A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management

Amit Kumar Jakhar
Jaypee University of Information Technology
Mrityunjay Singh (mrityunjay.cse045@gmail.com)
Indian Institute of Information Technology Una
Rohit Sharma
Jaypee University of Information Technology
Aman Sharma
Jaypee University of Information Technology

Research Article

Keywords: Blockchain, Electronic Health Records, Security, Privacy, Healthcare, Hyperledger Fabric, Hyperledger Composer, Access control

Posted Date: September 21st, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2048551/v1

Noname manuscript No.
(will be inserted by the editor)

A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management

Amit Kumar Jakhar · Mrityunjay Singh* · Rohit Sharma · Aman Sharma

Received: / Accepted:

Abstract Healthcare data is crucial and sensitive because it contains information about a patient's medical history, treatments along with actions. This information is frequently shared among different stakeholders of the system. As patients' information is vital, therefore, it must be kept accurate, up to date, secret, and available only to those who are authorized to access the specified information. Centralized systems are commonly used to maintain healthcare records which increases the security risk. Therefore, this study focuses on protecting the privacy and security of sensitive healthcare documents while sharing them across multiple healthcare participants. In this work, we proposed a privacy-preserving access control framework based on blockchain technology that uses consensus-driven decentralized data management on top of peer-to-peer distributed computing platforms to ensure the privacy, security, accessibility, and integrity of healthcare data. Blockchain technology helps to protect transactions from manipulation due to its irreversibility and immutability features. Furthermore, we comprehensively investigate the blockchain-enabled security requirements by including patients, doctors, chemists, and pathology labs as entities of the system that can share information through a proper channel. We have evaluated our proposed framework using Hyperledger Fabric and found that the developed framework reveals promising benefits in security, regulation compliance, reliability, flexibility, and accuracy.

Keywords Blockchain · Electronic Health Records · Security · Privacy · Healthcare · Hyperledger Fabric · Hyperledger Composer · Access control

Amit Kumar Jakhar · Rohit Sharma · Aman Sharma
Jaypee University of Information Technology, Waknaghat Solan, India 173234
E-mail: amitjakhar69@gmail.com . aman.sharma@juitsolan.in . rohittsharmaa12@gmail.com

Mrityunjay Singh* (Corresponding author)
Indian Institute of Information Technology Una, Saloh, Himachal Pradesh 177209 India
Tel.: +91-9045372346
E-mail: mrityunjay.cse045@gmail.com

1 Introduction

Over the decade, the healthcare sector such as medical institutions and insurance organizations are handling patients' records very carefully. These records are known as Electronic Health Records (EHRs) that considered to be an extremely critical asset from privacy and security aspects. EHRs contain very sensitive and personal data related to a person that should be kept secret and prevented from unauthorized access during the system design. An EHR includes detailed medical information about a patient such as a name, address, unique identity (UID), medical history, medical history of family members, medication procedures, prescribed medications, and other related data. EHRs are shared among various system stakeholders very conveniently to make effective and prompt patient care decisions along with that the shared information should be accurate, precise, trustworthy, and comprehensive among the intended recipients. However, the security and privacy of EHRs raise several challenges because cyber-attackers have performed several attacks on medical institutions to steal the health records of patients in the past few decades [7]. The personal and medical records are at high risk due to the cost of EHRs in the black market is approx $50 which is very much higher as compared to the cost of credit card details, i.e., $0.25 [3]. Therefore, governments introduced two regulation acts,

Health Insurance Portability and Accountability Act (HIPAA) 1996 [2] and General Data Protection Regulation (GDPR) Act 2018 [51], to cover the numerous guidelines on how to store, process, and secure the medical data in order to prevent scams and theft in the healthcare domain. However, the medical staff has disclosed the EHRs only for their financial gains although this ratio has dropped significantly because of the new litigations formed by governments all over the globe.

Various hackers still obtain the EHRs very conveniently even after formulating the strict guidelines for the healthcare sector by the government. For instance, *the hacker successfully obtained significant information about staff at Magnolia Health Corporation (MHC) using a spoofed email from the CEO. On the other hand, the National Health Service (NHS) was attacked and encrypted the NHS files in 2017; as a result, all 6900 appointments got canceled [35, 50] and there are many such examples reported in the literature for these kinds of thefts.* Moreover, the traditional medical records management systems do not maintain the transaction logs that help to trace the access details for patients' EHRs in the past. The targeting attacks not only affect the privacy and security of the patient but also spoil the reputation of the organization including the nation. The severity of these attacks is that they are common and easy to perform. The main reason behind these issues is data insecurity and the lack of technological understanding within the medical sector that causes some common attacks including ransomware and phishing for retrieving personal data [31]. As per GDPR guidelines, the patient records must be handled by data controllers and should be visible only to the respective departments after generating consent through a proper channel. The entire system should work on the access control mechanisms due to sensitive and confidential information stored in the system; it strictly prevents unauthorized access to EHRs.

Consequently, there is a need to develop a robust and reliable way that helps to achieve data security, confidentiality, availability, and integrity. That also alleviates the aforementioned issues and ensures secure access handling of EHRs over the internet. There are various popular ways adopted by healthcare institutions like cloud-based technology, encryption techniques, and many more to maintain the records properly and efficiently. Nowadays, blockchain is the most disruptive technology and has great potential with acclaim in the field of security. It is based on peer-to-peer distributed and decentralized architecture that gives importance to value and trust instead of an exchange of information [4, 5]. The amalgamation of blockchain complies with the GDPR's objective to keep data secure with access control to all users. The cryptographic hashes and distributed consensus mechanisms with smart contracts are used to achieve data integrity and consistency [21]. Several researchers believe that blockchain is a disruptive technology and can be linked to the healthcare industry to provide desired security for healthcare data by introducing various architechtures/frameworks [6,20,43,47,54,55]. As a result, this work focuses on the designing of a robust framework using blockchain technology that permits only authorized users, e.g., doctors, path-labs, chemists, etc., to access the critical information of a patient after acquiring permission. We have examined the proposed framework in various possible scenarios to validate its acceptability for healthcare applications. The main contributions of this work are summarized as follows:

- The compilation of the significant requirements of the healthcare application and assess the identified requirements and criteria.
- Developing healthcare data management framework using HyperLedger Fabric for the enforcement of access control mechanisms among various participants of the system like patients, doctors, path labs, and chemists.
- Establishment of specific testing criteria to evaluate the proposed framework's suitability for the healthcare application and mention the need for further development.

The organization of the paper is as follows: Section 2 presents the work related to our study and Section 3 describes the background of Blockchain technology. The ideal requirements for the healthcare application are elaborated in Section 4. Section 5 describes the proposed framework with desired use-case scenarios for the evaluation. Section 6 presents the results and discussion. Finally, we conclude our work in Section 7 with the possible extensions.

2 Related Work

This section presents the existing studies related to our proposed work to identify the significance of blockchain technology in healthcare applications and find out the possible research gaps that need to be addressed. In the literature, numerous frameworks have been proposed to counter the security issues to protect the EHRs from unauthorized access; these frameworks are classified as Cloud-based [1,36] and Blockchain-based [12,42] frameworks/architectures/solutions. Initially, cloud-based solutions have been proposed to manage patient records in the healthcare industry to minimize cost and improve efficiency and security [36]. These solutions are

Table 1 Description of 7-layer guidelines

Guideline name	Descriptions
The workflow must be as per formed regulations	Patients' information must be secured against a confidentiality breach.
Should supports Turing Completeness Operation	The healthcare application based on blockchain should support Turing Completeness Operations by keeping programming feature to solve any computation problem.
Blockchain platform should support user identification and authentication	Patients and Professionals should be identified/authenticate in the healthcare application.
Support interpretability	Interpretation of exchanged clinical data should be in some structural format.
Scalability for large populations	The application must be scalable and supports any number of users.
Cost-effectiveness	The blockchain solution must be cost-effective for large number of participants.
Should be patient-centered care model	Patients can control of granting access to their own medical records in the blockchain-based health application.

centralized, ubiquitous, and less expensive because they reduced the overall cost by almost 80%, and improve the accessibility of data from anywhere at any instant of time [1, 36, 36]. Koufi et al. proposed a cloud-based healthcare system that provides the EHRs accessibility to the doctors to improve the treatment process [30].

On the other hand, blockchain-based solutions offer the most effective solutions to provide privacy and security for EHRs. The popular existing healthcare applications are BitHealth and MedRec [12, 48]. The BitHealth application mainly focuses on privacy and uses the concept of Bitcoin for storing and protecting healthcare data. Bitcoin application is used to make payments and to retrieve the medical history of a patient by insurance companies and employs Proof of Work (PoW) consensus algorithms that cause it to consume more time and energy in the network. Moreover, if the size of the network is getting large and a lot of transactions are taking place then the whole network turns out to be highly inefficient. On the other hand, the MedRec application was designed by MIT to store and track EHRs records more efficiently [38]. In this model, patients have some degree of flexibility to restrict the professionals/doctors to access their information at any time. This project was based on Ethereum and uses the Proof of Stake (PoS) consensus algorithm that makes the whole network inefficient in terms of cost and power consumption. Personal data of the patient will be stored off-chain to make the network efficient but through this way users cannot determine whether the records are valid or invalid [32].

In Ref. [33], the authors have identified various key aspects of blockchain technology with numerous applications that are also relevant in healthcare applications. The authors stated that trust, consensus, immutability, or maybe a mix of these are critical research challenges in the blockchain. The feasibility of blockchain is one of the most important aspects of the healthcare applications that needs to be analyzed thoroughly before implementation. Wu et al. [54] have proposed an efficient blockchain platform to manage electronic medical records with different data formats to save network resources. Zhang et al. [55] have developed 7-layers guidelines for the blockchain to evaluate the insight into the healthcare application, however, they did not assign any priority to these guidelines. Table 1 presents a detailed description of the proposed guidelines. A statistical analysis of HyperLedger framework has been proposed to evaluate its effectiveness for developers, but they have not mentioned any specific application [8]. Gencer et al. [19] illustrated different scenarios to evaluate the blockchain application in the virtual environment with mining power, fairness, consensus delay, and time-to-win metrics; This project was known as 'Miniature World'. McSeth et al. [6] proposed a use case for healthcare applications to preserve privacy and access control between patients and doctors only. They have analyzed the security of EHRs for their application on different test-case scenarios in terms of data confidentiality, privacy, and access control metrics.

Gao et al. [18] conducted a survey on the applications of blockchain (e.g., healthcare, IoT (Internet-of-Things), and cloud computing applications) and identified the significant challenges during implementations. Although, they have focused on security issues and performance (i.e., availability and scalability), and concluded that the performance issue is one of the major challenges in blockchain to retrieve medical data, particularly in emergency situations. Bodkhe et al. [9] analyzed smart healthcare through IoT and specified numerous challenges related to transforming centralized to decentralized systems, cost, scale, throughput, and network latency; it required sophisticated circuitry to prevent double-spend attacks. Kassab et al. [29] have conducted a sur-

vey on existing blockchain-based healthcare systems to investigate the desired quality parameters for the application; they found that blockchain can be a supplementary technology but not a replacement of the healthcare system because that can only control a specific set of data. Zile et al. [56] believed that the adoption of blockchain is not a good idea till decentralization is required; otherwise network cost gets increased drastically as Bitcoin is the only successful use-case of public blockchain till now. Jianbo et al. [17] have proposed an automated evaluation of blockchain-based decentralized networks for healthcare applications. The other existing research projects have suggested the importance of blockchain technology in healthcare applications while the evaluation of their proposed schemes is not clear; however, they have tried to address the existing research gaps to manage EHRs in an effective manner [13, 23, 24, 26, 39, 44, 53].

From the literature, we found that most of the existing research has focused on the sharing of EHRs between patients and doctors; however, other entities like laboratories and chemists also play an indispensable role in automated and accurate information sharing for better treatment of a patient. In addition, EHR contains the personal and medical information of a patient, therefore, whole rights and control should be given to them to manage their health records while granting privileges to the intended professionals through proper channels. In this work, we compiled the findings and shortcomings of existing works to determine how to conduct the assessment process and fill out the research gaps in the healthcare domain using blockchain technology. Therefore, we proposed a blockchain-based healthcare framework to eliminate existing issues in an efficient way with proper access control mechanisms. The proposed framework grants permission to patients to share their EHRs in a more secure way by sharing their proper consent with respective doctors, path labs, chemists, etc. Patients can also revoke their consent as per their requirement and can stop the sharing of their EHRs with any other entities of the blockchain network. Finally, we have evaluated our proposed work with existing frameworks based on confidentiality, security, integrity, patient–user preference, and access control metrics; we found that our framework provides a better way to store and share EHRs among different entities of the system.

3 Basic Terminologies

This section presents an overview of blockchain technology and existing tools for the implementation of blockchain-based applications. A blockchain is a shared, decentralized, and immutable ledger that records transactions as blocks. The basic tools and techniques required to build a blockchain-based framework are HyperLedger Composer and HyperLedger Fabric.

