Implementing Blockchain based Architecture for Securing Electronic Health Record System

Prof Jeenath Laila N[1], Sathya M[2]

[1]Assistant Professor , Dept. of Computer Science and Engineering, Government College of Engineering, Tirunelveli.
[2]PG Scholar, Dept of Computer Science and Engineering, Government College of Engineering, Tirunelveli.

---***---

Abstract -*Modern healthcare systems are known for being quite expensive and complex. However, this can be decreased by using blockchain technology, better health record management, and insurance agencies. Blockchain was initially developed to offer decentralised records of financial transactions independent from centralised authorities or financial organisations. Improvements in medical record, insurance billing, and smart contract transactions have been made possible by advances in blockchain technology, which also provides a distributed database of transactions and permanent access to and security over data. The capacity to improve the interoperability of healthcare databases and expand access to patient medical information, device tracking, and prescription databases is a key benefit of employing blockchain technology in the healthcare sector. To properly prescribe medication, access to individuals' medical history is necessary, and blockchain technology has the potential to significantly improve the healthcare services framework. In this project, a number of blockchain-based improvements to present healthcare system restrictions are investigated, including frameworks and tools to gauge the effectiveness of such systems, including Hyperledger Composer. The suggested system employs blockchain in place of the client-server architecture used by conventional EHR systems to increase efficiency and security.*

Key Words: **Healthcare systems, Security, Chaincode, Electronic healthcare records**

1. INTRODUCTION

A blockchain is a peer to peer (p2p) distributed database (i.e., ledger) that maintains an ever-growing list of records, called blocks, that are linked and secured, typically using public-key cryptography [13]. With blockchain technology, new information is added to a block and made available to all nodes in a decentralized network, instead of being added to a centralized database in a traditional centralized system. Each block in the blockchain is identified by a hash value, which is usually generated using a secure hash algorithm (SHA-256) [13]. The hash value of the header (parent) of the current block is bound and stored in the next block (child) [12]. Blockchain participants have private keys that they can use to digitally sign and confirm transactions.

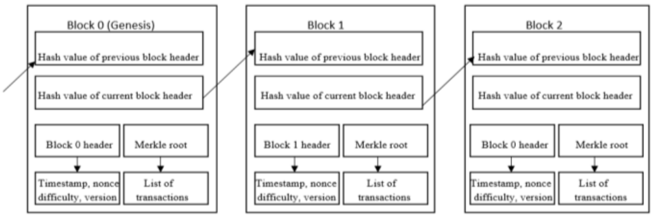

Block 0 (Genesis)
Hash value of previous block header
Hash value of current block header
Block 0 header
Merkle root
Timestamp, nonce difficulty, version
List of transactions
Block 1
Hash value of previous block header
Hash value of current block header
Block 1 header
Merkle root
Timestamp, nonce difficulty, version
List of transactions
Block 2
Hash value of previous block header
Hash value of current block header
Block 0 header
Merkle root
Timestamp, nonce difficulty, version
List of transactions

Fig-1: An example ledger with details of blocks

As shown in Figure 1, a block consists of a header containing metadata and a long list of transactions made in that block. A block header usually contains a timestamp, token, version and proof of weight. The timestamp indicates the time when the block was created; nonce is a random number generated by the consensus algorithm to compare the hash value of the block; version indicates the blockchain version number; and proof of difficulty is generated by a hash value that must be less than the current target hash value. The first block, known as the Genesis block, is hard-coded by embedding random data into the blockchain application [13]. In a block, all events are linked with each other using a Merkle tree [13]. A Merkle tree is an inverted binary tree that blockchain technology uses to summarize all transactions in a block. To form this tree, a pair of events is recursively compressed until they form only one root node at the top of the tree, called the Merkle RooT. Specifically, the Merkle is the root hash of all the transactions that make up a block of the blockchain. Every small change in the data changes the Merkle root hash value, resulting in an incorrect record. The most common cryptographic hash algorithm used to build a Merkle tree is the Secure Hash Algorithm (SHA-256). If there is an odd number of events, the hash of the last event is multiplied to produce an even number of events, resulting in a balanced tree. Blockchain can be permissionless or permissionless [11]. A permissionless network or public blockchain allows any user to create a personal address, join the network and participate in consensus, while a permissioned or private blockchain network allows only a limited number of nodes to join. Although each block has only one parent and one child, a valid block can temporarily have two or more children created when two or more nodes are added simultaneously to blocks leading to two or more branches from the same parent [12]. This situation is called "fork" and is eliminated by taking the chain that becomes longer than the others as the valid blockchain and invalidating all the others that are shorter (the orphan chain), where Figure 3 shows the bifurcated situation. It is possible. that the formed branches are of equal length; in this situation, the process of adding new blocks continues for all validation chains until one branch becomes longer than the others, thus valid.

