IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 26, No. 4, August, 2021, pp. 393-402
Journal homepage: http://iieta.org/journals/isi

Permissioned Healthcare Blockchain System for Securing the EHRs with Privacy Preservation

Katru Rama Rao[1*], Satuluri Naganjaneyulu[2]

[1] Dept. of CSE, JNTUK, Kakinada 533003, India
[2] Dept. of IT, Lakireddy Bali Reddy College of Engineering, Mylavaram 521230, India

Corresponding Author Email: krr.jntukphd@gmail.com

https://doi.org/10.18280/isi.260407

Received: 25 June 2021
Accepted: 9 August 2021

Keywords:
EHRs, blockchain network, data privacy and security

ABSTRACT

Healthcare data is very sensitive as many healthcare organizations will be very reluctant to share health data. However, sharing the healthcare data is having many more uses for both the patients as well as the research institutions too. Moreover, the existing Electronic Healthcare Record (EHR) management system will be stored in the central database in the form of plaintext. Whenever the data needs to be accessed from the database, the users will be requesting the required EHRs. However, this mechanism possesses the several challenges such as single point of failure, takes more time for user identification, interoperability issues, data recoverability issues, lack of privacy and security. This paper mainly focuses on providing security for the healthcare data, which can be shared among the various health institutions. Authentication and authorization are provided by establishing multiple certification authorities on the permissioned healthcare blockchain network. In this proposed model data integrity is also achieved by the concept of hashing of the electronic health records rather than storing it directly onto the permissioned healthcare block chain network.

1. INTRODUCTION

Blockchain is a distributed ledger of transactions, which is made up of blocks. Each block contains certain set of transactions which are verified by the validators (also known as miners) involved in the blockchain networks. It's a data structure has many interesting properties such as immutability, transparency, data integrity. Hence, the blockchain technology can be considered as "digital trust" in this modern era. Each block contains HASH (a message digest generated for the data in the block), timestamp (the time of its generation), nonce (a random number for maintaining the difficulty level in network), Merkle root. Hash of a block is dependent on its previous block. Likewise entire network is generated by linking up of all the blocks which are having certain valid transactions. There will be certain nodes known as the validators to verify the genuine transactions. These validators will be incentivized with certain credits such as data or certain amount of money to run the network. For instance, in the bitcoin blockchain [1], the validators will be rewarded by collecting the transaction fees and also by a reward for adding a block to the network successfully. In fact, there should be an incentive for these validators to the run the networks and lead this to achieve a consensus. As this mechanism with many such interesting properties can be extended to many other fields apart from the financial sector. The healthcare data management is one such field which can get more influenced with this blockchain mechanism [2-4]. Dealing with the personal healthcare data is very sensitive as many patients will be very reluctant to share health data. But, sharing the healthcare data is having many more uses for both the patients as well as the research institutions too. First of all, research institutions can use the data for many more scientific discoveries. For the patients the data sharing can be useful in accessing it from various remote locations. This paper mainly focuses on providing security for the healthcare data, which can be shared among the various health institutions. Authentication and authorization are provided by establishing multiple certification authorities on the blockchain network [5]. In this proposed model data integrity is also achieved by the concept of hashing of the electronic health records [6, 7] rather than storing it directly onto the block chain network.

2. LITERATURE REVIEW

The section presents the literature review of healthcare data field using blockchain. According to the research work [8-10] done on healthcare data sharing since 2004 to 2014. There are mainly 8 parameters are focused such as confidentiality, privacy, access control, integrity, data authenticity, user authentication, auditability and transparency. Till now the work has been done on providing security for the health care data sharing using the elliptical curve cryptography. In this work, our main aim is to design a blockchain network for secure health care data sharing using the concept of the bilinear pairings for signcryption scheme and identity based cryptography. This approach makes the technology computationally effective in data sharing. The following are the demerits observed for the existing EHR management system: Single point of failure, takes more time for user identification, interoperability issues, data recoverability issues, lack of privacy, security. In the classic

way of the EHR management, health records will be stored in the central database in the form of plaintext. Whenever the data needs to be accessed from the database, the users will be requesting the required EHRs.

Nalla and Reddy [11] presented a new identity based signcryption scheme for secure and authenticated data sharing using the concept of bilinear pairing based on elliptical curves. In this work it has been proven that the proposed ID-based signcryption scheme is better than the existing signcryption scheme by showing the comparison of the computations in both the schemes. This proposed signcryption model provides authenticity, non-repudiation, confidentiality and security. Peterson et al. [8] focused on the patient identification, security, infrastructure, interoperability. Data security (both privacy [12] and anonymity) are fundamental priorities for the system. In this work, it has been explored that how nodes in data sharing network may interact. Intuitively, it can be conceptualized that those nodes as individual institutions or providers. It has been envisioned a node not as a single institution, but as an entire blockchain-based data sharing network. That means not only cross-institutional sharing, but cross-network sharing as well. This would enable the institution/provider-based networks to grow and evolve, at the same time allowing them to connect to similar networks. This notion of aggregation, or nested blockchains, may be an approach to extending the reach of collaborations and sharing beyond local networks. For that purpose, all the EHRs should be following the same standards. The advantage to this approach is that consensus on a single identifier does not need to be reached and a patient may hold multiple blockchain addresses for different institutions. This model requires the patient to manage and maintain keys to these addresses using an electronic wallet. But for identifying the patients here MPI (master patient index is used here) which is centralized one. It can be transformed a decentralized one. Theodouli et al. [9] presented the capabilities of the blockchain by proposing a blockchain based model to provide privacy [13] and auditability for the health care data sharing. This methodology also shows the efficient way of handling access permissions of the health care data. Lin and Koo [10] applied blockchain technology on healthcare data management. In order to acquire the maximum benefits using this technology, blockchain has functioned as an access controller for the electronic health records. In the model proposed here, the data located inside the blockchain would be an index to the health records, time stamp of the health record's creation. The original health records will be stored in an off-chain storage called a "data lake". User is able to set his access control permissions very flexibly. There is a mobile dashboard is provided to show all the access control permissions clearly. After acquiring the permission to access the health care data, the healthcare provider queries the blockchain, gets authenticated by giving the digital signature to the blockchain. By combining the decentralized nature of the blockchain along with the digital signature [14] adversary cannot be able to impose as an actual user. The significant advantage of the blockchain is its disaster recovery and capability of fault tolerance. As the data is located in remote locations, there is no limitation of the single point of failure.