3.1 Blockchain Technology

The blockchain is decentralized (i.e., no centralized authority to control) and distributed architecture, known as a peer-to-peer platform, allocates tasks to a host of nodes and works in a group to form decisions on the behalf of the network. Each node is allowed to perform functions that are known as transactions and all the validated transactions are recorded in a distributed and immutable ledger as a block. Blockchain achieved popularity mainly from the cryptocurrency, i.e., BITCOIN, in the world of finance [37]. In the blockchain, a number of operations are being processed at every moment; each user is carrying his/her distributed ledger to identify frauds and verify the respective transactions at any point of time. The blockchain network keeps adding new validated blocks of transactions in the distributed ledger. All participants or nodes have equal opportunities for accounting ledger in the network and it assures a complete consensus within all nodes in the analogous blockchain [40, 41]. Blockchain technology forms a trust layer without having any third party for various business transactions [20]. In the current scenario, blockchain applications have extended and become the backbone for different applications. In the healthcare domain, blockchain technology plays a vital role to build podiums for storing, evaluating, and maintaining confidential healthcare information with a full-proof system.

A blockchain network can be classified as public (Permissionless), private (Permissioned), hybrid, and federated/consortium blockchain; the suitable blockchain network can be opted on the basis of the requirements of the use case. The private blockchain network is centralized and managed by an individual/organization, while, the public blockchain network is completely decentralized and managed by multiple users/organizations. The hybrid blockchain network combines the features of both public and private blockchain networks, and various users are allowed to control their data and only the subset of the data is available in the public domain or for a specific group of people.

- *Permissioned or Private blockchain network*: In this network, a person, an organization, or a group of organizations/people are permitted to communicate information and keep record of transactions efficiently.

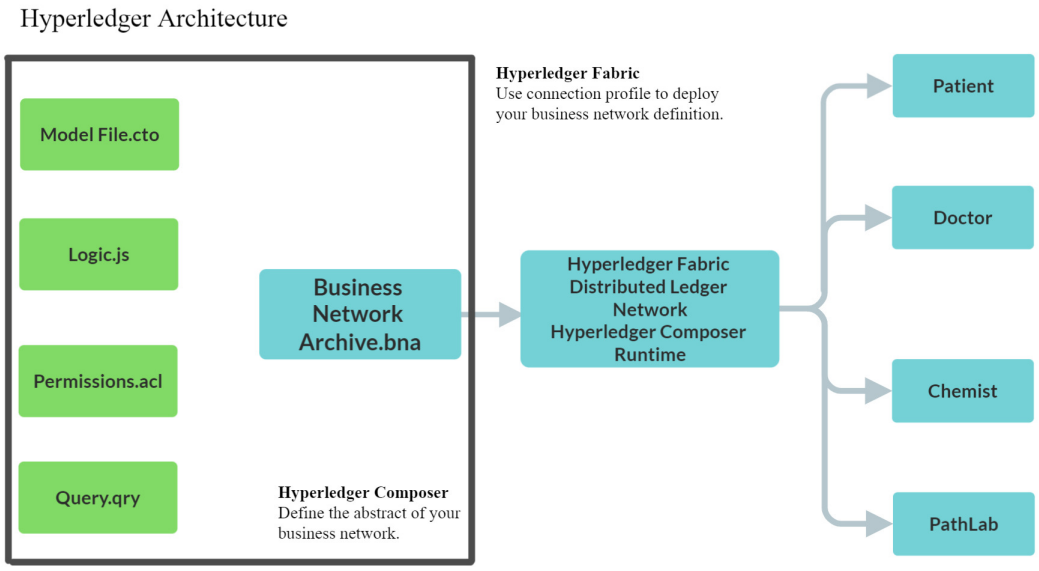

Fig. 1 Architecture of Hyperledger

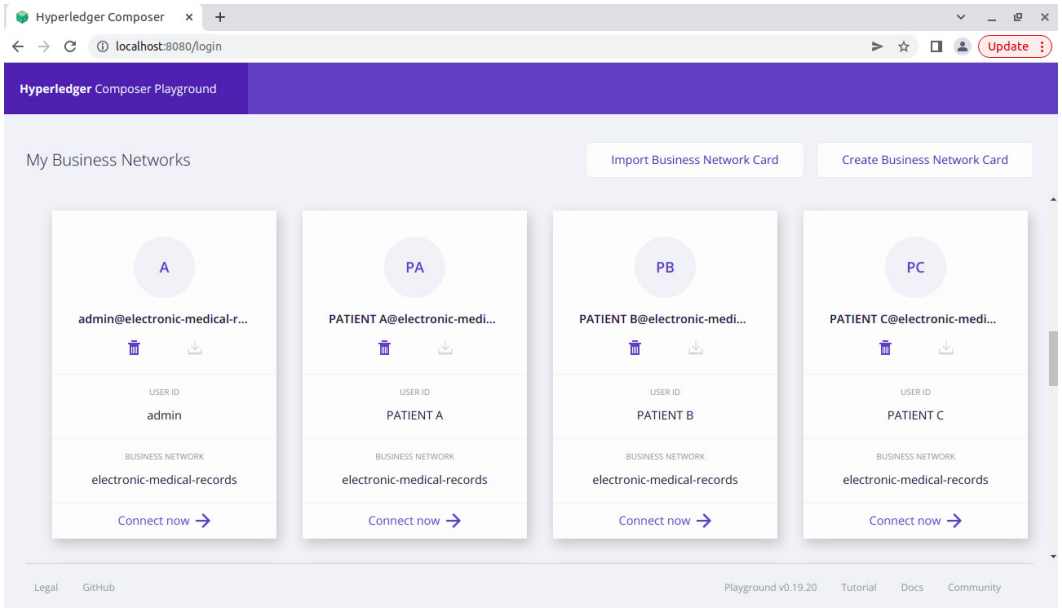

Fig. 2 Screenshot of Composer Playground

This network add-on a privileged layer to determine who can join the network with a unique identity and it is known to all other users of the network [28]. Exposing the identity of each user is actually reducing the chances of fraud. In this kind of blockchain network, usually Byzantine Fault Tolerance (BFT) is used to form a consensus among participants [11].

– *Permissionless or public blockchain network*: In this network, identities of all users are pseudonymous or unknown and any node can add a new block to the distributed ledger. Bitcoin and Ethereum are permissionless network; Bitcoin allows any node to take part for verification of transactions with the mining algorithms and Proof of Work (PoW) consensus protocol is used to counter the issue of anonymity [10], while, Ethereum allows a user to make and execute the code and Proof of Stake (PoS) consensus protocol is used to counter the issue of anonymity [34].

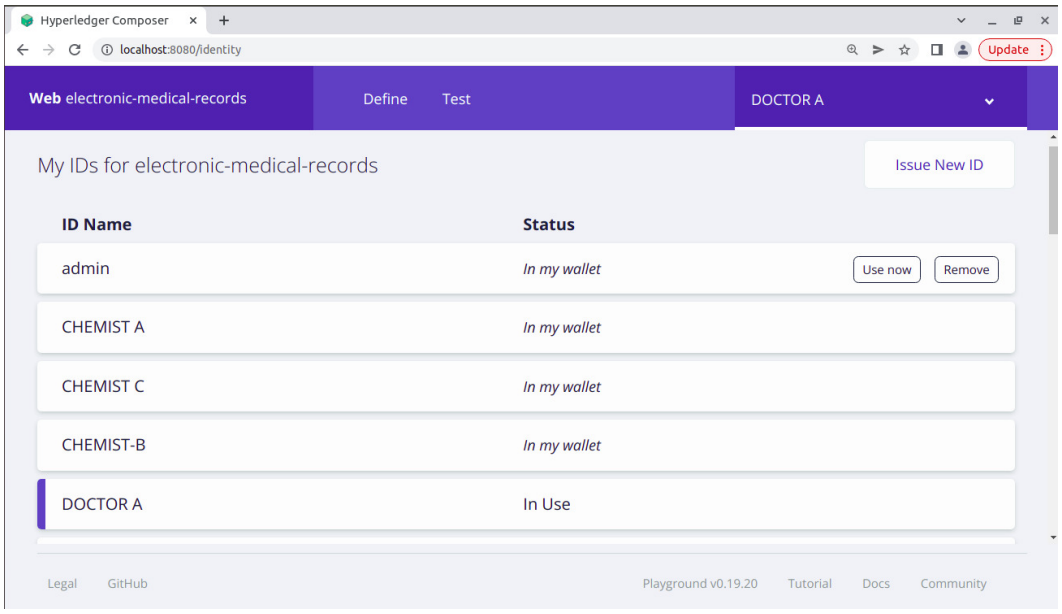

Fig. 3 Screenshot of Playground's Users

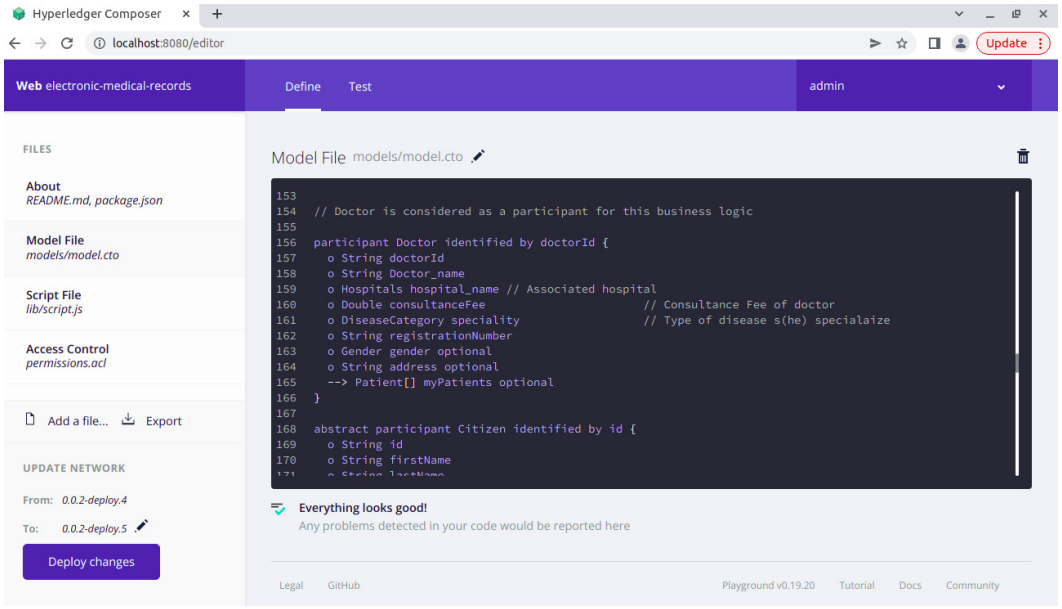

Fig. 4 Screenshots of Playground's define page

3.2 Tools for Implementation

This section describes the basic tools and techniques used to build our proposed healthcare framework. HyperLedger Composer and HyperLedger Fabric play a vital role in the implementation of a blockchain-based framework. HyperLedger Fabric is a framework that does not allow any modification while HyperLedger Composer provides a collection of tools to build a blockchain application. So, the details of the HyperLedger Fabric and HyperLedger Composer are provided in the subsequent section.

3.2.1 Hyperledger Fabric

The Permissioned blockchain is implemented with the Hyperledger Fabric and it is also an open-source blockchain project hosted by the Linux Foundation [25, 49]. It is currently one of the most popular blockchain networks that permit concerned stakeholders to join the network for altering the ledger or initiating transactions. The Hyperledger Fabric Network (HFN) can be designed with different nodes related to various organizations. Every node has its own unique identity in the Hyperledger Fabric network and it is provided by Member-

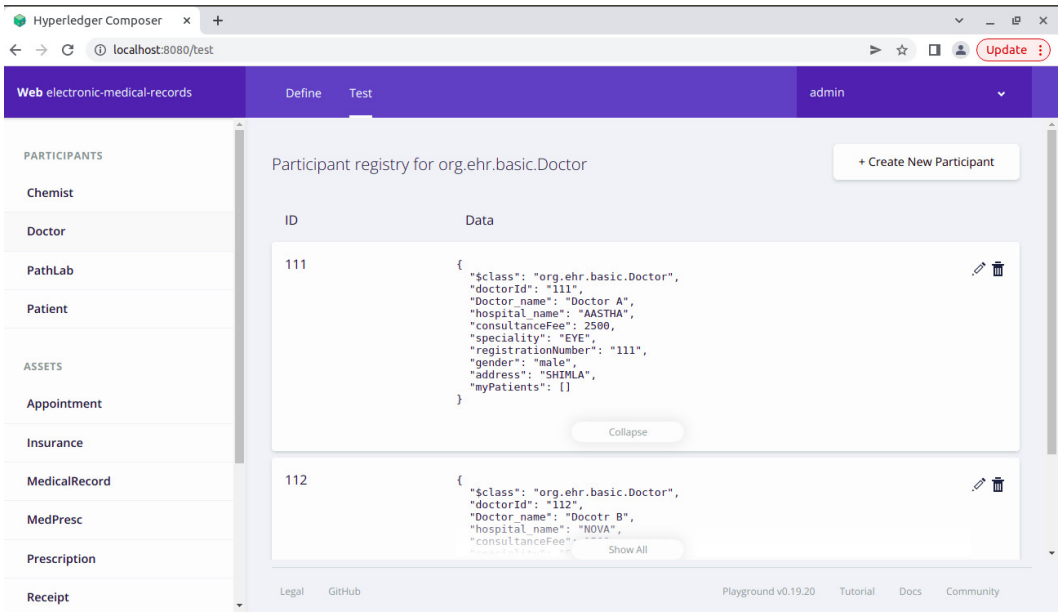

Fig. 5 Screenshots of Playground's test page

ship Service Provider (MSP) [16, 22, 27]. The role of the MSP is to generate the enrolment and transaction certificates for the clients and utilizes a specific consensus protocol that requires much lighter computational power than the PoW. The Fabric has the capability to form trusted sub-networks, called channels, and has a smart contract functionality that enables users to execute complex transactions as per their permissions.

