Securing EHRs Using Blockchain Technology

Sagarika Behera[1], Aarathi Nair[2], S. M. Divyavani[3], Sabita G[4], Sophia Maria Augustine[5]

[1]*Asst. Professor, Department of CSE, CMR Institute of Technology, Bengaluru*

[2, 3, 4,5]*Final Year, B.E, Department of CSE, CMR Institute of Technology, Bengaluru*

Abstract - Electronic Health Records (EHRs) are currently stored on centralized databases which make the medical data largely non-portable. Database storage can expose the data to integrity issues and accuracy problems especially in the medical field. Blockchain which is also a popular topic now- a-days is able to ensure data security while using the distributed and decentralized topology. In our proposed system patients themselves retain control over 'who can access their data'. The basic architecture includes building a network of trusted data repositories, to which a series of 'smart contracts' decide the connection. Utilizing the work of this proof of concept, the framework of Blockchain 4.0 Hyperledger Fabric will be implemented to solve the above stated problem. A Hyperledger Fabric Composer will be used to set up the development environment, running environment and playground for running the Blockchain. Besides these, Channel and Chaincode will also be used in this system.

Keywords: EHRs, Blockchain, Hyperledger Fabric, Hyperledger Composer, Chaincode

I. INTRODUCTION

Electronic Health Records or EHRs contain health data of patients which is sensitive in nature, and it is utilized by many authorized users within and across medical institutions. This can lead to integrity issues and accuracy problems. Hence, the use of blockchain as technology for secure retrievals and transactions ensures privacy and security of the patient's health data during several different types of clinical practices. We utilize the Hyperledger Fabric, which leverages container technology to host smart contracts called 'Chaincode' for applying specified code when certain conditions are fulfilled. Blockchain Technology delivers a distinctive chance to aid the medical sector. Our EHR solution allows the healthcare professionals to acquire an entire medical history of the patient in order to provide accurate medication and treatment. This solution then keeps logs of the interactions with that history on the distributed ledger of the system in a transparent, auditable and secure manner. This solution is an individual platform that complements the overall user experience and improves that. It also improves the care for patients by placing them at the center.

A Hyperledger Fabric is used that is based on a permission network, which indicates that all the participants are required to be authenticated in order to participate and transact on the blockchain. Here, all the members are enrolled into the Membership Service Provider (MSP) to create a permissioned network. MSP is able to manage the role and permission of each user in order to use the application. Therefore, all the users are authenticated and identified by the system while using it. Hence, the users who request and operate into the medical records must be granted permission in order to access certain information. The Hyperledger blockchain network is based on permissionning and requires users to validate as authorized to use it. The access control rules in the Hyperledger modeling define the various permissions. All the members are enrolled into the Membership Service Provider (MSP) to create a permissioned network. MSP manages the roles and permissions of each user in order to use the application.

Medical information often contains highly sensitive data; therefore a permissioned blockchain such as a Hyperledger Fabric serves to maintain the privacy that is highly required for such an application. A Hyperledger Fabric is a framework for blockchain infrastructure development for distributed ledger solutions which provides confidentiality, resilience, flexibility and scalability. This is a finer solution for accessing health records, as it boards multiple layers of permissions, which means that the owner of a data set has complete control over what parts of their data is accessed.

II. RELATED WORKS

D. C. Nguyen et.al.[2] discussed EHRs, which use a collaboration application integrating blockchain and the decentralized Interplanetary File System (IPFS) on a mobile cloud platform to build a transparent access control

mechanism using smart contracts to ensure safe collaboration of EHRs between various patients and other medical providers. The empirical results show that this proposal offers an effective solution for reliable exchange of data on mobile clouds while preserving patient sensitive health information against potential threats. This system assessment and security review also shows technological changes in the design of lightweight access control, minimal network latency with high standards of protection and data privacy, relative to current models of data sharing.

