Journal of Information Security and Applications 50 (2020) 102407

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Blockchain-based electronic healthcare record system for healthcare 4.0 applications

Sudeep Tanwar[a,*], Karan Parekh[a], Richard Evans[b]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India 382481
[b] College of Engineering, Design and Physical Sciences, Brunel University London, United Kingdom

ARTICLE INFO

Article history:
Available online 21 November 2019

Keywords:
Blockchain
Healthcare systems
Security
Chaincode
Electronic healthcare records

ABSTRACT

Modern healthcare systems are characterized as being highly complex and costly. However, this can be reduced through improved health record management, utilization of insurance agencies, and blockchain technology. Blockchain was first introduced to provide distributed records of money-related exchanges that were not dependent on centralized authorities or financial institutions. Breakthroughs in blockchain technology have led to improved transactions involving medical records, insurance billing, and smart contracts, enabling permanent access to and security of data, as well as providing a distributed database of transactions. One significant advantage of using blockchain technology in the healthcare industry is that it can reform the interoperability of healthcare databases, providing increased access to patient medical records, device tracking, prescription databases, and hospital assets, including the complete life cycle of a device within the blockchain infrastructure. Access to patients' medical histories is essential to correctly prescribe medication, with blockchain being able to dramatically enhance the healthcare services framework. In this paper, several solutions for improving current limitations in healthcare systems using blockchain technology are explored, including frameworks and tools to measure the performance of such systems, e.g., Hyperledger Fabric, Composer, Docker Container, Hyperledger Caliper, and the Wireshark capture engine. Further, this paper proposes an Access Control Policy Algorithm for improving data accessibility between healthcare providers, assisting in the simulation of environments to implement the Hyperledger-based eletronic healthcare record (EHR) sharing system that uses the concept of a chaincode. Performance metrics in blockchain networks, such as latency, throughput, Round Trip Time (RTT). have also been optimized for achieving enhanced results. Compared to traditional EHR systems, which use client-server architecture, the proposed system uses blockchain for improving efficiency and security.

1. Introduction

Smart technologies, such as the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning, and Virtual Reality (VR) and Augmented Reality (AR), have revolutionized the engineering and manufacturing sectors, including automotive, computing and electronics, and aerospace and defence. Healthcare systems adopted by healthcare providers, such as hospitals and general practitioners, are no exception. Over time, they have become more powerful and useful [1]. Smart technologies have also become increasingly competent at handling large data sets in real-time, enabling faster identification and determining of illnesses, with suggestions and comparisons of treatments now being automated. With the use of blockchain technology, transparency and communication between patients and healthcare providers is also enhanced.

This section introduces the relevant concepts related to smart technologies in the healthcare industry. We examine the development of smart technologies, and the necessary security requirements for implementation into the healthcare industry. An overview of blockchain technology is provided, including its benefits and how it can be applied to healthcare systems. Since the introduction of healthcare provision in the 1970s, the emergence of modular IT systems has been observed. This period is known as Healthcare 1.0. In this era, healthcare systems were limited and not coordinated with digital systems due to lack of resources. Similarly, bio-medical machines were not yet developed and did not integrate into networked electronic devices. During this period, paper-based prescriptions and reports were widely used in healthcare organizations which led to increased costs and time.

* Corresponding author.
E-mail addresses: sudeep.tanwar@nirmauni.ac.in (S. Tanwar), 17mcen16@nirmauni.ac.in (K. Parekh), Richard.Evans@brunel.ac.uk (R. Evans).

https://doi.org/10.1016/j.jisa.2019.102407
2214-2126/

The Healthcare 2.0 era was observed from 1991 to 2005. During this period, health and information technologies were combined to create healthcare systems, as we know them today. In this phase, digital tracking was introduced, providing doctors with imaging systems for analyzing patients' health. At the same time, new user-enabled technologies began to emerge in the healthcare industry, surfacing alongside the introduction of social media. Healthcare providers began to create online communities for information and knowledge sharing, store information on cloud servers, and provide access to documents and patient records via mobile devices, enabling ubiquitous access for both the provider and patient. During this period, critics expressed concern over misleading information and violation of patients privacy. Healthcare systems used networked electronic health management practices that integrated with clinical imaging systems to assist doctors to obtain more secure, accurate and timely access to patient data.

The advent of Healthcare 3.0 coincided with the concept of Web 3.0, enabling user-customization of how patient healthcare records were delivered. User interfaces became simpler and more bespoke, allowing for optimized and personalized experiences. Electronic Healthcare Records (EHRs) were also introduced, along with wearable and implantable systems, enabling real-time, ubiquitous tracking of patients' healthcare. Similarly, EHR systems [2] began to emerge which integrated stand-alone non-networked systems, including social media channels, to store patient information; this made the sharing of health data over networked channels, including social media, or between clinicians, using EHR systems, simpler. Interaction and communication between healthcare providers and patients was also enhanced.

From 2016 to the present day, we have experienced the Healthcare 4.0 era. This era was derived from the concept of Industry 4.0, where Hi-tech and Hi-touch systems are being introduced, using cloud computing, fog and edge computing, big data analytics, AI and machine learning, to build blockchains to support real-time access to patients' clinical data [3]. The main aim of this era is to enhance virtualization, enabling personalized healthcare in real-time. The focus is now on collaboration, coherence, and convergence, which can make healthcare more predictive and personalized.

1.1. Security in healthcare

Healthcare data requires a high-level of security and privacy. Privacy refers to persons having the correct rights to allow or disclose personal information to others. This demands consensus among healthcare providers and regulators, and the creation of agreed policies and procedures. Privacy is the starting point to determining who and whom should be allowed to access personal patient information [4]. In line with this issue, numerous security standards have been developed, such as HIPAA, COBIT, and DISHA, which have been applied to protect patients' health information. Healthcare security is also of paramount importance to healthcare providers to help safeguard the privacy of patients health information. This includes managing access control of patient information, security of patient data from unauthorized users, and the modification and destruction of stored data, etc[5]. As sizes of healthcare data increases, then there is need of security mechanisms to protect the data. Hence, the United States and other countries have developed security standards and regulations to protect their healthcare information.

1.2. Why security is important in healthcare?

Since the dawn of the Healthcare 4.0 era, healthcare providers have become evermore dependent on smart technologies. Such technologies assist in the management and diagnosis of patient illnesses, and help transmit, receive, and collect patient information for health record management. The fitness of data stored on EHR systems plays a critical role in the success of a healthcare provider [6]. Therefore, data must always be free of threats and secure at all times. If these conditions are not met, the technologies used may not function correctly or be deemed reliable.

With the advent of big data, the size and complexity of healthcare records is increasing and is still not optimized. Records are often duplicated, mismatched using different identifiers / naming conventions, and are made available on different networks and directories of healthcare systems. The security of healthcare records is becoming increasingly important for keeping data safe from security breaches and criminal activity. If unauthorized users are able to gain access to patient data, it can be sold or leaked to the market, with patients' personal information being revealed to anyone with access. This information may include addresses, telephone numbers, full names, etc. The privacy of patients' data is essential in successful healthcare management [7]. In light of these challenges, various countries have proposed or created regulated standards for healthcare systems, to prevent cyber threats, which helps improve confidentiality of patient information and confidence in the provider-patient relationship. At present, most healthcare systems use centralized client-server based architectures, where a central authority has full-access to the system. In this scenario, lack of privacy or security flaws may lead to failures in the system, resulting in cyber intruders potentially gaining access to patient data.

1.3. Blockchain technology

In recent years, research relating to blockchain and smart ledgers has gained in popularity due to the emergence of cryptocurrencies, such as Bitcoin and Ethereum. Blockchain stores and shares data in a distributed, trusted and immutable manner, removing intermediaries, and not requiring a centralized dependency for checking transactions [8,9]. Transparency in blockchain provides a less complicated method for accessing ledger-based transactions over networks; it connects with different computing powers from multiple nodes in the blockchain network, making it extremely powerful with respect to calculation speed [10]. Blockchain comprises various techniques and services, including Consensus Protocol, Hash Cryptography, Immutable Ledger, Distributed P2P Networking, and mining, which are now introduced in more detail:

- Consensus protocol: In a blockchain network, certain users have individual access rights to grant transactions that are updated in the system, known as consensus protocol;
- Hash cryptography: A blockchain uses SHA256 hash for adding transactions. This is developed by the NSA and is 64 characters long. Hash algorithms include features, such as one-way cryptography, deterministic, faster computation, the avalanche effect, and must withstand collisions;
- Immutable ledger: All transactions in a blockchain network are recorded, while the shared ledger cannot be modified or tampered with;
- Distributed P2P network: All transactions are broadcast over the network to different users to distribute and update the data; and
- Mining: Miners use blocks of nonce values to achieve hash values in the network. This requires high computation speed to achieve and obtain the reward.