3.2.2 Hyperledger Composer

Hyperledger Composer is a free and open-source framework for building blockchain applications which facilitates business network modeling, application implementation, and interaction with existing systems by supporting the Hyperledger Fabric infrastructure and runtime. The business network definition (BND), saved as an archive file with extension .bna, is to be deployed as it is ready. BND constitutes the four main files namely *model file*, *script file*, *access control file*, and *query file* as shown in Fig. 1.

- The *model file* is in-charge of laying out the network's structure and consists of three basic components: *assets*, *participants*, and *transactions*. *Assets* are the network's variables, *participants* are the network's nodes, and *transactions* are network functions that allow interaction between the assets and participants; Transactions are also used to keep the network up to date (e.g., transferring an asset).
- The *script file* consists of transaction logics that define numerous transaction functions; the script file is written in JavaScript. It also categorized the participants as per access rights for further processing of the transactions in the network to transfer assets among participants.
- In the corporate network, the *access control file* specifies the scope and the role of the user that determines their participation in creating, reading, updating, or deleting network items.
- The *query file* specifies the structure and function of network inquiries by maintaining a ledger of all prior transactions in the system.

The composer's playground user interface tool is used for configuring, testing, and deploying business networks. The composer's playground allows developers to simulate business networks using assets (i.e., *blockchain commodities* or *services*), participants (i.e., *blockchain members*), and transactions (i.e., *way to interact with participants through assets*). Fig. 2 and Fig. 3 exhibit the screenshot of the proposed framework playground that is used to simulate the application scenarios created in this study. The define page is used to construct the desired scenarios within the system of the system, while the test page is used to test the system. The screenshots of the define page and test page are shown in Fig. 4 and Fig. 5 respectively.

4 Requirements for healthcare applications

This section presents the ideal requirement of a healthcare application that needs to be supported by an effective system. The system should support proper security

features, regulations formed by governments to maintain EHRs, and validated before its deployment on the basis of rigorous testing approaches.

4.1 Security Requirements

The data must remain confidential, accurate, and accessible only to authorized users. Although it becomes difficult when multiple entities are requested to read and modify databases at any time. Therefore, it is an important aspect to ensure security by adhering to the proper channel of sharing information. An efficient healthcare application should support the following necessary features [7, 31]:

- *Confidentiality:* It can be achieved by ensuring that the application is on a permissioned blockchain and has restricted access for users to preserve data privacy. The participants have different roles and privileges to interact in the network. Furthermore, encryption should be used to make sure that data during transmission between the user and the blockchain is secure. Confidentiality is also essential in the blockchain because it directly counter phishing attacks and data breaches which is the most common attack on the healthcare industry.
- *Authentication:* The user authentication will be done on the basis of a unique identifier that is assigned to each user of the EHR system. Each user can be recognized with their identity while accessing any information within the network. In addition, different roles and privileges are assigned to the participants as per the system design to maintain data privacy.
- *Scalability:* An efficient EHR system should be scaled depending on the number of blockchain users so that the whole network would be capable and robust to work seamlessly.
- *Privacy and access control:* It can be achieved by the identification of each participant in the network. Only individuals with proper authorization to access some specific information, for instance, a doctor can access and edit a patient's record with the patient's consent only. Furthermore, every interaction between a patient and a physician will be recorded and later can be tracked from log files.
- *Data sharing:* A patient has the freedom to seek better treatment at multiple or specialized hospitals and clinics. Therefore, the healthcare system should facilitate the establishment of safe mechanisms for data sharing among all the intended recipients.
- *Patient control:* Patients can have access to their own records and combine their records with tagged notes along with some other relevant information available in their account, especially with chronic diseases. The system should also provide complete control over healthcare data and allow the other users to access the records excluding the emergency situation.
- *Integration:* A new system must be designed with the amalgamation of the above-said functionalities. In fact, blockchain-based EHR management systems are not supposed to replace existing systems only; rather, it is meant to integrate and deliver desired functionalities in a more efficient way.

4.2 GDPR Regulation

The government rules out the following privacy and security regulations in the world. GDPR defines a set of practical regulations on a variety of topics, including healthcare worker protection, standards practices, and health-record transfer methodologies. The GDPR recites data subjects to the following rights [51]:

- *Transparency:* Personal information should be treated legally and transparently.
- *Right to be forgotten:* Data subjects shall have the right to demand the erasure of personal data concerning them.
- *Right to rectification:* Personal information should be accurate and up-to-date; patients have rights to rectify the incorrect information or modify their personal data.
- *Right of access:* Personal data should be accessed securely and it should be hidden from unauthorized access; it also handles any damage or destruction of personal information.
- *Right to restrict access:* Patient have right to restrict accessing/processing of his/her personal data (e.g., *in the case of inaccuracy*).
- *Right to object:* A person has the right to object to an institution processing/using his/her personal data at any time.
- *Informed Consent:* Personal data should be obtained for specific, precise, and lawful reasons with informed permission. A patient should be able to comprehend who has access to their information with appropriate reason.
- *Data portability:* The individual has right to acquire and reuse their data across multiple services for their own interests (*i.e., data should have a common format*).

The *Right to be Forgotten* is one of the rights that the healthcare industry struggles while developing a blockchain-based application.

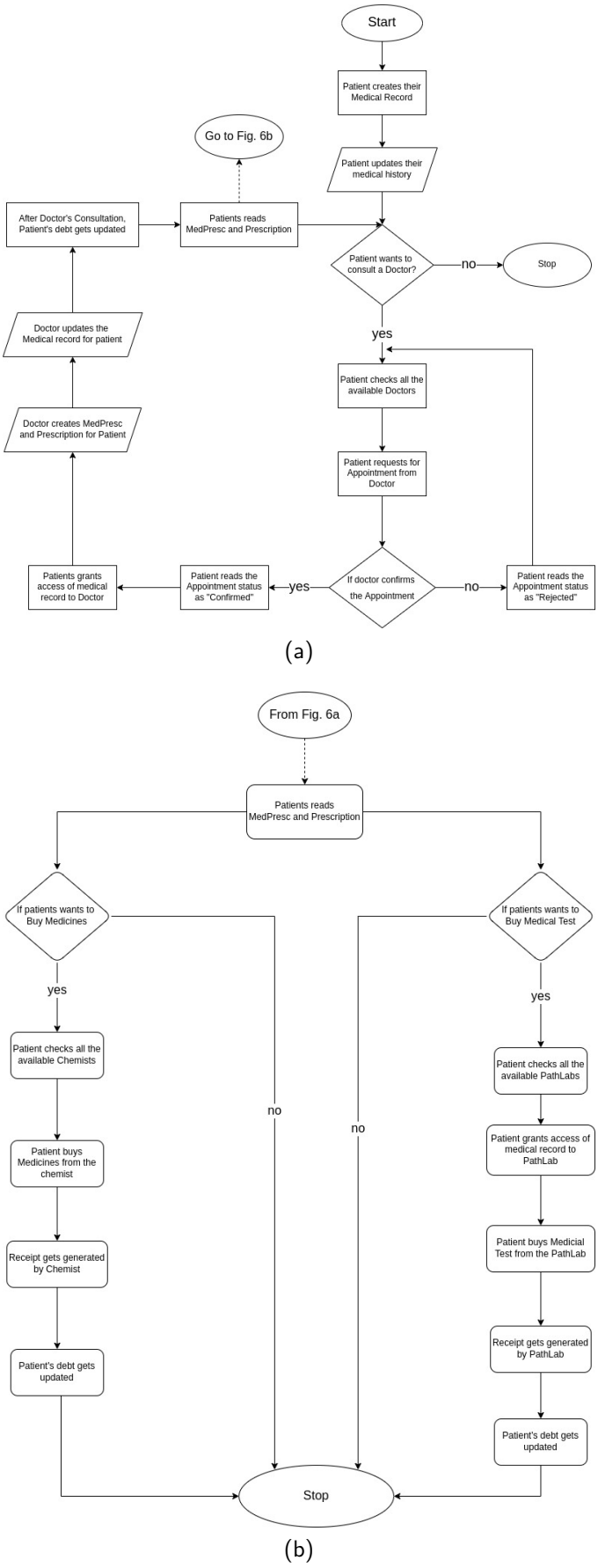

Fig. 6 Flow Chart of the proposed framework for healthcare application

Table 2 Descriptions of different tests used in proposed framework

Test ID	Test Description
0	Only Patients can Create Medical Records
1	Participants cannot view or delete a Medical Record that does not belong to them.
2	Doctor/PathLab can only update Medical Records they have been given access to.
3	Only the Medical Record owner can grant/revoke access rights from their Medical Record.
4	Only the owner of the Medical Record can delete their Medical Record.
5	Only Patients can create Appointments with Doctors.
6	Only Doctor can confirm an Appointment.
7	Doctor/PathLab can view only the assigned patients.
8	Only Doctors can create Prescription and MedPresc.
9	Only Doctor can provide consultation to the patient.
10	Only patients can buy medicines from chemists.
11	Only patients can buy medical tests from PathLab.
12	Whenever patients buy medicines or medical tests, the Patient's debt gets updated and a Receipt gets generated.

4.3 Testing Approaches

We have applied various tests to evaluate the critical components of our blockchain network ranging from security to fault tolerance. Hyperledger Composer helps to build a blockchain application and provides three types of tests: interactive tests, automated unit tests, and automated system tests. The different tests are designed based on the application requirements; each test has its own description and objectives that define its purpose and methodology with an expected result. The success or failure of a test case can be decided on the basis of the similarity between expected and actual results. HyperLedger Composer and HyperLedger Fabric are used to run all of the tests. Interactive tests are also employed exclusively to focus on the blockchain's subtleties and details; these tests are carried out by an individual, whereas automated tests are carried out by pre-written scripts. Automated tests are faster and more accurate, but manual/interactive testing is more appropriate for the project and more specific to the application. Human intuition is required to analyze certain features such as participant access control and many more as a part of the system. Despite the longer processing time, accurate and timely findings can be generated and it is useful to evaluate the quality of the system in the current application. Furthermore, to make the blockchain network versatile one needs several scripts but it would be a time-consuming process. In this work, we use the interactive testing strategy for validation, verification, permissions, and evaluating the performance of the blockchain network. Table 2 exhibits the description of various tests used to assess the access control and efficiency of the proposed framework.

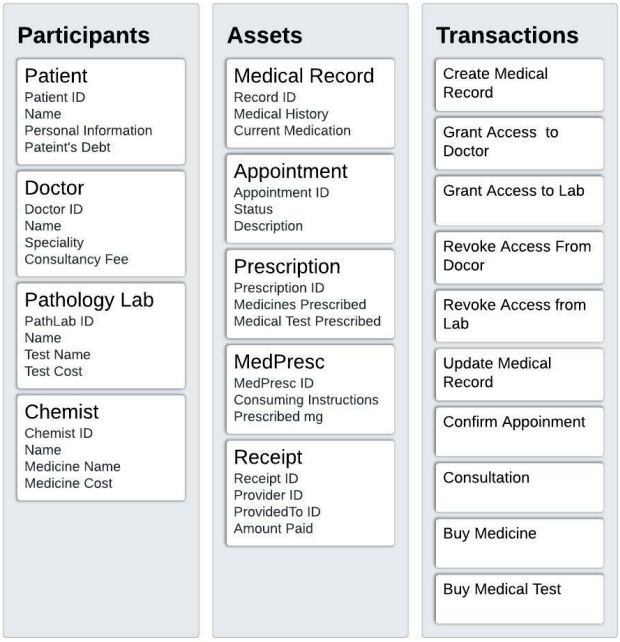

Fig. 7 Participants, Assets, and Transactions in Blockchain Network

5 Proposed Framework

This section describes the proposed framework for secure healthcare data management. Fig. 6 exhibits the flowchart of the proposed framework that depicts the overall working of a healthcare application that includes various participants, i.e., patients, doctors, path labs, and chemists, and their respective transactions. The transactions help to update the assets within the system.