Ekblaw et al. [7] proposed "MedRec" model which is a novel, decentralized record management system can handle EHRs [15], using blockchain technology. This model focused on achieving authentication, confidentiality, accountability and data sharing while dealing with sensitive healthcare information. Using Ethereum smart contracts it provides patients with efficient storage and data access in the required manner. There are three kinds of smart contracts are used in this model such as Registry Contract (RC), Patient-Provider Relationship Contract (PPR), Summary Contract (SC). Yue et al. [16] proposed a blockchain application called as "Health Data Gateway". This application makes the health care data sharing easy and provided privacy for the health care data of the patients [3]. This application is consisting three 3 layers such as data usage layer, data management layer, secure data exchange layer. Once the data is stored in health data gateway application can be retrieved many times for various requirements.

Yang et al. [17] extended the MedRec model proposed by Yue et al. [16] by appending signcryption and attribute-based authentication. This model, for secured health care data sharing, it has used both signcryption and attribute based authentication [2]. This approach is useful in:

1. to view the EHR as a single record
2. to verify the authenticity of the patients
3. efficient access control for the patients
4. to maintain a transparent audit log.

Only the smart contracts Patient provider relationships (PPR) are stored on the blockchain, using which the user extracts information from the EHRs which are located in the database. Entire EHRs are not stored on the blockchain to avoid the data redundancy problem. The application of signcryption is useful in providing the authenticity and efficient data access. Xue et al. [18] proposed a scheme known as private blockchain based access control (PBAC) which was used to provide security, privacy for smart homes. This PBAC scheme saves access records by using benefits of blockchain and reduces the computational overhead greatly.

Zhou et al. [19] (2019) proposed an access control scheme based on blockchain for the smart grids. Currently, most of the existing centralized access control schemes of the power grids are lacking in security, data integrity etc. This proposed model is based on identity based combined encryption and signcryption mechanism. It solves those issues by using the consensus mechanism in a consortium blockchain. In the proposed scheme to lower the computation cost, same key pair is used to sign, encrypt and signcrypt is used. Fan and Zhang [20] used a consortium blockchain on smart grids to provide it efficient and flexible regulation. In this work signcryption is used for acquiring multidimensional data in multiple receivers. In this proposed model, fixed size of blocks in the blockchain are used to regulate in the data received from multiple receivers. By utilizing the feedback received on the smart contracts, grid operators regulate the user power. The summary of related work includes supporting scheme, advantages, future work and benefited end users is shown in the below Table 1.

Table 1. Summary of related work

No.	Title	Supporting Scheme	Advantage	Future Work	End Users
1	Kevin et al.	Proof of interoperability	Security, interoperability of EHRs	Can be adopted among the multiple blockchain networks	Patients, medical institutions
2	Theodouli et al.	Proof of interoperability	(i) private and auditable healthcare data sharing and (ii) healthcare data access permission handling	Have immersive boosting in the medical field	Patients, medical research centers
3	Lin et al.		Access control to personal EHR, scalability, security and data privacy		Patients, doctors, smart devices
4	Ekblaw et al.	Proof of Work	authentication, confidentiality, accountability and data	Can be adopted by the pharmaceutical companies, insurance companies	Patient, researcher, public health authorities
5	Yue et al.	Centric Schema (ICS)	sharing of EHRs shows blockchains potential in health IT & research Patient controllable EHR by providing security, privacy	HDGs can communicate with other HDGs	Patients, hospitals, research institutions
6	Yang et al.	ABE (encryption keys)	Authenticity, integrin, confidentiality authenticity, flexible access control of EHR is achieved		Patients, users (can be medical institutions, researchers)
7	Xue et al.	PBAC scheme.	Safe storage, resistance to tampering data. solution for outsourcing challenge	Not only for smart homes can be applied to different scenarios	Owner, visitor, administrator,

3. SYSTEM ARCHITECTURE OF THE PROPOSED PERMISSIONED HEALTHCARE BLOCKCHAIN PLATFORM

This presents the proposed permissioned Healthcare Blockchain that provides more efficiency in storing the Electronic Health Records (EHR) in a secure way. It also provides the facility to trace back all the previous transactions that had occurred to a specific EHR including the timestamp attached to it. Basically, the overall architecture of the healthcare blockchain which was proposed here is having three modules with it such as 1. Users, 2. healthcare blockchain, 3. Off-chain database. In the proposed healthcare blockchain application, a user can be a patient or a doctor or a pharmacist or an administrator or a health insurer. They will be having different kinds of responsibilities in the permissioned healthcare blockchain application. All of those responsibilities of the users from the user group of this application are represented in Table 2.

Off-chain database contains the original EHRs, information regarding the billing and prescriptions. This off-chain database is an independent data repository. This entire information would be a valuable tool for further analysis of patient data and also for the research, disease prevention.

Table 2. User group and their responsibilities

Actor	Task
Patient	• Owns the data • Registers for EHR registration • Gets enrolled by endorser peers upon showing the required ID proof (Aadhar card/passport). • Controls and updates his data in EHR • Gets authenticated by the doctor
Doctor	• Approves the patient data to be stored in EHR. • Manages patient's demographics. • Has access to his authenticated patient's EHR. • Recommends other new doctor if needed.
Research institute	• Asks for patient's permission to get access to EHR • Provides related keywords for the required data from the EHR
Lab technician	• They collect data of patients using their devices (x-ray/Bp kind of data) • Verifies that data and updates into EHR. • Communicates with the authenticated doctor for that patient
administrator	• Checks patients' registration, enrollment details • Gives appointment to the doctor • Charges the bill
Health insurer	• Verifies and validates the data in EHR. • Checks registration and enrollment details of patient to provide them the eligible insurance. • Checks database if any changes are made, interacts with the medical staff to confirm.