It is possible to duplicate a blockchain network to another location e.g., within the same facility or healthcare delivery network, or as part of a national or international data sharing

program. This ability makes it possible to share healthcare data with researchers, partner facilities, or other interested parties e.g., insurance providers. Blockchain is linked within a network, which shares data and ensures that the data within the network is accurate, reliable and consistent. We can, therefore, add data to a blockchain at one location and distribute it to one or more locations within the same network. The new locations also share the data within the network, eventually distributing the new data to the entire network, and allowing location access to the latest data.

1.4. Advantages of blockchain technology

Blockchain technology uses a distributed network, containing data in tamper-resistant forms. Blockchain transactions are only updated or added through the creation of new hash values and, therefore, existing transactions cannot be modified. To understand this, the potential use of blockchain technology needs to be described against all features which make the blockchain unique from others:

- Distributed ledger: Transactions are appended in a distributed system on the network, which creates system recovery by eliminating a single point of failure or centralized entity;
- Consensus mechanism: Transactions are only updated when all verified users in the network agree to the condition of the transaction;
- Provenance: The complete data or asset's history is available on the blockchain network;
- Immutability: Records on the network cannot be modified or tampered with; thus, all information is secure and trusted;
- Finality: When a transaction is committed on a blockchain, it cannot be modified or reversed; and
- Smart contract: The codes are created on a blockchain network, and the computer and nodes execute on a triggered event. Hence, The codes are auto-executed within the time frame.

To this end, Blockchain has the potential to reduce transparency and security issues, such as trust of third parties at any stage of a transaction; this means that all intermediaries or third parties are eliminated with the advent of blockchain technology.

1.5. How transactions are created in a blockchain?

Blockchain has a complicated working sequence for verifying and validating transactions via a distributed ledger network, creating immutable, secure and consensus-based ledger technology. There are various steps required to complete a blockchain transaction. In the first step, the network node requests the transaction. The transaction is then broadcast to peer nodes of the network, including all PC nodes. The blockchain network then uses the SHA-256 algorithm to create a unique hash. All hashes are then linked through a previous hash; this makes an unbreakable network of transactions. If someone attempts to append a transaction, then it would be validated by the network node or by a smart contract, consensus. This immutable ledger, therefore, cannot be modified [11]; it can only be appended to the transaction of blocks. This process produces a secure and reliable decentralized system. By using an algorithm, it verifies whether the user is genuine. Examples of confirmed transactions include cryptocurrencies, contracts, patient healthcare records, and clinical data. After a transaction is verified, it is appended in the ledger for the creation of a new block in the network. The block has a structure that includes an Index, Time stamp, Data, Previous hash, and Current block hash. A new block is then appended to the blockchain, making it secure and free from change or modification. In the last step, the transaction is completed or committed to the network.

1.6. A scenario in the healthcare industry

Let's take an example of a clinician, who has six patients that require medical treatment. Patients arrive at the clinician with various symptoms, such as chest pain, constipation or headaches, and are evaluated in the accident and emergency department where they undergo necessary examination before treatment commences. One patient mentions that they have a primary care doctor, but that they do not use the same healthcare system, hence, the clinician has to access their EHRs to obtain previous records from that patient's primary care provider. The clinician receives some test data and identifies that the patient previously attended a care clinic, a few weeks ago, for chest pain. The clinician has to, therefore, log in to a third party healthcare record to obtain the patient's records from the care provider.

After reviewing this information, the clinician gets a better picture of the patient's prior medical history and previous treatment. It should be noted that, at this point, this would not be possible unless the patient informs the clinician of previous healthcare visits. After the careful review of the care clinic's notes, the doctor finds that the patient was referred to a specialist physician in another city. The clinician has to now identify the physician's name and their specialty, but does not have access to those healthcare records. After sending a request to the physician's office to obtain the EHR data, it takes several days to receive the data, which often may be complex and incomplete. The patient may also have healthcare data stored elsewhere, unknown to the clinician.

In this situation, if there is a blockchain registry where the patient's data is stored, the clinician can easily identify if the patient was seen at other clinics or another immediate care clinic. They can also view whether the patient had received treatment for the same conditions in another hospital. If the clinician had all of this information readily available, they would have had a better understanding of the overall health of the patient, and what previous treatment and investigations they had undergone, which would help reduce duplication and avoid unnecessary avenues of investigation; this would result in time and cost savings, increased efficiency, and enhanced patient-centered healthcare. These abilities are what gives blockchain the potential to dramatically impact the efficiency and costs of healthcare delivery. Fundamental problems experienced in healthcare delivery include lack of management of data, and how data can be made verifiable, immutable, and distributed. Blockchain technology, therefore, can be used to provide automated database services for aggregated and secure data.

1.7. Assessment of blockchain technology in healthcare

It is commonly understood that healthcare providers generate enormous amounts of data in various formats, including reports, financial documents, laboratory test results, imaging studies, such as x-rays and CAD scans, and measurements of vital signs etc. The extensive database being generated in healthcare settings is expanding at a rapid rate, with healthcare data suffering from various challenges, including access to data and how that data can be accessed outside of the healthcare facility. Blockchain offers the potential to improve the verification and integrity of such data. It also helps with the distribution of data within the network or facilities. These features create an impact to cost, data quality, and value of healthcare delivery within the system. Blockchain is an open, decentralized system that eliminates the 'middleman' [12]. Blockchain healthcare systems do not require multiple levels of authentication and provide access to data to everyone who is part of the blockchain architecture. Data is made visible and transparent for users. These features can help solve the various challenges faced by the healthcare industry today.

1.8. Adding blockchain to the healthcare ecosystem

The inclusion of blockchain in the healthcare industry is divided into four stages. In the first stage, healthcare providers have direct connection to the blockchain; all clinical data is tracked and stored in the existing health IT systems. Various data related to patients, using Patient IDs, is transmitted to the blockchain network via API. In the blockchain system, a smart contract is then used to execute the inward transactions. All transactions are committed in the blockchain network using patient public IDs that do not contain personal information. The blocks are created and chained through the immutable ledger. All transactions are then committed and uniquely identifiable. Consequently, reverse mining or query processing begins with the health provider via the APIs. The database of blocks stores only non-identifiable patient data, such as gender, age, and illnesses, etc. Clinical data is analyzed to uncover new insights. Finally, if the patient wishes to share his/her identity with the healthcare provider, they can share their private key. This is how the provider can then access the patient's data and provide solutions or care for identified symptoms. Obviously, the data remains confidential to those who do not have the private key of the patient.

1.9. Research contributions

The main contributions of this paper are described as follows. Firstly, using distributed ledger technology, we propose a system architecture and algorithm for a patient-centered approach to provide an access control policy with symmetric key cryptography to a different healthcare provider. We propose a blockchain-based approach for implementing a permission-based EHR sharing system with the use of the chaincode concept. Then, the proposed system is analyzed to establish how it fulfills the needs of patients, healthcare providers and other interested parties. Finally, we determine the best approach for performance optimization metrics of the blockchain system, in terms of latency and throughput, network scalability, and security.

1.10. Organization

The rest of the paper is organized as follows: Section 2 examines related works. Section 3 presents the system architecture and the problem formulation followed by the proposed algorithms. Section 4 describes the results obtained using various performance metrics and, finally, Section 5 provides conclusions and suggestions for future research.

2. Related work

Yup et al. [13] explored the blockchain approach for healthcare intelligence with regard to privacy of users. They proposed a data access control for privacy and designed the healthcare data gateway. Zhang et al. [14] proposed PSN-based healthcare to secure the system, designing two protocols for authentication and sharing of healthcare data within a blockchain network. Xia et al. [15] designed a blockchain-based approach for healthcare data sharing using cloud-based services. They proposed the Medshare system for access control, provenance and security of medical records. Liang et al. [16] designed a mobile-based healthcare record sharing system using blockchain, proposing a secure user-centric approach to provide access control and privacy using channel formation scheme. Jiang et al. [17] proposed a medical data exchange system using blockchain, consequently developing off-chain and on-chain verification for the security of the system's storage. Li et al. [18] explored data protection systems for healthcare, proposing algorithms for memory management that assist in data management. Fan et al. [19] proposed blockchain-based medical information of patients, improving consensus mechanisms to achieve enhanced security and privacy of data within system. Wang and Song [20] proposed a secure medical record sharing system using an attribute-based encryption mechanism. They used smart contracts to ensure the integrity and traceability of the health data. Guo et al. [21] presented an attribute-based signature scheme for multiple users in electronic health record management, using blockchain. In this attribute-based mathematical formulation, they aimed to achieve improved security of the system, using a decentralized approach for enhanced privacy.

