applied sciences

MDPI

Article

A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority

Aitizaz Ali [1], Hasliza A Rahim [2,3], Jehad Ali [4,*], Muhammad Fermi Pasha [5], Mehedi Masud [6,*], Ateeq Ur Rehman [7], Can Chen [8] and Mohammed Baz [9]

[1] Department of Software Systems and Cyber-Security, School of IT, Monash University, Subang Jaya 47500, Malaysia; aitizaz.ali@monash.edu
[2] Advanced Communication Engineering, Centre of Excellence (ACE), Universiti Malaysia Perlis, Kangar 01000, Malaysia; haslizarahim@unimap.edu.my
[3] Faculty of Electronic Engineering Technology, Pauh Putra Campus, Universiti Malaysia Perlis, Arau 02600, Malaysia
[4] Department of Computer Engineering, and Department of AI Convergence Network, Ajou University, Suwon 16499, Korea
[5] Department of Software Systems and Security, School of IT, Monash University, Subang Jaya 47500, Malaysia; Muhammad.FermiPasha@monash.edu
[6] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[7] Department of Biomedical Engineering, Foundation University Islamabad, Rawalpindi 44000, Pakistan; ateequr.rehman@fui.edu.pk
[8] School of Business, Monash University, Subang Jaya 47500, Malaysia; cche0213@student.monash.edu
[9] Department of Computer Engineering, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; mo.baz@tu.edu.sa
* Correspondence: jehadali@ajou.ac.kr (J.A.); mmasud@tu.edu.sa (M.M.)

Citation: Ali, A.; Rahim, H.A.; Ali, J.; Pasha, M.F.; Masud, M.; Ur Rehman, A.; Chen, C.; Baz, M. A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Appl. Sci.* **2021**, *11*, 9999. https://doi.org/10.3390/app11219999

Academic Editor: Eui-Nam Huh

Received: 7 September 2021
Accepted: 19 October 2021
Published: 26 October 2021

Abstract: Blockchain is a promising technology in the context of digital healthcare systems, but there are issues related to the control of accessing the electronic health records. In this paper, we propose a novel framework based on blockchain and multiple certificate authority that implement smart contracts and access health records securely. Our proposed solution provides the facilities of flexible policies to update a record or invoke the policy such that a patient has complete authority. A novel approach towards multiple certificate's authority (CA) is introduced in the design through our proposed framework. Our proposed policies and methods overcome the shortcoming and security breaches faced by single certificate authority. Our proposed scheme provides a flexible access control mechanism for securing electronic health records as compared to the existing benchmark models. Moreover, our proposed method provides a re-enrolment facility in the case of a user lost enrolment.

Keywords: blockchain; access control; efficiency; security; smart contracts; certificate authority

1. Introduction

The hyperledger fabric blockchain platform can be used for cross-organizational networks and it provides pluggable modules, such as encryption, identity management, consensus protocol, and membership services. Hyperledger is a consortium blockchain network, which contains different nodes, a smart contract or chain code, and a ledger containing a state database as well as a log of transactions. The Blockchain-based digital healthcare framework, also called hyperledgerfabric, is used to develop our proposed patient health record system (PHR). The hyperledger tool, also known as the distributed ledger technology (DLT), was first launched and introduced by the Linux organization to visualize different smart contracts based implementation for various platforms and approaches in the blockchain peer-to-peer (P2P) network systems [1].

To get a visualization of the network, the hyperledger composer is used for blockchain-based framework analysis. The hyperledger composer supports the permissioned and consortium blockchain, which means that all users are familiar with each other so that the entire network is entirely trusted and secure. Hyperledger composer supports Java, Go, Node.js, and so forth, for designing contracts and business networks. Healthcare is considered an important field in the health industry. In contrast to traditional medical diagnosis, a patient's body states, including heartbeat, diabetes, temperature, and additional various patient body statuses, can be monitored through several medical tracking devices for diagnosis [1] or improvement in health quality. This leads to the ease of an enormous amount of data sharing among organizations for medical diagnosis, biomedical research, and policy design. A physician might require the best treatment decision for a patient in real-time, stored in different hospitals.

Furthermore, the healthcare industry has brought a revolution in the healthcare economy [1]. In digital healthcare, patient health-related data sharing—a key factor for success—is considered to be trusted. Any loophole in the system could result in distrust among patients towards the e-healthcare market. An individual or multiple participants can maintain and manage a node inside a network. Nodes can be classified according to the functionalities, which are listed in the following subsections.

1.1. Distributed Ledger

Distributed Ledger (DL) is used to store the data of each node. However, distributed ledgers store the current state of the BC. The BC stores duplicates of the data during transactions. DL plays a vital role in the blockchain structure. Every record has a hash value, which is stored in the form of a merkle root tree within the DL [2].

1.2. Symmetric Cryptography

When both private and public keys are the same then it is called symmetric cryptography. Whereas when both keys are unique and different it is called asymmetric cryptography. In our proposed framework, we have used asymmetric cryptography, which provides more security as compared to symmetric cryptography [2].

1.3. Consensus Mechanism

The technique in which at least 51% of the peers agree to approve a specific transaction is called a consensus algorithm. This is also called the 51% technique in the blockchain.

1.4. P2P Network

A P2P Network is the combination of physically or virtually connected computers or electronic devices without a central entity. In the absence of a central entity, the BC system runs an algorithm which is called a consensus algorithm. This consensus algorithm approves the decision taken by 51% of total nodes in a network [3]. Due to the emergence of crypto technology, such as Ethereum and Bitcoin, research related to blockchain has gained most of the attraction for researchers [4]. Blockchain has the capability to store and share data in a decentralized manner, which is immutable and trusted. BC avoids intermediate parties, and it does not require any central entity to check the transactions [5,6]. In order to achieve trust within a network and among peers, the blockchain is considered to be a less complex method for sharing PHR. It combines diverse computing powers from several nodes in the network which make it more applicable for high computational power and speed [7]. The blockchain platform provides numerous applications and processes, which include consensus Protocol, Hashing, P2P topology, Immutable Ledger, and mining. The protocols that govern the blockchain network are called smart contracts [8].

1.5. Hyperledger Fabric

Hyperledger Fabric is a blockchain tool used for a cross-organizational network that relies on Linux. It supports adjustable modules, such as encryption, identity management, and consensus protocol and membership services. The hyper-ledger is also called a consortium blockchain network. This network contains different nodes; a smart contractor chaincode, and a ledger containing a state database and a log of transactions. An individual or multiple participant can maintain and manage a node inside a network [9]. Nodes can be classified according to their functionalities. The main contributions of our paper are as following: We have proposed a novel algorithm for the cross domain blockchain framework for accessing healthcare records.

1. In this research, we have used certificate authority for the first time in the cross-domain, which provides public and private keys. It is very important that each organization must have one or two intermediate CAs;
2. We have achieved high throughput in the case of security and computational power;
3. Our proposed access control techniques are attribute based control, which is flexible enough that it can easily be adjusted for the cross domain blockchain;
4. Our novelty also falls in such a way that we have used hyperledger fabric, which supports the consortium blockchain for hospitals and in the case of both private and public healthcare systems.
5. For signature endorsement, we have introduced the ring signature, which is considered a lightweight signature and ultimately leads to more security.

The rest of the paper is organized as follows. In Section II, we provide the literature review. Section III explains the problem formulation, and the introduction of the proposed framework. In Section IV, we have illustrated the details of the proposed methodology and explained the proposed algorithms. Section V provides details for certificate authority and its formulation. In Section VI, we provide the experimental setup, dataset details, results and its discussion. Section VII concludes the paper and provides directions for future works.

Motivation

Cloud computing is regarded as a distributed and flexible storage platform that can be accessed anytime and anywhere on a demand basis. Data outsourced to the cloud can be considered insecure as the patient has no control over PHR, which potentially leads to more security threats. Security is the primary concern when dealing with medical records in the Cloud. The digital health record is one of the most valuable records potentially stored in the Cloud, which makes it more attractive for threat actors to find vulnerabilities that expose digital health records due to their value and price in the market. Regardless of current advancement in access control models and frame-works, there still exist many issues. These issues in the current approaches identified are the absence of measuring granularity in authorizing [10], and dependencies over identity, role or MAC (Mandatory Access Control)/DAC (Discretionary Access Control) schemes [11]. Currently, the access control system only relies on users' ID, role-, or attribute-based mechanisms. Through analysis and comparison, it is observed that ABE (Attribute Based Encryption) is the optimal access control model among existing access models. The Public-Key encryptions do not fulfil the security requirements for attribute based encryption. In our proposed approach, we will use the Attribute Based Signature (ABS) because it provides the anonymity of the signer [12]. The main motivation for our research is that our proposed scheme is able to provide security to the subject, and object. Moreover, to get strong PHR confidentiality, a fine-grained and flexibility is provided with user anonymity through a modified access control and a low computational cost.