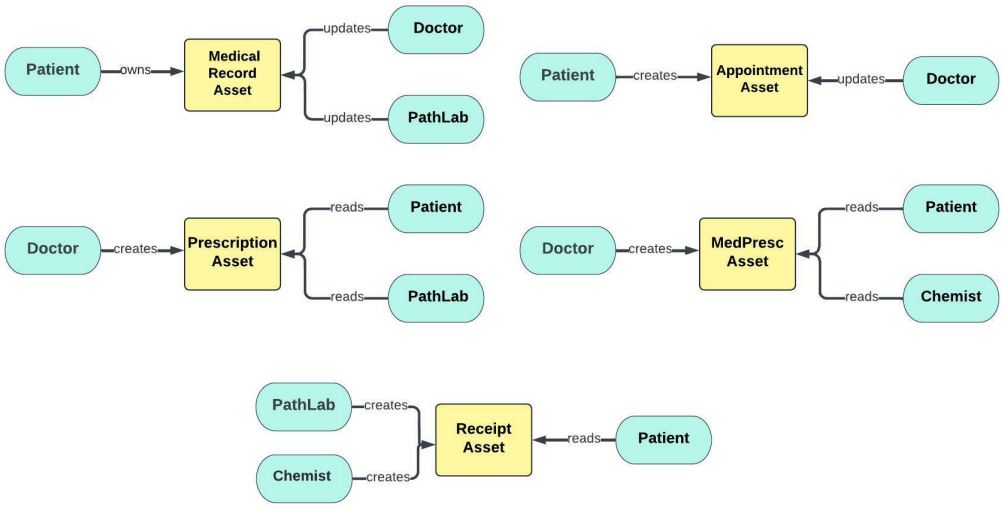

Fig. 8 Interactions among the participants and assets along with desired operations

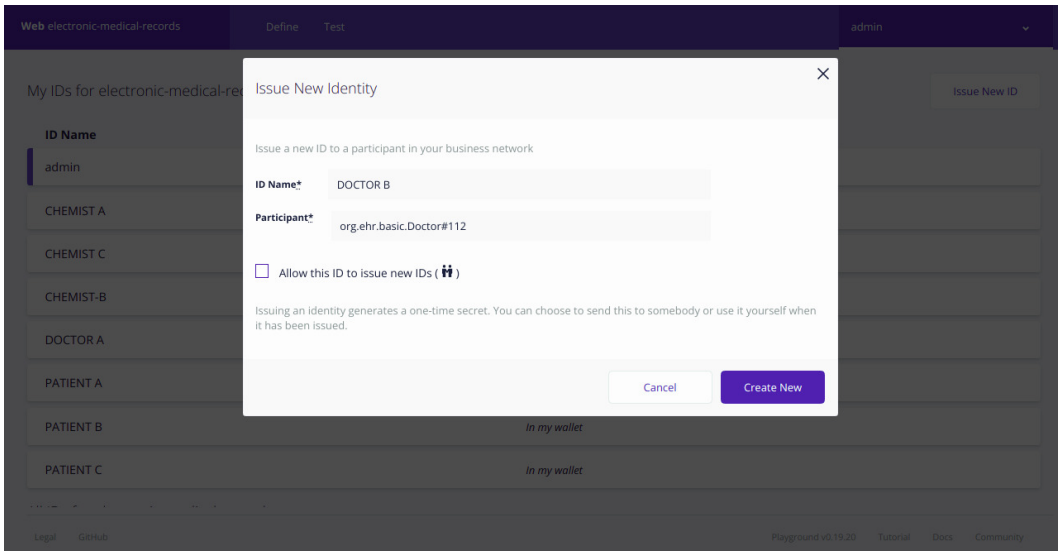

Fig. 9 Screenshots of the UID allotment for a new blockchain user

5.1 System Design and its Implementation

The healthcare system is mainly designed from the business perspective to highly secure medical data using blockchain technology. Fig. 7 exhibits that the proposed framework involved mainly three entities: *Participants*, *Assets*, and *Transactions*; each entity has its own description in the network. The participants are *patients*, *doctors*, *pathology lab*, and *chemists*. The assets are *medical records*, *appointments*, *prescriptions*, *medpresc*, and *receipts*. The following transactions are supported by our proposed framework: *create medical records*, *grant access to doctors*, *grant access to labs*, *revoke access from doctors*, *revoke access from labs*, *update medical records*, *confirm appointments*, *consultations*, *buy medicine*, and *buy medical tests*. Fig. 8 depicts the various assets and participants with interaction in the blockchain network. Relationships inside the system show how different parties have access to a variety of transactions to perform different operations.

5.2 Participants and their respective roles

In our proposed framework, there are four types of participants, i.e., Patients, Doctors, Chemists, and Path-Labs, to access the health records. Each participant has a UID assigned by the system administrator for their unique identification in the blockchain network. Fig. 9 exhibits the screenshot of the UID allotment for a new blockchain user; here, we have registered a doctor as a new user with an ID *name* “Doctor A”

Table 3 Participants' roles and their respective Access Rights

Roles	Access Rights
Admin Member	
	– Has full access to all users and system resources. – Adds Participants to the blockchain network. – Read, Create, Update, and Delete all participants' information.
Doctor	
	– Read, Create, Update, and Delete his/her information. – All Participants can see all doctors. – A Doctor sees only the list of patients they are authorized to modify. – Read, Update Medical records for which they have permission. – Read, Create, Update Appointment. – Read, Create, Update Prescription. – Read, Create, Update MedPresc. – Confirm an Appointment with the patient. – Make Consultations for assigned patients.
Patient	
	– Read, Create, Update, and Delete their own participant Information. – Read, Create and Update Medical records. – Grant Access to Medical Records to Doctor and PathLab. – Revoke Access to Medical records from Doctor and PathLab. – Read all assets, i.e., Appointment, Prescription, MedPresc, Receipt. – Create an Appointment with the Doctor. – Buy Medicine from the Chemist. – Buy a Medical Test from the PathLab.
PathLab	
	– Read, Create, Update, and Delete their own participant Information. – All Participants can see all Labs. – A Lab sees only a list of patients they are authorized to modify. – Read, Update Medical records for which they have permission. – Read Prescription. – Read, Create Receipt.
Chemist	
	– Read, Create, Update, and Delete their own participant information. – All Patients can see all Chemists. – Read MedPresc. – Read, Create Receipt.

and his *UID* assigned by the system administrator is "org.ehr.basic.Doctor#111". Each participant within the system has different roles; the system administrator grants access rights to each participant depending on their role. The access rights are: *create*, *read*, and *modify* the records of the patients. The details of the aforementioned participants' roles and their respective access rights are described in Table 3.

5.3 Operations

To achieve secure healthcare data management, our framework facilitates several mechanisms that restrict unauthorized access of data within the network; it also imposes several policies to regulate the interaction through different transactions among the participants and assets. The screenshot of the supported transactions is shown in Fig. 10. The assets are Medical records, Appointments, Prescriptions, MedPrescs, and Receipts and are maintained using JSON files. The participants interact with assets through a smart contract that also defines a set of operations. These operations help in granting privileges on specified information of the healthcare records. The smart contract supports a set of primary functions to interact with the assets that are as follows:

- *Create Medical Record:* This function allows patients to create their medical records by generating a record ID on the blockchain network. Only Patients are permitted to create Medical Records in the network.

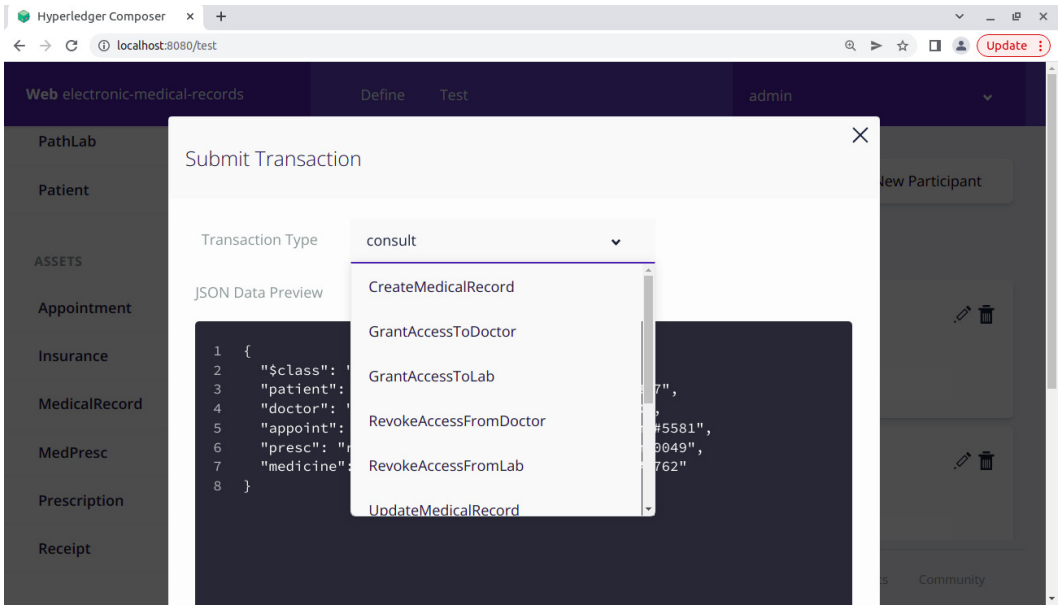

Fig. 10 Screenshots of the list of Transactions supported by the system

Fig. 11 UML use case diagram for Basic Scenario

Fig. 12 UML use case diagram for Permissioned Scenario

– *Grant Access:* This function allows patients to give access rights to their medical records to the other participants, i.e., *Doctors* and *Pathology Labs*. The patient has to provide DoctorID/PathLabID and the RecordID to give access to Medical Records.
– *Update Medical Record:* This function allows Patients and medical practitioners to make updates to an already existing Medical Records.
– *Revoke Access:* This function allows patients to revoke privileges from Doctors and Pathology Labs to access their Medical records. The patient needs to provide DoctorID/PathLabID and RecordID to revoke access rights.
– *Confirm Appointment:* This transaction is used to get an Appointment by enquiring about the available appointment time of the doctor. The doctor can confirm or decline the appointment request of a patient as per his/her schedule. The appointment asset is stored to see the status of the appointment and when the doctor updates the status then it shows either "*confirmed*" or "*declined*".
– *Consultation:* This function is used to record interaction between doctor and patient during an appointment. It allows doctors to prescribe medicines and/or tests to the patient, in return the patient is charged consultancy fees by the doctor. The fee

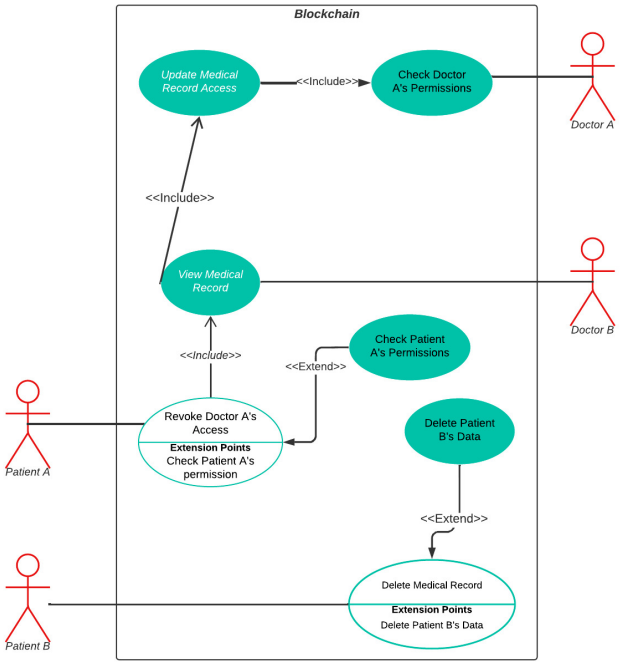

Fig. 13 UML use case diagram for Purging Scenario

is updated in the patient's debt. After successfully implementing this transaction, the status of the appointment changes to "*consulted*".

- *Buying Medicine:* This transaction is used to record the purchase of medicines by patients from the assigned chemists. Whenever this transaction is invoked, the chemist provides the receipt and charges the patient for the given medicines.
- *Buying Medical Test:* This transaction is used to record medical tests conducted by a pathology lab. Whenever this transaction is invoked, the pathology lab provides the receipt, and a fee is charged to the patient.

5.4 Scenario Design

We have considered the four different scenarios to analyse the usefulness of the proposed framework. These scenarios are *Basic Scenario*, *Permissioned Scenario*, *Purging Scenario*, and *Encryption Scenario*.

5.4.1 Basic Scenario

Fig. 11 exhibits an overview of the basic scenario with the help of a UML use case diagram. The participants involved in this scenario are Member A, Patient A, Doctor A, Chemist A, and PathLab A. We have considered this scenario to compare alternative access control policies between a general user and a blockchain user (such as patients, doctors, chemists, and path labs). The authorized users are only able to examine/access data over the blockchain, while everyone else/others are unaware of any participants involved in the transactions. In addition, we use a strong hashing function and shared ledger concept; both of them confirmed this scenario. A copy of the transaction should be given to the participants involved in the transaction as shown in Fig. 11. Member A, Patient A, Doctor A, Chemist A, and PathLab A are added as non-admin members on the blockchain. When Patient A creates a medical record and grants access to PathLab A then it is able to access Patient A's medical record. In a similar way, when Patient A buys medicines from Chemist A, then Patient A and Chemist A will be able to access the receipt. Meanwhile, Member A will not be able to see the medical record or have any clue about anyone on the blockchain because he is not a part of the transaction initiated by Patient A.

