Journal of Computer Science

Original Research Paper

Empowering Privacy: Harnessing Hyperledger Fabric to Safeguard EHR Systems

[1]Vidhi Thakkar and [2]Vrushank Manharlal Shah

[1]Department of FCAIT, GLS University and Research Scholar, Indus University, Ahmedabad, Gujarat, India
[2]Department of Electronics and Communication, Indus University, Ahmedabad, Gujarat, India

Article history
Received: 10-03-2023
Revised: 19-05-2023
Accepted: 24-05-2023

Corresponding Author:
Vrushank Manharlal Shah
Department of Electronics and Communication, Indus University, Ahmedabad, Gujarat, India
Email: drvrushankshah13@gmail.com

Abstract: The Blockchain boom began with the debut of Bitcoin. The application of blockchain technology is expanding rapidly. Various sectors such as supply chain, logistics, research, healthcare, government, banking, media, and entertainment have already embraced this ground-breaking, decentralized technology. The healthcare industry is at the top of the list with significant blockchain potential. This article discusses the permissioned blockchain powered by Hyperledger Fabric and its privacy-preserving features like identity mixer, multichannel, private data collections, and transient field. This study considers the EHR systems scenario and proves how these privacy protection techniques of Fabric could protect the privacy of healthcare organizations' sensitive data. We evaluate existing studies on the use of the Hyperledger Fabric framework for EHR systems. We discovered that their implementation has data privacy and user privacy concerns that can be addressed in our future studies.

Keywords: Electronic Healthcare Record Systems (EHRs), Hyperledger Fabric, Permissioned Blockchain, Privacy-Preserving Mechanisms, Private Data Sharing

Introduction

Blockchain is one of the most revolutionary technologies of the twenty-first century. It is effective in promoting decentralization and retaining system integrity (Leng *et al*., 2021). It has gained popularity not just in crypto assets but also in various other industries. Numerous industries, including those in education, healthcare, IoT, logistics, supply chain, etc., have adopted blockchain for security, authentication, and privacy. Recent studies and proof-of-concept implementations show the value of blockchain technology in the healthcare sector. Integrating blockchain into the healthcare industry can ease many healthcare use cases such as retaining a complete history of the patient healthcare data, patient-centric electronic health records, remote monitoring, tracing and securing medical supplies, easy exchange and traceability of electronic health records, insurance management and many more (Yaqoob *et al*., 2021; Kaur *et al*., 2021; Agbo *et al*., 2019). The Healthcare industry deals with sensitive medical data and protection is of utmost importance (Dubovitskaya *et al*., 2020). In this study, we have considered the Electronic Health Record (EHR) sharing system scenario and show how this blockchain technology can facilitate transactions across networks in a private, safe, and trusted manner. EHR systems store patients' core electronic medical data. Recently this EHR data has become more susceptible to intrusion as internet usage and digital healthcare systems grow (Chenthara *et al*., 2020). The increased incidences of healthcare data breaches are a crucial factor and boosted blockchain adoption in the healthcare business.

There are three types of blockchain technology: Permissioned, private, and public (Kaur *et al*., 2021; Butt *et al*., 2022). A public blockchain such as Ethereum is largely anonymous. This prohibits the use of blockchain technology in scenarios where particular organizations join a consortium to deal with one another but do not want their data exposed to the public. Private blockchains restrict access and forbid unauthorized network use by members of the general public. In a private blockchain such as Enterprise Ethereum, all peers of the network are regarded equally, and no access control method or architecture is provided for the creation of transactions for certain groups. To solve this issue a permissioned (Agbo *et al*., 2019; Dubovitskaya *et al*., 2020) blockchain such as Hyperledger Fabric enters the scenario with correct access control mechanisms. Hyperledger Fabric technology combines the advantages of both private and permissioned blockchains. Fabric offers a variety of ways to create

private transactions between a few organizations while hiding information about the transaction from other organizations (Brotsis *et al*., 2020).

One of the most widely used permissioned blockchain solutions is Hyperledger Fabric. Fabric is utilized for industry-specific applications that deal with assets maintained off-chain (Hyperledger Fabric, 2022). Medical information is highly sensitive, both socially and legally. The Healthcare industry requires faster consensus algorithms and short block confirmation times before being admitted to the chain. Because Fabric enhances transaction performance, trust, and traceability, it is more appropriate for managing and sharing health records (Leng *et al*., 2021; Kaur *et al*., 2021). Through access control policies and smart contract rules, the owner of a piece of data can decide which portions of that data are available (Dubovitskaya *et al*., 2020; Chenthara *et al*., 2020; Mani *et al*., 2021; Wang *et al*., 2021). In recent years, few Hyperledger Fabric-integrated permissioned EHR solutions have been published. However, none of them maintains user and transaction privacy during transaction consensus. The two privacy concerns in relation to blockchain-integrated EHR solutions are user privacy and data privacy. The issue with adding private information to the ledger in Fabric is that everyone will have access to it. In the EHR sharing use case, healthcare organizations do not want to reveal transaction information to other network members. This information can reveal many private data related to the transaction such as input parameters of a transaction, the sender of the transaction, which node has endorsed this transaction, and who has ordered this transaction into a block. However, this disclosure makes EHR transactions linkable. Healthcare organizations prefer to keep some data private to themselves or communicate with a subset of peers of the network only. Fabric offers Private Data Collection (PDC), transitory field, Identity Mixer, and advanced patterns for fine-grained access control, allowing only a select group of participants to exchange private data.

Background

Hyperledger Framework

Hyperledger is an open-source distributed ledger framework. It offers various other projects under its umbrellas such as Hyperledger Besu, Iroha, Fabric, Sawtooth, and Indy as well as tools like Hyperledger Avalon, Explorer, Cello, Cactus and Caliper and libraries like Hyperledger Aries, Ursa. Among them, Fabric is the most deployable distributed ledger than any other permissioned blockchain solution (Leng *et al*., 2021).