Uddin et al. [22] designed a system architecture based on a continuous patient monitoring system, using a patient centric agent in the main module; they enhanced the security and privacy of the proposed system with taken simulations. Sun et al. [23] introduced a distributed attribute-based signature scheme for medical systems based on blockchain, while also proposing a blockchain-based records sharing protocol with supporting algorithms. Poslad and Poslad [24] discussed current issues and proposed an access control policy for electronic medical records with finer granular access within the system. Yang and Li [25] designed architecture for securing electronic healthcare records based on distributed ledger technology and also improved the interoperability of health records between different organizations. Thakkar et al. [26] explored two approaches for performance evaluation of the system of blockchain framework, optimizing performance with aggressive caching and configuration endorsement policy. Sukhwani et al. [27] analyzed the performance metrics of the hyperledger fabric framework. Gorenflo et al. [28] proposed the optimization for performance for blockchain framework and design architecture, configuring it to reduce input/output, and computation for enhanced performance. Finally, Chen et al. [5] proposed the searchable encryption scheme for electronic healthcare records using blockchain. They designed an algorithm for indexing healthcare records and a two-part evaluation scheme. The relative comparison of the state-of-the-art blockchain-based approaches to secure EHR systems is given in Table 1.

3. Proposed approach

In this section, the proposed approach for electronic health record sharing, based on blockchain network, is introduced. Consequently, the blockchain-based EHR sharing system architecture is proposed. Various methods and configurations for the block transaction in the network are deployed. In the proposed system, a shared symmetric key and private key enable the EHR to be distributed to other participants in the blockchain network. The most appropriate EHR sharing algorithms for the smooth operation and less communication time are also discussed in Table 1.

3.1. System architecture

The blockchain based EHR system architecture is described in this section. There are four participants in the propoed system as shown in Fig. 1: Patient, Clinician, Lab and System admin. In this system, various assets or smart contracts are defined, including, but not limited to: CreateMedicalRecord, GrantAccessToClinician, GrantAccessToLab, RevokeAccess, RevokeAccessToLab as shown in Fig. 1.

The system workflow is simple to use. Participants register through the client application or SDK, requesting an enrolment certificate via a Membership Service Provider (MSP) to the certificate authority. Then, the certificate authority issues the certificate and private key with a new ID to enrol the participant. All transactions are distributed over the hyperledger fabric blockchain network. Participants have different roles in the system and can

Table 1
State-of-the-art blockchain-based approaches to secure EHR systems.

Author	Year	Objective	1	2	3	4	5	6	7	Pros	Cons
Yup et al. [13]	2016	To discover blockchain-based healthcare intelligence with privacy.	√	√	✗	√	✗	√	✗	Records controlled by patients.	Design illustration only.
Zhang et al. [14]	2017	To develop a secure health system for an extensive network.	√	✗	√	√	✗	✗	√	Share load of network.	No mature schemes.
Xia et al. [15]	2017	To design blockchain-based health sharing with cloud-based services.	√	√	√	√	√	✗	√	Access control mechanism	Scalability, key management.
Liang et al. [16]	2017	To use blockchain for the sharing of healthcare records and collaboration in mobile health usage	√	√	✗	✗	√	✗	✗	Secure merkle root tree for transactions, data Sharing and healthcare Collaboration.	Interoperability
Jiang et al. [17]	2018	To develop a blockchain-based system for medical data exchange.	√	√	√	√	✗	√	√	Joins the approach of off-chain storage and on-chain verification for privacy and authenticity.	System performance and fairness, and complex access control.
Li et al. [18]	2018	To review data protection systems for health data	√	✗	√	√	√	√	√	Immutable, cryptographic algorithms and memory management helps manage leaked data.	Paper-based records are easily lost, slow rate, low memory.
Fan et al. [19]	2018	To strengthen efficient and secured health record sharing with a blockchain network.	√	√	√	√	√	√	√	Record management and sharing from EMR systems, and access mechanism.	Miners higher computation power leads to down system.
Wang and Song [20]	2018	To provide a secured EHR system with cloud-based help of attribute-based cryptosystem and blockchain.	✗	√	√	√	√	√	✗	Identity-based encryption to encrypt database, ensures integrity and traceability.	Deployment is yet to be complete.
Guo et al. [21]	2018	To propose a secure ABE scheme with multiple authorities for blockchain in EHRs	✗	√	√	√	√	√	√	Immutability of the information ledger.	Interoperability, privacy.
Uddin et al. [22]	2018	To explore continuous patient monitoring with a patient centric agent.	√	√	√	√	√	√	√	Lightweight encryption and authentication, tamper proof, and protection against single point of failure.	End-to-end delay.
Sun et al. [23]	2018	To propose a decentralizing attribute-based signature for healthcare using blockchain.	✗	√	√	√	✗	√	√	Verifiable, secure sharing of large-scale and distributed EHR, anonymity, and non-repudiation.	Attribute certificates, storage capacity.
Poslad and Poslad [24]	2018	To suggest access policy to EMR based systems using blockchain.	√	√	✗	√	✗	✗	✗	Finer granular control	Theoretically proven.
Yang and Li [25]	2018	To design architecture for secure EHR based on blockchain.	√	√	✗	√	✗	✗	✗	Secure records model.	Implementation.
Thakkar et al. [26]	2018	To evaluate blockchain platform performance and optimization.	✗	√	✗	✗	✗	√	√	Ability to simulate network performance.	Scalability.
Sukhwani et al. [27]	2018	To develop a permission-based blockchain platform.	√	√	✗	√	✗	√	√	Identified permission blockchain integrity.	Scalability.
Gorenflo et al. [28]	2018	To scale a blockchain network using fabric.	√	√	✗	√	✗	√	√	Demonstrable capability of blockchain network.	Increased computing power needed.
Chen et al. [5]	2019	To design a searchable encryption for EHR using blockchain.	√	√	√	√	√	√	√	Security analysis with searchable encryption algorithm.	Scalability.
Proposed approach	2019	To design and propose an efficient blockchain-based EHR sharing system with enhanced security and privacy.	√	√	√	√	√	√	√	Permission-based EHR system with cryptography key, Design access control policy algorithm with smart contract, Achieves performance optimization of the system.	-

1 : Architecture 2 : Access control policy 3 : Algorithms 4 : Encryption key 5 : EHR sharing system 6 : Framework 7 : Performance evaluation.

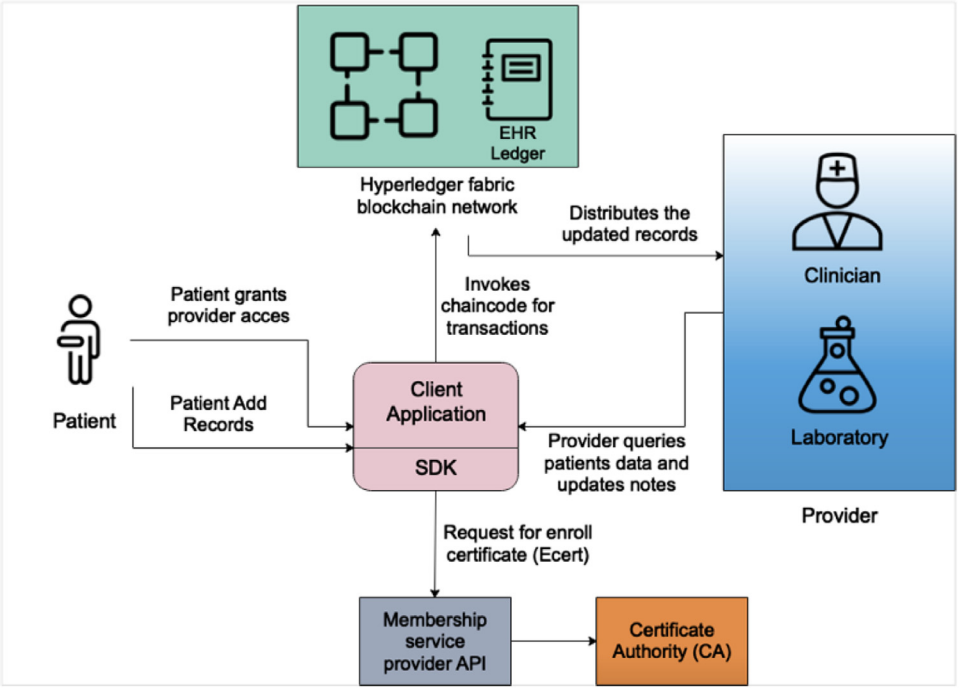

Fig. 1. System architecture.

only access records that they have been granted access. Patients can add records using the client application, which invokes the chaincode for committing a transaction to the network. After committing the transaction into the blockchain network, the updated transactions are distributed over the network; this ensures that every transaction over the network is distributed to every participant in the system and that each transaction cannot be modified or deleted by unauthorized users. Transactions are only added to the previous hash with a timestamp, so the network is fully secure.