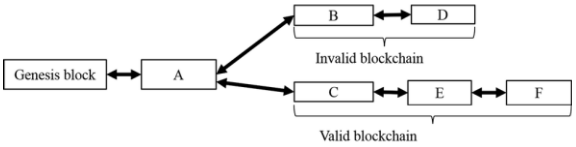


Fig -2: Blockchain validation for the fork situation

Nodes in the blockchain network perform a consensus algorithm to confirm transactions. Several consensus algorithms are available for blockchain technology, such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Proof of Difficulty (PoD) [6,13]. In PoW, mining nodes that want to add (mine) a new block to the blockchain must first solve a complex mathematical puzzle that requires a lot of computing power. A miner who solves the puzzle adds a new block and is paid in bitcoins. Unlike PoW, in PoS, the node that creates a new block is deterministically chosen based on its contribution (wealth). PoS saves the energy needed to solve the mathematical puzzle in PoW, and only a validator is needed to validate new transactions and blocks. DpoS tries to solve the consensus problem by using delegates. It uses a real-time voting and reputation system to create a limited number of trusted agents that validate and validate blocks. They are allowed to create blocks and add them to the blockchain network, as well as deny malicious nodes from participating in adding blocks.

1.1 Blockchain and Electronic Health Record

Blockchain can enable a comprehensive, interoperable and secure electronic information system data, where healthcare consumers are the ultimate owners of their electronic card devices. These events and records are generated by different nodes in the network, such as a service provider or a consumer downloading health data. Blockchain provides authentication of data on the chain by requiring users to provide a signature and timestamp with a private key to access the data. Therefore, the logic built into the blockchain allows consumers the best of both worlds, providing access to doctors when needed, while protecting data from unauthorized users. The use of multiple digital signatures via PKI and cryptographic hashes ensures that healthcare metadata and EHR hashes travel securely over the network and are only available to parties with the correct public keys for access. Using blockchain digital signatures to create a unique patient identifier ensures that all records on the chain with that identifier are linked to create a comprehensive EHR for that patient across all of their providers and payers. The health metadata blockchain avoids the scalability challenges that placing large data-intensive EHR records directly on the blockchain can present to the technology.

1.2 Medical Blockchain Platform

Medical BC allows various healthcare providers, such as doctors, hospitals, laboratories, pharmacists and insurance companies, to request permission to access and interact with patient data. Every interaction is auditable, transparent and secure, and recorded as a transaction in Medical BC's distributed ledger. It is built on the permission-based Hyperledger Fabric architecture, which allows different levels of access; patients control who can see their records, how much and for how long. The blockchain is currently under development. Medical BC is collaborating with Wings and Hyperledger to bring the platform to life. Medical BC aims to provide patients and healthcare providers with the following key benefits: information can only be accessed using the patient's private key; even if the database is hacked, the patient data is unreadable (all encrypted). Patients can fully control access to their health information; patients control who sees their data and what they see Instant transfer of medical data, where every member of the decentralized network of healthcare blockchain would have the same information about the patient; the risk of errors is lower and patient care is better.

2. LITERATURE SURVEY

Lixia Chen et al. [1] proposed that electronic health records reduce the cost of traditional medical data storage. EHRs are designed to allow patients to manage their medical information. Data users have limited access to the EHR. At the same time, patients do not share their private medical information with data users, demonstrating the value of patient EHR security and privacy. Regarding the use of electronic health records, an encrypted search of such data must be carried out. Based on this, a permissioned blockchain-based medical information system is presented, which uses cipher-based attribute encryption to control data confidentiality and medical information access. The premise to ensure the privacy of the patient's identity is the use of a polynomial equation to combine arbitrary keywords, after which blockchain technology is combined. In addition, the proposed system has a keyword indistinguishable from keyword attacks selected based on the random oracle model.

Shang Jiang et al. [2] proposed a blockchain-based platform called BloCHIE for health information exchange, which is proposed to overcome the challenge. First, the requirements for sharing health information from different sources are analyzed. Based on the above analysis, two loosely coupled blockchains are used to process various health data. EMR - circuit for electronic patient records and PHD - circuit for personal health services. Off-chain storage and on-chain authentication are combined to meet both privacy and authenticity requirements. Finally, two compression algorithms are proposed to improve system performance and user controllability.