Healthcare blockchain contains the up-to-date history and modifications done to the electronic health records and other information present in the off-chain database. Blockchains are suitable especially for dealing with the limited sized information. Having vast amount of data on the blocks of a blockchain increases managing costs and also the data redundancy problem. So, to avoid this problem, off-chain database is used to store the entire EHRs. Only the modifications performed to these EHRs are tracked and saved as the transactions of the proposed permissioned healthcare blockchain. The healthcare blockchain contains different peers. There is no limit on the number of peers to be kept on the blockchain platform. Each peer will contain the individual copy of the distributed ledger with them. This is useful in maintaining the consistence of the distributed ledger eventually. Ledger will be consisting of the blockchain having the interlinked blocks with certain set of transaction inside them. These transactions can be any changes made to the electronic healthcare records (EHR) or create requests of EHRs or any sort query proposals made to the off-chain database.

Each peer will be associated with an access control policy which will define certain set rules to be followed while making a transaction and to verify it whether it is matching with all the remaining peers or not. To execute any operation inside the peer there has to be some system code attached to it. This specific system code is technically termed as a smart contract. In hyper ledger fabric platform, we call this as chaincode. The following Figure 1 represents the overall architecture of the healthcare blockchain application.

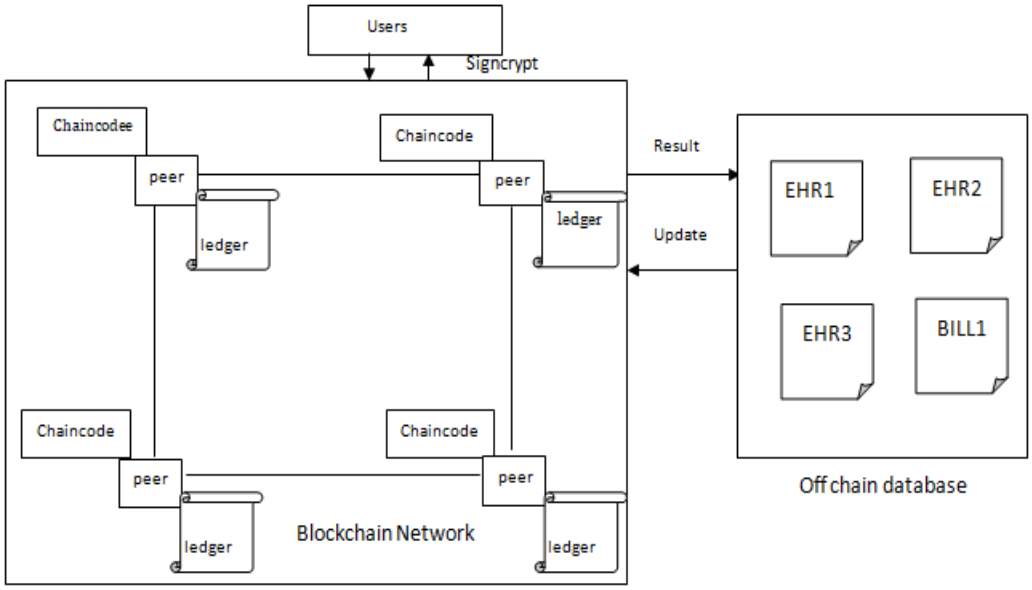

Figure 1. Overall architecture of the proposed healthcare blockchain application

From the user's point of view, "the smart contract" which is needed to run various kind of operations or the transactions and "copy of the distributed ledger" are provided as the applications. The peers in the healthcare blockchain network are broadly classified into two categories such as validating peers and the non-validating peers.

3.1 EHR generation and EHR sharing in the healthcare blockchain

After getting enrolled successfully, the patient will get permission to access the healthcare blockchain platform with the issued certificate. The proposed work uses operational procedures to propose a transaction to create an EHR and sharing the EHR in the blockchain network. Using a specific client application, patient provides his health-related information to be stored onto the EHR. Then the client creates request for the transaction proposal to invoke a chaincode function on the endorser or the validating peers using POST method. The invoked chaincode get executed, the produced transaction results are passed back to the client. According to the access control policy which was already defined, the client application verifies the produced results of the transaction proposals. Then client application sends the endorsed transactions to the ordering service. This ordering service arranges the endorsed transactions in a chronological manner by channel and generates blocks of transactions per channel. For the validation purpose, the ordered blocks of transactions are broadcasted to all the peers on the channel. Every peer appends the block to the chain, EHR record is saved onto the current state database. Eventually, to notify that an EHR got created an event gets emitted to the client application.

3.2 Distributed ledger storage of the healthcare blockchain application

Ledger structure basically consists of two parts in it, such as world state and blockchain. World state means, the current state of the ledger. This world state is like a snapshot of the transactions in the ledger given at a specific point of time. This world state keeps varying according to the transactions. Couch DB is a popular and efficient state database which provides advanced query support when the chaincode's data is framed in the java script object notation (JSON) format. To get information or the content from the couch DB, data should be framed in the JSON format in order to implement the content based queries. Blockchain is the entire transaction log that has happened in the entire network. World state in the ledger structure makes the time efficiently utilized as it avoids the process of traversing the entire transaction log each time when it's needed. Unlike the world state,

blockchain is a data structure that stores simple operations and all the changes made to the world state in a sequence manner including the time stamp at which it has occurred. In the blockchain all the transactions are grouped into blocks and then those blocks are cryptographically linked together in the form of a chain in a timely order is shown in Figure 2.

The executed transactions will be grouped together into blocks. Each block will be associated with specific "key, value pairs". These key value pairs in the world state are stored into the hash tables. These hash tables will be having the pre-decided number of blocks. To find the required bucket number in which the key presented, there will be a hash function to be executed. The smart contract [21] in the block chain network is also termed as Chaincode. This chaincode can be provided as a transaction to be distributed to each and every node in the network. Generally, this chaincode is kept as a separate sandbox and managed by the validator. At Docker container is used to run the chaincode.