Records are updated and visible to every user in the blockchain network. The providers, like clinicians and laboratory staff, can query required data over the network. If the patient grants access to view and update their records into the EHR ledger network, then the clinician or laboratory participant can view and update whenever needed for permission records of the patients.

3.2. Proposed algorithms

The EHR sharing system has four types of participants, including admin, patients, clinicians, and laboratory staff. The precise execution of admin in a blockchain network is shown in Algorithm 1. The enrolment certificate of admin is requested from the certification authority. The admin has full access to the system, including write, read, update, and removal of participants. If clinicians, patients or laboratory staff are valid, then admin is able to issue a relevant ID to each participant for enabling access to the blockchain network. If the behavior of the participant is found to be inappropriate, then admin can remove that participant with a remark over the hyperledger blockchain network. Table 2 lists all acronyms used in the algorithm.

The systematic execution of the patient module is shown in Algorithm 2. In this, the patient node requests a private key for login to the network administration. After being granted access to the blockchain network, the patient has various rights, such as read, write, and revoke EHR records. This procedure for the patient node uses its identification to the blockchain network. If the patient has a valid node, then patient, clinician, and laboratory staff records can be viewed or searched over the network. If M_{PID} is in a patient's hyperledger network, then M_{PID} can grant access to the clinician node for reading and updating the medical records in the

Algorithm 1 Algorithm on Admin Working.

Input: Enrolment Certificate (E_C) requested from Certification Authority (C_A)
Output: Access to P_{HL}, C_{HL} and L_{HL} transactions for all (P_{HL}, C_{HL}, L_{HL}) ϵ B_N
Initialization: N_{Admin} should be valid node. N_{Admin} can Write/Read/Update/Remove nodes C_{ID}, P_{ID}, L_{ID}

```
1: procedure ADMIN( P_ID, C_ID, L_ID)
2:     while (True) do
3:         if (C_ID is valid) then
4:             Add_Clinician to the blockchain Network
5:             Add_Clinician(B_N, C_ID)
6:             Grant_access(C_ID, U_Name, P_K)
7:         else
8:             Not_exist(C_ID)
9:         end if
10:        if (P_ID is valid) then
11:            Add Patient to the blockchain Network
12:            Add_Patient(B_N, P_ID)
13:            grant_access(P_ID, U_Name, P_K)
14:        else
15:            Not_exist(P_ID)
16:        end if
17:        if (L_ID is valid) then
18:            Add Lab to the blockchain Network
19:            Add_Lab(B_N, L_ID)
20:            grant_access(L_ID, U_Name, P_K)
21:        else
22:            Not_exist(L_ID)
23:        end if
24:    end while
25:    int N; {0 means bad behaviour, 1 means good behaviour}
26:    for all („) do
27:        if (behaviour_node(N) then
28:            Not update(C_ID, P_ID, L_ID)
29:        else
30:            Remove_update(C_ID, P_ID, L_ID)
31:        end if
32:    end for
33: end procedure
```

Table 2
Abbreviations.

P_{HL}	Patient hyperledger
C_{HL}	Clinician hyperledger
L_{HL}	Lab hyperledger
N_{Admin}	Network admin
B_N	Blockchain network
C_{ID}	Clinician ID
P_{ID}	Patient ID
L_{ID}	Lab ID
P_K	Private key
U_{Name}	Username
P_{REC_I}	Patient records
M_{PID}	Medical records of patient

Algorithm 2 Algorithm on Patient Working.

Input: I_D and key requested from N_{admin}
Output: Get access to P_{HL} transactions
Initialization: P_{HL} should be valid node. P_{HL} can Read/Write/Grant/Revoke EHR records.

```
1: procedure PATIENT(P_ID)
2:     while (True) do
3:         if (P_ID ∈ B_N) then
4:             if (P_REC_I not B_N) then
5:                 Create_records(P_ID, P_REC_I, B_N)
6:             else
7:                 Update_records(P_ID, P_REC_I, B_N)
8:                 Read_records(P_ID,P_REC_I, C_ID, L_ID, B_N)
9:             end if
10:        else
11:            Not_exist(P_ID)
12:        end if
13:        if Visit(P_ID, C_ID, L_ID, B_N) then
14:            M_PID = Medrecord(P_ID)
15:            if then M_PID ∈ P_HL(B_N)
16:                Grant_records(M_PID, C_ID, L_ID, B_N)
17:            else
18:                (C_ID, L_ID) ← NOTIFY("Medical record does not exist")
19:            end if
20:            if (M_PID ∈ C_ID, L_ID Treatment_completed(P_ID)) then
21:                Revoke_records(M_PID, P_REC_I, C_ID, L_ID,B_N)
22:            else
23:                (C_ID, L_ID) ← NOTIFY("P_ID voluntary revoke M_PID")
24:                Revoke_records(M_PID, P_REC_I, C_ID, L_ID,B_N)
25:            end if
26:        else
27:            Not Visit
28:        end if
29:    end while
30: end procedure
```

blockchain network. Step 17 suggests that if the medical records are not available, then the system should notify the clinician that the medical history of such patient is not found. After that, the patient can revoke access from the laboratory staff member or clinician in the network after the treatment is completed or if the patient does not want their data to be shared. Step 20 suggests that if M_{PID} is in the clinician or laboratory staff hyperledger network, then the patient can revoke access using calling method to revoke in the blockchain network. Otherwise, the patient can notify the clinician or laboratory staff by voluntary revoking access and then using calling method to revoke.

The precise working of the clinician module is depicted in Algorithm 3. In the input step, the clinician requests a key from the network admin to enable login. In the output phase, the clinician is granted access for clinician hyperledger transactions. The node should be a valid node. If C_{ID} belongs to the blockchain network, then patientś medical records are granted to the clinician. The clinician is then able to read and update the permissioned EHR in the system. If the clinician does not have accessed to the patientś IDs then they can write records in the hyperledger network. A clinician can also search available clinicians and laboratory staff over the network.

Algorithm 3 Algorithm on Clinician Working.

Input: I_D and key requested from N_{admin}
Output: Get access to C_{HL} transactions
Initialization: C_{HL} should be valid node. C_{HL} can Read/Write Permissioned EHR records by the patients and write medical records of the patients.

```
1: procedure CLINICIAN(C_ID)
2:     while (True) do
3:         if C_ID ∈ B_N) then
4:             if (Granted M_PID ∈ C_ID then
5:                 Read_records(C_ID, P_REC_I, M_PID, B_N)
6:                 Update_records(C_ID, P_REC_I, M_PID, B_N)
7:             else
8:                 Write_records(C_ID, M_PID, B_N)
9:                 Read_records(C_ID, L_ID, B_N)
10:            end if
11:        else
12:            Not_exist(C_ID)
13:        end if
14:    end while
15: end procedure
```

The systematic execution of lab working is shown in Algorithm 4. In this, laboratory staff request the private key from the network admin. In the output of the input request, if the node is found to be valid, then access is granted over the hyperledger network. The working of the lab node is similar to the clinician node. The lab node can read medical records and write a report on the results from patientś testing, such as blood or immunity reports, etc. This node can also search all available laboratory staff and clinicians over the network.

Algorithm 4 Algorithm on Lab Working.