2. Literature Review

In the existing system, most of the researchers also surveyed and reviewed the basic security problems in IoT (Internet-of-Things) based healthcare system. They categorized these problems depending on the low-level, intermediate-level, and high-level layers of the IoT. In the literature, the problems related to security and privacy in healthcare systems are briefly discussed to leverage the security of IoT at diverse stages. Additionally, a parametric analysis of IoT attacks and feasible remedies has been provided up to certain limits. Some of the researchers considered the attack indications and mapped them to feasible solutions suggested in the literature. They also discussed the way blockchain can be utilized for solving some relevant IoT security issues [13]. They outlined and identified security in IoT, but the role of blockchain and the importance of its security in the IoT is discussed very little. Kim et al. [14] used the blockchain as a tool for healthcare intelligence keeping in view the privacy of users. Data access control for privacy was proposed by them and devised the healthcare digital gateway. The main issue in this system is that it does not support cross organization and fine-grained access control. Jiang et al. [15] proposed a healthcare framework, based on PSN (Personal Secure Network), to secure the digital health system. The author has designed two novel techniques for the validation and allocation of clinical data within a distributed network.The overall complexity of the said framework is high and also has security vulnerabilities to attacks. Chen [16] evaluated the performance parameters in a novel way for the hyperledger fabric framework. Chakraborty et al. [17] proposed a cloud-based framework using blockchain. The author of [18] designed a prototype of a cross domain access control system in order to provide efficient security to clinical records. This system is called coarse grained access control.

In [19], the authors discuss the healthcare information exchange, and a mechanism to store and share a huge amount of data related to healthcare. Moreover, to reduce the deviation of the transaction response times, the authors of [20] propose a fairness dependent packing of data from Industrial IoT using Permissioned Blockchains. Similarly, the authors of [21] discuss the efficiency and privacy issues in blockchains using multi-keyword search over the encrypted data.

A coarse-grained access control is one that is lacking in precision. Shen et al. designed a prototype of a cross domain access control system in order to provide efficient security to clinical records. This system is called coarse grained access control. A coarse grained access control is one which is lacking in precision. In addition, a coarse grained access control framework affects the performance of an access control. Lazaroiu et al. [22], in their research work, designed a clinical data exchange system based truly on blockchain, and later developed a series verification mechanism for improved security and privacy of the systems. The authors of [23] proposed a healthcare model for data privacy in order to manage data through blockchain. Sengupta et al. [24] devised blockchain-based health information in order to provide security and privacy throughout the healthcare system. The problem with this approach was a lack of flexibility and a cross-organizational approach. Wang et al. in their proposed approach provide better security to record and share patient clinical information using an attribute-based encryption scheme. In this approach, they integrated SC to ensure the reliability and to provide a facility to monitor the PHR sensitive data. Guo et al. designed an attribute-based signature (ABS) method for clinical users in order to manage medical health records truly based on blockchain. In this technique, the objective was to achieve optimum privacy of the delivered model through a P2P technique for efficient privacy. Uddin et al. proposed a framework to monitor and trace patient history related data. This system relies on a node controlled by authorized patients in the main module of the system; through this approach, the author had better security of the system through various experiments and variation in datasets. This approach has computational overhead due to its complex mechanism for monitoring. Sun et al. devise an ABS based encryption technique scheme for an electronic health record system. They also developed a P2P-based records sharing protocol that supports algorithms. Yang et al. proposed an EHR system in order to provide security for clinical records using distributed ledger technology (DLT). Further, the author has justified an improved cross organization sharing of health records using access control policies. Honor et al. [25] designed a novel approach to measuring the efficiency of a framework using blockchain. Performance optimization regarding caching and configuration authorization policy were achieved through this approach.

Peng et al. [26] provide a detail method for the analysis and evaluation of the optimization for the provenance and performance of a blockchain framework and developed a framework by configuring it to reduce input/output. However, this approach was considered complex computationally. They achieved an enhanced performance by reducing the computation time. Last but not least, Esposito et al. [27] proved novelty in the design of the secure searchable encryption (SSE) model for electronic healthcare records using blockchain. The algorithm takes an index of healthcare records as an input and then provide a related search using SSE. Patel et al. proposed a peer to peer approach based on the privacy-preserving digital health blockchain for connecting remotely medical sensors and devices [28]. They proposed the idea of an improved blockchain framework appropriate for IoT devices. This proposed framework of these authors works in a distributed environment to provide more privacy to a clinical system. In summary, the authors aimed to provide a solution to the issues related to blockchain using IoT devices. The problem with Kim et al. [29] is that its security and computational cost are high and its performance is poor in the case of security breaches such as collusion and phishing attacks. Hang et al. [30] proposed a blockchain-based method to facilitate verification of 5G networks. This method was based on software defined networking (SDN). The main advantage of this technique is that they eliminate the cost of re-authentication when devices usually exchange in between cells in 5G networks. Figorilli et al. proposed a peer to peer approach based on privacy-preserving digital health blockchain for connecting remotely medical sensors and devices [31]. They proposed the idea of an improved blockchain framework appropriate for IoT devices. This proposed framework of these authors works in a distributed environment to provide more privacy to a clinical system. In summary, the authors aimed to provide a solution to the issues related to blockchain using IoT devices. The drawbacks of the existing methods and prototypes are that most of them rely on a centralized system. Being dependent on a centralized system makes the PHR and EHR system more vulnerable to security breaches. Another issue was related to a cross domain authorization access approach. The existing system provides cross domain authorization access but it lacks at providing security to collusion attacks and social engineering attacks.

To provide trust, using blockchain for patient health record sharing has been widely explored within the last few years [32]. Zhu et al. implemented their early implementation through blockchain and was treated as a storage purpose for storing clinical data. In reference 3, the author has used the consortium blockchain as a tool for health data to get access control auditing and data privacy but they are using blockchain as storage rather than as a trustworthy tool. This approach leads to computational overhead. In MeDShare, the author proposed a prototype for the sharing of patient medical data to third-party research institutes in cloud repositories. In order to access clinical data, the author has used a smart contract for data auditing. The main issue with the MeDShare prototype is the lack of trust in cloud computing. In the recent literature, most of the authors proposed a design for medical image sharing in which the source files are still stored at the end of healthcare domain [33].

3. Problem Formulation and Research Design

The mechanism that we follow to design a multiple certificate based authorities framework for healthcare systems and to evaluate its performance is illustrated in Figure 1. Our main contribution to this research includes the following:

1. We identified the features that affect the performance of a cross-domain framework in a healthcare system;
2. We pre-process and elaborate these features;
3. We have developed a novel algorithm for secure access control and a keyword search mechanism using a cross-domain blockchain based framework;
4. An experimental evaluation is applied using the Internet three layer topology. These layers are called User layer, Local domain and Public Domain;
5. To place multiple sensors, the topology is portioned into several domains with the sensors placed using an effective sensors placement algorithm and smart contracts such that the delay between the blocks and transactions is minimum;

6. The performance results of the proposed framework are compared with the benchmark scheme using blockchain tools, Matlab and Pycharm.

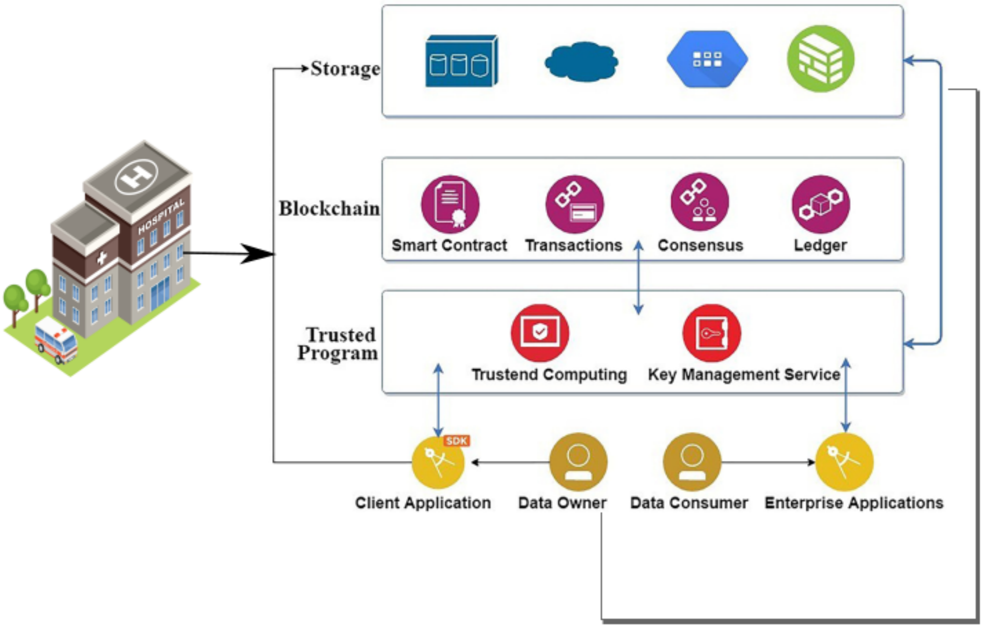


Figure 1. Workflow of the proposed framework.