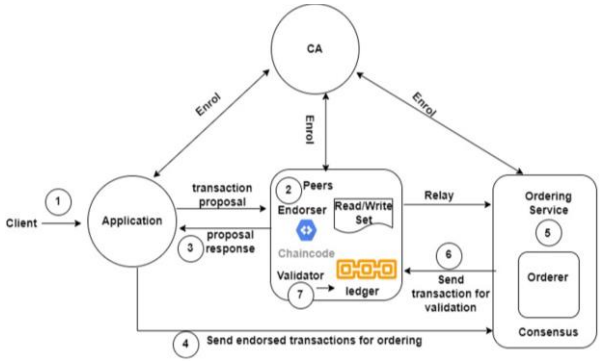

Fig. 1. Hyperledger fabric transaction flow

Hyperledger Fabric

Hyperledger Fabric creates a private permissioned network, visible only to the stakeholders registered with the authority (Androulaki *et al*., 2018). Fabric supports a modular approach that incorporates extensibility, flexibility, and the ability to modify any component independently of the rest of the system. Fabric offers many SDKs for programming languages like Node.js, Java, Python, and Go. The Fabric uses container technology to host a smart contract (Chaincode) with application logic (Chenthara *et al*., 2020). The consensus process is broken down into three parts by the consensus technique in Fabric: Endorsement (execution), ordering, and committing (validation). Figure 1, depicts the Fabric 2.0 transaction flow with seven steps and three phases namely endorser, orderer, and validator. A transaction proposal is first sent by the client and then endorsers simulate the proposal by executing a chaincode and preparing read/write sets. Later, this would be given to an order where sorting and packing of transactions are done. The orderer combines many transactions into a single block and broadcasts the sorted transactions to all validator peers on the network. Finally, when the validator has checked each transaction, the committer saves this data on the chain. This three-phase "execute-order-validate" transaction workflow helps in achieving high scalability, performance, and modularity.

The Fabric also supports unique access control and data isolation mechanisms such as policy, channel, transient fields, and private data collection (Wang *et al*., 2021). It supports private transactions and has an optimal speed of transactions on a real-time basis, which makes it the most suitable type of blockchain network for EHR systems (Leng *et al*., 2021; Agbo *et al*., 2019).

Hyperledger Fabric Components

Hyperledger Fabric consists of various components (Chenthara *et al*., 2020; Hyperledger Fabric, 2022; Androulaki *et al*., 2018; Hyperledger Foundation, 2020; Uddin *et al*., 2021) like peer nodes, clients, ordering

service, membership, and chaincode. Each of them has a specific purpose and plays a distinct role. The beauty and the hard part of the components is customization.

Peer: A peer can be an endorser, an orderer, a validator, an anchor peer (through which other peers can discover and interact), or a leader peer (for the purpose of allocating blocks to peers).

Channel: To enable private and secure communication among various network parties, channels are built.

Chaincode: Chaincode is a self-executing program. They are installed on the endorser nodes only. Chaincode will be executed when certain conditions are met and the outcomes of the transaction execution are sent to the blockchain network and subsequently added to all peers' ledgers.

Fabric CA: Fabric Certification Authority (CA) handles enrollment certificate issuance and identity registration.

MSP: Membership Service Provider (MSP) issues node credentials for authentication and authorization.

Ledger/database: A ledger in Fabric is composed of transaction logs and a world state. The world state retains the most recent outcome following the completion of transactions. CouchDB or LevelDB can be used as the World state.

Ordering Service: The Ordering Service nodes construct a global order of transactions and generate blocks that are disseminated to peers. The ordering services supported by Fabric are Solo, Raft, and Kafka. Although Kafka has been dropped in a later version of Fabric and the Solo's implementation has been deprecated. Only Raft is working on the latest version of Hyperledger Fabric V2.x.

Cryptogen and Configtxgen: The Fabric has a tool called Cryptogen that can generate the necessary cryptographic materials, like ×509 certificates and signing keys, for the entire network members. Cryptogen generates a crypto-config.yaml file for the network's basic topology. Configtxgen reads the file configtx. yaml. Configtx. yaml defines the target network's definitions. Organizations, peers, policies, ACLs, capabilities and other structure configurations are all defined.

Private data collection: The fabric supports unique security mechanisms such as private data collection. Using this feature private data can be shared with approved organizations, whereas public data can be shared with all organizations on a channel without the need for a separate channel.

The Notion of Privacy and How Hyperledger Fabric Deals with It

In a permissioned network such as Hyperledger Fabric, members of the network can conduct secret and confidential transactions using a channel, which functions as a private "subnet". However, the privacy of the patients is violated because the ledger that contains all transaction-related data is shared across channel members:

So, how do we deal with the below-listed questions?

1) How to ensure your transactions are seen by a certain set of people?
2) How to ensure your data remains private and confidential?

Notion privacy deals with data privacy and user privacy. It complicates with the notion of replication and decentralization. While dealing with Hyperledger Fabric blockchain-integrated applications, the below-listed parameters of privacy should be considered:

- Transaction data privacy: Input parameters to transactions to know which smart contract is being executed during the transaction execution process. To hide the input parameters of the transactions, Fabric supports a Transient Field mechanism
- State data privacy: Smart contract output is an internal state managed by a smart contract and recorded to the ledger. These state data can be stored in Private Data Collections (PDC) to preserve privacy
- Smart contract privacy: Logic of the chain code, which will be on the blockchain and be accessible by a certain set of authorized users only. To solve these concerns, Chaincode can be installed on selected peers only who are responsible for the endorsement
- User privacy: User anonymity and unlinkability are important aspects of user privacy. User anonymity is the ability to transact without disclosing the identity of the transactor by masking user-level credentials in the ledger. The ability of a transactor to throw several transactions without being linkable is known as unlinkability. Zero-knowledge proof and identity mixer can be used to address these issues

The permissionless blockchain platforms do not provide any of these privacy features, except pseudo-anonymity. It is left to the applications to explicitly handle them. This is why healthcare organizations, where it is crucial to protect the privacy of patients' sensitive information, will benefit more from using the Hyperledger Fabric permissioned blockchain. The need to combine the privacy of medical data on the one hand with the desirea to enhance healthcare quality is one of the most challenging issues facing healthcare organizations today. Hyperledger Fabric, a permissioned blockchain technology can be a viable solution to these issues.

Materials and Methods

In this study we have applied Hyperledger Fabric's privacy protection mechanisms such as channel, private data collections, transient field, Identity Mixer for EHR sharing scenario to achieve privacy inside the network. In Fabric, there are two ways to accomplish this: At the application level, utilizing channel and identity mixer with ZKP, and at the chaincode level, using private data and transient filed. These mechanisms can be used for EHR systems to enhance privacy inside the blockchain network. For dealing with the private data of healthcare organizations, this study implement channel, PDC, Transient Field features in Hyperledger Fabric's Node.js SDK and Identity Mixer using Hyperledger Fabric's Java SDK v2.4.

Channel

A channel is a private "subnet" that enables two or more network users to conduct hidden, private transactions (Hyperledger Fabric, 2022). Channels hold transactions, chain codes, access control policies, configuration, and membership data. This data is utilized to manage the channel as well as the network's security, privacy, and scalability. Every channel has a separate distributed ledger where all of the transaction-related information such as digital signatures, timestamps, input and output data, and transaction IDs are stored. However, revealing channel data to the whole network might reveal confidential details about a transaction.