The concepts of centralized, decentralized and distributed architectures are briefly explained with the help of relevant examples and important applications [3]. It gives an overview of how the consensus algorithms are used to secure blockchain. Since health data is seen to be very sensitive in nature, emphasis on the security implementations utilizing blockchain is discussed in detail. This case study also addresses the several drawbacks faced by variety of health systems designs and also provides with suggestions and recommendations for future projects, researches and developments having improved functionalities. Sara Rouhani, et al. [4] discusses inability to access medical data (produced by a physician) in a timely and efficient manner is a serious problem in the delivery of health care worldwide. Guang Yang, et al. [5] discusses about distributed ledger which is completely immutable. A ledger is nothing but a chain of blocks which is time-stamped. The ledger is essentially a chain of blocks connected by cryptographic hash functions, in which each block has the previous block's hash value. To the current blockchain a new block can be added. The block can be appended to the existing chain each time a new block has to be added. Due to the sensitivity of the data, the access control is of utmost importance. Due to the inherent characteristics of the blockchain, it has a great potential in the field of managing Electronic Health records. The decentralized and immutable features of blockchain technology are discussed in detail [6], which allows for autonomy and anonymity. Blockchain brings in a lot of honesty to the doctors in the patient health history point of view, as it is immutable. Hence the data remains confidential without affecting its integrity in real time, which in turn reduces errors. MedRec is a distributed system which gives an individual user control over his/her identity and the distribution of their information [7]. Blockchain is used to control a series of smart contracts which will determine who can access the data. The servers here are connected and maintain a growing blockchain, as opposed to the network. Those servers are the network's managing members. A 'proof of work' algorithm is used to protect the blockchain's credibility.

A. Azaria et.al shows us that block chain technology is used to implement a decentralized system for the maintenance of electronic medical records (EMRs) [8]. It is suggested that the blockchain could be considered as a set of decentralized compute resources, each such resource being an individual entity which could transcend between two states through cryptographic transactions. These entities were associated with a logic that would distinguish a transaction from being valid or not. For every valid transaction, the blocks would undergo a transformation, such a transformation is known as 'smart-contracts'. Ethereum blockchain was employed to implement smart-contracts, thereby developing a record management system which could furnish medical information to the patients as well as all medical service providers. Blockchain properties were used to design the system in such a manner that the data would remain confidential, tamper-proof and easily accessible. This design facilitated data miners with large pools of anonymous medical data, which could be used to interpret the wide array of medical treatment patterns and socio- economic demand patterns.

III. KEY TECHNOLOGIES

Utilizing the Hyperledger Fabric Framework by the Linux foundation, we can easily develop industry oriented blockchain applications. The general flow of blockchain infrastructure applications created using blockchain is discussed in this section as depicted in Fig 1. This figure describes the typical structure and flow for a blockchain network having a business application. The set of users would interact with the main user interface and doing so will end up invoking some type of query to the database. The SDK or Software Development Kit will verify the blockchain's global state and the blockchain will be queried via service-based RESTful APIs. The blockchain network will inform other peers in the network for consensus. The chaincode is responsible for the access control policies in the blockchain network. After the positive consensus, a transaction in the distributed ledger containing several other executed transactions will be submitted to the blockchain, whereupon a corresponding key-value pair will be generated or updated depending on the type of request. A token of 128-bit is generated whenever a new user is created, and that token is also stored in the database for the backend. The credentials are verified whenever the user logs in the application and the corresponding token is retrieved from the backend via the RESTful API. The application now passes the user tokens with every query and the token is verified in the backend using the RESTful API.

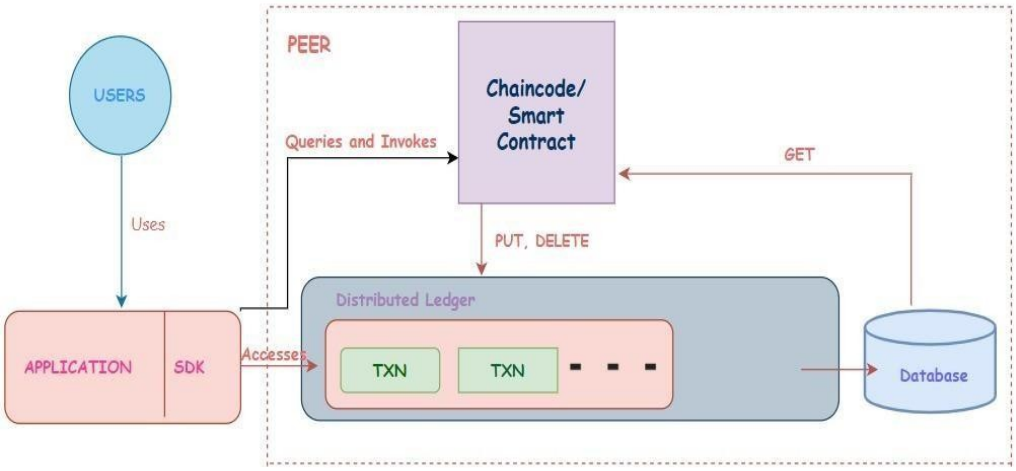

Fig 1: Generalized Blockchain Application diagram

The structure of blockchain network and different components are shown in the Fig. 2. This figure describes the blockchain structure as described and explained in [9]. The different components are as follows:

- **Blockchain Structure:** A blockchain is a growing list of records, called "blocks" that are generally linked to each other using cryptography. Blocks are data structures with the intent of bundling transaction sets and being spread to all network nodes. These blocks are established by miners. Each of these blocks contains a previous block's cryptographic hash, a timestamp, a nonce and transaction data generally represented as a "Merkle tree." A preceding block hash (Prev hash) in a sequence is a tamper-proof sequence because a hash is very sensitive as a function of the design. So, to change any variable of any one of the hashes in a given block would cause a domino effect, altering all of the previous transactions in the block.

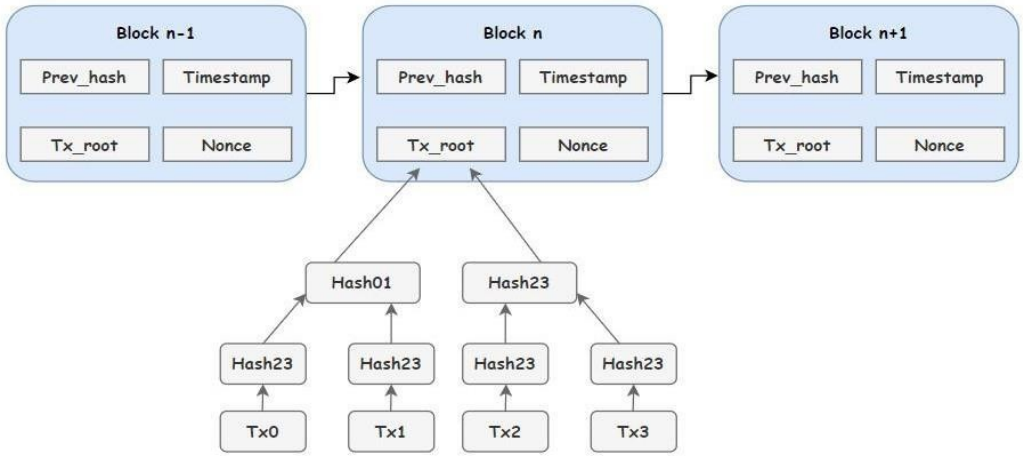

Fig 2: Structure of Blockchain Network (Referred from https://en.wikipedia.org/wiki/Blockchain)

- **Nonce:** A nonce is a "number used only once." A nonce is a 32-bit (4-byte) numerical string for a bitcoin block. This is generally called a "target hash" that miners solve for.

- **Merkle Tree:** A Merkle tree lists all transactions in a block by generating a digital fingerprint of the entire collection of transactions, enabling a consumer to verify if a transaction is included in a block or not. These are generated by hashing pairs of nodes continuously, until just one hash remains which is called as Merkle Root.
- **Smart Contracts:** Smart contracts are program files that specify the conditions for verifications and authorizations. They are pre-defined in nature and it is impossible to tamper with its contents. This allows for

smart contracts to ensure security and fraud prevention, which can act as a result from its transparent nature. Ethereum Technology utilizes such smart contracts under the blockchain technology.

- **DApps:** DApps refers to decentralized applications that do not have a centralized infrastructure. The backend structure of DApps is decentralized in nature with respect to storage and communication. Decentralized nature of the application allows for the generation of a peer to peer network which is the core concept of the blockchain technology.