Hui Li et al. [3] hypothesized that advances in digitization and cloud storage have led to the conversion of data from paper to electronic devices. Interoperability between different hospital systems hinders information sharing. In order to meet the high requirements of information sharing, some researchers have proposed relative systems of cloud storage and data processing technologies to provide suitable solutions for compression storage and processing requirements. To solve the above problems, MedBlock, a blockchain-based information management system, is offered for patient information processing. In this system, an advanced consensus mechanism achieves consensus on EMRs without high energy consumption and network congestion. MedBlock also has high security, combining custom access control protocols and symmetric encryption

Rui Zhang et al. [4] proposed a distributed attribute-based signature system for health blockchain that provides effective privacy-preserving verification of HER data authenticity and signer identity. In addition, a comprehensive on-chain and off-chain shared storage system for efficient storage and authentication of HER data is described. Analyzes and tests show that the system is effective and usable

Guan Yan et al.[5] proposed that public health workers provide different health services in different locations. Users who grant access rights to databases can request regular user records from other service providers if necessary, for example, looking at related records to make a diagnosis. Due to the lack of standardized system integration, managing the entire healthcare system is currently a major challenge. Often, the demands of users and healthcare providers have also raised questions about data interoperability, security and privacy. Therefore, a blockchain-based architecture is proposed to improve the interoperability issues of current HER systems and prevent user record corruption and malicious misuse. A blockchain-based architecture for electronic health information systems (HER) is presented. The proposed architecture also introduces a new incentive mechanism for creating new blocks on the blockchain. The architecture is independent of specific blockchain platforms and open to further extensions, making it potentially suitable for other electronic storage systems that require protection against tampering and abuse.

Hao Wang et al.[6] proposed a secure EHR system based on attribute-based encryption and blockchain technology to achieve confidentiality, authentication, medical data integrity, and access control support. In the proposed system, attribute-based encryption (ABE) and identity-based encryption (IBE) are used, and identity-based signature (IBS) is used to implement digital signatures. To achieve the different functions of ABE, IBE, and IBS in a single cryptographic system, a new cryptographic primitive called Combined Attribute-Based/Identity-Based Encryption and Signature (C-AB/IB-ES) is introduced. This makes system management easier, and there is no need to implement different encryption systems for different information security requirements.

Rui Guo et al.[7] argued that electronic health records (EHRs) are controlled by hospitals rather than patients, making it difficult to seek medical care from different hospitals. Patients need to focus on the details of their treatment and regain control of their medical information. This technology provides patients with comprehensive, immutable information and access to EHR data without the need for providers and care locations. EHRs are encapsulated in a blockchain, attribute-based signature model with multiple authorities. In addition, there are several institutions that do not have a reliable single or central device that generates and distributes patient public / private keys, which avoids the problem of escrow and validates decentralized data storage on the blockchain. By sharing secret seeds of pseudo-random operations between powers, this protocol resists N secret attacks from N-1 corrupt powers. With unforgeability and complete privacy, this attribute signature scheme is secure in a random oracle model.

Qi Xia et al. [8] pointed out that the dissemination of patient medical records brings various risks to patient privacy, because malicious activity in those records seriously damages the reputation, economy, etc. of all parties directly or indirectly related to the data. The system is based on blockchain and provides data origination, review and management of shared medical information in cloud storage across big data entities. The design uses smart contracts and an access control mechanism that effectively monitors data behavior and prevents intruders from accessing data when violations are detected. It uses smart contracts and an access control mechanism that effectively monitors data behavior and revokes access to violated rules and data. Performance is analyzed and compared with state-of-the-art solutions for sharing data between cloud providers and entities such as research and medical institutions without compromising data protection.

According to Liang. X. et al. [9], mobile and wearable technology enable personal health data to give significant and growing value for healthcare, benefiting both care providers and medical research.The current systems for storing and sharing personal health data have a number of possible privacy flaws and risks, hence a novel user-centered solution for exchanging health data is suggested. In order to guarantee privacy utilising a channel formation scheme and improve identity management using a membership service powered by blockchain, this proposal uses a decentralised and permissioned blockchain. For the purpose of exchanging health information with healthcare professionals and health insurance providers, a mobile application is used to gather data from medical equipment, wearable personal gadgets, manual input, and other sources.The system is constructed throughout the implementation of Hyperledger Fabric.

Xiao Y. et al [10] proposed a blockchain-based Healthcare Data Gateway (HDG) architecture that allows patients to easily and securely own, manage and share their data without compromising privacy. health systems keeping information private. The proposed model ensures that patients own and control their health information; a simple unified indicator-centric scheme (ICS) allows organizing all kinds of personal health information in a practical and simple way. Based on the architecture, patients do not need to trust any third party and are always aware of who is using the data and how it is being used. A decentralized platform makes it easier to make legal and regulatory decisions about the collection, storage and sharing of patient data.