5.4.2 Permissioned Scenario

Fig. 12 exhibits an overview of the permissioned scenario with the help of a UML use case diagram. The permissions' range used to *create*, *read*, *update*, and *delete* operations are tested. Patients, Doctors, Chemists, and PathLabs all have distinct permissions based on the situation, as given in Table 3. The purpose of this scenario is to see how Fabric permissions may be used to set up and manage authorizations and access control for various sorts of users in the blockchain network.

5.4.3 Purging Scenario

Fig. 13 exhibits an overview of the purging scenario with the help of a UML use case diagram. According to this scenario, all patients should have total control over their medical records, which includes the option to grant/revoke access to their medical records as well as the power to delete the records from the network. The GDPR stipulates that a user's right to be forgotten must be respected. As shown in Fig. 13, Patient A has granted permission to Doctor A and Doctor B for accessing his/her medical records, but now Patient A revokes access to his/her medical records from Doctor A. In addition, Patient B is allowed to delete his medical record from the blockchain.

5.4.4 Encryption Scenario

We use asymmetric key cryptography in this scenario. The system administrator issues a pair of public and

Algorithm 1 Creating and updating Medical Records

Require: A Doctor D_x with their D_{pkx}
Ensure: Updated medical record

procedure CREATEANDUPDATEMR(D_x, D_{pkx})
  The procedure of creating and updating Medical records
  P_x with P_{prkx} creates MR_x ▷ Patient with his private key creates a medical record
  $P_x \rightarrow MR_x(D_{pkx})$ ▷ Patient Grants access to medical records using Doctor public key
  For each user u, given access to MR_x
  if (Permission == "ALLOWED" and Role = "Doctor" or "PathLab") **then** ▷ Algorithm checks whether Access Control permission is ALLOWED or DENIED to access MR_x
    $D_x \leftarrow$ Decrypt $(D_{prkx}(MR_x))$ ▷ Doctor decrypts Medical Record with his Private key
    $D_x \rightarrow$ Update $MR_x(P_{pkx})$ ▷ Doctor encrypts updated Medical Record with patient public key
    $P_x \leftarrow$ Decrypt$(P_{prkx}(UHR_x)$ ▷ Patient decrypts updated Medical Record with his Private Key
  else if (Permission == "DENY") **then**
    D_x cannot view MR_x
  else
    Nothing is happened
  end if
end procedure

private keys to all the participants of the blockchain network. We use Algorithm 1 to create new medical records or to update/modify the existing medical records of the patients. Table 4 exhibits the notations used in Algorithm 1. Here, we assume that the number of participants in the network is x, where x can be any positive integer. Algorithm 1 describes the steps involved in the creation and updation of a medical record.

Table 4 Descriptions of different tests used in proposed framework

Symbol	Descriptions
P_x	Patient
D_x	Doctor
C_x	Chemist
PL_x	PathLab
MR_x	Medical Record
P_{pkx}	Patient Public Key
P_{prkx}	Patient Private Key
D_{pkx}	Doctor Public Key
D_{prkx}	Doctor Private Key
UHR_x	Updated Health Record

6 Results and Discussion

This section presents an analytical discussion on various executed scenarios in the blockchain environment for healthcare application. We have validated our proposed framework on different scenarios as described in the previous section. We have developed and deployed our prototype on a system Intel Core i5 processor with 8 GB of memory and Ubuntu OS (version 20.04.1LTS). The prerequisites for installing Hyperledger Fabric and Composer are Node 8.9 or higher, npm v5.x, Docker Engine Version 17.03 or higher, Docker-Compose Version 1.8 or higher, git 2.9.x or higher, Python 2.7.x. The components necessary to set up the development environment are composer-cli and other components like composer-rest-server that helps in encryption and decryption tasks. Composer Playground 0.19.20 and VS-Code 1.51.1 are installed in order to create and execute a business network. Finally, Hyperledger Fabric is installed to design our proposed framework for the healthcare application. Now, we discuss the evaluated results on the basis of different performance parameters such as *privacy & security*, *adherence of regulations*, and *accessibility* and then compare our proposed framework with the existing system/frameworks.

6.1 Privacy and Security

The proposed blockchain-based framework assures a patient's privacy by providing the flexibility for specifying granular access control across his/her EHRs. Moreover, it considers access control mechanisms between the users of the network by including smart contracts. There is no way to access medical data by any entity of the blockchain or malicious users without having ac-

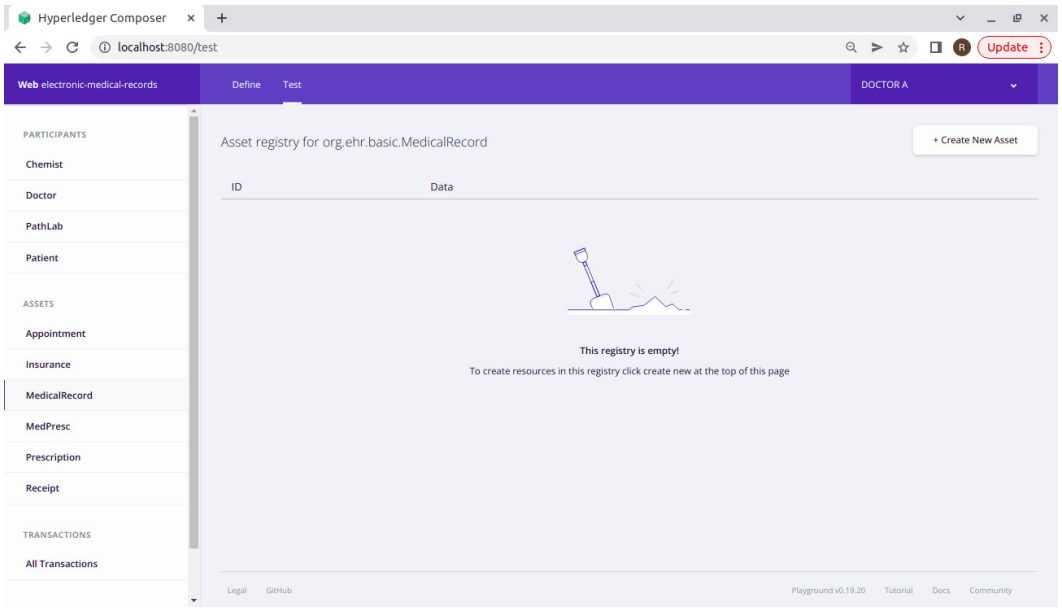

Fig. 14 Screenshot of Doctor A has no access to Medical Records

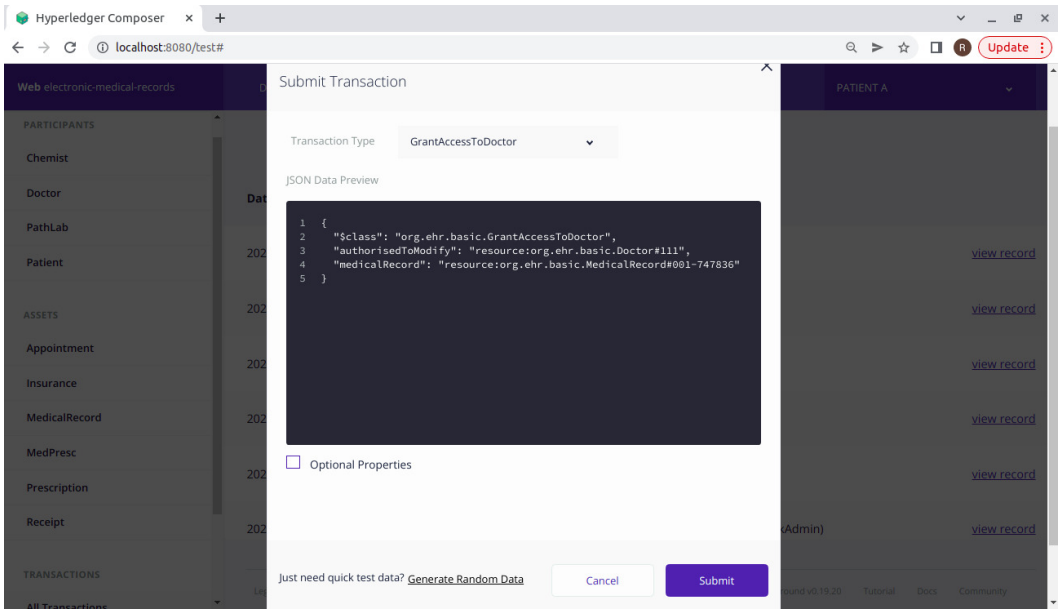

Fig. 15 Screenshot of Patient A grants medical record access to Doctor A

cess privileges. Even, doctors can only see the list of patients, who have been granted access rights to their medical records in the network.

Hyperledger Fabric is constructed according to access policies that dictate access to the stores such as smart contracts, transactions, and ledger through channels. These channels consist of nodes in which the privacy protection and confidentiality of medical records are defined and it protects the medical records against various security breaches like ransomware and similar kinds of breaches. Even though, a blockchain network is decentralized, does not have a single point of failure or central repository for intruders to infiltrate and each node has its own copy of the ledger. The notion of shared ledger assures that data inside the system is true and immutable at any moment. To assess the performance of the proposed framework, we used the Hyperledger Composer playground because the healthcare transaction is recorded as a hash value in the blockchain network. The analysis of the implemented prototype reveals that the proposed framework is tamper-resistant against attacks.

As aforementioned, access control has been employed in the basic scenario to limit resource usage to designated

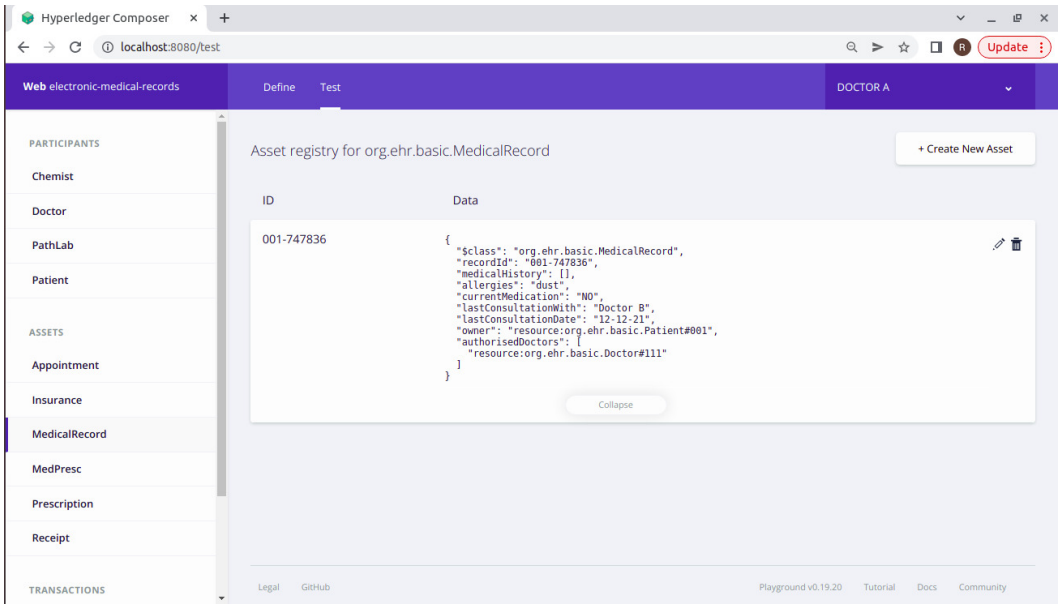

Fig. 16 Screenshot of Doctor A has access to the Medical Record

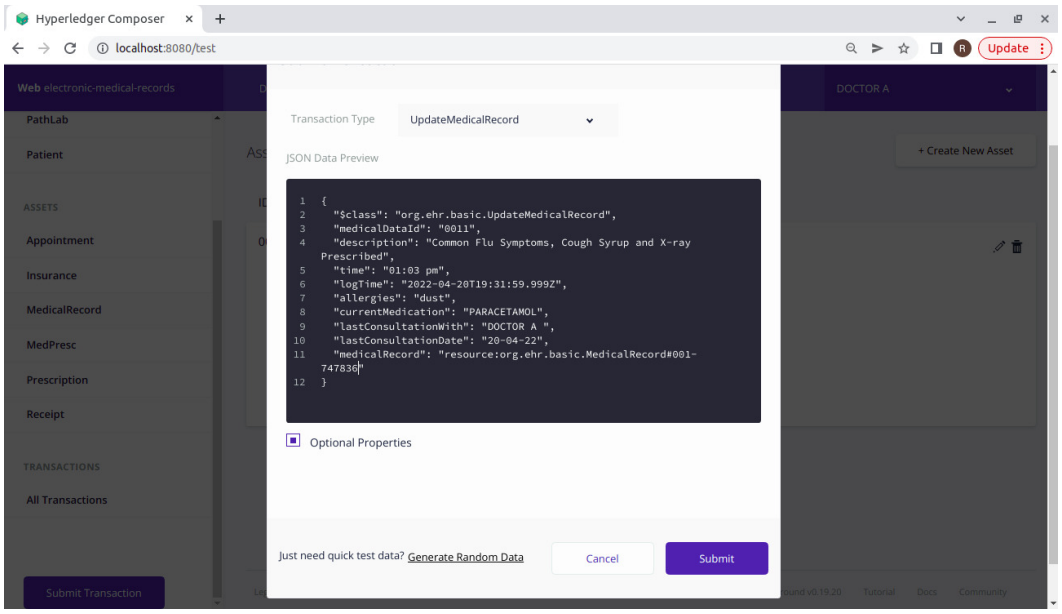

Fig. 17 Screenshot of Doctor A can Update the Medical Record

roles (patients, medical practitioners, and medical institutions). A superficial degree of secrecy is maintained to keep the personal information hidden from blockchain members. Furthermore, the basic scenario demonstrates two fundamental blockchain concepts, i.e., *hashing* and *shared ledger*, to provide an appropriate level of integrity. Each transaction is hashed with *SHA-2* which assure users that the correctness and non-alteration of the transaction. SHA-2 algorithm is more secure that has never been breached; it is nearly hard for attackers to change or fabricate a transaction that matches the hash of a block in the blockchain transaction.