IV. PROPOSED SYSTEM

Fig 3 shown in this section describes the architecture of our proposed system. The proposed architecture of the blockchain application considers three types of users: Doctors, Patients and Researchers. The users will use the web user interface (UI) application to perform view, request or update to the data. Once the web server receives the request from users, then it will go for verification from Chaincode. The web server is only allowed to access the Blockchain after it is verified by Chaincode. After that, the Blockchain will check the participant role and permission that will be assigned by the Membership Service Provider (MSP). All the members in the Blockchain must be identified in order to perform any actions. If the user permission is allowed, then the Blockchain will perform retrieve or update to the medical record according to the user's request received by Blockchain.
This proposed architecture is a proof of concept for the healthcare industry, where multiple hospitals with already existing large centralized databases can expand their current systems by incorporating such high level of security technology pertaining to transactions of assets like sensitive health data.

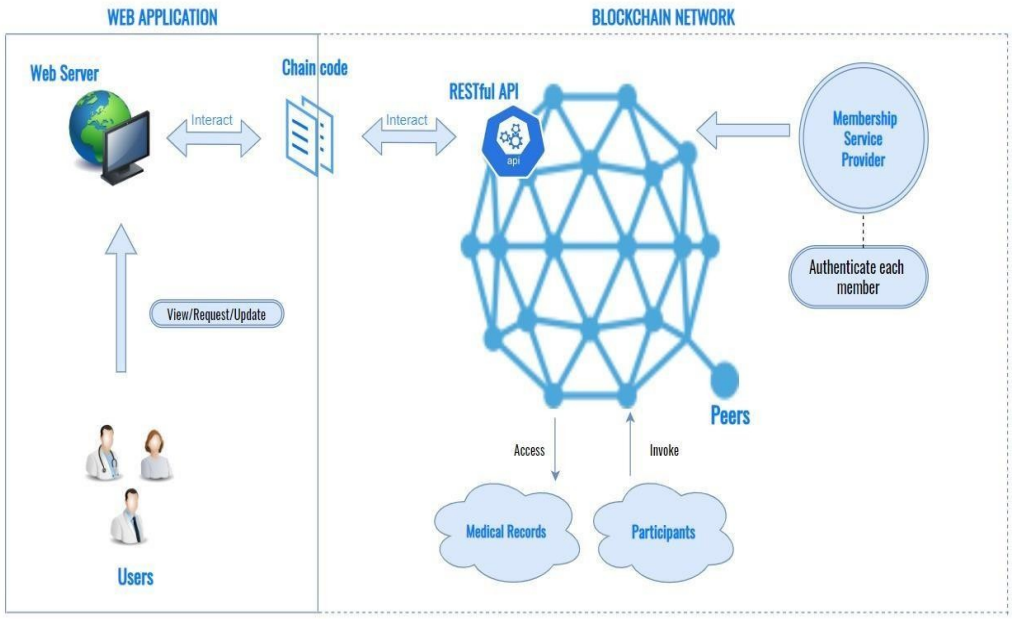

Fig 3: System Architecture

Any interactions with the health records are recorded as network transactions. Transactions are viewable only to the transaction-related participants. Examples of how transactions happen in the application are given here.

Patient Write Access Grant:

- Patient gives write access permission to Doctor for the medical records.
- Doctor's ID is attached on the blockchain to Patient's asset.

Patient Read Access Grant:

- Patient gives read access permission to Doctor for the medical records.

- Doctor's ID is attached on the blockchain to Patient's asset.

Doctor Referring Patient:

- Doctor updates the permissions to allow another Doctor to read the Patient's medical record
- Chaincode will check that the referring Doctor has permission to write on the medicalrecord
- Referred Doctor's ID is added to Patient's authorized asset
- Patient must add referred Doctor explicitly to his authorized list for write permission

Pseudo code for building a Blockchain Application:

BEGIN

1. Start the Fabric
2. Prepare the Fabric for development / deployment
3. Deploy the .bna Archive File using:
   yo hyperledger-composer: businessnetwork

a. Model File (.cto) to define the participants, assests, and transactions.
b. Script File (.js) specifies the functions to execute the defines transactions.
c. Access Control File (.acl) specifies the access control business rules.

4. Generate the admin card
5. Start the Rest Server
6. Build a web application using Angular / React etc depending on the business requirements
7. Stop fabric END

V. RESULTS AND DISCUSSIONS

Fig 4(a) and 4(b) depicts the process to start the fabric. This is the first step to deploying any type of business network on a blockchain using Hyperledger Fabric.