3.1. Proposed Framework

Doctors or patients who have access to read patient privacy are granted access to the patient's health records. Using an attribute-based access control policy based framework with multiple certificate authority can provide more security and fine-grained access control. The participants first register with blockchain through a blockchain manager. Then, in the second step the user searches for specific records and request them. The request of the participants triggers the smart-contracts to check the user attributes and privacy criteria. The access of reading corresponds to the action of reading the patient's privacy. Our proposed framework logically comprises of four modules such as:

(1) The patient query subsystem.
(2) The private blockchain subsystem.
(3) The healthcare smart contract subsystem.
(4) The healthcare privacy subsystem.

The patient query subsystem provides management related to patient privacy data and also provides services to the other sub-parts of the framework. The blockchain subsystem includes private blockchains for doctors and a private blockchain for healthcare systems with patient privacy. Figure 1 represents the flow of the proposed healthcare applying subsystem. The data flow of healthcare applying smart contracts is shown in Figure 1.

- Step 1: In the first step the participant who wants to access a specific record using our proposed framework login to the healthcare login system and then searches for the desired patient health record. When the participants find the specific records, then the participants start to apply for the access. We have designed a novel algorithm through which the participants can interact with the blockchain based healthcare system in a secure way. Patients can encrypt their healthcare related meta data and can upload it to the blockchain. In this case, a token is issued to each healthcare record for security purpose and ease of search;

- Step 2: Our proposed smart contracts trigger the privacy module of the healthcare system. The privacy smart contracts first check the required access control and the digital certificate issued by CA. It is used to first check whether the privacy access rights are still available for the request.
- Step 3: After the smart contract confirms that the requested user has sufficient requested rights. The smart contracts then trigger confirmation of the participants requested for EHR [20].
- Step 4: After the smart contract confirms that the users have enough privacy rights then access is granted , and the participants can access the electronic health record according to the authorization level.
- Step 5: Finally, the smart contract is used to recalculate and update privacy in the healthcare private blockchain.

3.2. Parts of the Proposed Framework

- Client: In our proposed network client responsibility is to invoke transactions.
- Peer: Peers in our framework are used to maintain and update the ledger.
- Orderer: The main responsibility of the orderer is to monitor the transactions.
- Client Node: The main responsibility of this node is to (1) Submit transaction–invocation to the endorsers (2) Transaction-proposals to the orderer (3) connect both peer and orderer nodes.
- Peer Node: The actual responsibilities of this node are two, that is, (1) Verify transactions (2) It updates the ledger after receiving ordered states from the orderer.
- Orderer Node: There are two main responsibilities this node, that is, (1) In order to guarantee delivery, it broadcasts a communication service (2) after verification of the endorsement message, it delivers transactions to the peer.
- Certificate Authority: We have used multiple certificate authorities in our proposed framework in order to provide public and private keys to the authorized users. In the absence of a single CA, the intermediate CA can be used.

4. Methodology

We have used Spyder IDE (Integrated Development Environment) and Origionlab for our experimental evaluation and analysis. For statistical data analysis, we used the matlablib library. The benefit of using the matlablib library also helps to import pandas that can offer data analysis and transformation of data. We have recorded the Pcap file of transmission control protocol (TCP) during the transaction from P2P nodes and noted the execution and creation time during the transaction. A Pcap file comprises TCP files, transfer and receiving times, source and destination port. For best visualization, the caliper tool is used. During the evaluation phase, transaction rate, execution time, latency, number of peers, CPU utilization, and storage utilization used be evaluated. In order to show different viewpoints graphically during the evaluation phase, the matlablib library is used. We have carried out and evaluate each experiment for the performance of our proposed system. The performance of our framework is compared with the benchmark models in order to prove the evaluation and hypothesis. In this proposed research, multiple use cases are used in the simulation. We have divided our experiment into two use cases such as into one organization—one peer, two organizations—one peer, three organizations—one peer, two organizations—two peers, and three organizations—two peers.

4.1. Results and Proposed Method Implementation

4.2. Proposed Algorithms

Our Proposed PHR access control system has four types of users. These users mainly consist of administrators (Admin), patients (Pt), physicians (Phy), clinicians (Cl), and hospital staff (Hs). The detailed execution of an administration part in our proposed framework is shown through Algorithm 1. These algorithms consist of enrolment certificates (EC). The certification authority is responsible for the enrolment certificate. The admin module can access the system with exclusive rights. The administration part can read, write, update, and can revoke any participants. If physicians, patients or laboratory staff provide valid attributes, then the admin has the right to issue a relevant ID to each participant (authorized user) for providing access to the proposed framework. If a user behavior is found to be wrong, then the admin has the right to remove that participant with a remark from the hyperledger blockchain network. Table 1 describes all the terms used in the algorithm. Algorithm 2 describes the working of the patient sub-module. To log into a patient node, a request is made to admin for a private key. After being granted access to the blockchain network, the patient can read, write, and revoke PHR records. In this algorithm, for the patient, the module uses its attributes as the key to identify an authorized user [33].

Algorithm 1 Admin Node Selection

```
Input: Enrolment Certificate (EC) requested from Certification Authority (CA)
Output: Access to P$_id, C_id\ and\ L_id\ transactions\ for\ all((P_id, C_id, L_id)B_N)$
Initialization: NAdmin should be valid node.
NAdmin can Write/Read/Update/Remove nodes $(C_id, P_id, L_id)$
Procedure Admin $(P_id, C_id, L_id)$
  while (True) do
    if ($C_id$ is valid) then
      Add_Clinician to the blockchain Network
      Add_Clinician $(B_N, C_id)$
      Grant_access $(C_id, U_Name, P_K)$
    else
      Not_exist $(C_id)$
    end if
    if ($P_id$ is valid) then
      Add Patient to the blockchain Network
      Add_Patient $(B_N, P_id)$
      grant_access $(P_id, U_Name, P_K)$
    else
      Not_exist $(P_id)$
    end if
    if ($L_id$ is valid) then
      Add Lab to the blockchain Network
      Add_Lab $(B_N, L_id)$
      grant_access $(L_id, U_Name, P_K)$
    else
      Not_exist $(L_id)$
    end if
  end while
  int N; 0 means bad behaviour, 1 means good behaviour
  for all (,,) do
    if (behaviour_node (N) then
      Not update $(C_id, P_id, L_id)$
    else
      Remove_update $(C_id, P_id, L_id)$
    end if
  end for
end procedure
```

Table 1. Summary of notations.

Notation	Explanation
P_{HL}	Patient_hyperledger
C_{HL}	Cliniciant_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
PK_{id}	Private Key
U_{name}	Username
PHR_{name}	Patient records
P_P	Prime Number
H_H	Hash Function
G_G	Cyclic Group
N_N	Number of Transactions
id_{id}	Medical records of the patients

Algorithm 2 Admin Node Selection.

```
Input: ID and key requested from Nadmin
Output: Get access to PHL transactions
Initialization: PHL should be valid node. PHL can Read/Write/Grant/Revoke EHR records.
procedure Patient $(P_i d)$
while (True) do
if $(P_i d B_N)$ then
if $(PREC\_InotB_N)$ then
Create_records $(P_i d, PREC\_I, B_N)$
else
Update_records $(P_i d, PREC\_I, B_N)$
Read_records $(PID, PREC\_I, CID, L_i d, B_N)$
end if
else
Not_exist $(P_i d)$
end if
if Visit $(P_i d, C_i d, L_i d, B_N)$ then
MPID = Medrecord $(P_i d)$
if then $(MP_i d, PH_L, B_N)$
Grant_records $(MP_i d, C_i d, L_i d, B_N)$
else
$(C_i d, L_i d)$ = NOTIFY (Medical record does not exist)
end if
if $(P_i d C_i d, L_i d\ Treatment - completed\ (P_i d))$
then
Revoke-records $(MP_i d, P_i d, C_i d, L_i d, B_N)$
else
$(C_i d, L_i d) = NOTIFY(P_i d\ revoke\ MP_i d)$
Revoke-records $(MP_i d, P_i d, C_i d, L_i d, B_N)$
end if
else
Not Visit
end if
end while
end procedure
```

4.3. Algorithm 1 for Admin Node Selection

Our proposed algorithm for the admin node is mentioned below: It consists of three main modules, that is, Input, Output and Initialization.

The working of the patient node is described through Algorithm 2.

4.4. Algorithm 2

This is for patient node selection. The details of the algorithm are as follows. The admin checks the user's access rights and the privacy of each electronic health record through smart contracts. If the user has enough rights and fulfills the criteria, then he or she is eligible to access the electronic health records otherwise denied.

4.5. Algorithm 3 Clinician Node

Algorithm 3 provides a complete picture of the clinician node. In the input step, login access is provided to the clinician by a network admin via a request for a key. The output of the algorithm provides the grant of access key to the clinician. If the clinician id (CID) is valid, then he or she can access the PHR from the proposed framework. According to the policy, the clinician is then allowed to read and update the permission allotted PHR inside the network.