3.3 Designing chaincode of the healthcare blockchain platform

Chaincode is designed and implemented by using the hyper ledger fabric, which makes it really easier to be suitable for the industrial purposes by providing the service of subnetworks. By this concept of isolated subnetworks or the specific channels which need to be installed among the selected peers according to the convenience more flexibility as well as the efficiency is achieved. The chaincode consists of the script, query definitions and the access control rule. In the proposed health care blockchain application it can be patient, doctor, nurses or any other users from the identified users group. User group types and models must have a unique identifier to be identified by the network. A patient's electronic health record (EHR) contains the general information such as personal information and medical history about a diagnosis.

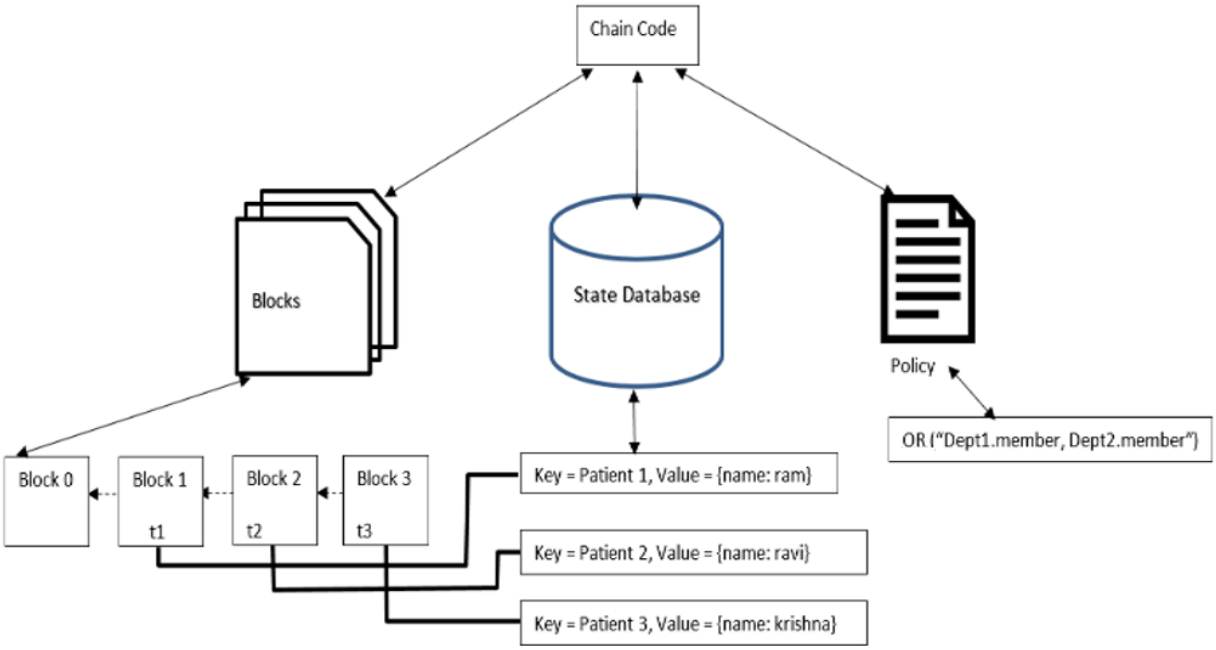

Figure 2. Storage of EHR in the blockchain network

3.4 Querying the EHR in healthcare blockchain application

Using GET method doctor can request the API endpoint for querying the EHR from the state database by providing the patient's ID as the input. As the chaincode associated for that request queries only the ledger, as all of the peers keep a copy of the ledger in their local database the platform would not submit the transaction to the membership service. As the information is already presented I their local database, no consensus process is required. So, the result of the proposed query is provided immediately.

3.5 Data portability and privacy preservation of EHR data

Data portability means to transmit the EHR Data from one provider to another provider without any trust between the them. The EHR Data should not be corrupted while transmitting from one provider to another provider i.e. the original EHR Data sent from the provider should be received to another provider by taking the privacy concerns. EHR Data can be structured or commonly used but it should be in format such that it will be readable by the machines. But the question arises here is that "The EHR Data is portable [22] here that easily or there are some difficulties?" EHR Data cannot be directly transferred from one device to another easily because of interoperability [23] and difference in standards between the two devices. So, to transmit the EHR Data from one device to another we need to take the following things in consideration. Both the devices should have broadly accepted standard. Both the devices should be interoperable. Data portability standards which are globally accepted now for all the devices were first introduced by General Data Protection Regulation (GDPR). According to GDPR data portability right has two phase structures.

In the first phase it says that each individual should have a duplicate copy of their information i.e. EHR Data in commonly used, structured and machine-readable format. But the GDPR doesn't exactly describe what does above 3 words ("Structured", "Commonly used", "Machine-readable format"). So different people interpret as different because of

not clear definition about the three terms. When one device receives some EHR Data in some format like ".pdf" or ".zip" then they may face some complications for understanding the EHR Data or transmitting the data. Hence the right format of EHR Data is required to transfer the data. If the EHR Data is structured i.e. In "CSV" or "JSON" format. These formats of EHR increase the possibilities of their interconnection as well as it EHR Data can be used again and again because it has well defined structure, so it is easily understandable.

1. EHR Data format should be commonly used. But the EHR Data formats changes for different types of industries. If the communication is being done between the devices in music industry, then mostly EHR Data format will be "MP3" or "AAC". If the formats are not common then formats are taken from "Article 29 Working Party's Guidelines" which provides open formats for all types of data.
2. If the data is in Machine-readable format, then it is easier for the devices to identify process and excerpt the data.

3.6 Control of the diffusion of all EHR information is achieved using Blockchain

Control of the diffusion of all such information is possible with the Blockchain system; it could be controlled if the transfer of the data has been done in some well-defined manner. Using this technology, the EHR data is noticeable i.e. it can be easily searched. This will provide a clear view of different types of data that if it has been shared between different providers. After the data has been collected, we can apply different kind of analytics to analyze the data for efficient decision making. However, after the data has been analyzed then that data should not be provided to any provider only with the permission of patient.