The permissioned scenario builds on the top of the basic scenario by implementing multiple access rules that ensure privacy among various blockchain participants. The access of patients' data in the blockchain has drastically reduced by assigning separate permissions and roles to different users to alleviate the risk of data breaches. Fig. 14 exhibits a snapshot of the proposed system which illustrates that *Doctor A* cannot access any patient's medical records without his consent to access the records. Similarly, Fig. 15 exhibits a snapshot of the proposed system in which *Patient A* has granted access to *Doctor A* to access his/her medical

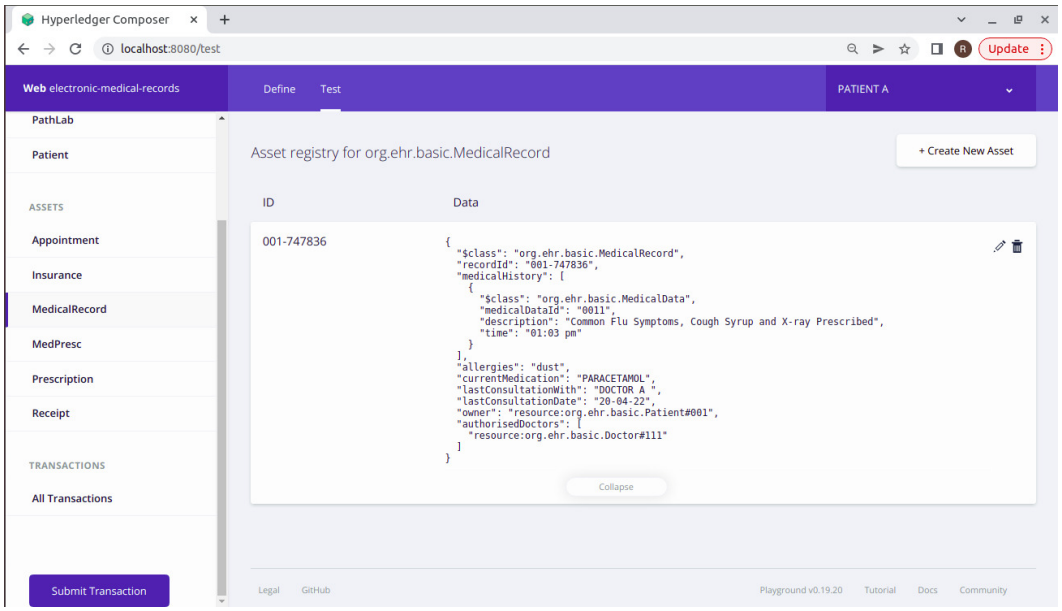

Fig. 18 Screenshot of Patient views Medical Records

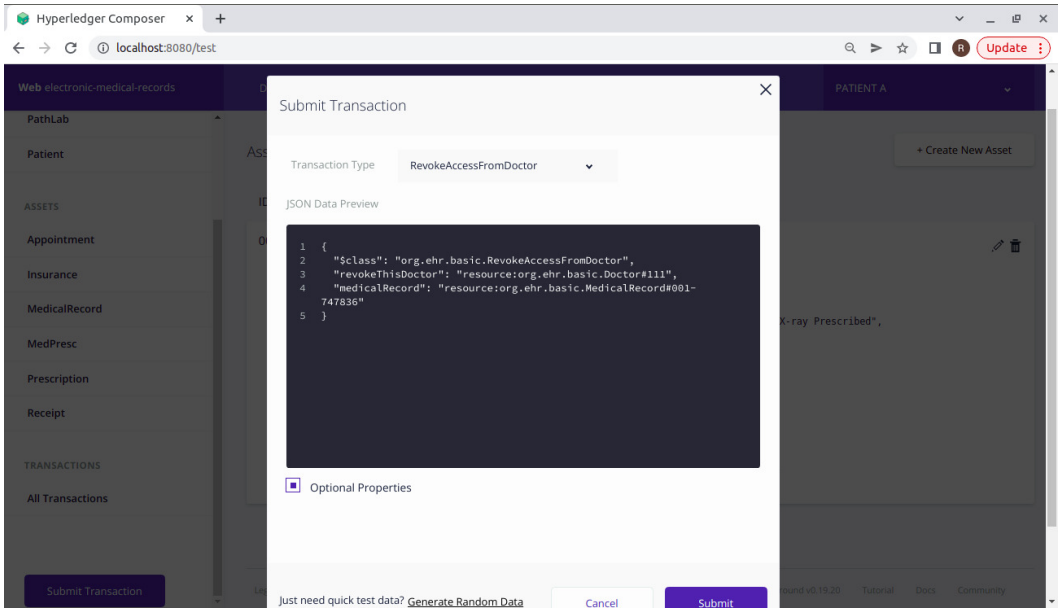

Fig. 19 Screenshot of Patient removing Doctor ID: #111, from their Medical Record

records, and thereafter *Doctor A* can read and update the medical records of *Patient A* as shown in Fig. 16 and Fig. 17 respectively.

In the Encryption Scenario, information is protected from outsiders that ensures complete privacy and security of EHRs. Each block holds a hash of a transaction, which will update in the future whenever an asset gets modified. As a result, tampering with the ledger is a computationally challenging task; it ensures that all the assets are protected from any alteration. In addition, the rules and degrees of access control prohibit participants from gaining access to health records without the patient's permission in the blockchain.

6.2 Adherence to regulations

The foundation of this work also complies with the GDPR standards [31], which has been tested on the basic and permissioned scenarios. Patients can view their medical data as shown in Fig. 18, while patients can restrict or remove data access rights from the Doctor/PathLab as shown in Fig. 19 and a list of the suc-

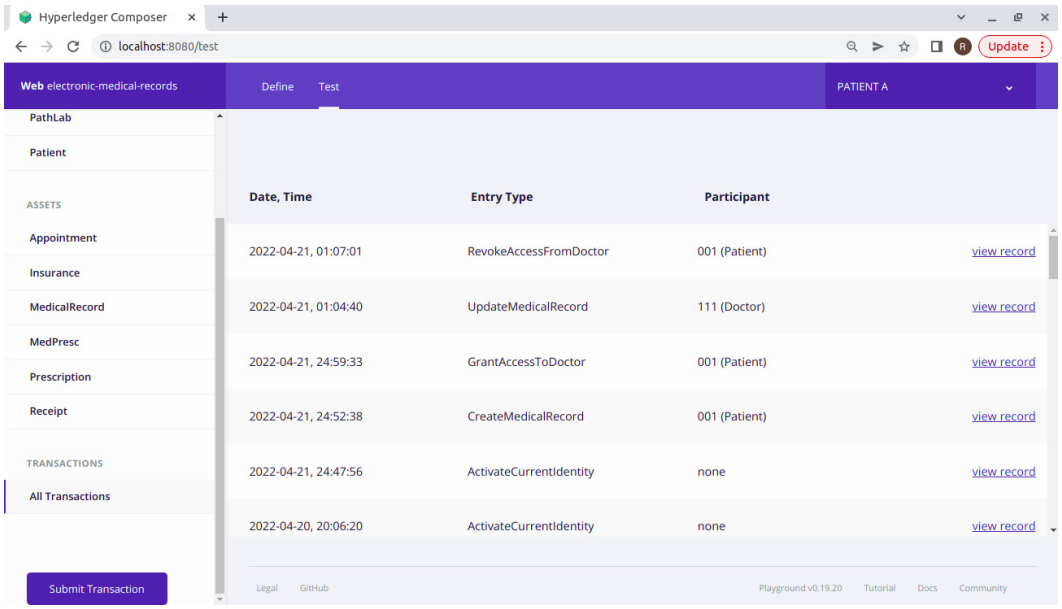

Fig. 20 Screenshot of Successful Transactions List

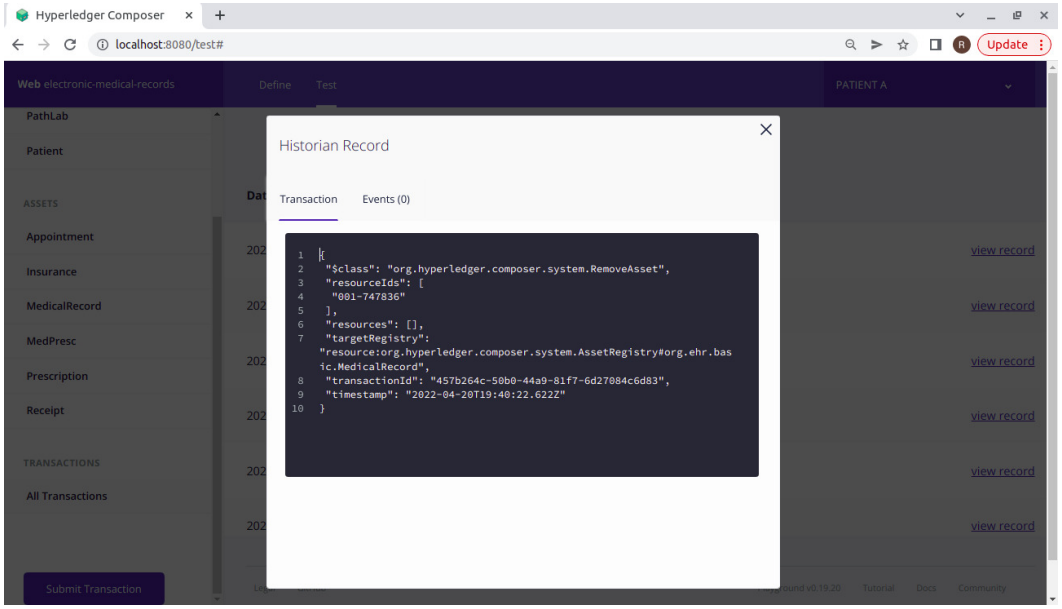

Fig. 21 Screenshot of Patient deleting his/her Medical Record

cessful transactions in the network is shown in Fig. 20. Patients can also determine how long the Doctor/PathLab has access rights to their medical records in the permissioned scenario thereafter these rights will be revoked automatically by the blockchain network (according to the *Right to erase policy*). Although blockchain does not permit removal or control shared data in the network. Therefore, alternative access control rules are required to allow patients to give access rights to their medical records. In accordance with the GDPR [31], the *right to access* and *right to restrict access* ensure the patient's control over their medical records. Patients should also be certain that unauthorized access to their data is not permitted because the data solely belongs to them.