Algorithm 3 Admin Node Selection.

```
Input: ID and key requested from Nadmin
Output: Get access to CHL transactions
Initialization: CHL should be valid node. CHL can Read/Write Permission allotted EHR records by the patients and write medical records of the patients.
procedure Clinician ($C_i d$)
while (True)
do
if ($C_I DB_N$) then
If
(Granted $MP\_i_d C\_i_d$)
then
Read_records ($C\_i_d, PREC\_i_d, MP\_i_d, B_N$)
Update_records ($C\_ID, PREC\_Id, MP\_i_d, B_N$)
else
Write_records ($C\_i_d, MP\_i_d, B\_N$)
Read_records ($C_i d, L_i d, B_N$)
end if
else
Not_exist($C\_i_d$)
end if
end while
end procedure
```

4.6. Algorithm 4: Lab Node

The working of the Algorithm for the lab node is discussed as below. Algorithm 4 is mainly comprised of the lab staff (clinic or hospital supporting staff). The lab staff requests the private key from the admin to access to specific patient health records for treatment. The detail is described as below:

Algorithm 4 Lab Node Selection.

```
Input: I_d and key requested from N_Admin
Output: Get access to L_HLtransaction
Initialization: L_HL should be valid node. L_HL Can Read/Write Permissioned PHR records by the patients.
procedure Lab
If (L_id B_N))
If Granted (M_ (P_id), L_id)
then
while (True)
do
Read_records (L_Id, P_ (rec_id, ) M_id, B_n)
Write_reports (L_Id,P_ (rec_id, ) M_id,B_n)
else
Read_records (L_Id, L_Id, B_n)
end if
else
Not_exist (L_Id)
end if
end while
end procedure
```

4.7. Algorithm 5 Attribute Based Signing

The working of Algorithm 5 is explained below in an algorithmic structure. The proposed algorithm is used to sign the user transactions. The user is given public and private keys for encryption and decryption by certificate authority. The user can use these keys for signing the transactions as well.

Algorithm 5 Attribute Based Signing Algorithm.

```
    Input:Signature master public key $MK_public$ of domain
    system parameters $P_S$, $message\ M_0, e's\ identity\ I_De, and\ digital\ signature\ (h_0, S_0)$
    Output: Verification result: succeed or fail.
    Convert the data type of $h_0$ to integer
5:  if h 0 $\in$ [1, N $-$ 1] does not hold,the verification fails
    Compute element t = g $h_0 in G^T$
    Compute integer h = $H_2(M||w, N)$
    Compute integer l = (r $-$ h) mod N; if l = 0, go to step 2)
    Compute integer h1 = H1(IDe| |hid, N)
10: Compute element P = $[h_1]P_2 + P_pubsinG2$
    Compute element u = $e(S_0, P)inG^T$
    Compute $w_0 = u \cdot tinG^T$
    converts the data type of $w_0$ into a bit string
    Compute integer $h_2 = H_2(M_0||w_0, N)$.
15: if $h_2 = h_0$ holds, the verification succeed
    Otherwise, the verification fails
```

4.8. Data Type

The data for our proposed framework are supposed to be PHR [30–32]. PHR can be divided into three classes: PHR privacy attributes, explicit id, and quasi-d. Explicit id is normally used as a patient's identity that indicates a patient, such as an ID number, name, and cell number. Q-ID(Quad Identity) similarly suggests the patient's biodata and home address, such as age, date of birth, and home or office address. Privacy-related information refers to a patient's sensitive attributes, which include a type of illness and patient income or resources. To publish the patient health data and to maintain patient data, it is necessary to ensure that the individual attributes of the new dataset are appropriately processed.

Most of the existing approaches do not provide any anonymity. Our proposed framework provides a novel technology approach that includes anonymity, diversity, and confidence. As traditional anonymity has been widely used in the literature, it does not give any particular limitations to sensitive data. This issue in technology leads the attackers to attack the consistency and to drop the collusion attack to identify sensitive data and personal contact, and, alternatively, a loss of privacy. Participants: Doctors, Patients, Nurses, Lab technician and Admin are the main users in our proposed framework. Admin node know the configuration and policies of the framework and aware with Transport Layer Security (TLS), Public Key Infrastructure (PKI) and Membership Service Providers (MSPs).

4.9. System Initialization

The proposed scheme consists of three stages:

1. system setup
2. Data generation
3. Storage
4. Data Search and Access Control

4.9.1. Phase 1: System Setup

Setup(α): Input security parameter (α)

$$let\ (G_1)\ and\ (G_2)\ be\ two\ multiplicative\ cyclic\ groups\ with\ generators\ p. \tag{1}$$

$$Assume\ (g_1),\ (g_2)\ are\ two\ generators\ of\ (G_1). \tag{2}$$

Let e : $(G_1) \prod (G_1) \Longrightarrow\ (G_2)$ be an admissible bi linear map.
The system randomly selects $\alpha, \beta \in$ Z $*$ p , computes g α 2 , g β 2 , g β (α1) .
Select four hash functions H1 : 0, 1 $* \rightarrow$ Z $*$ p
H2 : G_1 (Z $*$ p) H3 : Z $*$ p $\rightarrow$ G2 H4 : G2 $\rightarrow$ 0, 1 $*$.
The system parameters PP = (p, e, $g_1, g_2,$ g α 2 , g β 2 , g β (α) 1 , $G_1, G_2, H_1, H_2, H_3, H_4$)
Master secret key msk keeps secret msk = (a, B)

4.9.2. Encryption

We have used attribute based encryption techniques in order to encrypt the transaction. For the key exchange, we have used ring signature, which is more lightweight as compared to group signature or AES (Asymmetric Encryption System). It provides more security and anonymity against collusion attacks.

$$[(2+n)K+1]C_e x + (2K+1)C_m + (2K+1)C_m \tag{3}$$

$$\prod_{x=0}^{n} x - x_j/x_i - x_j. \tag{4}$$

4.9.3. Decryption

Decryption is performed at the receiver end having boththe public and private keys at the same time. An authorized user having the correct attributes can decrypt the cipher-text. Keys are exchanged through CA among authorized and certified users in the proposed framework. The time complexity equation for decryption is explained as below: Where the K is the number of certificate authority, n is the size of the message and C represents the cipher-text, respectively.

$$[(n+1)K+1]C_p + nKC_e + [3+(2+n)K]C_m \tag{5}$$

$$X = Qk \in ICe(C_2, D_k, u), Y = e(C_3, D_1k, u) \tag{6}$$

$$S_k = Q_a k, j \in A_k meC_k, j, D_j k, u\delta ak, j, A\tilde{}j_m(0) \tag{7}$$

$$m = C_1 X/YQk \in IC_S. \tag{8}$$

4.9.4. Data Generation

Data are generated by doctors, clinicians and patients by uploading the meta-data to the blockchain and secondary data to the DB.

4.9.5. Storage

In our proposed framework, data (EHR or PHR) are divided into two portions, that is, metadata and secondary data. Meta-data are stored in the blockchain ledger whereas 80% data are stored using a data-base.

5. Proposed Certificate Authority and Its Formulation

Our proposed certificate authority plays a very important role in the proposed framework integration with multiple CA. We chose the Hyperledger-Fabric CA as its certificate authority for Hyperledger Fabric.

5.1. Function of Our Proposed CA

From the literature, it is very clear that Fabric CA performs the following functions on a blockchain network:

- Registration Identities: For registration identities we use a Lightweight Directory Access Protocol (LDAP) as the user registry.
- Issuance of Enrolment Certificates (ECerts): Enrolment is a process whereby the Fabric CA issues a certificate key-pair. It is observed that each pair of keys contains a signing certificate and a private key, which creates the identity. Although we have evaluated that CA generates private and public keys locally through a Fabric CA client. Therefore, the public key is sent to the CA which returns an encoded certificate—the signing certificate.
- Our proposed CA for the hospital performs both Certificate renewal and revocation as well.

First, start a CA search for a fabric-ca-server-config.yaml file which contains the CA configuration parameters. Our proposed CA search for the file on the directory and if the file is not there, a default one is created before the CA is deployed.

5.2. CA Topology Used for Our Proposed Framework

The topology of CAs on our proposed framework varies during the participation and interconnection of the organizations.

5.3. Setup of Certificate Authority (CAs)

The number of CAs depends on the volume of a blockchain based network and number of attributes authority. In our proposed framework, we have used dual CAs for each domain. These two CAs are called an organization CA and a TLS CA, respectively. We have used TLS CA for communications purposes in the network between peer to peer nodes in the domain. Therefore, certificates are provided by TLS to each peer. We have integrated and organized multiple CAs on the other side, used to generate organization and node identities. Because this is a distributed ledger, the ordering service should not be part of the same organization as the peers.