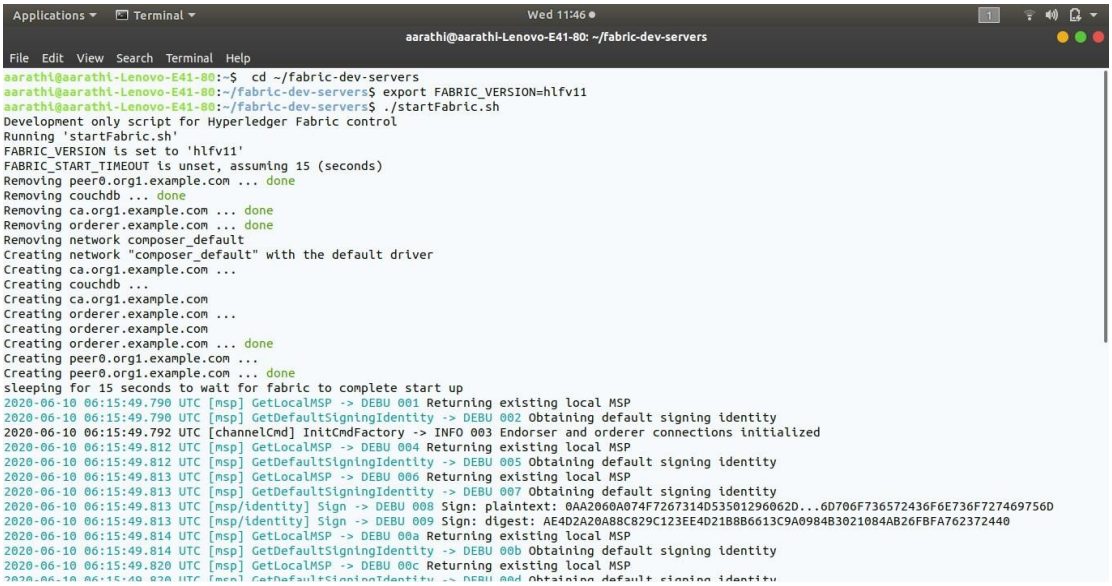

Fig 4(a): Start Fabric

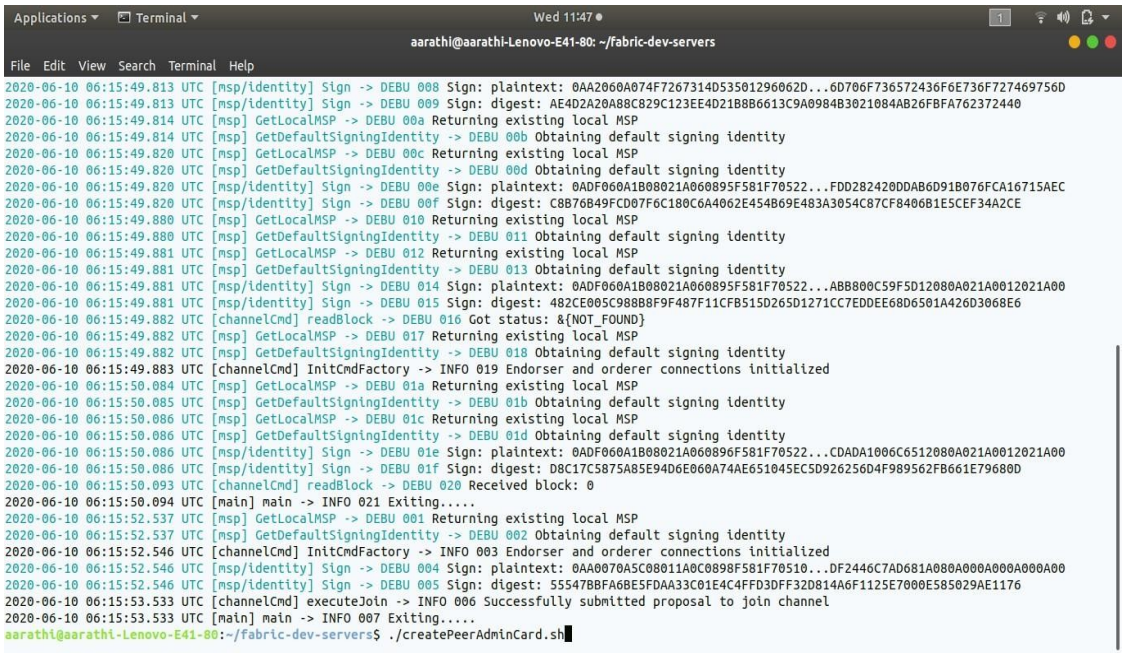

Fig 4(b): Fabric Started

Fig 5 depicts the creation of the first peer in the network. This is called the PeerAdmin. Having administration capabilities this peer now has the privileges to add authorized peers to the network if needed.