3. PROPOSED SYSTEM

However, in terms of EHR management, traditional blockchain solutions have two major drawbacks. First, while the blockchain can ensure data integrity, it lacks adequate access control mechanisms to encompass the activities of various actors. Second, the blockchain block size is too limited for EHR data that contains images (eg, X-ray, CT scan and MRI) and/or video (eg, ultrasound). A hybrid architecture using both blockchain and edge nodes is proposed to facilitate attribute-based EHR data access control. This is achieved using Hyperledger Composer. Specifically, the Hyperledger Composer Fabric blockchain implements smart contracts programmed with access control lists (ACLs) to enforce identity-based access control of EHR data and record legitimate access events on the blockchain for traceability and accountability. A hybrid architecture using the Hyperledger Composer Fabric platform was proposed to validate the design. In addition, several experiments were conducted to validate both smart contracts and access control policies, which show that the proposed system can maintain traceable access returns and transaction records for EHR data management. System performance was evaluated by testing multiple transaction processing times and average response times to unauthorized EHR data requests in various settings. Hyperledger Composer Fabric supports ready-made chaincode written in Go and JavaScript, as well as in other languages such as Java by installing the corresponding modules.The process flow of a blockchain transaction can be summarized in four main steps shown in the Fig. 3:

1. **The healthcare organization stores information in the blockchain:** The healthcare organization provides services to the patient and stores the patient's data (a doctor can write a note or a pharmacy can dispense medicines) in the existing healthcare IT system. The data fields and the patient's public identifier are then pushed to the blockchain via APIs.

2. **The transaction is completed and uniquely identified:** each transaction is encrypted and given an identity stored on a blockchain containing the public (de-identified) ID of the patient [2].

3. **Healthcare organizations and institutions can make requests directly from the blockchain:** Healthcare organizations and institutions send their requests through APIs and use the patient's public ID on the blockchain to retrieve encrypted information. Patient information (eg, age, gender, disease, physician) is now visible and can be analyzed for new insights.

4. **Patients can specifically give anyone access to their medical information:** a patient's private key links their identity to blockchain data. This private key can be shared with new healthcare organizations that can use it to decrypt patient data. Thus, the data is not identifiable to those who do not have the key.

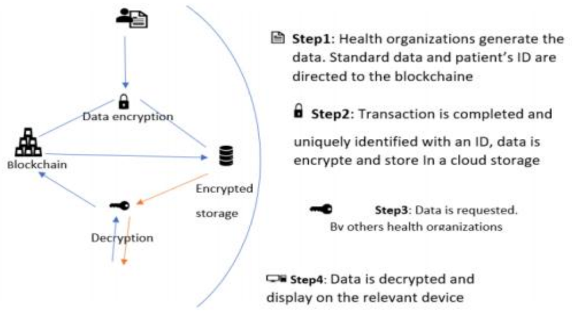

Data encryption
Blockchain
Encrypted
storage
Decryption
Step1: Health organizations generate the data. Standard data and patient's ID are directed to the blockchaine
Step2: Transaction is completed and
uniquely identified with an ID, data is encrypte and store In a cloud storage
Step3: Data is requested.
Bv others health organizations
Step4: Data is decrypted and display on the relevant device

Fig -3: Basic Blockchain's process flow

3.1 System Architecture

The figure shows a hybrid architecture that facilitates access control of EHR data using both blockchain and edge nodes. The following entities that contribute to architecture are listed.

1. Patient: The patient is the person who owns the EHR data being used. The patient can define the principles of use of the EHR data belonging to him.

2. Health care provider: A health care provider (eg doctor and nurse) is a legal entity that needs access to patient EHR data. The health care provider actively seeks access authorizations from patients.

3. Smart sensor/imaging device: A smart sensor is a device that collects EHR data from patients and sends it to the edge node. Imaging equipment can include X-rays, CT scans, MRIs and ultrasounds that generate EHR data about patients.

4. EHR data: EHR data is data owned by patients that can be accessed by authorized healthcare providers.

5. Blockchain: Blockchain is used as an architectural controller that manages access control policies and acts as an unauthorized access protocol.

A web application based on the Hyperledger Composer Fabric blockchain is designed and developed to implement and evaluate the access control mechanism. As shown in Figure 4, the Hyperledger Composer Fabric infrastructure includes four programmable components. The first part is to definenetwork properties in a template file (.cto), which includes participants, URLs, events and an access control log. The second part is to write smart contracts in a script file(.js), which contain the event handling functions. The third part is to define ACL rules for different participants in the Access Control File (.acl). Finally, database queries are defined in the Query File (.qry).