The GDPR stipulates that individuals' right to be forgotten which Purging Data Scenario analyzes and can erase their own data in Composer, whereas other users cannot delete someone's medical records, as shown in Fig. 21 and Fig. 22 respectively. Some blockchain application developers advised that applications built on Hyperledger should not store any sensitive documents and personal data should be maintained in an off-chain database to comply with legislation. As aforementioned,

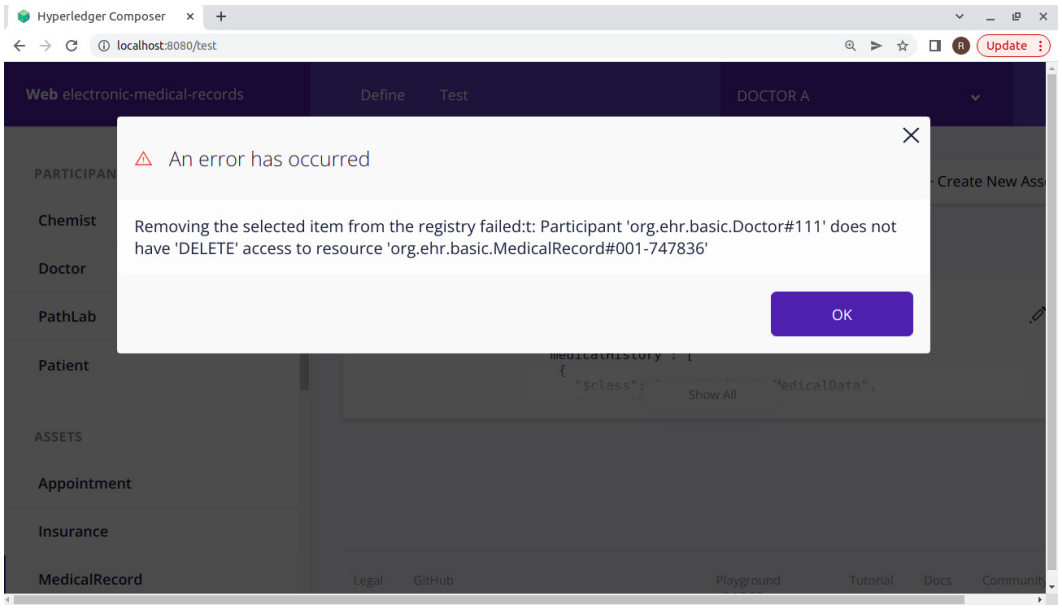

Fig. 22 Screenshot of Doctor cannot delete patient's Medical Record

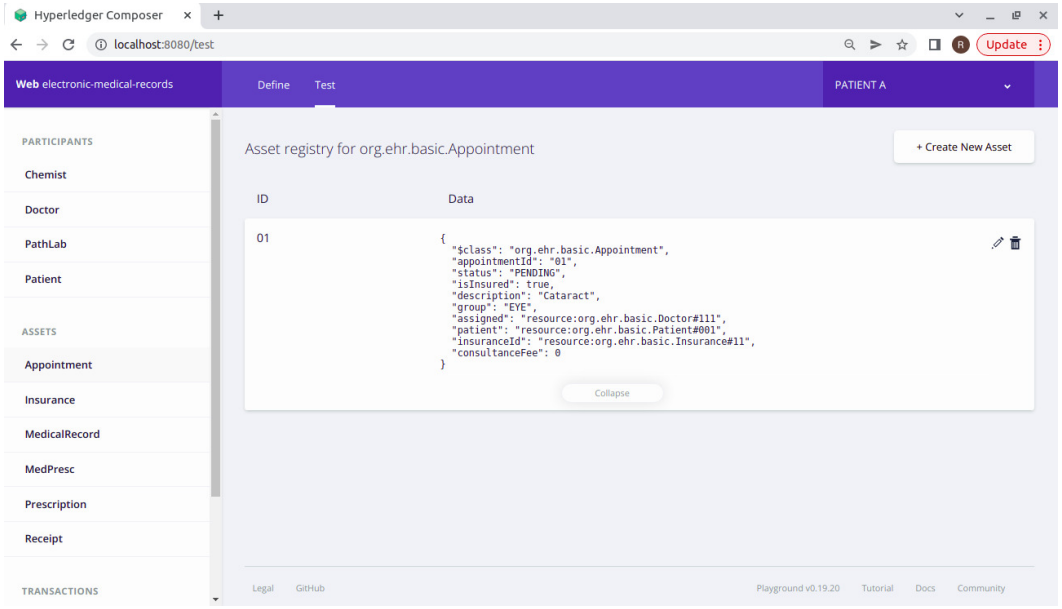

Fig. 23 Screenshot of Patient A requests an Appointment from Doctor A

patients have total access control over their medical records, therefore, deletion can be handled by denying access to all other users of the blockchain network.

6.3 Accessibility

Patients can access medical records, doctor's prescriptions, and receipts very easily from their individual accounts under the proposed healthcare framework. Patients need their previous medication history frequently or may take physical copies of their medical records whenever required. Prescribers utilize an easy user interface of the proposed framework to update medical histories through the decentralized ledger. Sometimes healthcare practitioners can immediately lookup medication histories of concern when a patient visits other medical facilities with proper consent from the doctor. These facilities do not need to collaborate with a collection of privatized central repositories because blockchain is decentralized in nature and can handle all those issues very efficiently.

In the proposed framework, a patient is allowed to request an appointment from the available pool of doc-

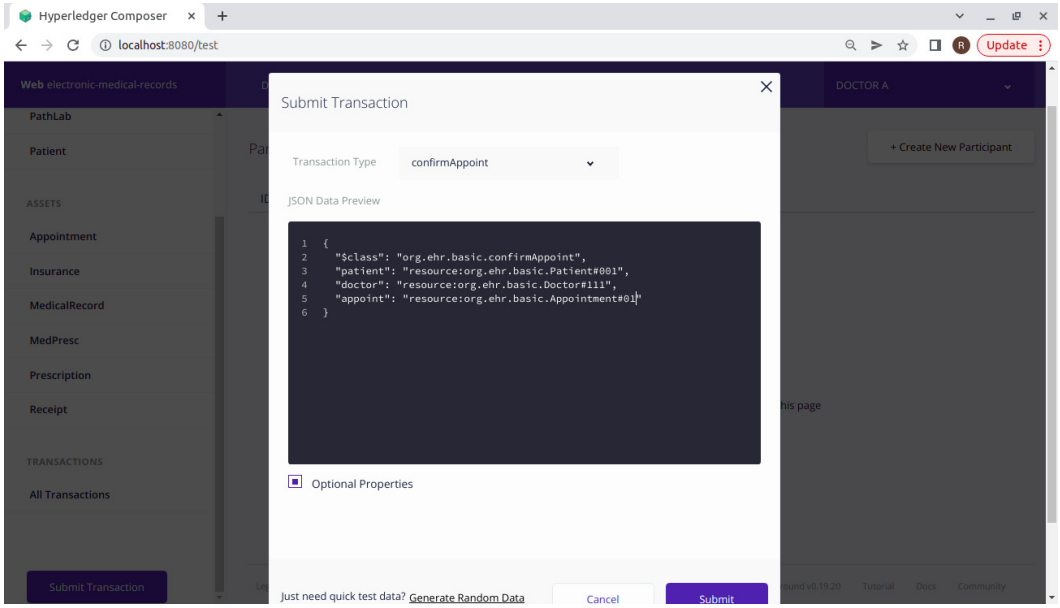

Fig. 24 Screenshot of Doctor A confirms the Appointment

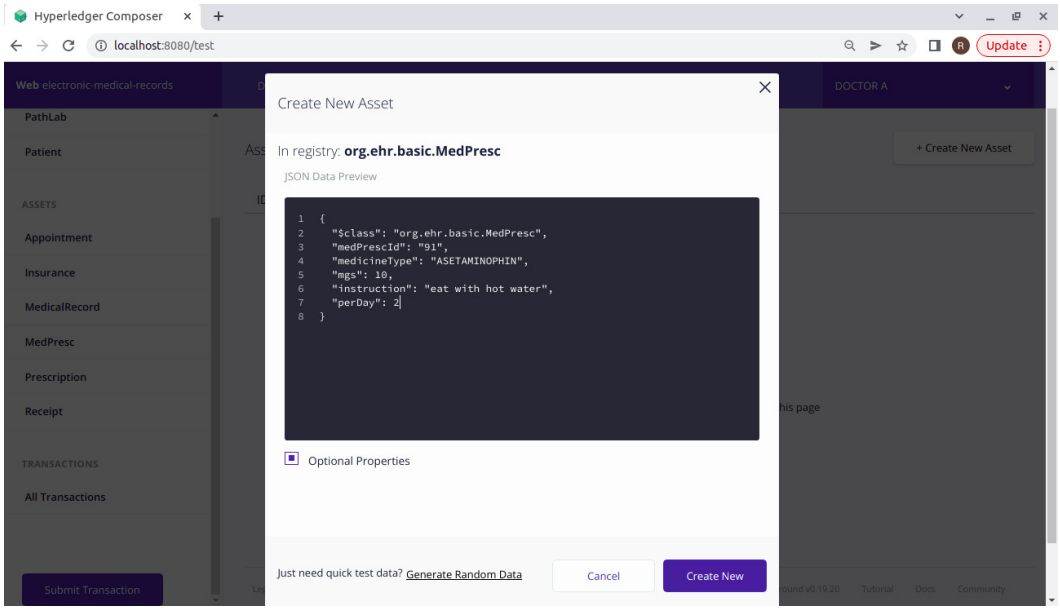

Fig. 25 Screenshot of Doctor A creating MedPresc Asset

tors in the blockchain and selected doctors have the right to confirm or deny the appointment as per schedule, as shown in Fig. 23 and Fig. 24 respectively. Suppose, Doctor A confirms the appointment of patient A, then Doctor A will create assets such as MedPresc, and Prescription and also provide consultation to the patient, as shown in Fig. 25, Fig. 26, Fig. 27 and Fig. 28 respectively. Fig. 29 shows the scenario when Doctor A provides consultation to Patient A, the status of the appointment changes to consulted and Patient A's debt gets updated in the account. Similarly, the interaction between intended Chemist's/PathLab and patients get recorded to ensure accessibility for all the participants on the blockchain and unauthorized users are not aware about any of the user or transaction in the network. The proposed framework also accommodate historical records for auditing, which keep track of transactions made by the participants at any time and it is also immutable for any user of the blockchain network. All in all, the proposed framework provides all the required functionalities and security to keep patients' data safe and confidential from unauthorized access in the blockchain networks for healthcare application.

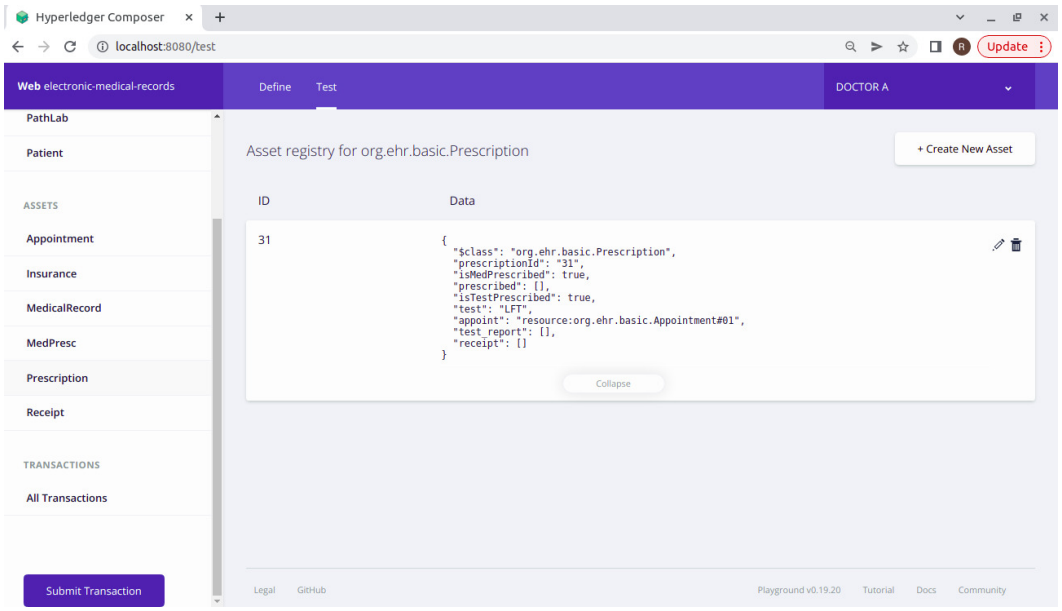

Fig. 26 Screenshot of Doctor A creating Prescription Asset

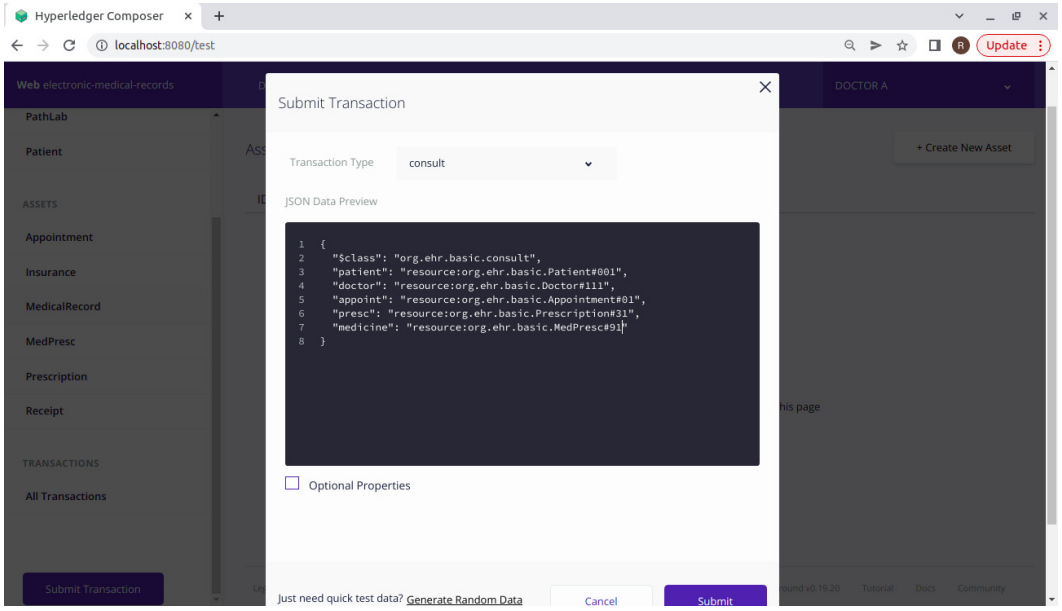

Fig. 27 Screenshot of Doctor A providing consultation to Patient A

Table 5 A comparative analysis of the proposed framework with existing blockchain-based frameworks

