the hackers can sell data for a premium on the black market(especially in the dark net), so hackers have a big incentive to focus their attacks on the healthcare industry.' [1] The second issue EHR systems has is lack of patients privacy. Without the knowledge of patients, EHR data is being manipulated and their data is being distributed to various sources. 'Medical ethics rules, state laws, and the federal law known as the Health Insurance Portability and Accountability Act (HIPAA), generally require doctors and their staff to keep patients' medical records confidential unless the patient allows the doctor's office to disclose them.' [2]

For the security purposes, EHR has employed many advanced technologies like password-based authentication, biometrics and other. But due to the advancement of hacking tools and techniques, these security technologies easily fails to provide a reliable and fault tolerant EHR system. EHR in maintaining the patients rights is way too abstract or not even has existed yet.

The medical data is a sensitive data so there should be a secure storage platform for health data along with a right given to the patient(not the healthcare organization) for controlling the distribution of the data. EHR using the blockchain technology perfectly fits for this purpose. The blockchain technology is the distributed ledger technology in which all the records of the transactions are kept among multiple peers in the blockchain network. The peers in the network use various advanced security technologies like cryptography tools and other consensus algorithms for invoking a

transaction. Here transaction in medical record data can be a doctor creating a new record for the patient or patient giving permission to access his/her medical data. This advanced security technologies employed by the blockchain technology makes the medical data immutable(unchangeable) making the EHR system more reliable and fault tolerant. The role-based features of blockchain technology give the patient full control of their data for the distribution among healthcare providers or biomedical researchers.

II. Blockchain Technology

As mentioned in the earlier sections blockchain technology helps to mitigate the challenges of the current existing electronic health record systems.

> Blockchain is a chain of blocks where blocks are linked together which forms a chain. Blockchain size grows with the growth in the number of transactions. Blocks record the sequence of transactions and time they were registered into the blockchain. Each block contains transaction data, timestamp, and the cryptographic hash of the previous block. The hash value of previous blocks link the blocks together and prevents blocks from being altered or tampered leading to blockchains key attribute of immutability.

First, the hash links of the blocks which prevents any block from being altered or block being inserted between them. In the blocks, transaction logs are maintained which are like a traditional double entry bookkeeping. Referring to the electronic health record the transactions can be creating a medical record, authorizing the medical record by the patient, viewing the medical record and so on. All these invoked/queried transactions are kept in the block. If an intruder(or hacker) tries to insert/alert a block(faking a transaction) in the formed blockchain(of electronic health record), he/she won't make a success so easily. The obvious of the failure(for an intruder) is each block in the blockchain contains the hash of the block's data and a hash of the previous block. As the data in the block changes, its unique hash also changes making an intruder a problem as he should perform several fake transactions until the complete valid blockchain forms. Here the data in the block can be the information about authorizing the doctor by the patient to view the medical records or can be something else. This what makes the blockchain more secure and almost impossible to change the contents of the block(immutable blocks).

Second, what if the intruder has the sufficient computations power to make the all the blocks(of the blockchain) valid in a very short period of time. He/she will make into the blockchain and can create problems. If this happens in electronic health record using blockchain technology, the patient will be in trouble or can even take his life. As the patient's health data is most the important asset when it comes to getting the good treatment. Seeing this, blockchain technology has a Smart Contract facility which makes the blockchain more secure by setting the transaction rules among the participants. To be more precise, for the electronic health record permissioned blockchain along with Smart Contract facility make sure that only the valid participants are invoking/querying the transaction in the blockchain.

Furthermore, each participant with its roles can be defined in the Smart Contract. For example, in case of Electronic health record only doctor participant is able to create a medical record for its patients and also patient is the only participant to make his data available to health organization or biomedical researchers.

Third, as blockchain is the distributed ledger technology all the contents of blockchain(ledger) is shared among multiple peers operating in different host machines in the blockchain network. In case of Electronic health record using blockchain technology the ledger which contains transaction logs are also distributed among multiple peers(in different in host machines). This solves the problem of a single point of failure of centralized existing electronic health record systems. Hackers also try to intercept the system using various hacking tools and techniques like Denial of Service(DoS) attacks, ransomware attacks etc. To avoid this blockchain technology uses various advanced cryptography tools and techniques.