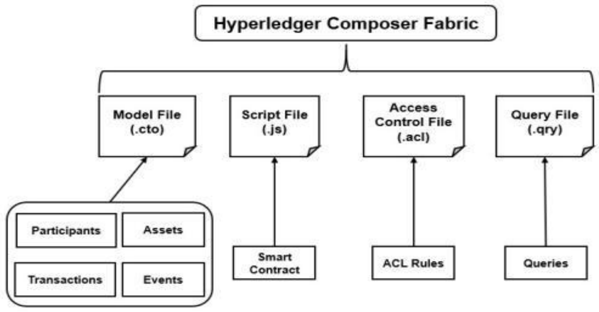


Fig-4: Hyperledger Composer Fabric Infrastructure

This EHR system model consisted of the following four parties: EHR server, N facility, patients, and data certifiers. As shown in Figure 6, the EHR server is just like a cloud storage server responsible for storing and sending EHRs. N authorities are various organizations such as hospitals, health insurance organizations, medical research institutes, etc., which are responsible for receiving registrations and exchanging patient information. Patients can create, manage, administer the data controller has the right to access and verify this signature.

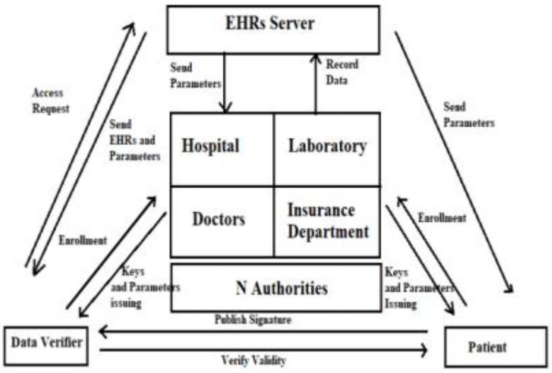


Fig-5: The EHR system model

3.1.1 Implementing Hyperledger Composer Fabric Blockchain

A web application based on the Hyperledger Composer Fabric blockchain is designed and developed to implement and evaluate the access control mechanism. Hyperledger Composer Fabric is a blockchain application platform that provides a modular and extensible architecture that allows components such as a consensus mechanism to be connected and used. Additionally, it uses container technology to host smart contracts called "chaincode" that contain the system's application logic.

3.1.2 Creation of Participants in the Network

Participants register using the client application or SDK. All transactions are shared across the hyperleader fabric blockchain network. Patients can add records using a client application that calls a chain code to link the transaction to the network. Once a transaction is committed to the blockchain network,updated transactions are shared across the network. The administrator has full access to the system, including writing, reading, updating and deleting participants. If doctors, patients or laboratory workers are eligible, the administrator can give each participant an appropriate token that allows access to the blockchain network. If a participant's behavior is found inappropriate, an administrator can remove the participant with a note via the hyperledger blockchain network..

3.1.3 Defining Access Control Lists using Smart Contracts

Patient's EHR address is stored as a personal asset on the blockchain network. An access control list (ACL) allows physicians to obtain patient EHR addresses while the patient can only obtain their own EHR address. The request process is defined as an event process in the smart contract, and the participants who initiate it send their requests. Finally, all historical search events are stored as immutable and traceable EHR access control logs on the blockchain network. After the edge nodes have collected the patient's EHR data, the patient can enforce an ACL policy on their EHR data. By defining an ACL policy, it can determine which data users can read, write, and update content. In other words, we provide conditions and restrictions on: "who" can do "what" on the blockchain ledger

.3.1.4 Committing Transactions to the network

The records are updated and visible to every user of the blockchain network. Service providers, such as doctors and laboratory workers, can request the necessary information online. If the patient gives the right to view and update their records in the EHR registration network, the physician or laboratory participant can view and update the patients' consent records as needed. After accessing the blockchain network, the patient has several rights, such as reading, writing and canceling EHR records. This operation of the patient node applies this identification to the blockchain network. If a patient has a valid node, patient, physician, and laboratory personnel data can be viewed or searched online. The doctor also has access to his list of patients, which includes first and last names. If a physician wants to retrieve a specific patient's EHR data, he or she must submit a transaction request by entering the patient's ID number. Once the request is submitted, the system returns the patient's EHR. At the same time, the blockchain network permanently records this search operation as a transaction transaction, including the transaction ID and timestamp.

4. RESULTS AND DISCUSSION

Fig. 5 shows the experimental setup on Hyperledger Composer Fabric with two doctors and five patients as participants where each participant has a unique digital ID to log into the blockchain.Fig. 6 shows the process of creation of new participants in the network.