Input: I_D and key requested from N_{admin}
Output: Get access to L_{HL} transactions
Initialization: L_{HL} should be valid node. L_{HL} can Read/Write Permissioned EHR records by the patients.

```
1: procedure LAB(L_ID)
2:     while (True) do
3:         if L_ID ∈ B_N) then
4:             if (Granted M_PID ∈ L_ID then
5:                 Read_records(L_ID, P_REC_I, M_PID, B_N)
6:                 Write_reports(L_ID, P_REC_I, M_PID, B_N)
7:             else
8:                 Read_records(L_ID, L_ID, B_N)
9:             end if
10:        else
11:            Not_exist(L_ID)
12:        end if
13:    end while
14: end procedure
```

3.3. Deployment phase

The blockchain-based framework, called hyperledger fabric, and its sandbox, called hyperledger composer, are used to develop the proposed electronic health record system. Hyperledger project is the open source permission based Distributed Ledger Technology (DLT). It was developed by Linux foundation to support various smart contracts and logic for implementing multiple applications in the blockchain network. Hyperledger composer is a sandbox in which the smart contract can be performed and tested through visualization of the network. It is a permissioned and consortium-managed blockchain, meaning that all participants are known to each other, so that the network is fully trusted and secure. This framework is not domain specific and hence, supports Java, Go, Node.js, etc. for developing contracts and business networks. It also

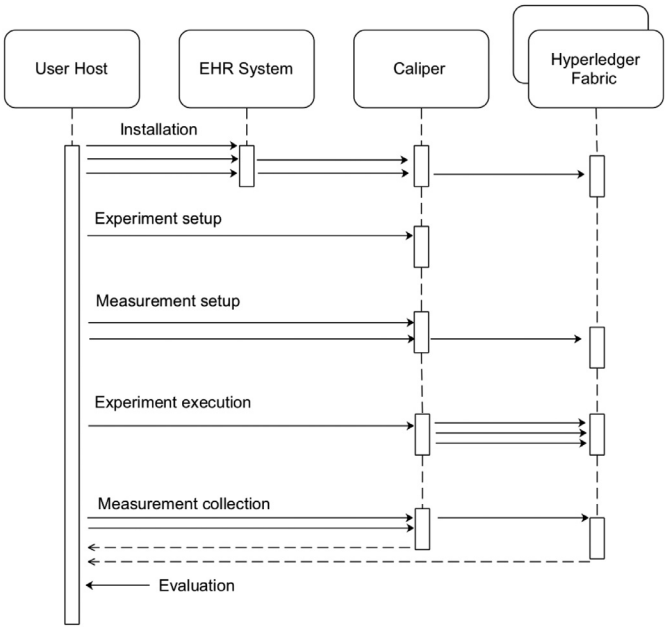

Fig. 2. Framework workflow.

provides secure interaction between different participants and organizations that use the Crase Fault Tolerance (CFT) and Byzantine Fault Tolerance (BFT) consensus mechanism that do not require more cost for mining.

To work with hyperledger fabric and composer, "Docker" is utilized for setup and initialization. Docker is an operating system level container, which can be used by a developer and/or system administrator. It is useful for creating, deploying and running hyperledger-based applications or business networks in the container. It allows the developer to package-up all dependencies and functionalities into one container. By using docker, the hyperledger fabric and composer network can run inside the container.

3.4. Measurement phase

In this phase, the whole framework is organized into a network. Fig. 2 depicts that the main host has a flow of installation of the developed or experimental system with hyperledger dependencies. During preparation, the host's role is to execute the EHR system that is connected to the caliper tool hyperledger environments. During the second phase, the primary host setup of the experiment takes place with the caliper framework. After that, the setup of measurement is held to the caliper and hyperledger hosts. During measurement, all nodes are monitored by installing Wireshark that captures the packets with tcpdump and synchronized local loopback server of the docker container. Through use of the Wireshark network performance tool, the response trip time of the network, TCP pcap file, etc. are measured and monitored. By generating the pcap file, all the visibility of the packets and network nodes are complete. Hyperledger fabric consists of peers, orderers and Certificate Authority (CA).

After the measurement is completed, an experiment execution has taken place with caliper and hyperledger environments executed in virtualization of the node using Docker. With the configuring of the pre-measurement script, the various experiments are performed in the caliper. The measurement collection is retrieved from the hyperledger caliper, including all transaction data. After all these steps are complete, the evaluation of the system takes place.

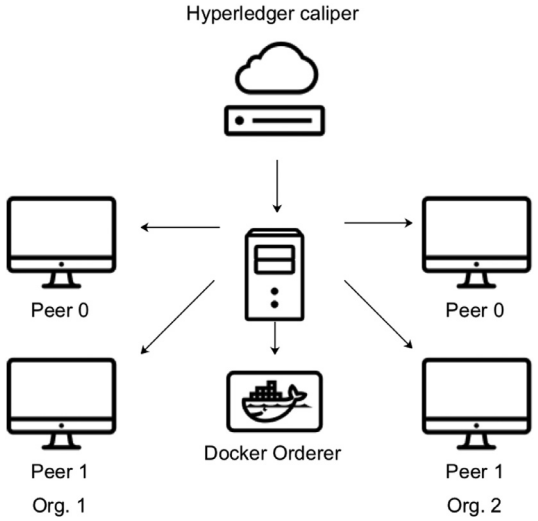

Fig. 3. Network structure.

3.5. Evaluation phase

3.5.1. Pre-processing

Evaluation is critical to check system performance and scalability in a directed way. It begins with the pre-processing stage. All network traffic can be obtained with the help of the Wireshark pcap file. This analyzes all network traffic that filters only for TCP messages that are transmitted with hyperledger fabric. In the framework, all communication is done via a gRPC protocol - this runs on the top of the TCP.

3.5.2. Reporting

Evaluation is achieved using spyder IDE which runs on anaconda navigator. It uses matlablib which allows the drawing of statistical data. It also imports pandas3 that offers data analysis and transformation of data. The python3 programming language is used for creating graphs in the evaluation phase. Network data is also taken into account via the Wireshark tool and saved in the pcap file, which reads all TCP packets, sending times, source port and destination port. All the network IPs are replaced with the node naming of the hyperledger caliper and peer organization for better visualization. The caliper report file of HTML contains all the transactions that are performed during evaluation, such as transaction send rate, throughput, latency, organizations, peers, max CPU usage, and memory usage, which are extracted and then processed for transformation. Data is then visualized via matlablib in various viewpoints.

For the evaluation of the system, various experiments are described to demonstrate the capability of the EHR system, providing insights into the benchmarks of the Hyperledger Fabric. In this study, multiple use cases are simulated, including one organization - one peer, two organizations - one peer, three organizations - one peer, two organizations - two peers and three organizations - two peers. Each organization has various ledger peers in the network which are used for carrying a copy of the ledger. A single orderer host is responsible for the creation of blocks, while the Caliper host executes the workloads. Thus, every host is a part of the star topology and carries out the following measurements and evaluation, as shown in Fig. 3.

4. Performance analysis

In this section, the evaluation of the proposed system is described with simulation settings and evaluation metrics. The dis-

cussion on obtained results by varying parameters like block size, endorsement policy, block creation time, etc. is also presented. Results are shown concerning performance latency, throughput, by network capturing, etc. Different scenarios with varying configuration are visualized through graph plot.

4.1. Simulation settings

Hyperledger caliper is a benchmarking tool that is used for the blockchain network. It supports various hyperledger frameworks, such as fabric, composer, sawtooth, iroha, etc. In this paper, caliper tool is used to verify and execute the performance of the system and its various parameters, including latency, throughput, CPU usage, memory consumption, disk write/read, network I/O, etc., and metrics for the evaluation of the system. The configuration parameters are modified as per assessment, such as block size, block time, endorsement policy, channel, resource allocation, and ledger database etc. The simulation PCs have the following configurations:

- 2 Core CPU (Intel Core i5 1.3GHz (Turbo Boost up to 2.6GHz) with 3MB shared L3 cache)
- 4GB memory
- 1 Gbit/s network
- 120GB SSD

4.2. Scenario 1: Basic experiment

Various observations are taken into account for understanding and evaluating the hyperledger platform of blockchain technology. The first experiment is conducted under different measurements and executed in five rounds of writing the transaction into the network of the ledger with 1000 transactions in each round at few rates of 50, 100, 150, 200, 250 transactions per second.

The transaction time gives the performance of the blockchain network. Fig. 4(a) shows different lines that contain the time taken to successfully complete the transactions in the unusual configuration of the network.

1org1peer, 2org1peer, 2org2peer depict different performances of transactions. The results are taken on five rounds and each round has 1000 transactions with different rates tps. The 1org1peer takes 140s to reach 5000 transactions. Similarly, 2org1peer reaches 3000 transactions, and 2org2peer reaches only 2000 transactions in 140s. It is, therefore, clear that with the increase in organizations and peers, the time needed to execute transactions increases.