We implemented a hyperledger fabric because it provides the ability to configure a dual-headed certificate authority as well in situations when there is a single CA that includes an organization's identity enrolment CA, which we termed an organization CA and a TLS CA, respectively. Both of these types of CA operate on the same CA node and port but are addressable by a different CA name. We have also discussed the most important parameters required for CA files in more detail later, allowing each CA to have its own configuration but is beneficial when you want both CAs to share the same back end database. In Figure 2, it is shown that the block header is created during the transaction using the proposed method based on CA. CH2 represents the hash of the current block. In most of the scenarios, it is acceptable for one TLS CA to be used to issue certificates to secure communications for an entire organization. In some cases it is possible that, for intermediate CA, it is allowed to assign the same TLS CA as the root CA rather than having their own dedicated TLS CA.

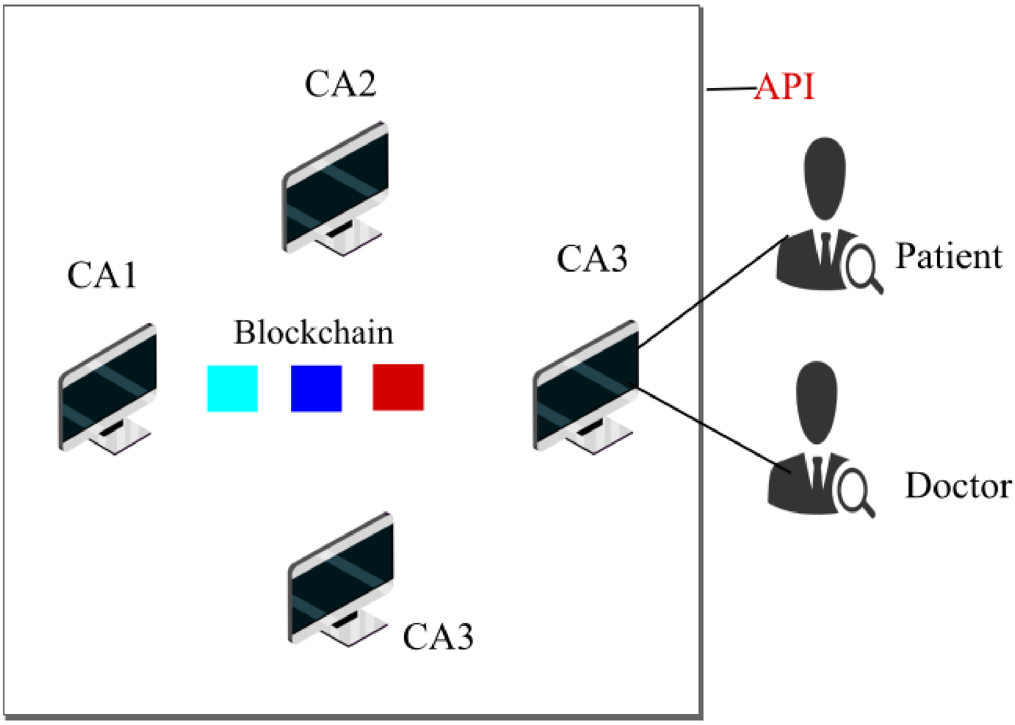


Figure 2. Certificate Authority and its configuration using the proposed method.

5.4. Deployment of Multiple Certificate Authority

After implementation, we deployed the multiple CA, which is based on the organization CA and the TLS CA. The TLS CA communicates through smart-contracts and algorithms that we have proposed. However, we deployed TLS CA separately before the organization CA in order to generate the TLS certificate for the domain CA. According to our proposed method, first TLS CA is deployed, then we deployed the organization CA. The organization CA is followed by any intermediate CAs according to our proposed method. The structure of deployment of the proposed CA provides more security as compared to a single CA.

5.5. Configuration of Certificate Authority

We used three steps to configure settings on the Fabric CA server and client. The setting that we performed includes the following three steps:

1. We used Hyperledger-Fabric CA for our own proposed framework and our proposed policies using CLI commands;

2. We set the selected environmental variables in order to override configuration file settings;

3. Lastly, we configure the fabric file for storing the records .

5.6. Proposed Multiple CA Method

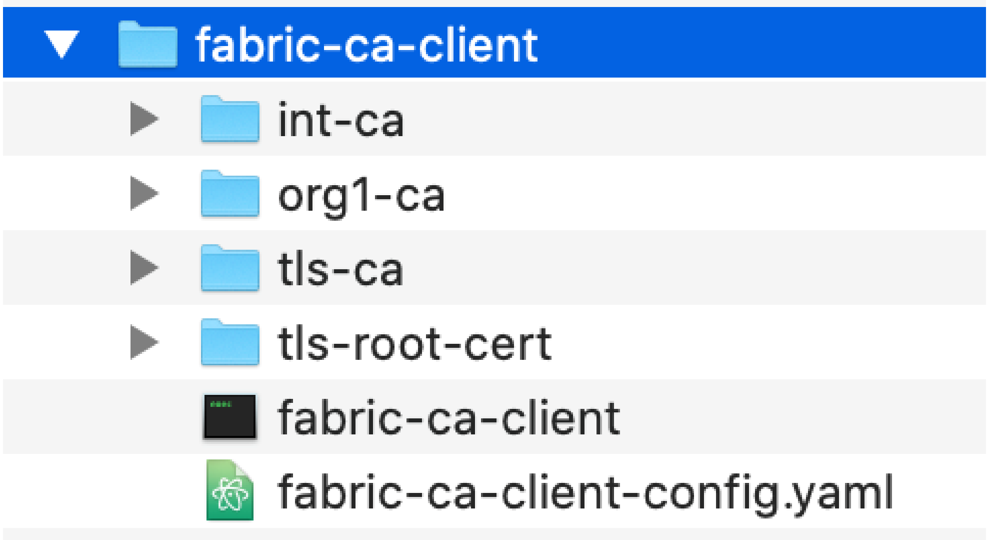
In the first stage, we rename the CA according to the organization requirements. The name represents the organization that this CA serves. This ca.name is used when targeting this server for requests by the Fabric CA Client. The key file attribute is the private key and certfile is the public key.

In our proposed framework, we provided contributions during CA configuration that permit every CA to preserve its own configuration but still share the same back-end user database. We entered the cafiles values, using the path fabric-ca-server-config.yaml of the second CA server, which is based on the TLS server. The setting of the secondary CA consists of all of the same elements and can be found in the primary CA server config file except port .

For our experimental analysis, we have used only one type of database to be connected with the blockchain using hyper-ledger Fabric as below:

1. SQLite (SQLite Version 3)

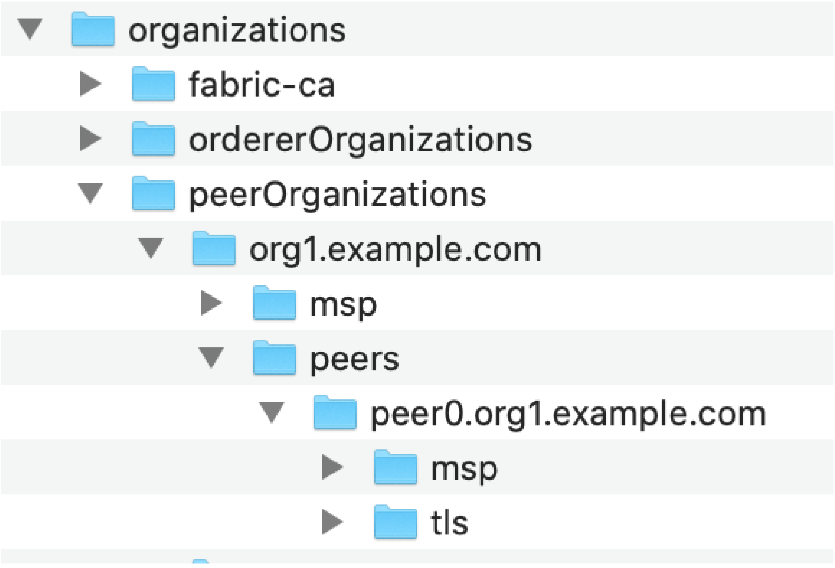
Figure 3 shows the certificate authority we have created for the hospital and healthcare organization. Actually, we have used the Hyperledger Fabric tool for our simulations.



```
▼ fabric-ca-client
    ▶ int-ca
    ▶ org1-ca
    ▶ tls-ca
    ▶ tls-root-cert
      fabric-ca-client
      fabric-ca-client-config.yaml
```

Figure 3. Certificate Authority and its configuration using the proposed method.