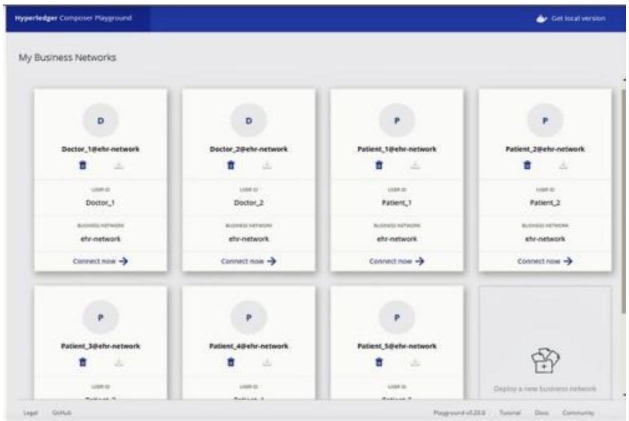
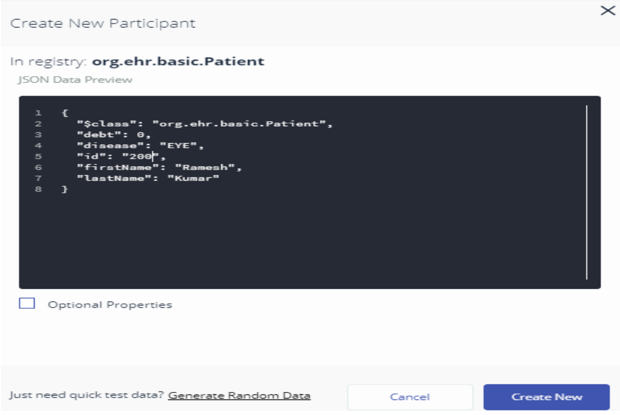


Fig-5: Blockchain based EHR network login window



In registry: **org.ehr.basic.Patient**

JSON Data Preview

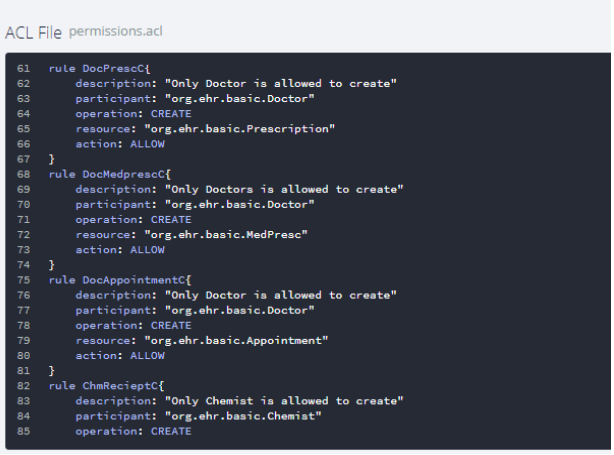
```
{
  "$class": "org.ehr.basic.Patient",
  "debt": 0,
  "disease": "EYE",
  "id": "200",
  "firstName": "Ramesh",
  "lastName": "Kumar"
}
```

☐ Optional Properties

Just need quick test data? Generate Random Data

Fig-6 : Creation of participants in the blockchain network

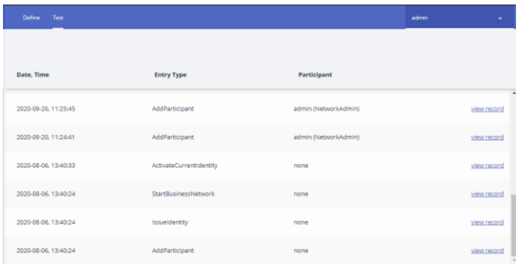
Fig. 7 shows the declaration of ACL in the proposed blockchain network.Fig. 8 and Fig 9committed transactions in the network and the details of the transactions committed respectively.



ACL File permissions.acl

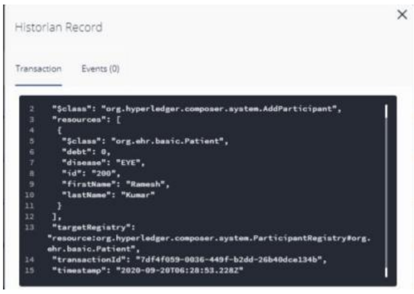
```
rule DocPrescC{
    description: "Only Doctor is allowed to create"
    participant: "org.ehr.basic.Doctor"
    operation: CREATE
    resource: "org.ehr.basic.Prescription"
    action: ALLOW
}
rule DocMedprescC{
    description: "Only Doctors is allowed to create"
    participant: "org.ehr.basic.Doctor"
    operation: CREATE
    resource: "org.ehr.basic.MedPresc"
    action: ALLOW
}
rule DocAppointmentC{
    description: "Only Doctor is allowed to create"
    participant: "org.ehr.basic.Doctor"
    operation: CREATE
    resource: "org.ehr.basic.Appointment"
    action: ALLOW
}
rule ChmRecieptC{
    description: "Only Chemist is allowed to create"
    participant: "org.ehr.basic.Chemist"
    operation: CREATE
```