Existing Fabric integrated EHR studies have applied various encryption mechanisms to ensure the privacy of ledger data. But the encryption method can decrease system performance and it is also difficult to manipulate or validate encrypted data. Apart from that, storing patients' heavy medical records degrades blockchain performance. Also, the size of a block and GDPR make data storage on blockchain problematic. To deal with these problems, it is recommended to store actual data on off-chain storage, such as in the cloud, or on IPFS, and transaction metadata on the blockchain only. To protect the identity of the patient, the information that is accessible to all the entities should also be stored anonymously. Even though from the encrypted patient identity of the ledger, transacting users can be identified and data privacy is not offered concerning the orderer because the orderer can look into who has endorsed the transaction, which smart contract has been performed and what were the input parameters for the transaction. Therefore, using channels for EHR sharing systems cannot have privacy.

Multichannel

A channel allows a certain group of network users to communicate privately and securely. The visibility of transactions and data between various network participants can be isolated and limited using multiple channels. When a subset of organizations on a channel needs to keep data secret from other organizations on the channel, they can create a new channel that only contains the organizations that require access to the data. Each channel would maintain its broadcast mechanism and transaction ordering takes place independently of other channels. Figure 2, shows a two-channel example for Fabric Java SDK.

Figure 3, shows an example where two channels and three organizations are built in the Fabric network. Three organizations org1, org2, and org3 each of which has a peer Peer0 are being built into a network. There are two channels here: Channel1 (org1, org2 and org3) and Channel2 (org1 and org2).

```
// Create and join first channel
String chname1 = "ch1";
ChannelConfiguration config1 = new ChannelConfiguration(new File("chn1.tx"));
Channel channel1 = client.newChannel(chname1, orderer, config1, client.getChannelConfigurationSignature(config1, user));
channel1.joinPeer(peer);

// Create and join second channel
String chname2 = "ch2";
ChannelConfiguration config2 = new ChannelConfiguration(new File("chn2.tx"));
Channel channel2 = client.newChannel(chname2, orderer, config2, client.getChannelConfigurationSignature(config2, user));
channel2.joinPeer(peer);
```

Fig. 2. Multiple channel example in fabric SDK

DOI: 10.3844/jcssp.2023.1292.1304

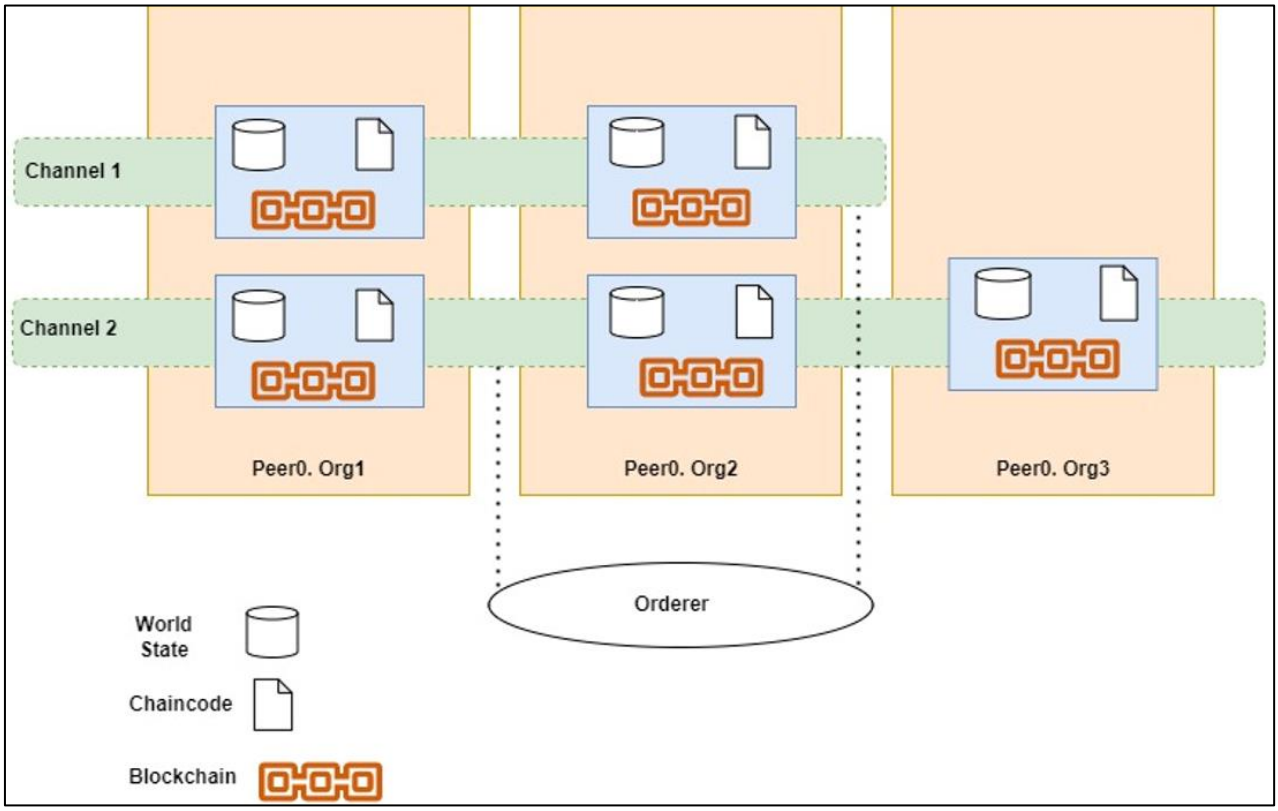

Fig. 3: Multiple channels

Healthcare organizations want to transact with one another over the same channel without letting another organization view confidential data. To solve this concern, multiple channels can be created. However, for each channel, participating peer has to maintain different world state database, blockchain ledger, and chaincodes also. Also, the creation of a network with many channels brings down decentralization, limits interoperability, and raises network overhead. After all, organizations want to hide the data and not the transactions, so multichannel is not the best option.

Private Data Collections

Private Data features allow a subset of organizations to transact with one another over the same channel without the danger of another business seeing confidential information (Private Data, 2020). Creating separate channels in each scenario adds extra administrative complexity and prevents use cases where data has to be private between certain organizations. Private data enables data privacy within a channel while reducing the number of channels.

In Fabric v2.0, an implicit collection for each organization is introduced and application chaincode can be used even if no collection is explicitly defined. Figure 1 depicts the two parts of a ledger as well as the location of the private data. Figure 4 depicts the two parts of a ledger as well as the location of the private data. There are two main elements of private data collection. First is Private Data and second is the Hash of the data. The private data that you provide in your specification of private data collection is passed from peer to peer using the gossip protocol to other organization that has been specified in the policy. On the peer, a private database stores private data. this information remains confidential. The ordering service can't see the private data. A hash of the data that is endorsed, ordered, and written to each peer on the channel. This hash serves as transaction proof and is auditable.