In the mathematical formula of transaction latency. Suppose, T_L is transaction latency that is time taken for using the network. C_T is the confirmation time for the transaction, and changes with network threshold N_T. S_T is submit time for the transaction in the blockchain network as given in Table 3.

$$\text{Transaction latency } T_L = (C_T * N_T) - S_T$$

The average latency of the performance testing using caliper report is shown in Fig. 4(b). In this figure, latency is measured in seconds. It depicts the latency of the communication and writing transactions success rate. 1org and 1peer have much less latency as compared to 2org1peer and 2org2peers. In various rounds, when transaction rate increases, then latency time also increases. More organizations and more peers show higher latency. The low latency is a result of higher throughput. Therefore, latency and throughput are inversely proportional. In the mathematical formula of transaction throughput, suppose, T_T is transaction throughput that is success rate of the transaction with defined tps. T_{CT} is the transaction committed on the entire network. The invalid or failed transactions are subtracted with total transactions time T_{TS} at many committed nodes N_{CN}.

$$T_T = T_{CT}/T_{TS} * N_{CN}$$

Fig. 4(c) depicts the throughput against transaction rates. The throughput is taken against 1org 1peer, 2org 1peer, 2org 2peers. The throughput reaches the highest 70 tps in 1org 1peer network

Table 3
Basic measurement.

Parameter	Configuration
Rounds	5
Transactions	1000 per round
Transactions mode	Write
Rate	50 to 250 tps
Varied Factor	–

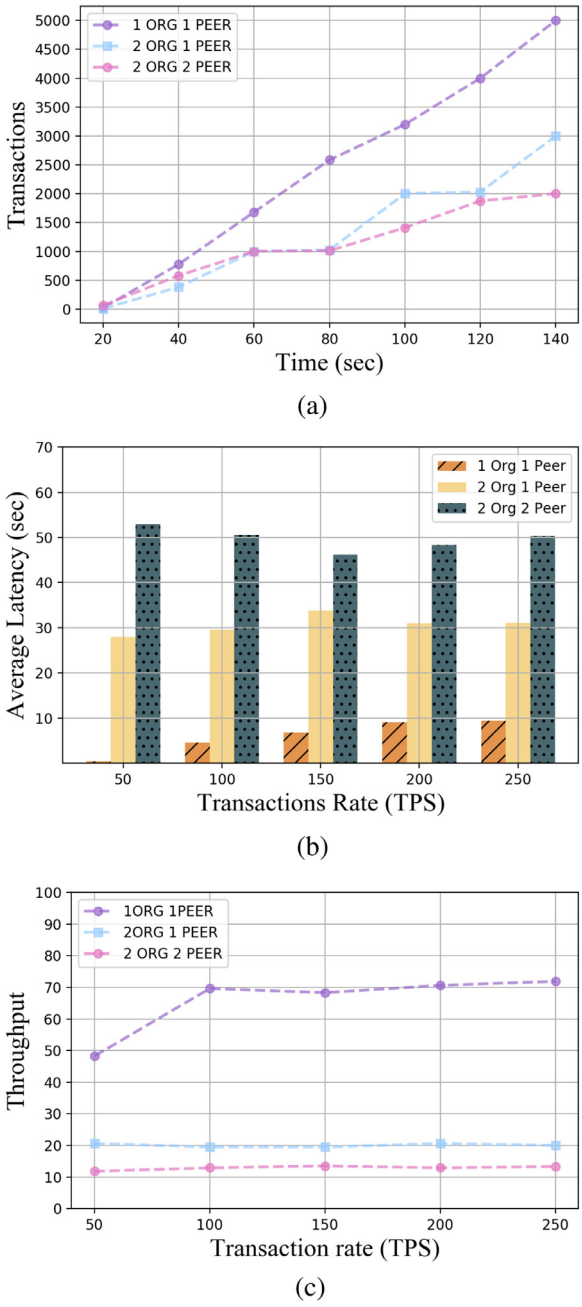

Fig. 4. (a) Transactions commit time, (b) Transactions average latencies (c) Transactions throughput.

Table 4
Calculation with varied transaction mode.

Parameter	Configuration
Rounds	3
Transactions	1000 per round
Transactions mode	Read
Rate	100, 200, 250 tps
Varied Factor	–

settings, while 2org 1peer and 2org 2peer decreases the throughput to 20 tps, and 10 tps, respectively. This shows higher latency and gives the communication gaps to achieve better performance.

4.2.1. Measurements with varying transaction mode of querying the transactions are as follows

In this measurement of the hyperledger caliper, there are three rounds taken to perform a test. In the configuration file, the transaction mode is changed to read state with 100, 200, 250 tps rate.

In the mathematical formula of reading transaction latency, suppose, R_L is reading latency; that is time taken for a reading request submitted and its reply on the network. S_T is submit time and R_R is a time when the response is received as shown in Table 4.

Read latency $R_L = R_R - S_T$

In the mathematical formula of reading transaction throughput, suppose, R_T is reading throughput. This is measured as the total number of reading operations achieved in various time intervals or seconds. R_O is the total number of reading operations, and T_T is the total time in the second format.

Read throughput $R_T = R_O - T_T$

After measuring the writing of transactions, querying of the transactions with different network sizes are shown in Fig. 5(a). In this, as compared to the writing of transactions, querying of the transaction is much faster. Fig. 5(a) shows lower transaction latency. In this, for higher network size simulation of 2org 2peer, the average latency is maximum only 12s, as compared to the writing of transaction having a maximum of 50s in various rounds. It is therefore clear that querying the transaction on the blockchain network is much faster than writing a transaction.

Fig. 5(b) shows a higher throughput compared to previous writing transaction throughput. The querying transaction, mode achieves the near about 50% of higher throughput compared to writing mode.

4.2.2. Evaluation of resource consumption on various nodes

For resource consumption, when executing caliper testing for the network, various parameters are measured such as average CPU consumption, memory, incoming traffic, outgoing traffic, disc read/write, etc. Fig. 6 depicts various peers, while orderer CPU consumption is shown. In this, the 2org 1peer network size is used for evaluation. Here, orderer has the minimum CPU consumption, but the outgoing traffic from the node is about 15MB per second in different rounds of the test.

Multiple peer nodes having different traffic and consumption of memory and CPU are shown in Table 5.

4.2.3. Wireshark tcpdump network traffic statistics

The network traffic and its statistics are captured during the execution of the caliper on the EHR system using the Wireshark tcpdump. In this, during execution, the packets are captured using Wireshark and saved in a pcap file. The outgoing network traffic is shown in Fig. 7 with the execution time of the evaluation. The max packets per second are achieved at 800 packets/s.

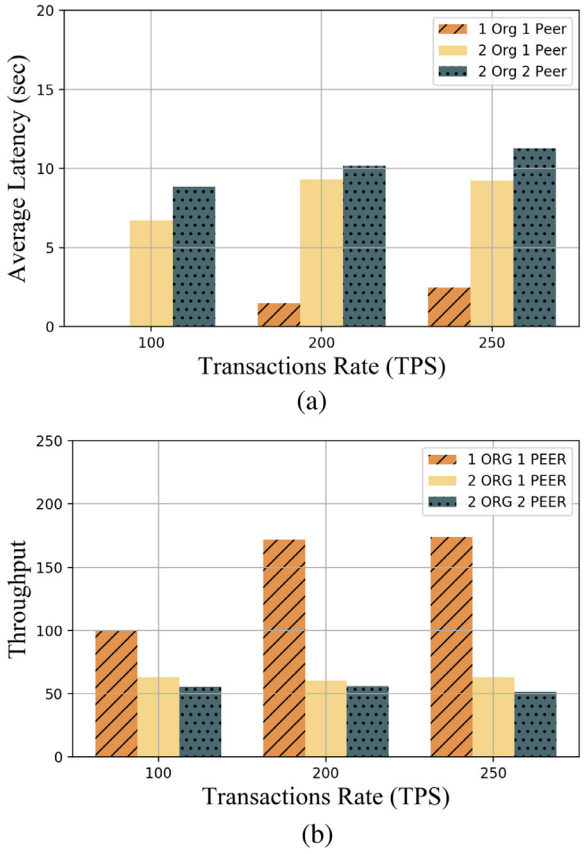

Fig. 5. (a) Calculations with querying transaction latencies, (b) Calculations with querying transaction throughput.

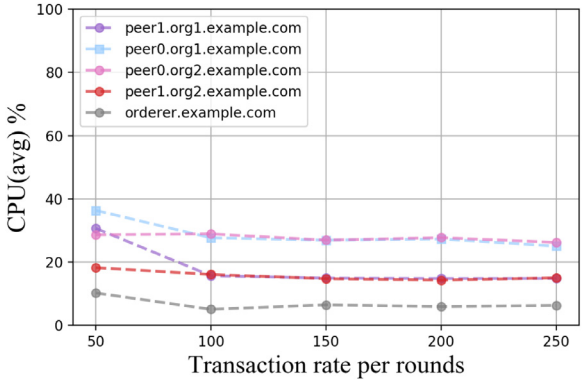

Fig. 6. Resource consumption.