Fig-7 : Declaration of Access /Control Lists



Date, Time	Entry Type	Participant	
2020-09-20, 11:25:45	AddParticipant	admin (NetworkAdmin)	view record
2020-09-20, 11:24:41	AddParticipant	admin (NetworkAdmin)	view record
2020-08-06, 13:40:33	ActivateCurrentIdentity	none	view record
2020-08-06, 13:40:24	StartBusinessNetwork	none	view record
2020-08-06, 13:40:24	IssueIdentity	none	view record
2020-08-06, 13:40:24	AddParticipant	none	view record

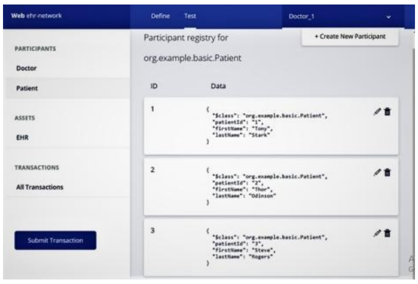
Fig-8 : Committed transactions in the network



```
  "$class": "org.hyperledger.composer.system.AddParticipant",
  "resources": [
   {
    "$class": "org.ehr.basic.Patient",
    "debt": 0,
    "disease": "EYE",
    "id": "200",
    "firstName": "Ramesh",
    "lastName": "Kumar"
   }
  ],
  "targetRegistry":
 "resource:org.hyperledger.composer.system.ParticipantRegistry#org.
 ehr.basic.Patient",
  "transactionId": "7df4f059-0036-449f-b2dd-26b40dce134b",
  "timestamp": "2020-09-20T06:28:53.228Z"
```

Fig-9 : Details of Committed transactions

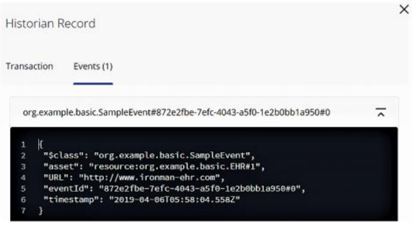
The patient has various rights, such as read, write and revoke EHR records. If the patient has a valid node, then patient, clinician and laboratory staff records can be viewed or searched over the network. Also, a doctor is allowed to access his/her list of patients, including ID numbers first and last names as shown in the Fig. 10:



Participant registry for org.example.basic.Patient

ID	Data
1	{ "$class": "org.example.basic.Patient", "patientId": "1", "firstName": "Tony", "lastName": "Stark" }
2	{ "$class": "org.example.basic.Patient", "patientId": "2", "firstName": "Thor", "lastName": "Odinson" }
3	{ "$class": "org.example.basic.Patient", "patientId": "3", "firstName": "Steve", "lastName": "Rogers" }

Fig-10: A doctor accesses his/her list of patients

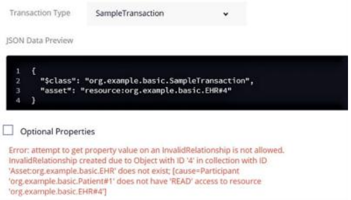


org.example.basic.SampleEvent#872e2fbe-7efc-4043-a5f0-1e2b0bb1a950#0

```
{
 "$class": "org.example.basic.SampleEvent",
 "asset": "resource:org.example.basic.EHR#1",
 "URL": "http://www.ironman-ehr.com",
 "eventId": "872e2fbe-7efc-4043-a5f0-1e2b0bb1a950#0",
 "timestamp": "2019-04-06T05:58:04.558Z"
}
```

Fig-11 :A doctor can retrieve his/her patients' EHRs

If a doctor wants to retrieve one specific patient's EHR data, the doctor needs to submit a transaction request by entering the patient's ID number. Upon submitting the request, the system will return patient's EHR. At the same time, the blockchain network will permanently record this retrieval action as a transaction event, including the event ID and the timestamp as shown in the Fig. 11.For instance, if a patient attempt to retrieve the EHR data of another patient, the system will reject this transaction request and return an error message indicating that this request is not allowed, as shown in Fig. 12