This feature can be clubbed for EHR applications where one or more healthcare organizations/peers want to keep data private for themselves or certain organizations without letting anyone know about it. We have made three collections below in the config.json file Fabric Java SDK. As a result, org1 and org2 can transact with one another on the same channel without fear of other organizations seeing private information. For example, doctor's consultation charges, disease information of a patient or patient giving his consent to another doctor, or the patient has consulted 10 times a doctor. All these transactions should be kept confidential.

DOI: 10.3844/jcssp.2023.1292.1304

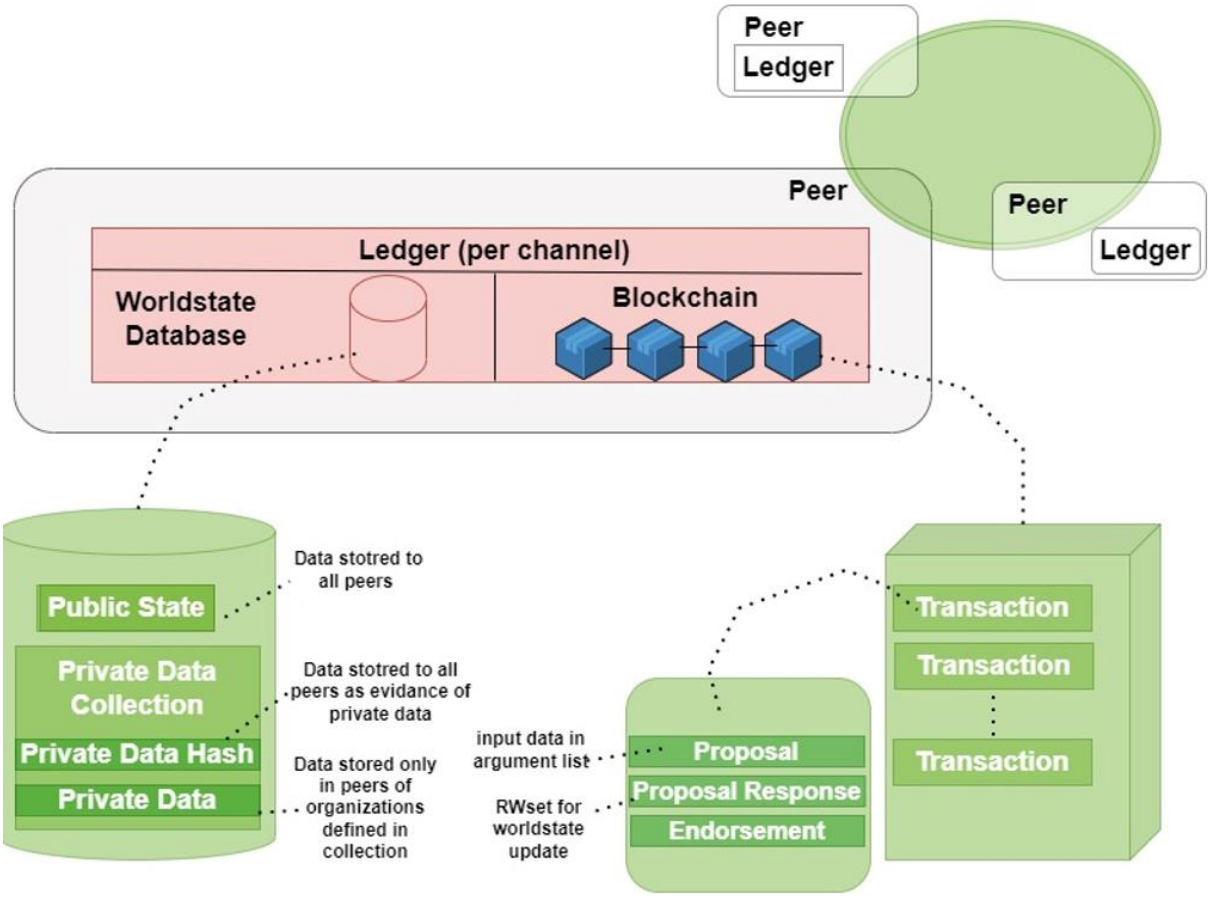

Fig. 4. Private Data example

Collections are defined in a JSON file called collection definition, which lists all the collections' properties. When the chaincode specification is authorized and committed in Fabric Java SDK v2.4, this file is specified.

Example of collections_config.json

```
[ {
 "name": "asset",
 "policy": "OR ('Org1MSP.member', 'Org2MSP.member')",
 "requiredPeerCount": 1,
 "maxPeerCount": 1,
 "blockToLive":1000000,
 "memberOnlyRead": true,
 "memberOnlyWrite": true
 },
 {
 "name": "Org1PC",
 "policy": "OR ('Org1MSP.member')",
 "requiredPeerCount": 0,
 "maxPeerCount": 1,
 "blockToLive":3,
 "memberOnlyRead": true,
 "memberOnlyWrite": false,
 },
 {
 "name": "Org2PC",
 "policy": "OR ('Org2MSP.member')",
 "requiredPeerCount": 0,
 "maxPeerCount": 1,
 "blockToLive":3,
 "memberOnlyRead": true,
 "memberOnlyWrite": false,
} ]
```

Below is an example of creating the data definition in the chain code. The medical data transfer sample divides the private data into three separate definitions according to how the data will be accessed. The first collection is for both organizations, the second collection is only for org1 and the third collection is for org2.

Org1 and Org2 peers' private data:

```
type PatientInfo struct
{
```

```
PatinetID string `json:"patientID"`
Name string `json:"patientname"`
Age int `json:"age"`
OrgName string `json:"Hospname"`
}
```

Org1 Private Data:

```
type Org1PrivateDetails struct
{
 Charges int `json:"fees"`\\fees of a doc
 No_of_Patient int `json:"no_of_patient"` \\No of patient
    visited
}
```

Org2Private Data:

```
type Org2PrivateDetails struct
{
Salary int `json:"salary"` // salary of doctor
AppraisedValue int `json:"appraisedValue"` //value given
to doctor
}
```

Figures 5-6, we have represented data collection in the ledger for peer0.org1 and peer0.org2. We can observe that org1.peer0 and org2.peer0 both can access the Patient Info collection. However, the collection org1privatedetails is accessible only by peer0.org1. It is because this data is written on the collection for org1. We can see the actual data is in the \$\$p database, whereas the hash of the actual data is in the \$\$h database. We can observe that the real data for org1 is saved in peers of org1, whereas the data hash is kept in all peers within a channel (in both org1 and org2 as well). The same scenario works for peer0.org2. The collection org2privatedetails is accessible only by peer0.org2.