The measured network statistics are shown in Table 6. In this, various measurements such as packets, time span, average pps, size, etc. are taken into account. There are 49,275 packets captured in the execution of the 2 org 1 peer scenario.

4.3. Scenario 2 : Experiment with varying block time

In this experiment, the optimization of the network is performed. Varying the measurement of block creation time in configuration of the hyperledger caliper for EHR system achieves varying results. Table 7 shows the configuration of the caliper that is used for the experiment.

Fig. 8(a) shows the transaction latency of the 2 org 2peer network configuration. Here, for achieving minimum latency, the optimization metrics were considered. After increasing the endorse-

Table 5
Resource consumption of various parameters.

Type	Name	Memory(avg)	CPU(avg)	Traffic In	Traffic Out	Disc Write
Docker	peer1.org1.example.com	276.0MB	15.70%	4.3MB	440.4KB	6.2MB
Docker	peer0.org1.example.com	207.5MB	27.70%	6.6MB	3.5MB	6.2MB
Docker	peer0.org2.example.com	206.0MB	28.93%	6.6MB	3.6MB	6.2MB
Docker	peer1.org2.example.com	224.1MB	16.10%	4.3MB	439.0KB	6.2MB
Docker	orderer.example.com	59.9MB	5.07%	3.9MB	15.5MB	4.6MB

Table 6
Network statistics of 2org 2peer.

Measurement	Captured
Packets	49,275
Time span, s	286.907
Average pps	171.7
Average packet size, B	1202
Bytes	59,231,147
Average bytes/s	206 k
Average bits/s	1651 k

Table 7
Varied block time measurement.

Parameter	Configuration
Rounds	5
Transactions	1000 per round
Transactions mode	Write
Rate	50 to 250 tps
Network size	2Org 2Peer
Varied Factor	Block Time
Endorsement Policy	2 of : {signed-by: {0, 1}}

ment policy block creation time, the caliper results default into block time. The result shows 1.5x decrease in the latency of the network, which helps to increase the performance of the EHR system. For transaction rate of 50 having the minimum latency of about 27s which is down from about 52s. For 250 tps having 37s which is also down from the 50s. This is an achievable performance of the system by modifying the default network configuration of the hyperledger.

Table 8
Varied block time measurement with reading mode.

Parameter	Configuration
Rounds	3
Transactions	1000 per round
Transactions mode	Read
Rate	100, 200, 250 tps
Network size	2Org 2Peer
Varied Factor	Block Time
Endorsement Policy	2 of : {signed-by: {0, 1}}

The transaction throughput is shown in Fig. 8(b). It depicts the varying block time with the policy of the network giving better throughput and performance with respect to committing time and success rate of the transaction. By combining optimization overall throughput, it improved by 1.75x for 50 to 250 tps.

4.3.1. Read transactions with varying block time

The read transaction mode is used to read the received transaction with a defined time interval. Table 8 shows the configuration of the read transaction. For achieving the better performance of the system, endorsement policy and block time for transaction reading are modified in the network.

The optimization of the blockchain with varying block times for creation is beneficial in the reading or querying of transactions. The optimized performance is shown in Fig. 9(a) with transaction rate and its latency. In terms of optimization, the latency of the system is decreased by 40%, which are achievable results for the overall network performance. The average latency of default 250ms block time is 9s and modifying policy and block time by 2s has only a 4s latency. For max tps of 250 having a default block time

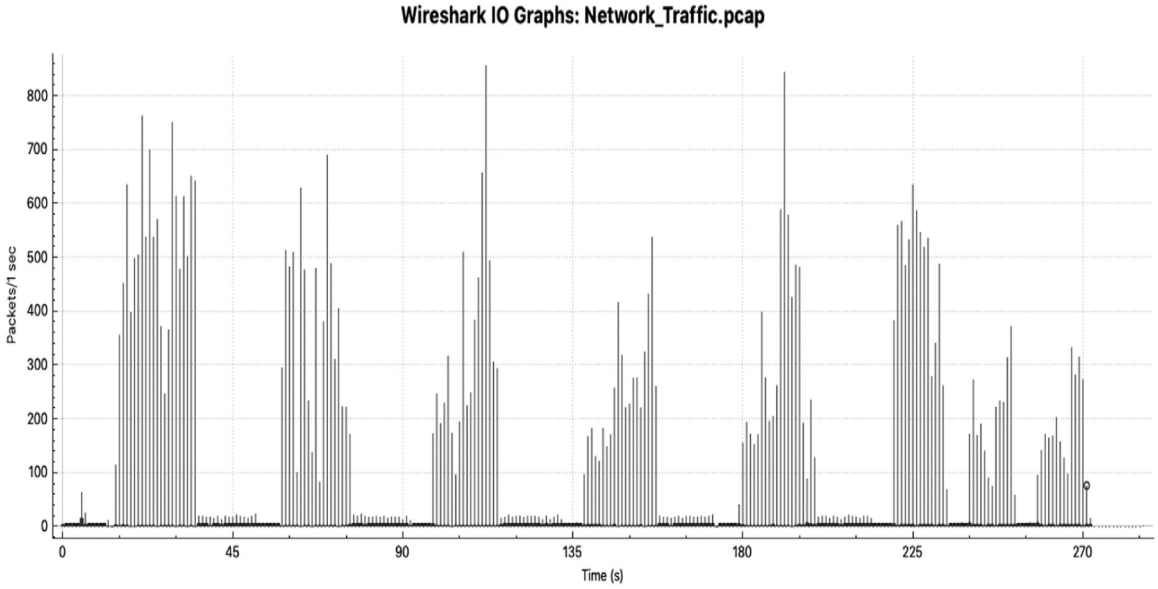

Fig. 7. Network traffic.

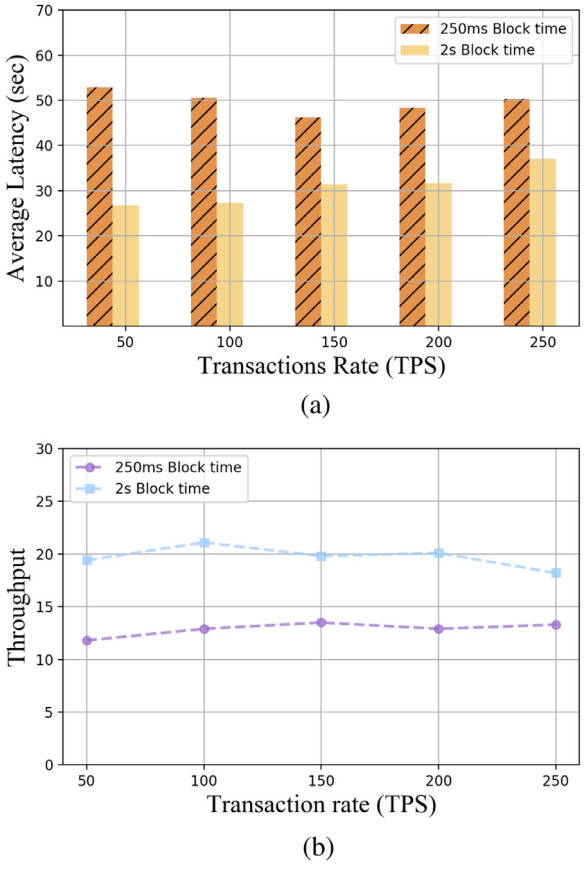

Fig. 8. (a) Transaction latencies with varying block time, (b) Transaction throughput with varying block time.

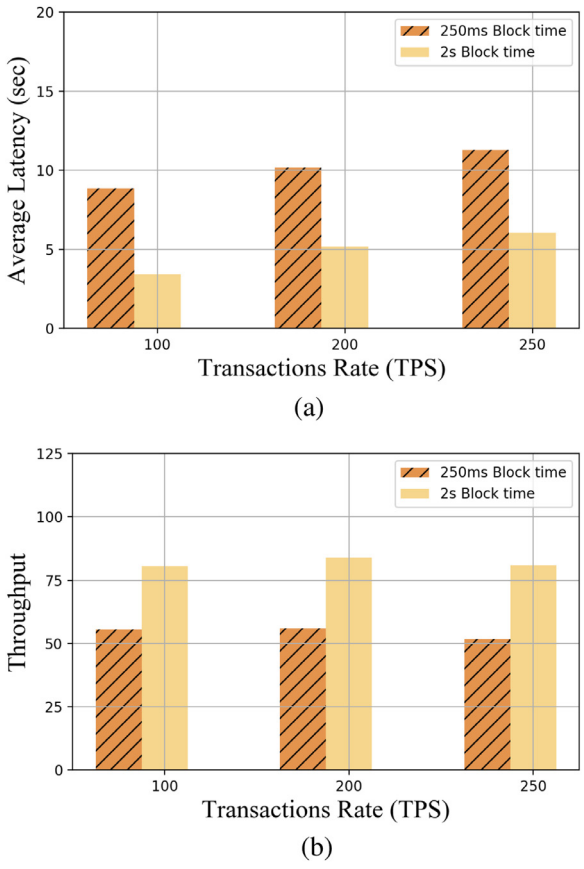

Fig. 9. (a) Querying transaction latencies with varying block time, (b) Querying transaction throughput with varying block times.