4. IMPLEMENTATION AND RESULT ANALYSIS

The section presents the Implementation and Result Analysis of the healthcare blockchain based using hyper ledger platform is represented in the following Figure 3. The represented network topology includes the departments such as cardiology, neurology, gynecology and ophthalmology which are designated as D1, D2, D3 and D4. All these four departments will be having a common agreement of network policy (NP)that they will setup and initialize a blockchain network. D1, D2 departments will be functioning under a common subnetwork represented as channel 1 and likewise for D3, D4 departments there is channel 2. Channel 1 functions according to the rules governed in the channel policy CP1. It is controlled by the peers P1 and P2, in which the chaincode CC1 and ledger L1 are placed. Likewise, for channel 2 there is channel policy CP2 under departments D3, D4. This channel 2 is controlled by the peers P3, P4 which holds the chaincode CC2, ledger L2. Single department can hold multiple peers. The ordering service manages the network services such as adding a new peer to the network and removing a specific peer from a network. In the healthcare blockchain network using the hyper ledger fabric, peers can dynamically change. All these changes regarding the peers can also be stored in the form of the transaction to maintain the accountability in the healthcare blockchain network. The ordering service communicates with the channel1 and channel2 for the purpose of ordering the transactions in a block. There are client applications in the blockchain network which are represented by A1, A2, A3 and A4. They communicate with other entities of the network using the channels C1 and C2. Each department is provided with a Root certificate authority (Root CA) and this root CA is internally controlled by the hierarchy of the four CAs such as RA, ECA, TLS-CA and TCA. This CA issues all the PKI based certificates to all the departments in the blockchain network. The network topology of the healthcare blockchain platform is represented in the following Figure 3.

In the proposed healthcare blockchain network, transactions can be creating, updating and deleting of the electronic health records which are stored in the off-chain database. Some of the transactions can also be like transferring data among the connected peers of the blockchain network. To transform the open permission less blockchain network to the permissioned blockchain, membership service is added to the blockchain network which verifies the nodes and authenticates them to interact with the blockchain network. In open blockchain [24], any peer or node can come pose transactions and able to view the content inside the ledger.

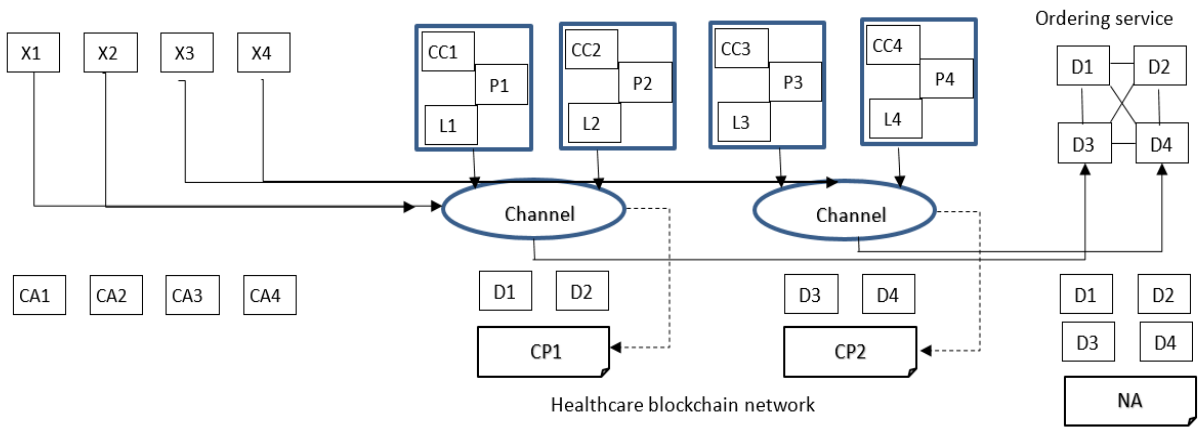

Figure 3. Healthcare blockchain network in hyper ledger fabric

But this leads to the security issues which may arise so highly in the future. Because, in the proposed healthcare blockchain mainly patient's personal health data is dealt this needs to be managed so confidentially. For that sole purpose, rather than using the open permission less blockchain, permissioned blockchain is used. In the permissioned blockchain only the peers who got registered and enrolled to the membership service will only be allowed to submit their

required transaction proposals to be performed on the EHRs. To improve more privacy in the proposed blockchain network, subnetworks concept is introduced which is achievable with the implementation in the hyper ledger fabric platform. The hyper ledger platform is solely dedicated to the industrial purposes such as providing more flexibility and privacy with help of the subnetworks among the required set of peers. This makes the content and transactions of one set of peers which needs to be kept confidential from the other set of peers. Only the eligible peers can be allowed to access the content of other peer's transactions. Using the concept of subnetworks, any number of peers can be grouped together and make their details hidden to the remaining unauthorized peers. In the proposed permissioned healthcare blockchain platform, user gets enrolled through the four certificate authorities such as RA, ECA, TLS-CA, TCA which will get synchronized collaboratively managed by the root certificate authority (Root CA) in a hierarchical manner. Say here in the healthcare blockchain there are four departments named cardiology department, neurology, ophthalmology and radiology departments. Each department has three peers. Those peers in the departments will contain certain smart contract and data storage to verify the transaction proposals or to write the transaction blocks to the ledger. The distributed ledger records all the transaction in a chronological manner to make the users to be known what has happened to their EHRs clearly. Consensus protocols and the cryptographic properties such as signcryption using identity based cryptography (IBC) are implemented to achieve the consistence of the distributed ledger.

Root CA in the membership service abstracts away all cryptographic details of the operations, and provides the user with required certificate services. Each peer will be consisting of the world state, blockchain, smart contract and access control policy. World state is a kind of snapshot, in which the current state of the distributed ledger at a given point of time is saved. This world state keeps on changing along with the modifications done to the actual ledger. Blockchain is the entire record of the transaction log and the changes made to the EHRs. Ledger is the combination world state and blockchain. To perform all these transactions and various operations with help of predefined smart contracts. Access control policy is set of certain conditions to be followed while designing and proposing a specific transaction in the health blockchain application. Client application on the behalf of the user will be external to the blockchain network and to interact with the world state, invokes the smart contract.

