International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

ELECTRONIC HEALTH RECORDS ACCESS SYSTEM USING HYPERLEDGER FABRIC

Adesh Adikane[1], Nikhil Akole[2], Ashutosh Auti[3], Shubham Bhosale[4], Prof.Nalini Mhetre[5]

[1-4]B.E. Student, Dept of Computer Engineering, Sinhgad College of Engineering, Vadgaon, Pune-411041, Maharashtra, India
[5]Professor, Dept of Computer Engineering, Sinhgad College of Engineering, Vadgaon, Pune-411041, Maharashtra, India

---

Abstract— *In tough times of covid social distancing is a must and now with a high level of patient mobility across hospitals sharing health records without physical contact is paramount. Especially for the patients suffering from chronic diseases like cancer, diabetes, kidney failure, etc...With informed knowledge of the patient's history, doctors can make proper clinical decisions that are smarter and less risky. Traditional health records sharing was cumbersome as it involved fax and other methods that could lead to germ spread and also they were vulnerable to mal-practices like a violation of privacy. So considering these factors we are building a system that will provide a seamless and sophisticated method of sharing the health records through the EHR(Electronic Health Records)access system.*

Our aim is to design a system that will provide fluent, secure, seamless sharing of health care data across multiple health practitioners. The system will ensure privacy protection and guarantee the security of the health care data, including access control policy specified by the patient.With the use of permissioned Blockchain i.e. Hyperledger and integration with a web-based interface which will be used by the patients and doctors to do the EHRs transaction

***Keywords*— EHR, Hyperledger Fabric, Blockchain, Data Sharing, Privacy, Security.**

1.INTRODUCTION

For prompt medical care, timely sharing of electronic health records (EHR) across health practitioners is essential. A patient's history of health, tests, diagnoses, and treatments provides the necessary knowledge for doctors to make clinical decisions that are smarter and less risky. Access to EHR history is also preferred by individual patients to support personal and family engagement to take wise medical decisions and also to avail different medical treatments.[1]

In current practice, if a patient needs to transfer his clinical data from one hospital to other, he is typically required to sign paper-based consent that specifies what type of data will be shared and the information about the recipient. Traditionally the EHR data is shared through fax or mail and often takes days or even months for the records to become available. This is mainly due to a lack of systematic infrastructure support for secure and trustable EHR data sharing which may result in adverse complications if proper treatment is not met on time. Secure data sharing is crucial to present sufficient collaborative treatment and care choices for patients. The current system lacks standard architecture, failing to ensure proper security and access control for patients once data are shared. There could be a single point of failure in the traditional database systems which could lead to failure of the sharing of data.Blockchain has emerged as a trending technology to overcome the traditional drawbacks and maintaining security as well.[2]

In an emergency condition, the medical staff needs some necessary elementary and valuable health information about the patient for treatment and the patient is in no condition to tell about his health information.[3] Now this kind of situation can be avoided by developing some health record access policy. The health records can be stored electronically on the device and there is much cloud-based storage system for this purpose but privacy and confidentiality of health records is a must. The experience with Google Health wallet has shown that patients are concerned about their privacy and aware of the potential risk that their sensitive data might be misused. However, the data can be stored in encrypted form for increased security and privacy.[4]

To alleviate these problems and make sure fast and secure access to electronic health data we are building a system that would be patient-centric where the permission to give access to the health records data to doctors is decided by the patient. With the help of our system, we aim to ensure that patient data are securely, efficiently and accurately shared. Furthermore, Our system is designed as a single, fully trusted entity that is responsible for managing and storing EHR data from multiple patients. In case of emergency, our access policy will help doctors to get access to patient's health records. Blockchain technology is known for security purposes so by using hyper ledger blockchain and cloud-based storage for scalability we are trying to achieve seamless and secure sharing of health data.