Table 9
Varied block size measurement with reading mode.

Parameter	Configuration
Rounds	5
Transactions	1000 per round
Transactions mode	Write
Rate	50 to 250 tps
Network size	2Org 2Peer
Varied Factor	Block size with transaction rate
Endorsement Policy	2 of : {signed-by: {0, 1}}

is 13s and with the updated configuration it decreases to 6s of the read latency.

As commonly understood, latency is inversely proportional to throughput and hence, the read throughput is increased with updating configuration of the block time and policy. Fig. 9(b) shows that for 100 tps, transaction throughput is increased from 52 to 78 and also for max tps of 250 having achieved performance from 50 to 73 throughput for the transaction over the blockchain network. We can therefore conclude that the read throughput is improved by 1.5x.

4.4. Scenario 3: Experiment with varying block sizes

In this third scenario, varying max transaction limits per block size in the caliper configuration file is shown to affect the endorsement policy with different transaction rates. In this analysis, varying block sizes into half of its default size and its different transaction rates are taken into account for achieving optimization in the blockchain network.

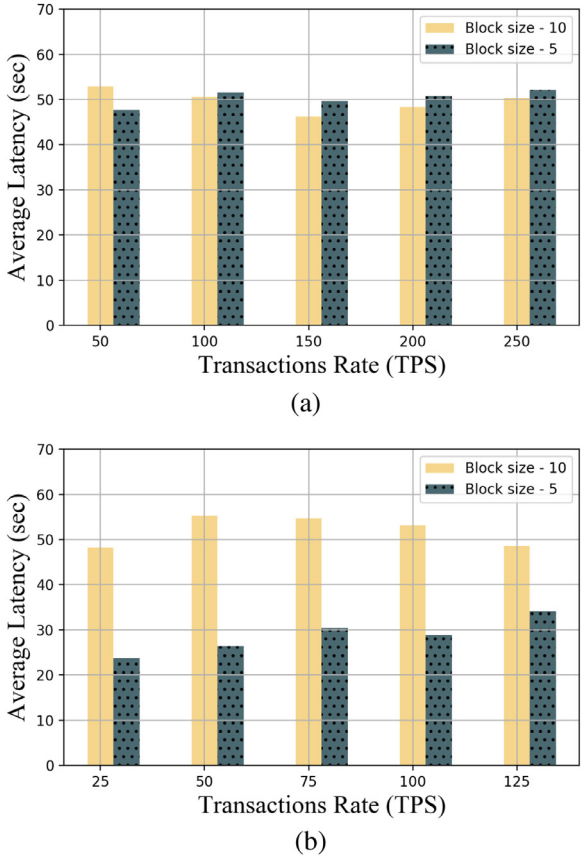

Fig. 10. (a) Transaction latencies with varying block size for higher TPS, (b) Transaction latencies with varying block size for lower TPS.

In the blockchain network, the block size is an important parameter for the performance of the system. For the first experiment with modifying size of block, this is shown in Fig. 10(a). Here, the maximum transaction per second rate is taken, such as 50, 100, 150, 200, 250. The evaluation is done on block size 10 and 5. The result of the evaluation does not affect the latency of the committed transaction. Block size 10 has a marginally lower latency than block size 5 as shown in Table 9.

After modifying the block size in the previous experiment, configuring block size with a lower transaction rate shows more improved results, as shown in Fig. 10(b). Here, the minimum transaction per second rates are taken with 25, 50, 75, 100, 125. By using this configuration, block size 5 has improved results by about 1.75x of lower latency time. Similarly, an improved transaction throughput of nearly 1.75x is observed.

Through experimentation, it is observed that lower Transactions Per Second (TPS) on smaller block sizes result in improved performance of the system. Similarly, a higher Transaction Rate (TPS) on a larger block size results in enhanced performance of the blockchain system.

5. Conclusion

The use of blockchain in healthcare systems plays a critical role in the current healthcare market. It can result in automated data collection and verification processes, correct and aggregated data from various sources which are immutable, tamper resistant and provide secured data, with reduced probability of cyber crime. It also supports distributed data, with redundancy and fault tolerance of the system. In this paper, current challenges faced by the healthcare industry are discussed. We propose a system architecture and algorithm for access control policy for participants to achieve privacy and security for patient data in the EHR system. Also, the implementation of a EHR sharing system, based on the blockchain network is given. The proposed work eliminates the central authority and a single point of failure in the system. System security is achieved through immutable ledger technology as any user cannot modify the ledger. Performance evaluation of the proposed system is completed using the caliper for various scenarios by configuring block size, block creation time, endorsement policy and proposed optimization for evaluation metrics, such as latency, throughput, and network security for obtaining better results. By optimizing the performance of the proposed system, it is improved by 1.75x and latency is decreased by 1.5x. This shows the blockchain capability and importance in various areas and proves that it could be the next revolutionary technology for replacing current healthcare systems.

Declaration of Competing Interest

There is no Conflict of Interest.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2019.102407.

References

[1] Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for healthcare 4.0 environment: opportunities and challenges. Comput Electric Eng 2018;72:1–13.

[2] Vora J, DevMurari P, Tanwar S, Tyagi S, Kumar N, Obaidat M. Blind signatures based secured e-healthcare system. In: 2018 International conference on computer, information and telecommunication systems (CITS); 2018. p. 1–5.

[3] Kumari A, Tanwar S, Tyagi S, Kumar N, Parizi RM, Choo K-KR. Fog data analytics: a taxonomy and process model. J Netw Comput Appl 2019;128:90–104.

[4] Vora J, Italiya P, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Ensuring privacy and security in e-health records. In: 2018 International conference on computer, information and telecommunication systems (CITS); 2018. p. 1–5.

[5] Chen L, Lee WK, Chang C-H, Raymond Choo K-K, Zhang N. Blockchain based searchable encryption for electronic health record sharing. Fut Gener Comput Syst 2019;95:420–9.

[6] Hathaliya JJ, Tanwar S, Tyagi S, Kumar N. Securing electronics healthcare records in healthcare 4.0 : a biometric-based approach. Comput Electric Eng 2019;76:398–410.

[7] Shae Z, Tsai JJ. On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th international conference on distributed computing systems (ICDCS); 2017. p. 1972–80.

[8] Mistry I, Tanwar s, Tyagi S, Kumar N. Blockchain for 5g-enabled IoT for industrial automation:a systematic review, solutions, and challenges. Mech Syst Signal Process 2019;135:1–19.

[9] Kabra N, Bhattacharya P, Tanwar S, Tyagi S. Mudrachain: blockchain-based framework for automated cheque clearance in financial institutions. Fut Gener Comput Syst 2020;102:574–87.

[10] Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Bheem: a blockchain-based framework for securing electronic health records. In: 2018 IEEE globecom workshops (GC Wkshps); 2018. p. 1–6.

[11] Alhadhrami Z, Alghfeli S, Alghfeli M, Abedlla JA, Shuaib K. Introducing blockchains for healthcare. In: Electrical and computing technologies and applications (ICECTA), 2017 international conference on; 2017. p. 1–4.

[12] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for ehealth data access management. In: Advances in biomedical engineering (ICABME), 2017 fourth international conference on; 2017. p. 1–4.

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

[14] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. IEEE Access 2016;4:9239–50.

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

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

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

[18] Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. J Med Syst 2018;42(8):141.

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

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

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

[22] Uddin MA, Stranieri A, Gondal I, Balasubramanian V. Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access 2018;6:32700–26.

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

[24] Zhang X, Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: 2018 IEEE International conference on communications (ICC); 2018. p. 1–6.

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

[26] Thakkar P, Nathan S, Viswanathan B. 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); 2018. p. 264–76.

[27] Sukhwani H, Martínez JM, Chang X, Trivedi KS, Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: 2017 IEEE 36th symposium on reliable distributed systems (SRDS); 2017. p. 253–5.

[28] Gorenflo C, Lee S, Golab L, Keshav S. FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2019. p. 455–63.