Fourth, to make the blockchain more secure it uses consensus algorithms in invoking the transaction. Consensus simply means coming into an agreement on certain decisions. In order to make the transaction safe and reliable in electronic health record systems before committing a transaction in the blockchain, a consensus algorithm is to be run. For example, Peers are the one who connects the application client and the application client sends the request to the peers. Before updating the contents of blockchain an agreement between the available peers (two or more than two) should come to the conclusion whether to commit a transaction or discard a transaction to the blockchain. In case of electronic health record systems, four or five peers can decide whether to discard/commit a transaction. The point to be noted here is we can also configure which two particular main peers(or more than this) nodes participate in running the consensus ignoring the other peers of the network in case of the peer failure(fault tolerant).

From the above definition and working principles of blockchain technology, it is clear that the use of this technology in electronic health record can be quite beneficial.

III. EHR application model implementation

As shown in Fig: 1, our proposed system architecture consists of three layers. The top most layer is the frontend which provides the mean to display the available stuffs to the user and collects the data from the user for processing. The frontend web applications are usually written in HTML,CSS and Javascript. Underlying the frontend layer is the middle layer which consists of Smart Contracts(business logic layer) made by using Hyperledger composer framework. Actually, all the requests made through the frontend interfaces goes through the Smart Contracts. Smart Contracts,as the name implies, it

is a smart contract which consists of modeling files, access control lists, transaction logic and so on. And the hyperledger fabric is the main backbone of the blockchain technology as it features distributed ledger technology, transaction invoking tasks and reaching the consensus between peer nodes. The last layer is the backend layer which comprises all the transactions logs in the form of blockchain and peers worlds state database like CouchDB which stores all the peers states data.

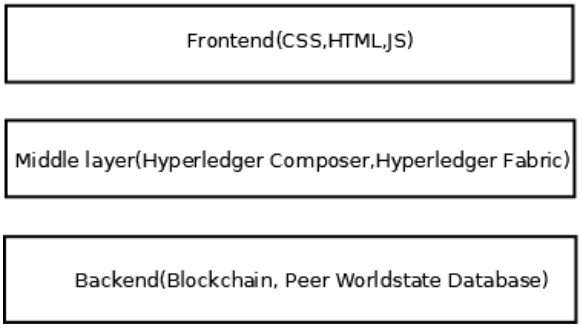

Fig. 1. Proposed system Architecture

A. EHR Blockchain network

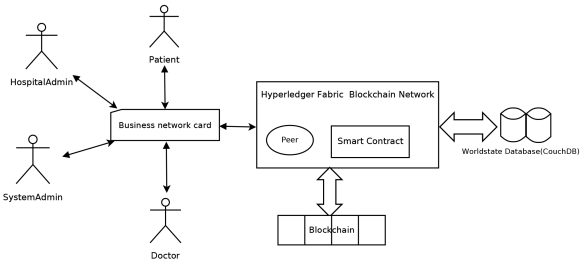

Fig. 2. Proposed EHR model

The Figure:2 shows the basic architecture of our platform. Our platform consist of mainly four participant System Admin, HospitalAdmin, Doctor and Patient. Each participant registered to our network consist of their own business network card. A Business Network Card contains the identity for a single Participant within a deployed blockchain network. Participant uses web application to interact with blockchain network. These web app uses REST API which is generated by hyperledger composer to call endpoints which are generated in accordance with the smart contracts of the business network. When the client applications calls one of the REST endpoints, the REST server will then submit a transaction to the blockchain network.

1) System Admin is the network administrator for our platform. Only SystemAdmin can add other participant (invoke transaction)and issue their identity in our blockchain network. After adding participant into the blockchain network a secret key and participant id is given to registered participant by the system admin.
2) Hospital Admin as a participant Hospital Admin registers doctor into particular hospitals and creates an appointment(invoke transaction) between doctor and patient.
3) Doctor as a participant can log in to his account and start the checkup session of the created appointment. Doctor can view patients previous record only after he has been authorized by the patient. Once authorized doctor can view and create new health record (invoke transaction) for the patient
4) Patient as a participant can log in to his account and can view his previous record(query transaction). Also Patient can authorize another participant so that other participant can view his medical record.