2. BLOCKCHAIN AND HYPERLEDGER FABRIC

2.1 Blockchain

The blockchain is a peer-to-peer distributed, decentralized, digital ledger consisting of records called as blocks.That are used to record transactions across many devices so that any involved block cannot be changed, without changing all previous and subsequent blocks.[5]

Each participant or node entity has the equivalent accounting ledger as all of the other participants or entity nodes in the system network so he can see his whole history of transactions. For security purposes, the blockchain uses the cryptography method.

The structure of blockchain consists of a sequence of blocks in which each one contains the cryptographic hash of the prior block in the chain. A consensus-based mechanism is used to prevent the complete chain from being modified or altered and to decide which block should be appended to the ledger. The distributed ledger is not controlled by anyone and all the participants on the network can view it. Before adding a transaction to the ledger, the transaction must be encrypted and verified by other nodes on the network using consensus protocols. Once the transaction is validated by the majority of nodes, it is added to the ledger and shared by all participants. The added transaction cannot be deleted or changed. Thus, transactions in the ledger are trustable, auditable, and immutable.

2.2 Hyperledger Fabric

Hyperledger Fabric is a new blockchain architecture designed as a modular general-purpose permissioned blockchain.[6] A Hyperledger Fabric blockchain consists of a set/group of nodes that form a network. Since Hyperledger Fabric is permissioned, all nodes that are participating in the network have an identity. The Hyperledger Fabric Certificate Authority (CA) for Hyperledger Fabric that offers features for registration of identities, issuance of Enrollment Certificates, and certificate renewal and revocation. A smart contract called chaincode is the core part of a distributed application in Hyperledger Fabric. It is a program written in Go, Node.js, or Java language that runs to implement the business logic and to create transactions[7]. Predominantly,two types of chaincode are available. One for developing applications that may be developed by untrusted developers. The other type is called as system chaincode that performs a certain task for managing the blockchain system. An endorsement policy is used to define and designate the peers that execute transactions. Hyperledger Fabric differs from other blockchain platforms in those transactions in the other platforms are sequentially executed on all peers after they are added to the ledger in some order.In Hyperledger Fabric, the transactions are first executed in any order using chaincode in predefined peers (endorsement peers) to determine the exact ordering that would provide the result before adding them to the ledger. Thus, a given chaincode can be kept private from peers that aren't part of the endorsement policy. It separates the transaction flow into three steps, (1) execution of transaction and checking its correctness,and then endorsing it; (2) ordering through a consensus based protocol; and (3) validating transactions as per application-specific trust assumptions.

3. METHODOLOGY

Hyperledger fabric is the building block of our application it provides us the framework and people can use it according to their application need. First of all, in our system we are going to set up our hyperledger fabric network, the network runs in the backend of our system. This is because any application will need a basic network to interact. The network is then ‘up’ using the specified command(meaning that the network is initiated to interact). Network setup consists of setting up the wallet, CA(Certificate Authority), channel, and gateway. A wallet is a set of user identities that with the use of the MSP adds the user into the system. A certificate authority can be called the registrar of the certificate i.e. it is the issuing authority of certificates to the user. The CA will issue the certificates of type ‘X.509’ to interact. Whenever a user is added to our system he/she will get a certificate issued by the certificate authority and also the private key. All information is stored in the wallet folder, which will create a file for the registered user.

The EnrollAdmin() is used to enroll the admin in the system in this scenario enrolling the admin and registering the app user are the interactions that take place between the application and the CA not between the application and the chain code. The user entities are called the assets in the context of hyperledger fabric(in our case they are doctor, patient, report). Assets can be defined as the one which has differences in the initial and the final state which are represented in form of key-value pairs.