Figure 3, shows the categorical structure of our proposed configuration for certificate authority and policy design. The role of the certificate is the authority to assign security keys to the users and to revoke the policies. We have provided and monitored the performance of the proposed system achieved through simulation and analysis metrics. The simulations results are achieved from the number of transactions and the information received through hyperledger fabric. We have used the Spyder IDE tool to create graphs for our analysis and discussion. We have achieved these results through the implementation of our proposed algorithm. Our target simulation parameters consist of block size, endorsement policy, block creation time, channel, resource allocation, and ledger database. Similarly, our results provide explanation of performance, latency, throughput, and computational overhead. In order to achieve optimum results, we used to vary the configuration of our simulation setup. We have provided the explanation of the desired results through graphs, which is discussed in the next sections. In Figure 4, we have provided the illustration of the certificate authority and the directories that we have created for our policies and smart contracts.



organizations
- fabric-ca
- ordererOrganizations
- peerOrganizations
  - org1.example.com
    - msp
    - peers
      - peer0.org1.example.com
        - msp
        - tls

Figure 4. Certificate Authority and its configuration using the proposed method.

6. Simulations and Results

In our proposed method, the Hyperledger caliper is used as a tool for P2P networks and for the smart contract simulations. Moreover, the caliper tool plays a primary role in the verification and execution of the system. Our simulation setting comprises latency, throughput, memory consumption, CPU usage and metrics for evaluating the system. In our experimental setup, the configuration parameters are modified as per assessment, such as block size, block time, endorsement policy, channel, resource allocation, and ledger database, etc. The specification required for our simulations and configuration setup meets the following hardware and software criteria given as follows. Core i7, Intel 2.7 GHz, RAM 16 GB, Hyperledger Caliper, Python, Chaincode, Origionlab pro.

6.1. Scenario 1: Basic Experiment

In this experiment, numerous observations have been recorded to analyze and evaluate the hyperledger platform of blockchain technology using PHR. We have carried out various measurements and performed it in ten series to write the transaction over the entire network for the ledger with number of transactions for each sequence under ratio rates of 100, 150, 250, 300 transactions per second.

6.2. Scenario 2: Experiment Using Variation with Block Time

In the second experiment, we have evaluated the optimization of the network. The experiments were carried out in measuring the block initiated time during the configuration of the hyperledger caliper for PHR. Through this experimentation, we used different variations of the simulation results. Figure 5 explains the comparative analysis for the deployment time for a number of transactions. In Figure 5 we conducted our experiments on our proposed access control policies using multiple CA. We categorized these policies into three groups, such as number of read requests, number of write requests and number of update requests. Then, we compared our proposed CA with the single CA for each read, write and update policy. it is clear that the deployment remains constant for deploying for the transaction of the same match. Here the match represents the block height and the transactions volume. It is very clear that our proposed access control takes less execution time as compared to a single CA. We used the same block height, same encryption and decryption techniques. However, at the end of our experiments we found that our proposed approach takes less computational cost as compared to a single CA for the same number of access control policies. Our proposed approach provides more security and flexibility in accessing the personal health records. If we look into the standard deviation of these values, then we observed that our proposed framework provides better than the benchmark. Our proposed system also provides less delay.

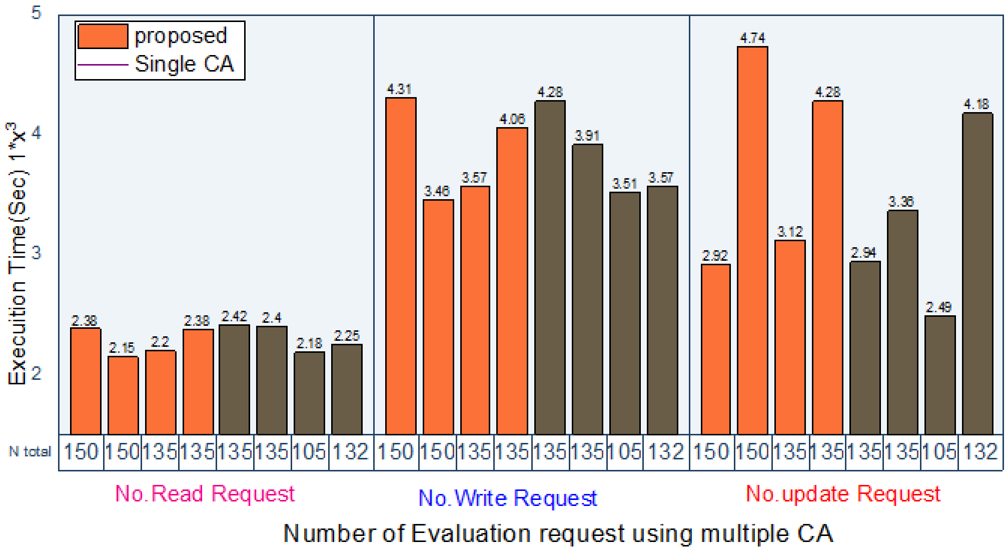


Figure 5. Comparative Analysis of evaluation request using Hyperledger Fabric multiple CA.

In Figure 6, we performed our simulations based on the number of attributes and time complexity in micro-seconds for the number of transactions and time complexity. We compared our results with time complexity and the number of transactions. Figure 6 shows that the time complexity depends upon the number of attributes. The greater the number of attributes the greater the time complexity. We kept the number of attributes very moderate in order to achieve less time complexity. It also explains the deployment confirmation time for the number of transactions ranging from 10 to 80 respectively. From Figure 6, it is evident that, by increasing block height, the number of matches also varies as logarithmic increase. The shaded green region indicates that most often, the transaction time is bearable and the delay is the minimum. In Figure 7, we plot the comparative analysis of the proposed framework with the benchmark models. We compared the average performance and throughput of our proposed framework and benchmark models. From the analysis of our proposed framework, it performs efficiently as compared to the benchmark models. We carried out our analysis of the number of evaluation requests in relationship with the execution time. Our proposed framework was analyzed and tested for 20 and 40 matched events or we can say that we have considered the evaluation of 20 and 40 groups of transactions, respectively. In Figure 8, we carried out experimental analysis based on the number of attributes authority, time complexity and number of transactions sent to each node through the proposed framework. It has been observed that the greater the number of authorities, the greater the number of transactions sent to the source. The range of the number of transactions are from 1000 to 10,000, respectively. We have observed from the analysis the number of transactions through our proposed framework and method can be sent up to 8000 using 25 attributes authority and multiple certificate authority. It shows the throughput of our proposed framework. It is possible through our proposed framework that with less time complexity, a greater number of transactions can be sent from source to destination using multiple certificates and multiple attributes at the same time. This makes our framework unique as compared to Medrec and Medchain.

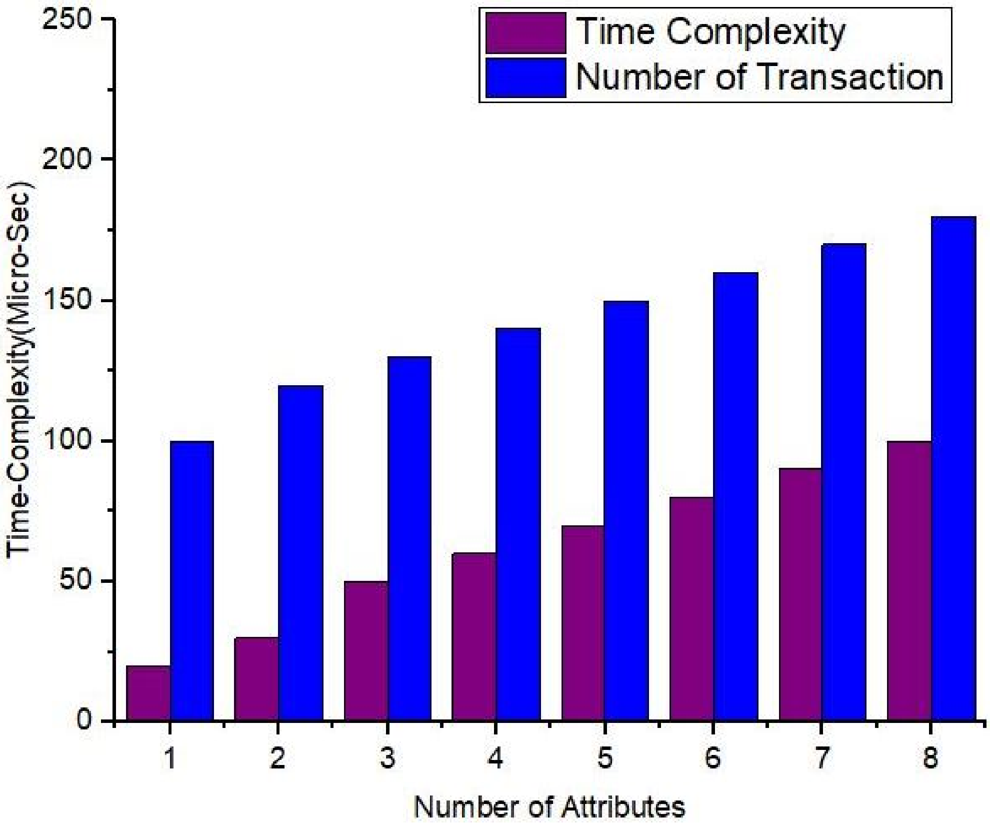


Figure 6. Analysis of number of Encrypted Transactions transferred versus Time Complexity based on number of attributes.