Models/Frameworks/ Systems	Confidential Information	Data Security	Data Integrity	Patient–User Preference	Access Control
Shen et. al. [47]	✔	✔	✔	✕	✕
Dwivedi et. al. [14]	✔	✔	✔	✕	✔
Rajpoot et. al. [45]	✕	✔	✔	✕	✕
Jagadeesh et. al. [46]	✕	✔	✕	✕	✕
Egala et. al. [15]	✔	✔	✔	✕	✔
Wang et. al. [52]	✔	✔	✔	✕	✕
Proposed Framework	✔	✔	✔	✔	✔

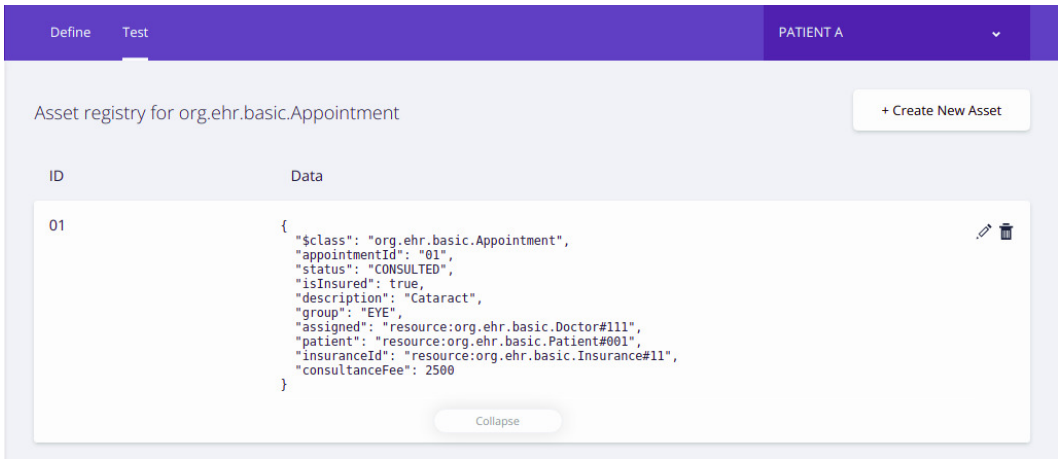

Fig. 28 Screenshot of Status of Appointment changes to "Consulted"

Fig. 29 Screenshot of Patient A's debt gets updated

6.4 Comparison with existing healthcare frameworks/systems

The proposed framework has been developed using the Hyperledger composer by considering the aforementioned policies that reduce the overall system overhead. To provide a comparative analysis, we have evaluated the existing blockchain-based healthcare systems by considering their strategies for designing security policies [14,15,45–47,52]. Along with that we have conducted a benchmark study to investigate the capabilities of our framework with respect to the other existing systems on the basis of various performance parameters such as access control, confidential information, data integrity, data security, and patient–user preference. Some significant parameters are also considered to evaluate the impact on the system performance during the analysis and found that our framework is satisfying most of the requirements that makes it more robust and reliable. Table 5 depicts the outcome of the proposed and existing benchmark studies on the basis of various performance parameters. From the discussion, we can conclude that our proposed framework satisfies the most of the significant quality parameters as required by the secure healthcare data management system.

7 Conclusion and Future scope

In this work, we proposed a new access control framework for the healthcare data management system using access control mechanisms and encryption techniques. The proposed framework is more secure, efficient, and accessible between different participants such as patients, doctors, chemists, and pathology labs. We have implemented this permissioned blockchain network using Hyperledger Fabric and Hyperledger composer in a systematic manner. Using the consortium model, we deployed smart contracts in blockchain technology to create security policies so that patients have control of the access rules of other stakeholders in the healthcare system. Furthermore, it offers significant potential for ensuring the privacy, security, integrity, time efficiency, and confidentiality of healthcare data, and granular access control management. The prototype pro-

vides a blockchain-based application for healthcare data management and fulfills certain fundamental requirements. In the future, firstly, we plan to make our framework more user-friendly by integrating it with a recommendation system, to assign a rank to doctors and pathology labs on the basis of their patients' experience or satisfaction. Thereafter, the patients' feedback reveals to all stakeholders on the blockchain network for effective recommendation to the patients. We can also incorporate the policies to access EHRs in emergency situations to grant access rights to doctors or other stakeholders by the nominated members of the patient.

Declarations

1. **Funding:** No Funding
2. **Conflicts of interest/Competing interests:** Not applicable
3. **Authors' Contributions:**
   - Amit Kumar Jakhar, Mrityunjay Singh, Rohit Sharma, and Aman Sharma contributed to the design of the proposed framework.
   - Amit Kumar Jakhar and Mrityunjay Singh contributed to formulating the problem and writing the research paper.
   - Rohit Sharma and Aman Sharma handled the implementation and validation part of the proposed framework.
4. **Availability of data and material:** Not applicable
5. **Human and Animal Ethics:** Not applicable
6. **Code availability:** Not applicable
7. **Ethics approval:** Not applicable
8. **Consent to participate:** Not applicable
9. **Consent for publication:** Not applicable

References

1. H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli. Risk analysis of cloud sourcing in healthcare and public health industry. *IEEE Access*, 6:19140–19150, 2018.
2. A. Act. Health insurance portability and accountability act of 1996. *Public law*, 104:191, 1996.
3. L. Adefala. Healthcare experiences twice the number of cyber attacks as other industries. *CSO ONLINE, Mar*, 6, 2018.
4. F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, A. Adnane, and E. Barka. Blockchain in internet-of-things: Architecture, applications and research directions. In *2019 International conference on computer and information sciences (ICCIS)*, pages 1–6. IEEE, 2019.
5. M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2):1676–1717, 2018.
6. M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur Rehman, and C. A. Kerrache. The case of hyperledger fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*, 2(1):100012, 2021.
7. S. T. Argaw, N.-E. Bempong, B. Eshaya-Chauvin, and A. Flahault. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC medical informatics and decision making*, 19(1):1–11, 2019.
8. T. Q. Ban, B. N. Anh, N. T. Son, and T. Van Dinh. Survey of hyperledger blockchain frameworks: case study in fpt university's cryptocurrency wallets. In *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, pages 472–480, 2019.
9. U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*, 8:54371–54401, 2020.
10. V. Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.
11. M. Castro and B. Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.
12. U. Chelladurai and S. Pandian. A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 13(1):693–703, 2022.
13. T. K. Dasaklis, F. Casino, and C. Patsakis. Blockchain meets smart health: Towards next generation healthcare services. In *2018 9th International conference on information, intelligence, systems and applications (IISA)*, pages 1–8. IEEE, 2018.
14. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326, 2019.
15. B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, 8(14):11717–11731, 2021.
16. N. Fikri, M. Rida, N. Abghour, K. Moussaid, A. El Omri, and M. Myara. A blockchain architecture for trusted subledger operations and financial audit using decentralized microservices. *IEEE Access*, 2022.
17. J. Gao, H. Liu, Y. Li, C. Liu, Z. Yang, Q. Li, Z. Guan, and Z. Chen. Towards automated testing of blockchain-based decentralized applications. In *2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC)*, pages 294–299. IEEE, 2019.
18. W. Gao, W. G. Hatcher, and W. Yu. A survey of blockchain: Techniques, applications, and challenges. In *2018 27th international conference on computer communication and networks (ICCCN)*, pages 1–11. IEEE, 2018.
19. A. Gencer and E. Sirer. Miniature world: Measuring and evaluating blockchains. *Cornell University*, 2016.
20. W. J. Gordon and C. Catalini. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, 16:224–230, 2018.
21. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh. Healthcare blockchain

system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7):1–7, 2018.
22. H. Guo, W. Li, M. Nejad, and C.-C. Shen. A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. *IEEE Transactions on Network and Service Management*, 2022.
23. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun. Habits: Blockchain-based telesurgery framework for healthcare 4.0. In *2019 international conference on computer, information and telecommunication systems (CITS)*, pages 1–5. IEEE, 2019.
24. J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta. Blockchain-based remote patient monitoring in healthcare 4.0. In *2019 IEEE 9th international conference on advanced computing (IACC)*, pages 87–91. IEEE, 2019.
25. H. Honar Pajooh, M. A. Rashid, F. Alam, and S. Demidenko. Experimental performance analysis of a scalable distributed hyperledger fabric for a large-scale iot testbed. *Sensors*, 22(13):4868, 2022.
26. K. M. Hossein, M. E. Esmaeili, T. Dargahi, et al. Blockchain-based privacy-preserving healthcare architecture. In *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*, pages 1–4. IEEE, 2019.
27. Hyperledger. Architecture explained read the docs. 2017.
28. H. Kakavand, N. K. De Sevres, and B. Chilton. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. 2017. *DOI: https://doi. org/10.2139/ssrn*, 2849251, 2016.
29. M. Kassab, J. DeFranco, T. Malas, G. Destefanis, and V. V. G. Neto. Investigating quality requirements for blockchain-based healthcare systems. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pages 52–55. IEEE, 2019.
30. V. Koufi, F. Malamateniou, and G. Vassilacopoulos. Ubiquitous access to cloud emergency medical services. In *Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine*, pages 1–4. IEEE, 2010.
31. A. Le Bris and W. El Asri. State of cybersecurity & cyber threats in healthcare organizations. *ESSEC Business School*, page 12, 2016.
32. A. R. Lee, M. G. Kim, and I. K. Kim. Sharechain: Healthcare data sharing framework using blockchain-registry and fhir. In *2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pages 1087–1090. IEEE, 2019.
33. R. Lewis. 30 things you can do with the blockchain: https://medium.com/yope-chain/30-things-you-can-do-with-a-blockchain-b23b2ab39664., 2016.
34. X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu. Towards decentralized accountability and self-sovereignty in healthcare systems. In *International conference on information and communications security*, pages 387–398. Springer, 2017.
35. S. Mansfield-Devine. Leaks and ransoms–the key threats to healthcare organisations. *Network Security*, 2017(6):14–19, 2017.
36. E. Markakis, Y. Nikoloudakis, E. Pallis, and M. Manso. Security assessment as a service cross-layered system for the adoption of digital, personalised and trusted healthcare. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 91–94. IEEE, 2019.
37. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.
38. N. Nchinda, A. Cameron, K. Retzepi, and A. Lippman. Medrec: a network for personal information distribution. In *2019 International Conference on Computing, Networking and Communications (ICNC)*, pages 637–641. IEEE, 2019.
39. P. Ndayizigamiye and S. Dube. Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in south africa. In *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pages 1–5. IEEE, 2019.
40. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman. Fairaccess: a new blockchain-based access control framework for the internet of things. *Security and communication networks*, 9(18):5943–5964, 2016.
41. A. Ouaddah, A. A. Elkalam, and A. A. Ouahman. Towards a novel privacy-preserving access control model based on blockchain technology in iot. In *Europe and MENA cooperation advances in information and communication technologies*, pages 523–533. Springer, 2017.
42. M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha. Standard electronic health record (ehr) framework for indian healthcare system. *Health Services and Outcomes Research Methodology*, 21(3):339–362, 2021.
43. C. Pirtle and J. Ehrenfeld. Blockchain for healthcare: The next generation of medical records?, 2018.
44. J. Qiu, X. Liang, S. Shetty, and D. Bowden. Towards secure and smart healthcare in smart cities using blockchain. In *2018 IEEE international smart cities conference (ISC2)*, pages 1–4. IEEE, 2018.
45. A. R. Rajput, Q. Li, and M. T. Ahvanooey. A blockchain-based secret-data sharing framework for personal health records in emergency condition. In *Healthcare*, volume 9, page 206. Multidisciplinary Digital Publishing Institute, 2021.
46. J. Ranjith and K. Mahantesh. Blockchain-based knapsack system for security and privacy preserving to medical data. *SN Comput. Sci.*, 2(4):245, 2021.
47. B. Shen, J. Guo, and Y. Yang. Medchain: Efficient healthcare data sharing via blockchain. *Applied sciences*, 9(6):1207, 2019.
48. T. D. Smith. The blockchain litmus test. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2299–2308. IEEE, 2017.
49. P. Thakkar, S. Nathan, and B. Viswanathan. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 264–276. IEEE, 2018.
50. E. Vayena, T. Haeusermann, A. Adjekum, and A. Blasimme. Digital health: meeting the ethical and policy challenges. *Swiss medical weekly*, 148:w14571, 2018.
51. W. G. Voss. European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer*, 72(1):221–234, 2016.
52. H. Wang and Y. Song. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, 42(8):1–9, 2018.
53. S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang. Blockchain-powered parallel healthcare systems based on the acp approach. *IEEE Transactions on Computational Social Systems*, 5(4):942–950, 2018.

54. S. Wu and J. Du. Electronic medical record security sharing model based on blockchain. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pages 13–17, 2019.
55. P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz. Metrics for assessing blockchain-based healthcare decentralized apps. In *2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom)*, pages 1–4. IEEE, 2017.
56. K. Zile and R. Strazdina. Blockchain use cases and their feasibility. *Applied Computer Systems*, 23(1):12–20, 2018.