Fig 5: Create a PeerAdmin Card

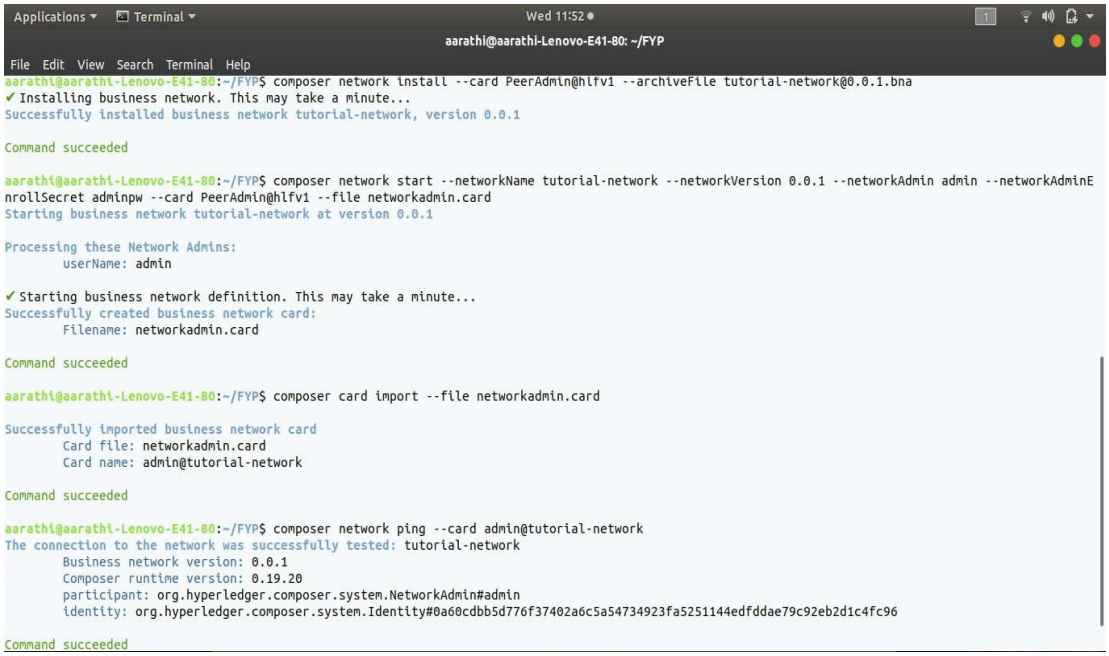

Fig 6: Deploying the business Network

Fig 6 corresponds to the various commands that are required to be executed for a successful deployment of the business network. The first command is for installing the business network that utilizes the PeerAdmin card. Next we need to start the business network and import the network admin card. Finally, we need to ping the network card to check for successful deployment of the business network.

Fig 7 depicts the commands to run the composer playground for testing of blockchain network. The playground needs to locally install in order to execute the testing purpose successfully.