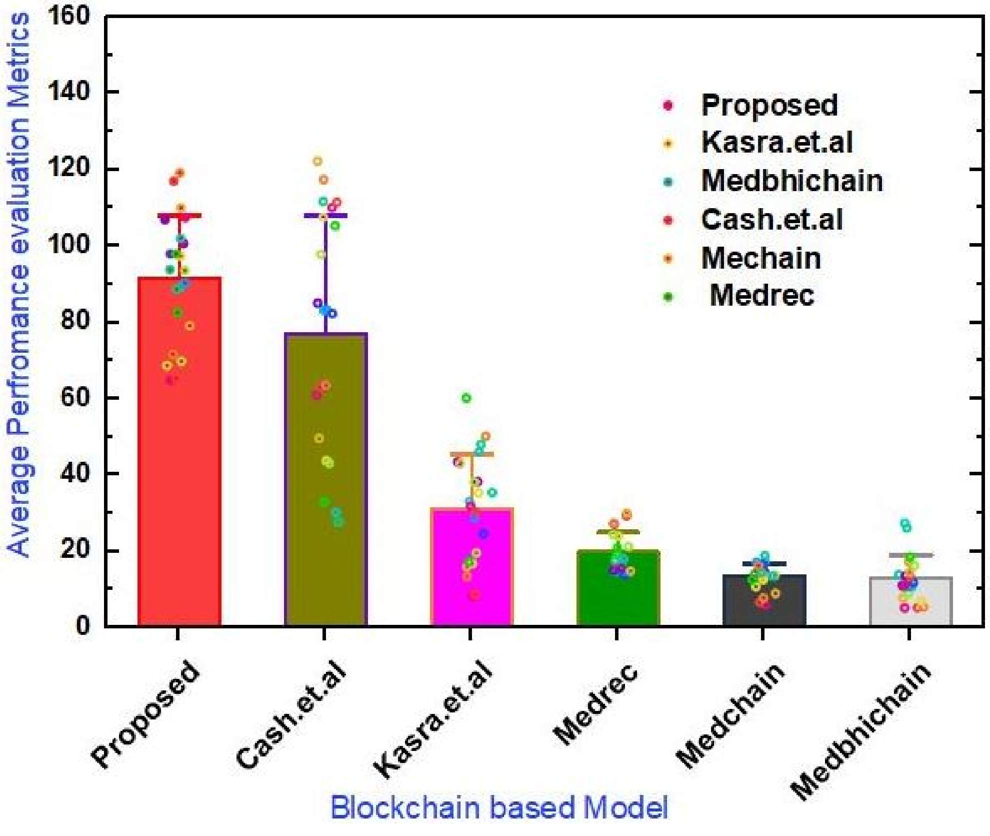


Figure 7. Comparative Analysis of proposed Framework versus Benchmark Models.

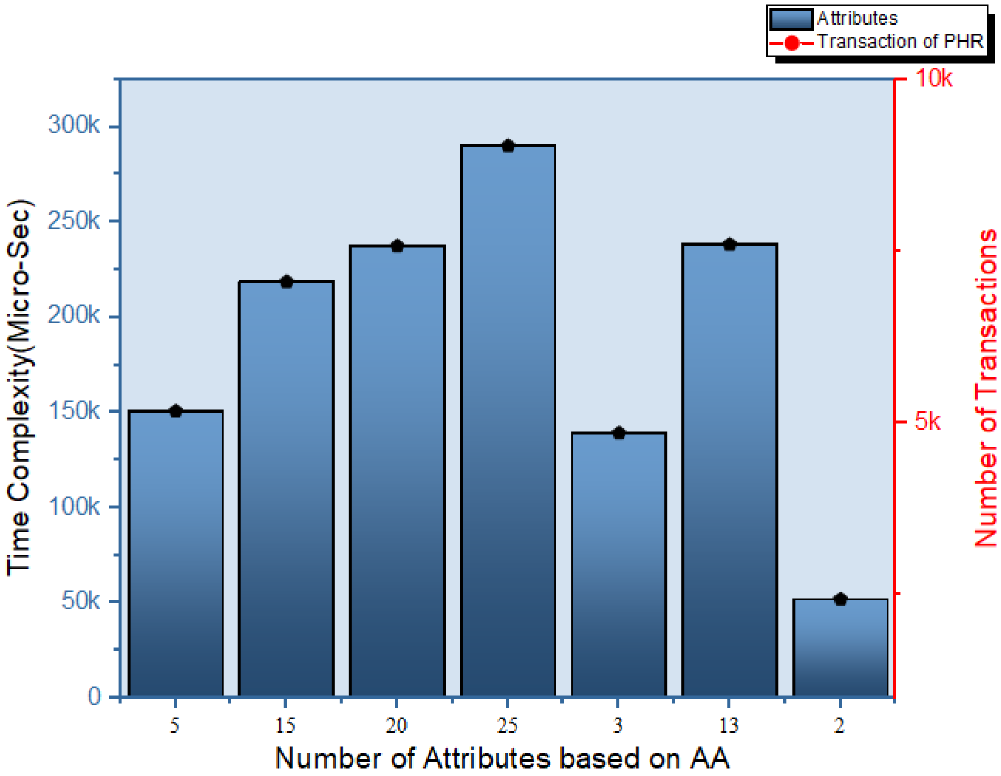


Figure 8. Analysis of deployment confirmation time.

In Figure 8, we plot simulation results based on the number of attributes authority (AA) and attributes versus number of transactions sent from one domain to the other domain. The results explain that the average number of attributes authority should be less than 10 in order to achieve the optimum computational cost. In Figure 9, we have compared our proposed access control policies for accessing the personal health records. These access control policies are updating, authentication, authorization and search policies. We have used the attributes such as confirmation time and number of policies. From the simulations its very obvious that authorization takes less time as compared to other policies hence it justified that our proposed access control algorithm is more secure and cost effective as compared to the benchmark models such as Medrec and Medchan.

In Figure 10, we plot the results of our experimental evaluations based on the proposed access control policies. We have categorized the access control policies. These policies are the read, write, delete , update and revoke policies. We have compared each policy with the execution time. From the simulation results, it is clear that the our proposed access control policies take less time as compared to the benchmark models.

Table 2 explains the comparative analysis of our proposed framework and the benchmark models. From Table 2 it is very clear that our proposed framework is more efficient in the case of security, privacy and by providing access control to the users in order to access their data securely.

For Cross-domain based access control using multiple CA we have conducted experiments, and plotted results in Figure 11. We considered different domain ranges from 0 to 400. From the simulation results in Figure 11, it is evident that our proposed framework is best up-to the 70 cross domain, respectively. In Figure 12, we have provided the simulation results based on the number of access control policies. These access control policies are used for authorization, authentication and update policies. Our main approach is authorization, which is more concern about security. From Figure 12, it is obvious that our proposed access authorization method takes much less time as compared to other policies. Hence, our proposed method is more secure and efficient as compared to other policies.

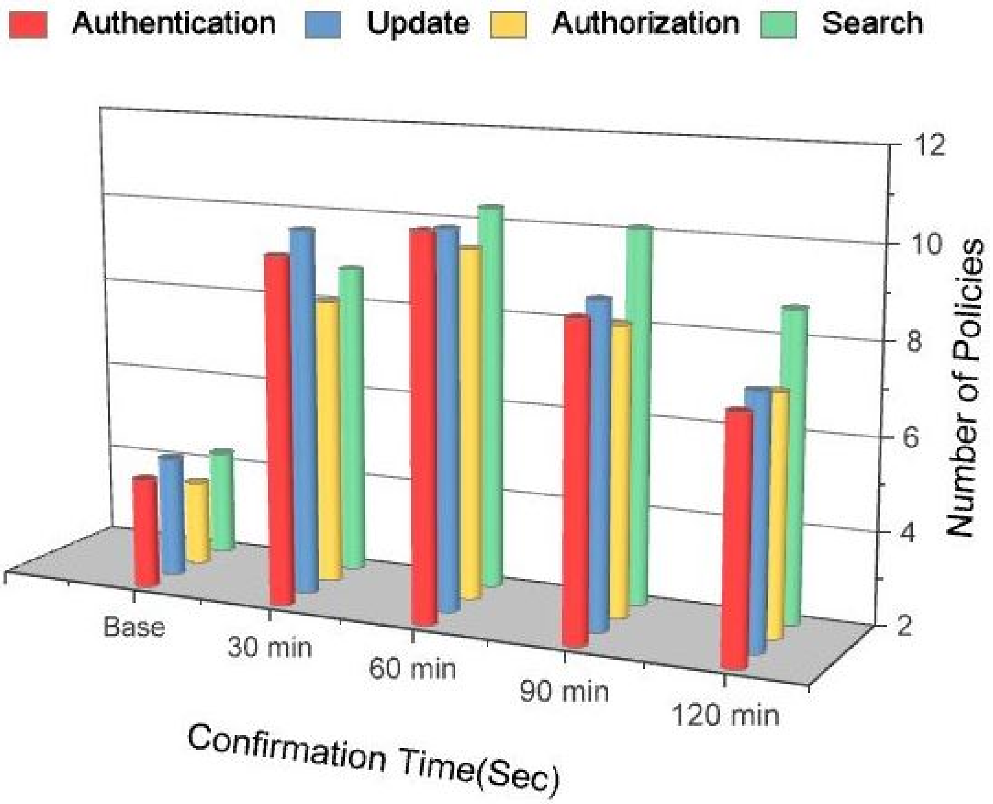


Figure 9. Analysis of Access Control Policies based on the number of attributes and certificate authority.