Data stored on PDCs can be discarded as they are not immutable as blockchain. Therefore, PDCs can be used to store the private and sensitive data of businesses, which makes them even more interesting in terms of GDPR. To solve GDPR compliance with PDC blockToLive parameter can be set in config.json.

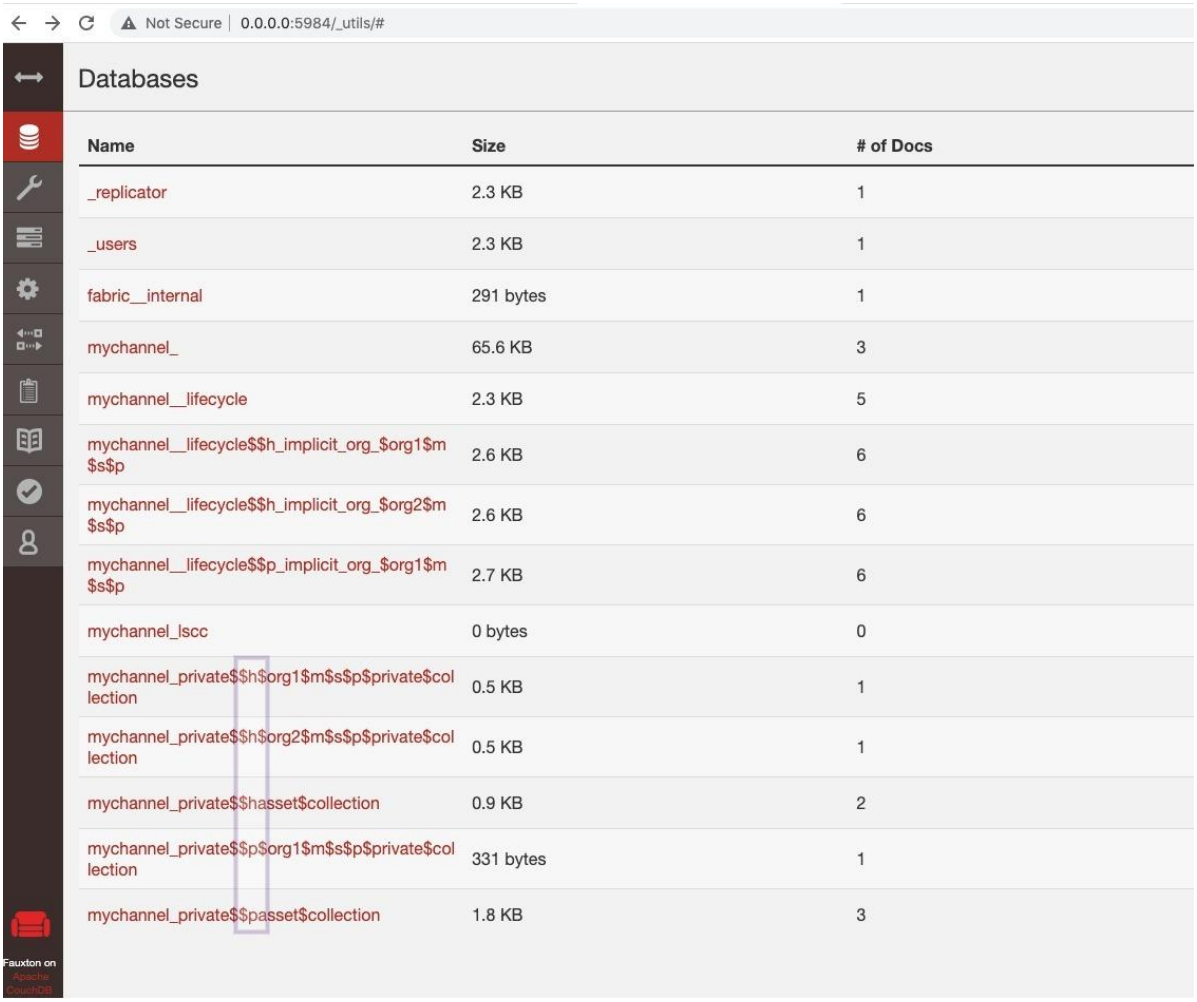

Fig. 5: Org1 PDC from the administrator panel of CouchDB

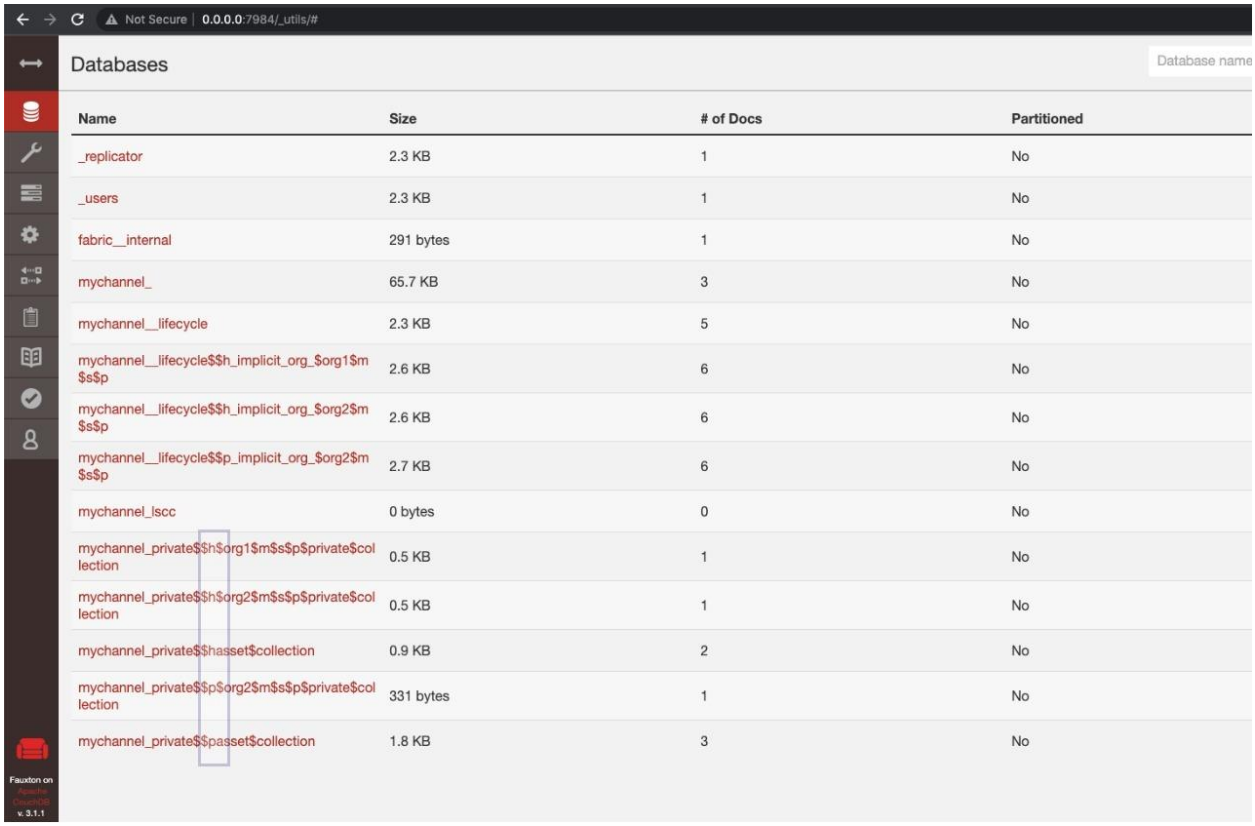

Fig. 6: Org2 PDC from the administrator panel of CouchDB

Transient Filed

Private Data is concerned with preserving the data privacy inside a defined subset of organizations, whereas Transient Data is an input technique for Private Data. Both are two distinct concepts from a technical standpoint. They can be used together to achieve a certain level of security in Hyperledger Fabric Applications (Using Private Data in Fabric, 2022). Passing any private data of a transaction proposal through the transient field will not be included in the transaction and, as a result, is not visible to unauthorized parties. The transient field data keys will only be accessible by chain code installed on the docker container, even the endorsers who execute the chain code cannot access them as shown in Fig. 7. Transient Data can be implemented when sensitive input data must not be recorded on the blockchain and private data to be stored in the world state database of the peer.

The encryption/decryption key can be passed using a transient field bypassing the endorser. This key can be processed by chain code to encrypt/decrypt data and later saved to the PDC of the peer for better privacy. Transient data is passed as binary data and base64 encoded in the terminal as shown in Fig. 8. Only a chaincode can access data passed through the transient field. A combination of PDC and transient filed features can be used to achieve data confidentiality inside a Fabric Network. However, using PDC for businesses has problems related to data privacy because all peers (inside and outside the subgroup) will preserve a record of private data hash as proof of data existence. So, a better option is to use transient data.

Identity Mixer and Zero Knowledge Proof