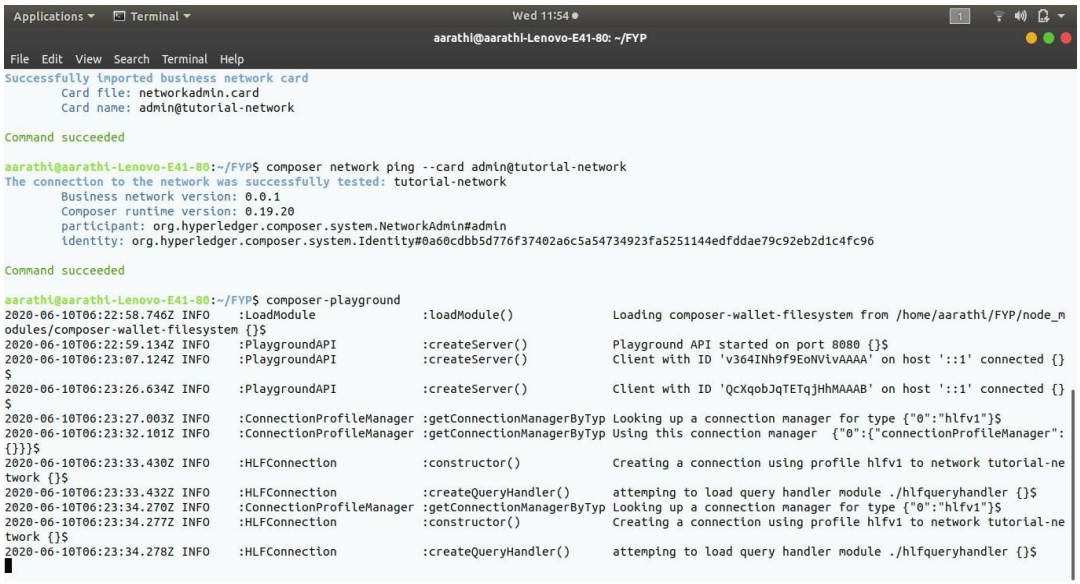

Fig 7: Composer Playground

After successfully deploying the business network, the blockchain network can be tested using the composer playground, a local IDE for testing blockchain applications. Fig 8 shows how we can build and define our blockchain network on the Hyperledger composer playground IDE. The modeling, logic and the access control files are defined using the playground and deployed accordingly as a blockchain business network. Multiple revisions of the archive file is also possible by utilizing the 'deploy changes' function.