4.1 User registration

User registration process is performed by the Registration Authority (RA). User, approaches the client for the purpose of sending the registration request to the RA. Client, on the behalf of the user, requests registration authority by submitting the legitimate identity credentials required such as passport. RA verifies the identity credentials provided by the client. If the submitted information is valid, RA stores those verified identity credentials in its local database. RA, then creates an account for the user and sends back the associated username and password to the client. Once the registration process of the user is successfully performed, the user is eligible to enroll into the permissioned healthcare blockchain application. Users after submitting the required, strong identity credentials to the membership service and got registered to it, will be provided with the credentials to install the client software. Then the users will submit the transactions to the blockchain network.

4.2 User enrollment process

The healthcare blockchain framework has four kinds of certificate authorities (CA's) such as RA, ECA, TCA and TLS-CA. The certificate authorities are responsible for generating the private keys related to public keys.

1. Step1: RA receives the username and password from the user. This means, the user has got formally registered into the database of the system.
2. Step2: The client requires TLS-CA certificate to check whether that the TLS handshake is properly setup with the server or not.
3. Step3: Client sends ECA, the registration request including its enrollment public key and some additional information like username and password. Using this submitted information by the user; ECA verifies whether the user actually exists in the database. Once it ensures that the user is eligible to submit his public key of enrollment, ECA will certify it.
4. Step4: Then ECA makes and sends back the enrollment certificate (Ecert) after signing it, to the client which holds enrollment public key of the user. Along with the Ecert, ECA will also send one more certificate named ECA-cert which prove to TCA that this Ecert is legitimate and created by proper ECA.
5. Step5: Client will verify that the enrollment public key inside the Ecert is send by the client or not. And also, it verifies the information inside of the Ecert is complete and well formed.
6. Step6: Then the client sends TLS-CA, a registration request along with client's public key and information regarding identity.
7. Step7: Then the TLS-CA verifies that whether the user is actually existing in the database or not. It creates a TLS-Cert which contains TLS public key of the user and signs it. TLS-CA sends the TLS-Cert along with its own certificate (TLS-CA Cert).
8. Step8: the client verifies that the public key inside the TLS Cert is the one originally submitted by the client and that the information in the TLS Cert is complete and properly formed.
9. Step9: the client stores all the certificates in local storage for both certificates. At this point the user enrollment has been completed.

In this enrollment process, distributed authentication [23] is ensured by verifying all certificates of the certificate authorities such as ECA-cert, TLS-CA cert, TCA-cert. If any certificate such as ECA-cert is verified means, its ensured that the certificate is actually coming from the authenticated CA. Eventually, it's proven that authentication is distributed among various certificate authorities rather than having single CA.