In Hyperledger Fabric, the endorser provides its identity and signature during transaction endorsement, therefore, to be validated later by the orderer. However, disclosing the identity of endorsing peers for EHR transactions may compromise patient privacy and make transactions linkable. To deal with these concerns, Identity Mixer can be implemented on top of the Hyperledger Fabric. Using this Identity Mixer MSP, the endorser node can sign the transaction by remaining anonymous, generating an unlinkable signature. Idemix cryptographic protocol suite (MSPIIM, 2017) uses ZKP to provide anonymity and unlinkability. It is associated with identity certificates that each participant needs to use for performing every action on the distributed ledger.

DOI: 10.3844/jcssp.2023.1292.1304

IDEMIX Protocol

Identity Mixer is a new form of membership provider that offers a strong privacy-preserving authentication solution. Figure 9, shows the working of the Identity Mixer. Idemix flows involve the user, issuer, and verifier as three different players. A set of user attributes is issued in the form of a digital certificate by an issuer, also referred to as a "credential." A "zero-knowledge proof" of ownership of the credential is afterward produced by the user, who also selectively discloses only the attributes they want to make public. The proof does not expose any further information to the verifier, issuer, or anybody else because it is zero knowledge.

Working on Identity Mixer

Identity Mixer can be implemented on top of the Hyperledger Fabric to enhance security and privacy (MSPIIM, 2017). It is associated with identity certificates that each participant needs to use for performing each action on the distributed ledger. Using IDEMIX, a user can generate new Transaction Certificates from the original Enrolment Certificates for each transaction as illustrated in Fig. 10. The user can generate a new key and only the auditor would have an idea of that key. Idemix Provides strong authentication and privacy-preserving features such as anonymity (the ability to transact without revealing the identity of the transactor) and unlinkability (the ability of a single identity to send multiple transactions without revealing that the transactions were sent by the same identity).