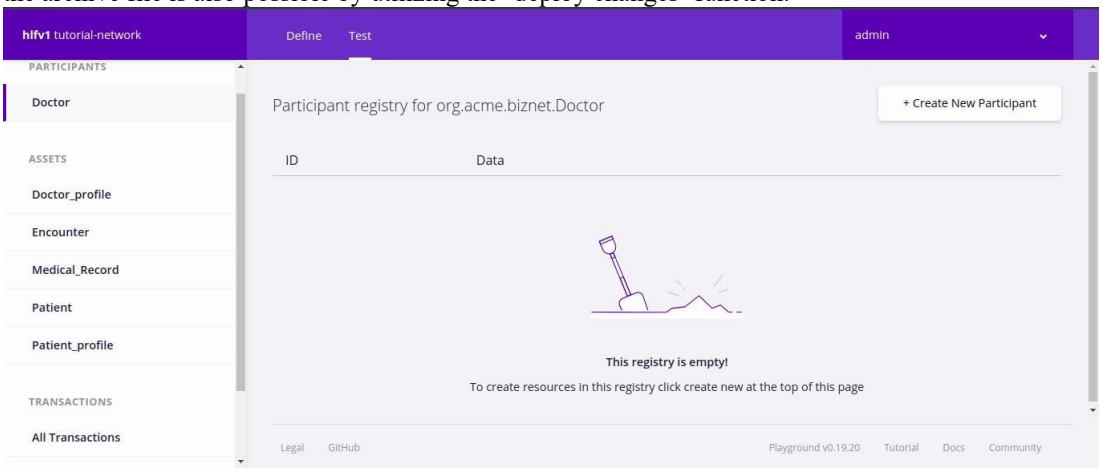

Fig 8: Testing the deployed .bna file

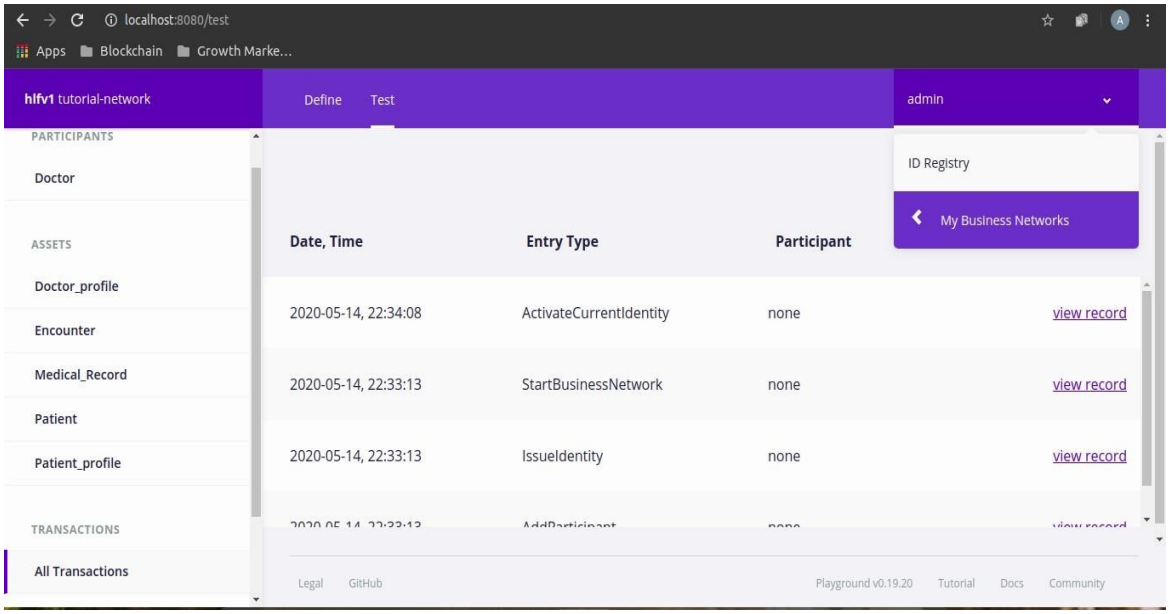

Fig 9: Transaction History

Fig 9 shows the transaction history. All the transactions such as creation, deletion, peer rights, etc. will be recorded and the records are immutable in nature. This is the main feature of a blockchain network. It displays all the transactions and this data cannot be modified. On the top right, we can even check out the current ID registry or even change the business network.

Depending on the business requirements and technical feasibility, the front-end User Interface can be developed. The proposed system acts as a proof of concept for the healthcare industry that have varying business requirements and accordingly appropriate tech stack can be used to develop the web application such as Angular, React js etc.

VI. CONCLUSION AND FUTURE SCOPE

The confidentiality and integrity is of high importance in the healthcare domain. The Blockchain 4.0 is implemented using Hyperledger Fabric framework provides a secure environment for storing the medical records. The proposed system provides control to patients, as they are the data owners with respect to the asset i.e. EHRs. This allows patients control over their own records and data users need to request for accessing data. Besides that, the medical records of patients are unified and stored distributed on Blockchain, so the doctors can retrieve it within seconds in order to make any medical decision based on the medical record. On the other hand, the medical research institutions do not need to worry about the quality and quantity of data samples anymore as the EHRs that they are allowed to access will act as useful datasets to carry out various researches which will benefit the medical industry. A responsive web application was designed for users to review on their own medical records. In addition, the web application allows doctors within the inter-hospital network and research institution to query data. A public ledger was also created to store the sensitive data from medical institutions. The current centralized method for storing medical records can be replaced by applying Blockchain technology. The patients' data can be retrieved more efficiently anywhere and anytime. In future we are planning to develop a mobile application which will be more convenient for patients to access their own medical information.

REFERENCES

[1] https://hyperledger.github.io/composer/v0.19/introduction/introduction
[2] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.
[3] Zubaydi HD, Chong Y-W, Ko K, Hanshi SM, Karuppayah S," A Review on the Role of Blockchain Technology in the Healthcare Domain", *Electronics*. 2019; 8(6):679.

[4] Rouhani, Sara & Butterworth, Luke & Simmons, Adam & Humphery, Darryl & Deters, Ralph, "MediChainTM: A Secure Decentralized Medical Data Asset Management System" 10.1109/Cybermatics_2018.2018.00258.
[5] Yang, Guang & Li, Chunlei & Marstein, Kjell, "A blockchain-based architecture for securing electronic health record systems", Concurrency and Computation: Practice and Experience. 10.1002/cpe.5479.
[6] Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G, "Applications of Blockchain Technology in Medicine and Healthcare", Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3
[7] Nchinda, N., Cameron, A., Retzepi, K., & Lippman, A, "MedRec: A Network for Personal Information Distribution", *2019 International Conference on Computing, Networking and Communications (ICNC)*, 637-641.
[8] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.
[9] Achanti, Akanksha & Behera, Sagarika & Reddy, Raghavendra, "A Secure Scheme for storing data on the cloud using Attribute-Based Signatures and Blockchain concept", 13. 110- 116. 10.21172/ijiet.133.17.