Smart Contract which is called a chaincode in hyperledger fabric is the most important part of the network. It provides the functionality to interact with the network. In the chaincode various functions are written which gets invoked whenever we work with the front end for example when a user suppose patient registers in the system RegisterPatient() function is invoked from the chaincode which takes all the information as a parameter and register it as a patient entity in the network. Whenever a user register in the network a wallet gets created with the wallet name as the hash key which is generated by taking email-id as input for hashing purpose SHA256 algorithm is used. A wallet contains a set of user identities(In our system as all the user information provided during registration will be stored on-chain), an application runs by a user selects one of these identities when it connects to a channel. Access rights to the channel resources, such as

the ledger are determined using this identity in combination with MSP(Membership Service Provider). Channel is a private subnet of communication between two or more network members the information of communication will not be known to other members by this confidentiality of the transaction will be maintained. Whenever a transaction is initiated by the user a channel will be created.

For record access purpose when the doctor enters the patient id an OTP is send to the mail of the patient for verification purpose, the network sends the hash-key of the OTP to the doctor so that when the patient tells the OTP to the doctor it compares it with the hash-key for validation of the OTP and if it is correct access of patient account is given to the doctor.

4. IMPLEMENTATION

We have provided a web portal to interact with the system. As mentioned the system consists of users the doctor and the patient.

Every user either patient or doctor has to their registration with the respective fields mentioned in the registration form. Whenever a user enters his details and hits the submit button a block is created in the system for that user and also the private key and the certificate generated from the Certificate Authority are stored in the wallet(a set of user identities). The wallet is being used the certificates allotted to the user from the CA have to be stored i..e-wallet.

When a patient visits a doctor(provided that they are registered in the system) to give access to the patient's records to the doctor he has to enter the email id of the patient which will generate the OTP and that is sent to the patients' mail id. Doctor then enters the OTP and thus can gain access to the patient's records.

Our system can be used as a repository of the medical documents where both the patient as well as the doctor can upload the reports(prescription or any other). The patient can upload the reports in PDF or PNG format. Whenever a patient uploads the report we are storing the date and time of upload of the report which is stored in the table which contains a field that will tell who has uploaded the report e.g. When the patient himself uploads the report the table will have entry self, when the report is uploaded by the doctor 'Doctor XYZ' the will show the entry in the field as Dr.XYZ.This tabulated data will help the patient to audit his account. Doctor while uploading the report can add the description of the file. The files uploaded can be viewed or downloaded.

The above explanation is regarding the normal scenario when a patient visits the doctor for regular checkups. But the question arises of how the same is managed during the emergency. Almost every hospital fills up the emergency form when the patient is brought to the hospital. When the doctor logins his account he will see two options normal patient visit and the emergency when he will hit the emergency button an emergency form will open which will contain fields like name of the person who bought the emergency patient to the hospital email id of the one who bought the patient, relation with the person who met accident(stranger/family member)by entering the fields OTP will be generated on the person who bought the emergency patient and by entering it the doctor will be able to gain the access to the patient's records. To provide information regarding the emergency such as who bought him to the hospital his contact number his mail id and also in which hospital he was admitted who treated him and also the hospital address all this information will be provided in the mail of the person. This feature enables the patient to have an audit of this account even during an emergency.

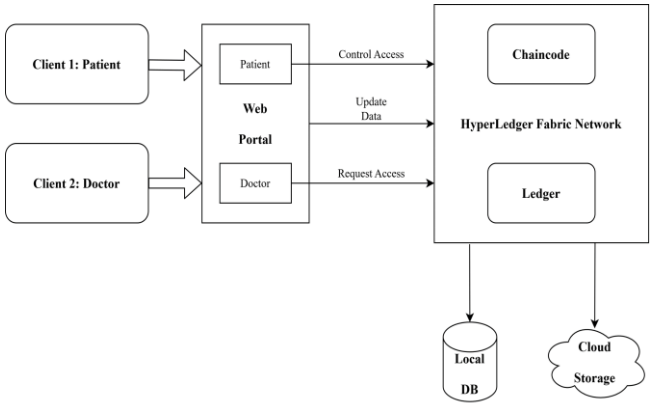

Fig -1: Architecture Diagram

EHR is a permissioned blockchain-based network. The proposed system is used by patients and doctors so to use the system they have to register on the system. The registration will be authenticated and validated by the MSP(Membership Service Provider). The user information will be stored on-chain and in the local database CouchDB. The shared and uploaded EHR data will be encrypted and stored off the chain in the cloud-based storage, only the patient will be able to initiate a record sharing request with his access policy and thus having full control of shared data.