These four participants or the actors in our business network. Each participant has his/her own roles, asset structure (data stored on blockchain) and access control rights. While adding a participant to the blockchain network a blockchain identity (digital certificate) is also created for that participant which is stored in the identity registry. Each participant are mapped/linked to their blockchain identity. These identities are used to determine the permission and access to resources and information in the blockchain network. For a particular type of users, their access control is defined in the ACL which is a part of the smart contract. Patient as a participant can view his/her record. A patient can authorize and grant access to his/her health information to other participant(patients and doctors) by changing his/hers access control policy. This access control policy defines other participants who can access current participants data for the specific amount of time. Once granted access only when a participant can use private transactions to query other users data from the blockchain network.

IV. Hyperledger Fabric (HLF) Blockchain techonology

There are many Blockchain technology platforms like Ethereum, Hyperledger Fabric and so on but the most suited technology for the secure storage of medical record of patient is the Hyperledger Fabric Blockchain platform. Hyperleger fabric 'do not require cryptocurrency(token free) and the overhead of a public consensus based network' [3]. Thus, It can assure the transactions without expensive mining computations. Furthermore, Hyperledger farbic provides a 'Privacy through Channels' [4]. This means there is a provision of creating a private channel in which only the known/valid peers are to meant to execute the transaction.

In the context of health record system, cryptocurrency is not a really necessary thing as it requires expensive mining computations degrading the overall performance

of the blockchain system. Moreover, Hyperledger Fabric can configure secret channel among the peers in which the transactions logs are only visible to the peers who are in that secret channel. Here in the context of health record system,we can say that doctor and patient exchange transaction privately in the created secret channel.

To make the network of peers more trustable, the permissioned blockhain uses various plugabble consensus protocols like Crash Fault Tolerant (CFT) or Byzantine Fault Tolerant (BFT) consensus protocols that do not require costly mining. And the most crucial feature is the Smart Contract or what Fabric says chaincode which is the logic layer of the Blockchain application. Smart contract contains all the logic of the blockchain applications like Role based access control(like who can do what) , the data models files for defining the participants identites and transaction logic of the blockchain applications. On the other hand, fabric platform uses hashing algorithm which is SHA256 for computing the hash values encoded in the blocks of the blockchain after the transaction has occurred. Before updating the ledger in the peer nodes , block validation is also performed.

A. Hyperledger Fabric Permissioned Blockchain network

Hypledger fabric blockchain platform is entirely based on Docker container technology. All the components of hyperledger fabric run inside the docker containers. Some key components are channel, Ordering service, Certificate authority, Peers nodes with its ledger and deployed smart contract along with its world state database. Channel is a private communication medium through various peers communicate privately with their unique identities. The ordering service makes sure that all the contents of the ledger among peers in the network achieve consistency. The certificate authority is responsible for creating certificates for the participants and peers in the blockchain network. Peer nodes in the hyperledger fabric can be of three types. The first type is the committing peer which hosts the ledger and chaincode and connects to the application clients. Second type is the endorsing peer which validates the transaction request by checking the signatures and other certificates of the transaction. And the third type is the Orderer peer which provides the ordering service in the blockchain network.

As hyperledger fabric architecture is modular in nature, we dont have to install chaincode and ledger in the endorsing and orderer peers. In addition, any number of endorsing peers can be configured as required. We can achieve this by specifying the endorsement policies in the blockchain network. Same goes for the orderer peer we can configure it as required. In the context of health care, in a private channel various peers communicate with each other making it a permissioned blockchain network.

B. Hyperledger Composer

Hyperledger Composer is a framework to build a smart contract for the blockchain application. It is built on the top of the Hyperledger Fabric. It can be written using NodeJS or Go language. In the context of health record system, we created the chaincode using NodeJS. In our smart contract for the health record system ,it consist of three types of resources they are Participant, Asset and Transaction. Chaincode is all written in a BANANA(bna) file. This file consists of several files like the model file, access file, script file, and query file. The model file describes each participant like SystemAdmin, HospitalAdmin, Doctor and Patient along with their attributes. For example Patient particpant consists of personal information and medical data assets defined in the model file. Also, we can configure various input validation for surety of valid input data in the model file. In access file it defines who can do what and who can see what. Some of the access control policies we have implemented are as follows:

- Only Doctor participant can create medical data.
- Only Patient participant can view his medical data.
- Only SystemAdmin participant can issue identities to the doctor/patient.
- Only Patient can share his medical data to others.