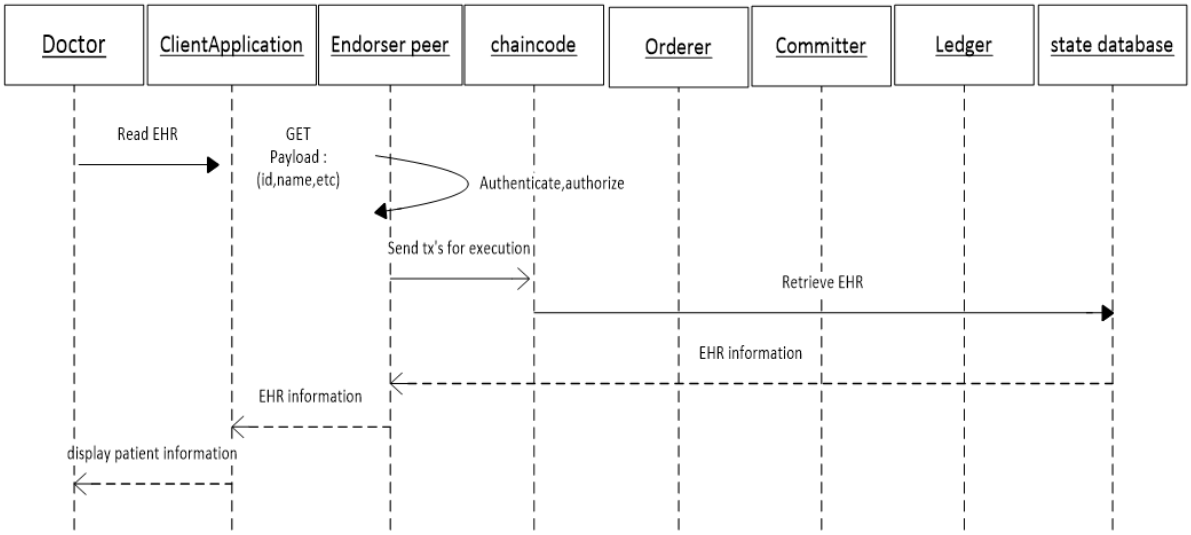

Figure 4. Accessing the EHR from the blockchain network

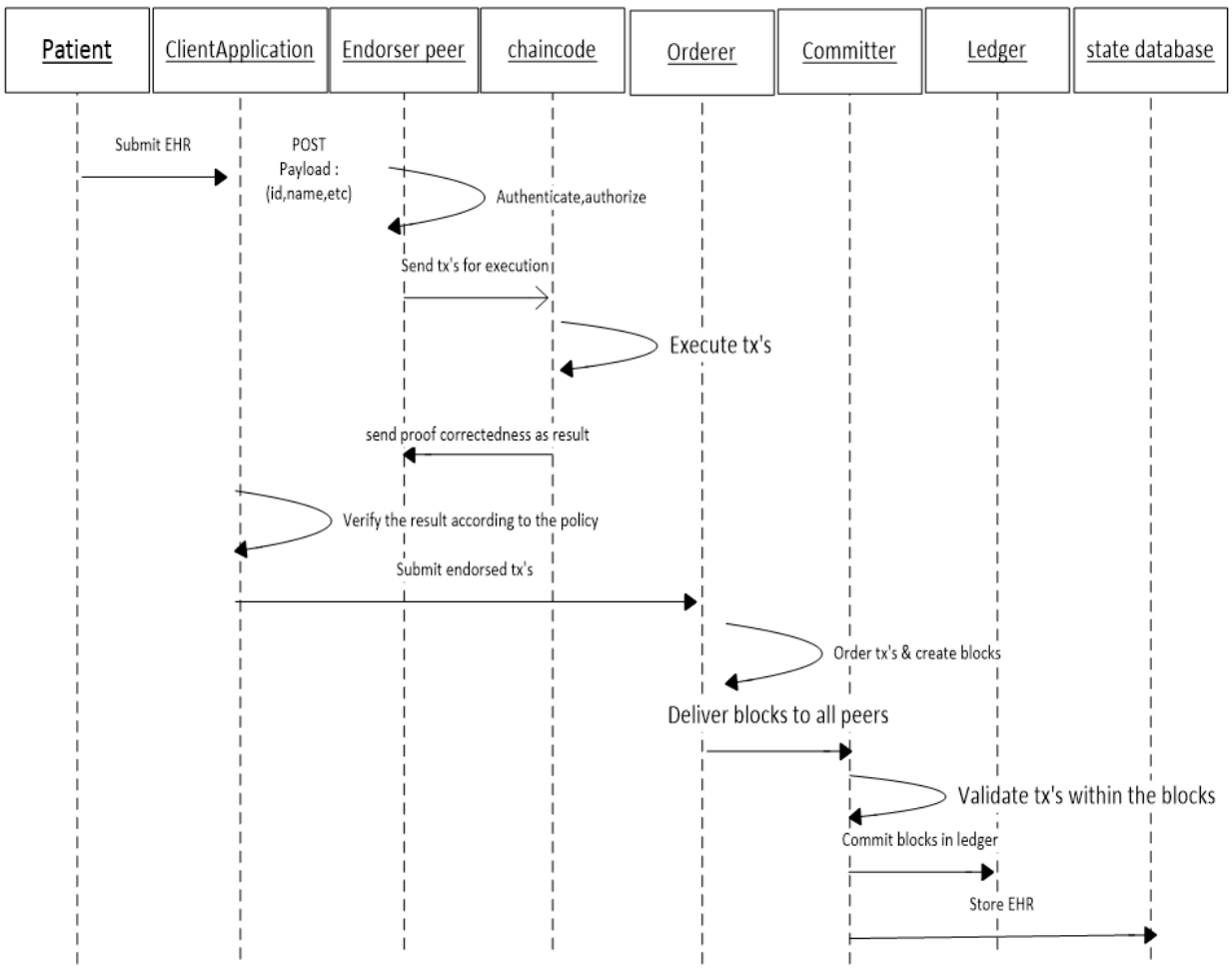

Figure 5. Transaction flow of creating the EHR in the proposed health care blockchain system

4.3 Transaction flow in the proposed health care blockchain application

To submit the transaction proposals in the form of user messages and to execute them successfully in the healthcare blockchain platform, first the user needs to be registered and enrolled to the system. The registration process of the user group is made complete by verifying the identity credentials provided by client application on behalf of the users. The registration authority (RA) owns the specific username and passwords of the users who have registered into the blockchain network and authenticates them by verifying the secret key obtained during the registration process. Then RA allows the verified users to get enrolled. Transaction flow starts with the user messages submitted by the client application to all the peers in the network. The

communication between the client application and healthcare blockchain network happens over the application called software development kit (SDK). Peers in blockchain network can be either validating peers (endorser peer) or the non-validating peers (committers). Validating peers or the validators simulate the transaction proposals and sign them. Simulating means the process of taking new transactions, executing them and updating the ledger with the current values. Validators are responsible for approving authorized users by giving them permission and deny the unauthorized users from accessing the blockchain network. Non validating peers only validate then transactions before writing the transactions onto the blockchain. Validators (endorsers) are a subset of the non-validators (committers) which hold the chaincode for executing the transactions of the users. First after receiving the transaction proposal from the user, validator will execute the transaction in their simulated environment by calling the required chaincode. Validator will not update the ledger immediately. That Validator collects the read and write set or RW set such as, the data which is read from the world state of the ledger and then the data which needs to be written onto the ledger upon executing the transaction during the transaction's simulation process. Validator signs the RW set and sends it back to the client application as shown in Figure 4 and Figure 5. Client application collects the signed transaction as response to the simulated transaction and along with this, includes the RW sets then sends to the membership service. In the membership service "orderer" is the node which responsible for ordering the endorsed transactions.

In the entire network consensus happens, simultaneously the RW sets and the signed transactions are submitted. Then this data ordered chronologically by the orderer into a block and then delivered to all the non-validating peers. Each peer validates the transaction whether it is matching with the world state at the moment. When each peer had validated the transaction, that transaction is updated into the ledger by make use of the instructions as shown in Figure 6.