In this implementation of an EHR system using Blockchain, EHR consists of three main participants:

i. Patients
ii. Doctors
iii. Admin

Patients play an important role as a participant in the EHR system. They own their health records that are being created and added to the blockchain. They can change their personal information. Therefore, they have the authority to regulate who all can access their records. There is also an

Emergency access policy where if the patient does not want to give access he can cancel it. The doctor is also a user who can upload medical data on the patient side. They are responsible for updating the health-related information in the records of only those patients who have permitted them to write into their records. They can change their personal information or profile.

Admin is the one who deploys the blockchain network, implements various contracts in the network, generates the key, and handles the encryption-decryption of the transaction data. He validates the users. Each medical record is owned by some patient who is registered on the network. Medical records are an important part of the network. Whenever a transaction is initiated some changes occur like updates in the records, modification in medication. The transactions are actions performed in the network like adding a participant in the network, creating a medical record, retrieving specific information from the network, updates in the participant's information, giving access to the clinician or lab, and taking away access from them. All the transactions performed history will be updated on the ledger so that patient will have full knowledge about whom he had given access to.

The patient whose medical records are to be accessed by the doctor can have his own permission rules it is on him if he wants to give only read access or read or write both. The metadata of the user that is userid, name, and all personal info will be stored in the local database CouchDB, and the medical records will be stored in the cloud storage.
The users can interact with our system through Web Based application

To interact with chaincode and to manage the system users i.e. patients and doctors, a web application and set of methods used for communication between user interface and server are required. For testing purposes, we take patients and doctors to each node. The technologies used for the implementation of web portals are HTML, javascript, cascading style sheets as well as bootstrap libraries.

5. Conclusions

EHRs play a significant role in improving patient care and enhancing the delivery of health care services. However, despite the huge benefits of this technology, there is increasing concern that patient's privacy and the security of the medical data will be compromised. These issues may hamper the widespread use of EHRs. In health care, a distributed ledger can be seen as a shared immutable and transparent history of all the actions performed by eHealth users; these actions include defining access control policies and sharing, accessing, and modifying the data. The system presently working when compared with the present systems we find that the system proposed way more scalable easy to understand as well as can be extended. The functionality of the prototype meets the requirements from a medical practice perspective. The system can also function in case of an emergency and will also provide email regarding the hospital information and also the person who admitted him, providing a pragmatic solution which the current system in the market lack. Building EHRs based on Hyperledger Fabric will ensure that patients have full access control to their records, patient's data are stored securely, and only verified participants can interact with patient's sensitive data. Implementing Hyperledger Fabric features on EHRs helps to ensure health information sharing among all parties on the network securely without concerns about exposing patient's privacy and confidentiality.

6. FUTURE WORK

We propose that the same system can be leveraged to make a fully sophisticated health care management system considering all the stakeholders in the actual scenario. Such as pharmacist can be used to manage the SCM(Supply Chanin management) as well as Insurance Service Providers LIC, GIC, etc.. can make use of the data to deepen the roots of the insurance sector in the country.

REFERENCES

[1] Hsiao C, King J, Hing E, Simon AE. The role of health information technology in care coordination in the United States. Med Care 2015 Feb;53(2):184-190. [doi: 10.1097/MLR.0000000000000276][Medline: 25464164]

[2] Using Blockchain for Electronic Health Records.

[3] EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain

[4] MedRec: Using Blockchain for Medical Data Access and Permission Management.

[5] An update on Google Health and Google PowerMeter. URL:https://googleblog.blogspot.com/2011/06/ update-on-google-health-and-google.html [accessed 2019-02-01]

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008.

[7] Blockchain for secure EHRs sharing of mobile cloud Based E-Health Systems.