In Script file, it contains all the logic for transaction processing. Various annotations of Hyperledger Composer were used for this to indicate which participant links to which data asset. It creates the method signature which can be used by the participant and overall logic for executing the transaction.

In Query file, it contains all the logic for executing queries so that the required data can be fetched easily. For example, we have written queries for fetching all the medical data belonging to one patient as one patient can have many medical data.

C. Deployment of the created Chaincode to the network

We then deployed the created SmartContract to the blockchain network. Here each peer (committing) hosts chaincode and ledger. This is the peer which gives service to the application clients. Application clients sends the request to the peer nodes in the network. Hyperledger composer server what we call the blockchain REST server generates REST API endpoints for each resource (participant, transaction, asset) of bna file. REST API endpoints directly connect with the application client and the blockchain server via NodeJS SDK connects to the peer of the blockchain network.

D. Hyperledger Fabric Blockchain identity

Each peer is given a certificate that contains the private key and digital certificate. Application clients must have a blockchain identity as issued by the Certificate Authority to interact with the Blockchain server. This blockchain

identity what we call the business network card contains all the certificates and private key to connect to the Hyperledger fabric network. Here SystemAdmin issues the application clients(doctor/patient) the business network card.

E. Chain and Worldstate Database

Hyperledger frabic stores data in two ways they are chain and worldstate database. Chain database contain the actual blockchain. Each block contain the transaction information and each transaction contains key/value pairs. Whereas, in the worldstate database all the last committed transaction value(asset) are stored according to the specific key. In the context of health record system, we have used CouchDB as the worldstate database which contains all the assets of each participant. As mentioned in the query file, we can apply queries to the asset data. Chaincode executes the queries based on data values saved in the CouchDB. Here the point to be noted is CouchDB database is introduced as all the heavy medical data shouldnt be saved on the chain database as it largely degrades the performance of overall blockchain system. In health record system, all the chaincode data values(JSON format) are stored in the CouchDB.

F. Hyperledger Explorer

It is one of the tool of the Hyperledger which show all the transaction logs, working peer nodes in the blockchain network and chaincode deployed to the network.

V. Result and Discussion

We can see use of blockchain in healthcare system reduces the operational cost in compared to paper based and traditional healthcare system reducing manual process. Also the speed of information distribution is also increased by using blockchain. There is no single point of failure in the system using the blockchain network. But users data security and anti-fraud is the main feature obtained from implementation of blockchain in healthcare. With the use of hyperledger fabric (private blockchain) can help to remove pseudonymous identity problem of public blockchain. In our blockchain network different participants have different asset structure and their own blockchain identity. Different participant have different rules defined on ACL defined in the smart contract which allows participant can query/create users assets by invoking specific transactions. Transactions are then stored in blockchain ledger and results of transactions stored in state database.

VI. Conclusion

This paper clearly describes how our proposed network platform avoids the single point of failure as it is a distributed ledger technology. Also, one of the important feature of this platform which is Smart Contracts. It facilitates the patient to access his/her medical data by providing him the rights to distribute the data to others. The valid medical data is the crucial asset when it comes to the good treatment of the patient as well as for a good research to the biomedical researchers. In addition, the privacy of the patient is also greatly considered. To conclude, the proposed platform is the most suited technology to address the challenges of todays existing electronic health record systems.

References

[1] Y.Niam (2017).Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches, [PDF], Available: https://www.brookings.edu/wp-content/uploads/2016/07/Patient-Privacy504v3.pdf, July 2018.

[2] Can Doctors Share Patient Information Without Permission?, [Online], Available: https://healthcare.findlaw.com/patient-rights/can-doctors-give-medical-information-to-others-without-permission.html, August 2018.

[3] Comparing HYPERLEDGER and ETHEREUM, [Online], Available: https://coinweez.com/hyperledger-vs-ethereum, August 2018.

[4] Hyperledger Fabric, A Blockchain Technology for Smart Contracts Development, [Online], Available: https://www.weblineindia.com/blog/hyperledger-fabric-blockchain-technology-smart-contracts, July 2018.

[5] A Blockchain Platform forthe Enterprise, [Online], Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/, July 2018.

[6] Guo, R., Shi, H., Zhao, Q. and Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. IEEE Access, 6, pp.11676-11686.