Transaction Type: SampleTransaction

JSON Data Preview

```
{
  "$class": "org.example.basic.SampleTransaction",
  "asset": "resource:org.example.basic.EHR#4"
}
```

□ Optional Properties

Error: attempt to get property value on an InvalidRelationship is not allowed. InvalidRelationship created due to Object with ID '4' in collection with ID 'Asset:org.example.basic.EHR' does not exist; [cause=Participant 'org.example.basic.Patient#1' does not have 'READ' access to resource 'org.example.basic.EHR#4']

Fig-11 :A patient cannot retrieve other patients' EHRs

The network was tested using Hyperledger caliper. Hyperledger caliper is a blockchain benchmark tool developed by Linux foundation that tests the network using the following parameters:

- **Transaction throughput:** the rate in which it commits valid transaction in the defined period of time.
- **Transaction latency:** transaction latency is the time taken between when the transaction is submitted and when the transaction is confirmed committed across the network.
- **Send Rate:** send rate is defined as number of transactions sent per second.

Table 1 and 2 indicates performance of the proposed hyperledger composer blockchain network. Increase in the number of transaction increases the throughput and send rate with latency. While an increase in the number of peers decreases throughput and increases latency while the send rate is constant for the same number of transactions. This is due to the fact that an update in the ledger now has more peers to send the proposed change for verification and final updation to their local copy of the ledger throughout the network.

Table -1: Performance analysis for thoroughput

Type of Architecture	No of transactions	Send Rate	Thoroughput
2 org 1 peer	10	11.1	4.2 tps
2 org 1 peer	100	10.1	5.5 tps
2 org 2 peer	10	11.1	2.8 tps
2 org 2 peer	100	10.1	3.6 tps
3 org 1 peer	10	11.1	3.3 tps
2 org 1 peer	100	10.1	3.9 tps

Table -1: Average latency for different transactions

Type of Architecture	No of transactions	Max. latency	Min. latency	Avg. latency
2 org 1 peer	10	1.56 s	0.87 s	1.30 s
2 org 1 peer	100	8.72 s	1.13s	5.07 s
2 org 2 peer	10	3.03 s	1.43 s	2.20 s
2 org 2 peer	100	18.21 s	1.43 s	9.21 s
3 org 1 peer	10	2.24 s	1.38 s	1.59 s
2 org 1 peer	100	16.73 s	1.03 s	10.29 s

5. CONCLUSIONS

The integration of blockchain technology in healthcare research can bring many benefits, including improved data sharing and tracking, enhanced transparency, and better privacy for patients. This proposal suggests an architecture that uses blockchain technology in national electronic health record (EHR) systems to ensure data integrity and interoperability. The framework offers secure record storage, granular access rules, and measures to address data storage issues, information asymmetry, and access control. Hyperledger Composer is used to execute smart contracts and impose access control policies, ensuring traceable access events and transaction records for EHR data management. By using blockchain, trust among healthcare organizations can be ensured, the overall cost of treatment can be reduced, and the standard of the healthcare industry can be improved. Although it may take time to adapt, including Hyperledger Fabric can provide an industrial standard for the field of healthcare, enabling the tracking of patient records from start to finish.

REFERENCES

[1] Niu, S., Wang, J., Chen, L. (2019) Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access.

[2] Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: a blockchain-based platform for healthcare information exchange. In 2018 IEEE International conference on smart computing (SMARTCOMP); 2018. p. 49–56.

[3] Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: efficient and secure medical data sharing via blockchain. J Med Syst 2018; 42(8):136.

[4] Sun Y, Zhang R, Wang X, Gao K, Liu L. A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th International conference on computer communication and networks (ICCCN); 2018. p. 1–9.

[5] Yang G, Li C. A design of blockchain-based architecture for the security of electronic health record (EHR) systems. In: 2018 IEEE International conference on cloud computing technology and science (CloudCom); 2018. p. 261–5.

[6] Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J Med Syst 2018; 42(8):152.

[7] Guo R, Shi H, Zhao Q, Zheng D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 2018; 776(99):1–12.

[8] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. Medshare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017; 5:14757–67.

[9] Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Personal, indoor, and mobile radio communications (PIMRC), 2017 IEEE 28th annual international symposium on; 2017. p. 1–5.

[10] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 2016; 40(10):218.

[11] Swan, M. (2015). Blockchain: Blueprint for new economy. Newton: O'Reilly Media, Inc.

[12] Antonopolous, A. M. (2014). Mastering bitcoin: Unlocking digital cryptocurrencies. Newton: O'Reilly Media, Inc.

[13] Nakamoto, S. (2008). Bitcoin: A peer to peer electronic cash system. https://www.bitcoin.org/bitcoin.pdf