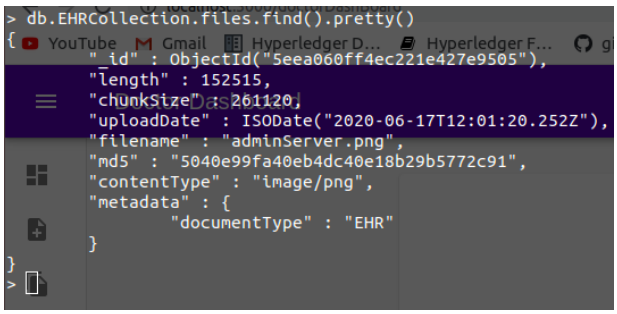

Figure 6. Updating of EHR in Blockchain system

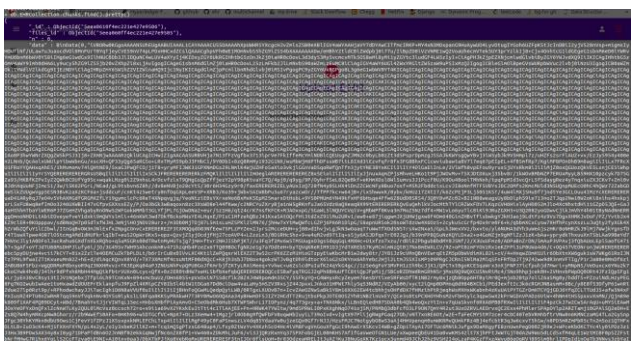

Figure 7. Secure Storing of EHR in Blockchain system

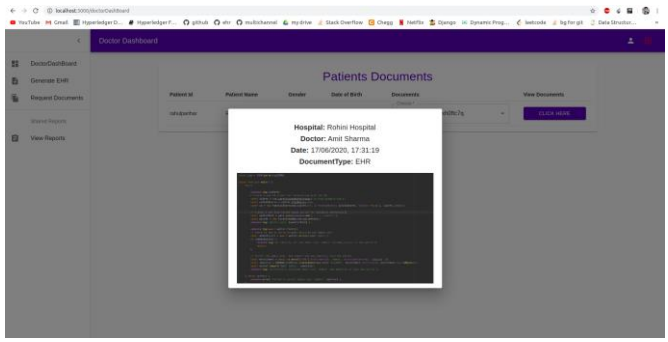

Figure 8. Accessing of EHR by the Doctor from Blockchain system

Then the updated EHR will be securely stored in blockchain system as shown in the Figure 7. Then the world state is RW set's write data. An authorized doctor is allowed to access the EHR from blockchain system as shown in the Figure 8. Finally, the non-validator notifies the user whether the transaction which was submitted by the user is successfully executed or not. To get notified by the peers, the client application needs to subscribe to the events respected to the operation it wants to perform. The entire transaction flow in the healthcare blockchain is represented in Figure 4.

5. CONCLUSIONS

This paper mainly focuses on securing the EHRs using permission blockchain system, which can be shared among the various health institutions. Initially, all patients, doctors and other members must register to the blockchain system. The Authentication and authorization are provided by establishing multiple certification authorities for these members of the network. In this proposed model data integrity is also achieved by the concept of hashing of the electronic health records rather than storing it directly onto the block chain network. Finally, privacy in blockchains can be ensured using cryptographic keys. One can share his public key with others because it doesn't reveal any kind of information about the user and it is difficult to derive private key just by knowing public key. In the future work, applying identity based cryptography to these EHRs in proposed blockchain for providing better distribution of keys.

REFERENCES

[1] Nakamoto, S. (2012). Bitcoin: A Peer-to-Peer Electronic Cash System. pp. 1-9.

[2] Guo, R, Shi, H., Zhao, Q., Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access, 6: 11676-11686. http://dx.doi.org/10.1109/ACCESS.2018.2801266

[3] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., Chen, Z.X. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos One, 15(12) e0243043. https://doi.org/10.1371/journal.pone.0243043

[4] Tang, F., Ma, S., Xiang, Y., Lin, C. (2019). An efficient authentication scheme for blockchain-based electronic health records. IEEE Access, 7: 41678-41689. http://dx.doi.org/10.1109/ACCESS.2019.2904300

[5] Kassab, M., DeFranco, J., Malas, T., Graciano Neto, V.V., Destefanis, G. (2019). Blockchain: A panacea for electronic health records. IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH), pp. 21-24. http://dx.doi.org/10.1109/SEH.2019.00011

[6] Shahnaz, A., Qamar, U., Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7: 147782-147795. http://dx.doi.org/10.1109/ACCESS.2019.2946373

[7] Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Proceedings of IEEE Open & Big Data Conference, pp. 1-13.

[8] Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K. (2016). A blockchain-based approach to health information exchange networks. In Proc. NIST Workshop Blockchain Healthcare, 1: 1-10.

[9] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., Tzovaras, D. (2018). On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1374-1379. http://dx.doi.org/10.1109/TrustCom/BigDataSE.2018.00190

[10] Lin, L.A., Koo, M.B. (2016). Blockchain for health data and its potential use in health it and health care related research. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, pp. 1-10.

[11] Nalla, D., Reddy, K.C. (2003). Signcryption scheme for Identity-based Cryptosystems. IACR Cryptology ePrint Archive 66.

[12] Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39(1): 283-297. http://dx.doi.org/10.1016/j.scs.2018.02.014

[13] Li, C., Palanisamy, B. (2018). Privacy in internet of things: from principles to technologies. IEEE, 6(1): 488-505. https://doi.org/10.1109/JIOT.2018.2864168

[14] Fromknecht, C., Velicanu, D. (2014). A namecoin based decentralized authentication system. 1-19.

[15] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S., Rodrigues, J.J.P.C. (2018). BHEEM: A blockchain-based framework for securing electronic health records. IEEE Globecom Workshops (GC Wkshps). https://doi.org/10.1109/GLOCOMW.2018.8644088

[16] Yue, X., Wang, H., Jin, D., Li, M., Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10): 1-8. https://doi.org/10.1007/s10916-016-0574-6

[17] Yang, H., Yang, B. (2017). A blockchain-based approach to the secure sharing of healthcare data. In Proceedings of the Norwegian Information Security Conference. 1-12.

[18] Xue, J., Xu, C., Zhang, Y. (2018). Private blockchain-based secure access control for smart home systems. KSII Transactions on Internet & Information Systems, 12(12): 6057-6078. https://doi.org/10.3837/tiis.2018.12.024

[19] Zhou, Y., Guan, Y., Zhang, Z., Li, F. (2019). A blockchain-based access control scheme for smart grids. In 2019 International Conference on Networking and Network Applications (NaNA), IEEE, pp. 368-373. http://dx.doi.org/10.1109/NaNA.2019.00070

[20] Fan, M., Zhang, X. (2019). Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access, 7: 35929-35940. https://doi.org/10.1109/ACCESS.2019.2905298

[21] Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

[22] Wong, J., Henderson, T. (2018). How portable is portable? Exercising the GDPR's Right to Data Portability, 911-920. https://doi.org/10.1145/3267305.3274152

[23] Ursic, H. (2018). Unfolding the new-born right to data portability: Four gateways to data subject control. Scripted, 15(1). https://doi.org/10.2966/scrip.150118.42

[24] Antonopoulos, A.M. (2017). Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media; 2nd edition.