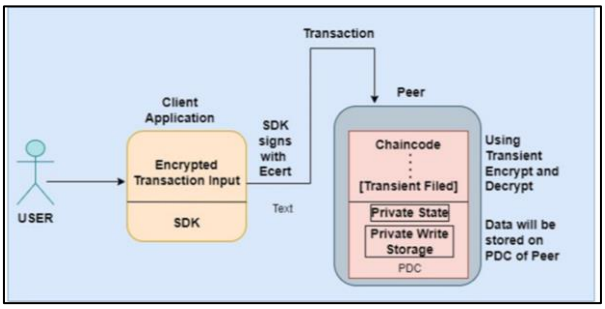

Fig. 7. Example of Transient Field combined with PDC

Fig. 8. Example of transaction with Transient Field

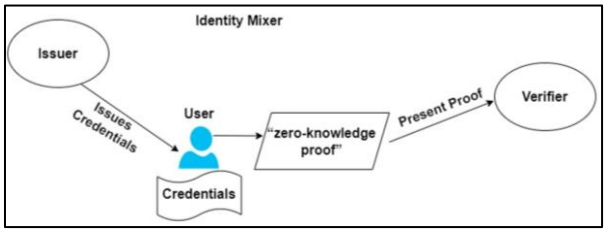

Fig. 9: Identity mixer

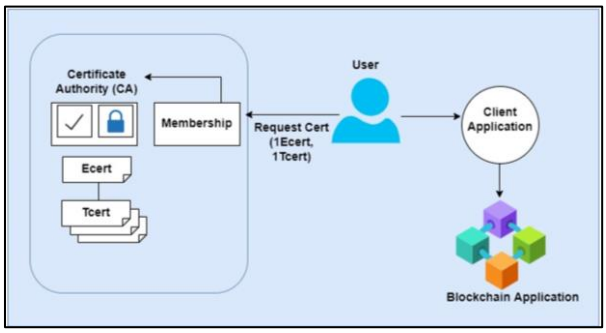

Fig. 10. Working of identity mixer

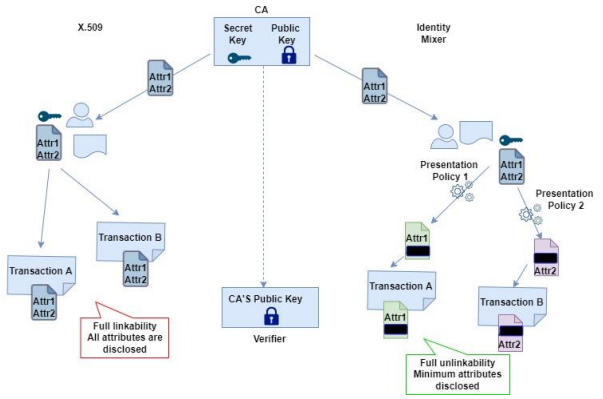

Fig. 11: Comparison of X.509 and identity

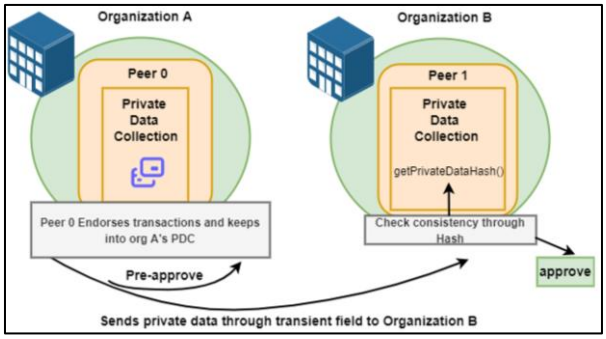

Fig. 12: Combination of transient and PDC

X.509 and Identity Mixer

Identity Mixer is a privacy-preserving cryptographic protocol. Idemix uses Zero Knowledge Proof (ZKP) to provide anonymity and unlinkability of transactions. This feature is highly suitable for healthcare applications where anonymity and transaction unlinkability are required. Using this protocol, entities/nodes of the EHR system that act as a client can view, update, and share private medical records while maintaining anonymity and privacy. Idemix also provides unlinkability means a single identity can send many transactions without exposing their identity. Compared to the conventional X.509, Identity Mixer signatures (Combined with zero-knowledge proofs) give advanced privacy protection shown in Fig. 11. With this IDEMIX client can hide attributes and reveal only selected attributes. Also, the original Enrollment ID will be hidden from the orderer and other peers. We can see in Fig. 10 that there is an unlinkability of signatures generated with the same credential as only selective attributes are disclosed.

Advanced Patterns

In Fabric, transaction endorsement is visible on the ledger and is not optimal for organizations dealing with private data. For EHR transactions, while a patient from Organization A gives consent to a doctor of Organization B, we wish to endorse this transaction with these two organizations only and we expect this information to remain hidden from other organizations. However, this endorsement is available on the ledger and will not preserve the privacy and anonymity of transactions or users.

To solve this concern of the Hyperledger Fabric, we can use the mixture of PDC and the Transient Filed mechanism. In Fabric v2.x, every organization has one Private Data Collection to store private information just for that organization. To accomplish privacy and anonymity of transactions, we can build a network by combining this Private Data Collection and the Transient Field as shown in Fig. 12. It is also known as a quasi-anonym endorsement. It allows two organizations to exchange information while keeping it hidden from the other organization, even if they are on the same channel. It's like there is a private token just for organization A and moved to the Private Data Collection of organization B when a certain transaction happens. It works in a way that consists of two transactions: Pre-approve and Approve. In Pre-approve, Peer 0 will write some information in the private data collection of organization A along with some metadata of that transaction which should be approved in the long term. Having a Pre-approve state, Organization A can send a transaction to Organization B for endorsement. Organization A can send this private data in a transient field to organization B. Later, B can decide based on the hash whether this transaction was pre-approved by organization A or not.

Permissionless blockchain systems do not provide any of these qualities of privacy. Instead., they offer pseudo-anonymity at best. As a result, these systems are incompatible with businesses, making permissioned blockchain systems the best option.

Results

Hyperledger Fabric provides a variety of techniques for dealing with complex business scenarios, such as the privacy protection issues posed by Healthcare data sharing. A flexible combination of these privacy protection measures can satisfy different privacy security needs. By using a private collection, transient field and channel mechanism, Hyperledger Fabric is able to isolate private data. Transactions can be completed without disclosing the identity by implementing Identity Mixer. This study shows practical exploratory of Hyperledger Fabric's privacy protections mechanisms to develop privacy-preserving EHR handling solution.

Discussion

This section examines the most recent research on sharing and managing EHR systems via Hyperledger Fabric.

Huang *et al*. (2019) suggested Medbloc, a secure EHR sharing platform built on Hyperledger Fabric. It was aimed at the healthcare sector of New Zealand. The system was created using the Fabric version 1.1 and the Practical Byzantine Fault Tolerant (PBFT) consensus mechanism. Using an access control system based on smart contracts, the medical records were encrypted and stored on the blockchain. Their system has several benefits, such as availability, effectiveness, and security. Mahore *et al*. (2019) suggested a permissioned blockchain paradigm to effectively maintain medical records in terms of privacy, security, scalability, and availability. By storing sensitive patient data off-chain and only retaining the hash of the data in a blockchain record, this approach solves the scalability problems of the blockchain. They have also employed a proxy re-encryption approach to transmit encrypted data from the patient to the provider. They created their solution using the PBFT consensus algorithm, the solo ordering service, and Hyperledger Fabric version V1.4. They have also statistically examined their strategy using the Hyperledger Caliper to determine how effectively it works.

Later in 2020, a couple of more studies were done with the goal of creating scalable and secure EHR-sharing systems utilizing the Hyperledger Fabric. Dubovitskaya *et al*. (2020) presented an ACTION-EHR for managing the medical records of cancer patients. Researchers and healthcare professionals will be able to exchange EMR data using the Fabric architecture. Patients' medical information is encrypted with public-key cryptography and kept on cloud servers off the blockchain.

Table 1: Existing fabric-integrated EHR studies

Reference	Fabric version	Private data collection	Transient field	Identity mixer
Huang *et al*. (2019)	Fabric V1.1	N	N	N
Mahore *et al*. (2019)	Fabric V1.4	N	N	N
Dubovitskaya *et al*. (2020)	Fabric V1.4	N	N	N
Tith *et al*. (2020)	Fabric	N	N	N
Chenthara *et al*. (2020)	Fabric V1.3 and composer	N	N	N
Stamatellis *et al*. (2020)	Fabric	N	N	N
Mani *et al*. (2021)	Fabric	N	N	N

The system guarantees accurate access control, data confidentiality, and EMR data accessibility. The ACTION-EHR blockchain network is built using the Membership Service, Orderer, Fabric v1.4 SDK, and couchDB for on-chain information management and permissions. Tith *et al*. (2020) used consortium blockchain and Hyperledger Fabric to create a distributed solution for merging existing EHRs. Through the use of a centrally located server and a proxy re-encryption method, encrypted data is transmitted from the patient to the physician. The eID has been salt-hashed to prevent transactions from being tracked on the ledger. With Hyperledger Fabric and Hyperledger Composer, they were able to achieve scalability, transparency, traceability, availability, and dependability with their approach. A framework for protecting electronic health records was developed by Chenthara *et al*. (2020) using permissioned blockchain technology. Huge EHRs were stored on distributed IPFS, but only encrypted hashes of the records were present on the blockchain. Better assurances of data quality, scalability, privacy, and interoperability are achieved in their new paradigm. The Fabric's components such as MSP, CA, PBFT consensus, CouchDB, and chaincode were used to create the system. They have increased scalability while assuring a high level of security and privacy thanks to their research. Stamatellis *et al*. (2020) developed the Hyperledger Fabric-based EHR management solution PREHEALTH, to protect patient privacy. The solution to ensure transaction anonymity and unlikability discusses Identity Mixer. The approach is compliant with GDPR and emphasizes Hyperledger Fabric's privacy-preserving features. The configuration data for Hyperledger Fabric, however, discussion regarding the implementation of identity mixer has not been given. Mani *et al*. (2021) introduced PCHDM, a patient-centered healthcare data management solution. To maintain health records, their strategy also makes use of off-chain and on-chain technologies. Hashes of medical records are safely stored with encrypted health data using IPFS technology. Byzantine Fault Tolerance (BFT) consensus is used to implement smart contracts inside secure containers. High levels of security, privacy, and scalability are thus possible. Hyperledger Caliper benchmarks for transaction latency, throughput, and resource utilization are used to assess performance.

The aforementioned Fabric-based EHR studies mainly focused on providing a solution where the patients can have complete control over their data and privacy of their data between permissioned organizations. These studies address the interoperability, immutability, scalability, performance, and data protection issues of permission-less blockchain-based EHR systems. Table 1 we have analyzed their work in terms of utilization of Fabric's privacy preservation mechanisms namely private data collection (for secure data and GDPR), Transient Filed (to secure transaction data privacy during consensus), and identity mixer (for user anonymity and unlikability during endorsement). The comparison shows none of them have taken into account or utilized the security and privacy-preserving features of Hyperledger Fabric. Only Stamatellis *et al*. (2020) have put out a safe EHR administration system utilizing the privacy-preserving capabilities of Hyperledger Fabric; however, their work has not shown any implementation details.

Conclusion

Blockchain technology has emerged as an innovative tool that has the potential to positively impact the healthcare industry by speeding up data collection and sharing integrated heterogeneous data. Keeping medical data safe and secure is the most prominent blockchain healthcare application at the present time. Integrating Hyperledger Fabric permissioned blockchain network with EHR systems helps stakeholders achieve maximum interoperability, security, privacy, and scalability. Several studies have proposed a blockchain-enabled Hyperledger Fabric architecture for EHR systems. However, it lacks privacy protection for the end-users. This study has explored Fabrics' robust privacy-protection techniques such as Channels, Private Data Collections, Transient Filed, and Identity Mixer. These mechanisms offer the scope of achieving explicit anonymity and privacy of transactions inside the network. In our future work, we will implement privacy preserving of Hyperledger Fabric using Java SDK V2.5.

Acknowledgment

I would like to thank my research guide Dr. Vrushank shah, Indus University for his guidance and constant encouragement to progress and complete this research work successfully.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contribution

Vidhi Thakkar: The paper Conceptualization, methodology and written.

Vrushank Manharlal Shah: The paper Reviewed.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all have read and approved the manuscript and no ethical issues involved.

References

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: A systematic review. In *Healthcare* (Vol. *7*, No. 2, p. 56). MDPI. https://doi.org/10.3390/healthcare7020056

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference* (pp. 1-15). https://doi.org/10.1145/3190508.3190538

Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G., & Shiaeles, S. (2020, October). On the security and privacy of hyperledger fabric: Challenges and open issues. In *2020 IEEE World Congress on Services (SERVICES)* (pp. 197-204). IEEE. https//doi.org/10.1109/SERVICES48979.2020.00049

Butt, G. Q., Sayed, T. A., Riaz, R., Rizvi, S. S., & Paul, A. (2022). Secure healthcare record sharing mechanism with blockchain. *Applied Sciences*, *12*(5), 2307. https://doi.org/10.3390/app12052307

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (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

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., ... & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, *22*(8), e13598. https://preprints.jmir.org/preprint/13598

Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y. C. (2019, August). MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 594-601). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00085

Hyperledger Fabric. (2022). A Blockchain Platform for the Enterprise. (2022). https://hyperledger-fabric.readthedocs.io/en/release-2.2/

Hyperledger Foundation. (2020). Hyperledger Fabric-Components Overview. https://wiki.hyperledger.org/display/HIRC/hyperledger+fabric+-+components+overview

Kaur, J., Rani, R., & Kalra, N. (2021). Blockchain-based framework for secured storage, sharing and querying of electronic healthcare records. *Concurrency and Computation: Practice and Experience*, *33*(20), e6369. https://doi.org/10.1002/cpe.6369

Leng, Z., Tan, Z., & Wang, K. (2021). Application of hyperledger in the hospital information systems: A survey. *IEEE Access*, *9*, 128965-128987. https://doi.org/10.1007/s00521-020-05519-w10.1109/ACCESS.2021.3112608

Mahore, V., Aggarwal, P. Andola, N., & Venkatesan, S. (2019, December). Secure and privacy focused electronic health record management system using permissioned blockchain. In *2019 IEEE Conference on Information and Communication Technology* (pp. 1-6). IEEE. https://doi.org/10.1109/CICT48419.2019.9066204

Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger healthChain: patient-centric IPFS-based storage of health records. *Electronics*, *10*(23), 3003. https://doi.org/10.3390/electronics10233003

MSPIIM. (2017). MSP Implementation with Identity Mixer. https://hyperledger-fabric.readthedocs.io/en/release-1.2/idemix.html

Private Data. (2020). Hyperledger-Fabric. Readerdoms'. https://hyperledger-fabric.readthedocs.io/en/release-2.0/private-data/private-data.html

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, *20*(22), 6587. https://doi.org/10.3390/s20226587

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability and availability. *Healthcare Informatics Research*, *26*(1), 3-12. https://doi.org/10.4258/hir.2020.26.1.3

Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger fabric blockchain: Secure and efficient solution for electronic health records. *Comput. Mater. Contin*, *68*(2), 2377-2397. https://doi.org/10.32604/cmc.2021.015354

Using Private Data in Fabric. (2022). https://hyperledger-fabric.readthedocs.io/en/latest/private_data_tutorial.html/

Wang, S., Yang, M., Zhang, Y., Luo, Y., Ge, T., Fu, X., & Zhao, W. (2021, July). On private data collection of hyperledger fabric. In *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)* (pp. 819-829). IEEE. https://doi.org/10.1109/ICDCS51616.2021.00083

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges and future recommendations. *Neural Computing and Applications*, 1-16. https://doi.rg/10.1007/s00521-020-05519-w