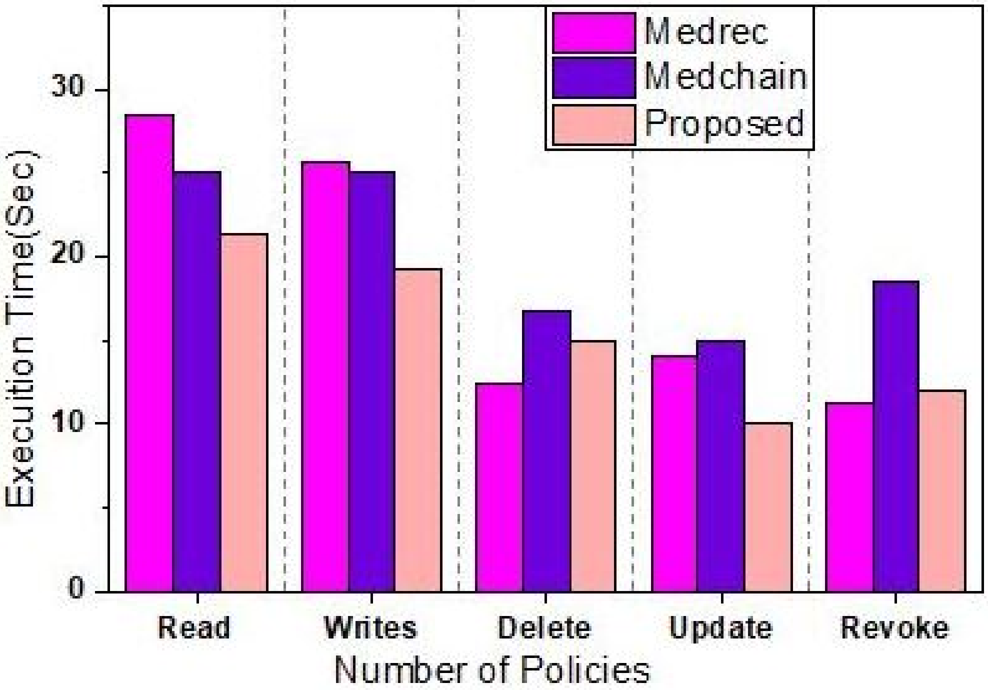


Figure 10. Comparative Analysis of proposed flexible Access Control policies based on number of Attributes Authority K = 1 with the benchmark models.

Table 2. Summary of comparison among proposed frameworks and benchmarks.

Framework	Medrec	Medchain	Medblock	Proposed
Tamper proof	yes	No	No	Yes
Non-repudiation	yes	No	No	Yes
Replay Attack	yes	No	No	Yes
Collusion Attack	Yes	No	Yes	Yes
Block Search	No	No	No	Yes
Privacy	Yes	No	No	Yes
Metadata	No	No	No	Yes
Data Stream	yes	Yes	No	yes

Figure 13 represents the simulations of our proposed algorithm and smart contracts using certificate authority. These simulations represent the throughput of our proposed framework and the number of percentages of confirmed transactions, respectively. We have compared our proposed framework with single certificate authority using the number of attributes and communication overhead. Figure 13 shows that our proposed framework performs better than the benchmark models due to the least communication overhead. In Figure 13, we have explained our proposed access control policies based on the number of attributes. The x-value represents the number of attributes and the Y-value represents the execution time value, respectively. We have implemented our proposed policies in smart contracts using chain code. Figure 14 provides the simulation results for the number of attributes versus storage overhead. It shows our proposed approach consumes less storage space as compared to single CA. This shows that our proposed approach is more efficient as compared to the single CA.

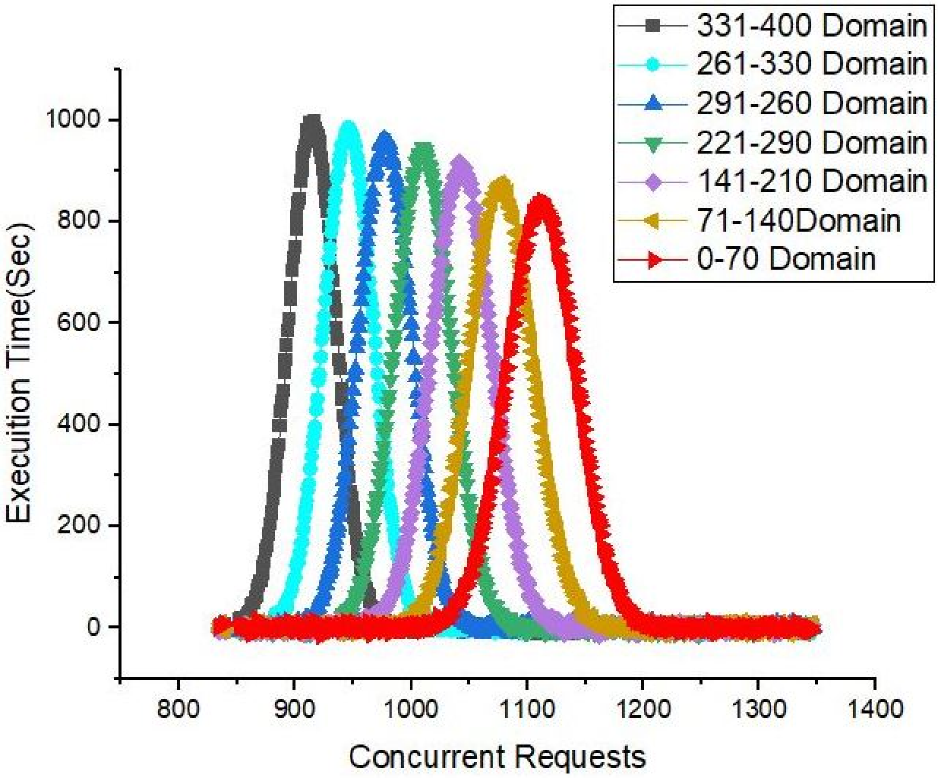


Figure 11. Comparative Analysis of proposed flexible Access Control policies based on number of Attributes Authority K = 1 with the benchmark models.

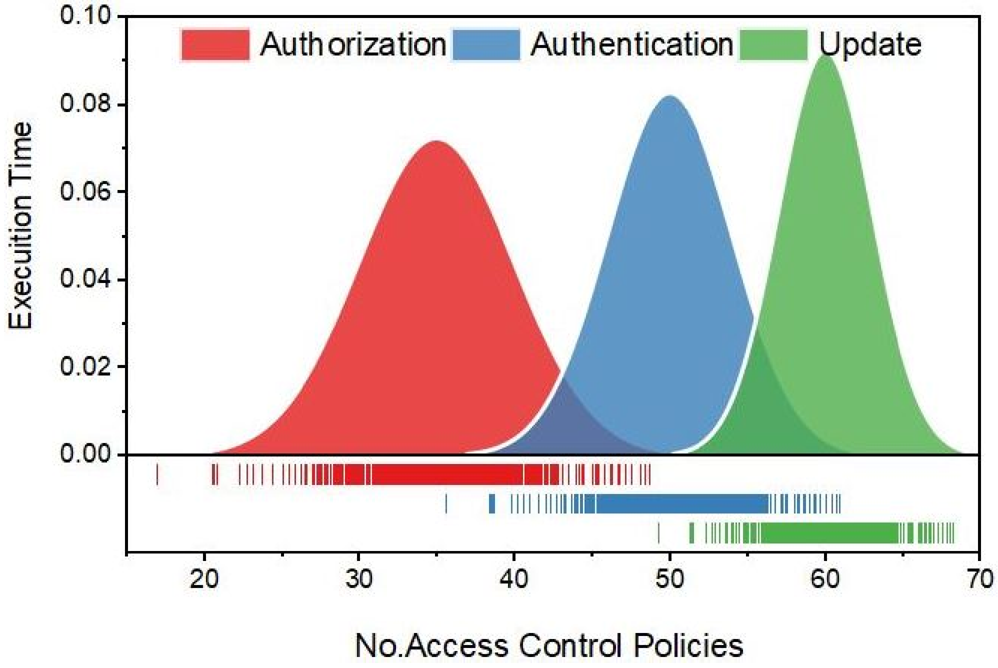


Figure 12. Comparative Analysis of proposed flexible Access Control policies based on number of Attributes Authority K = 1 with the benchmark models.

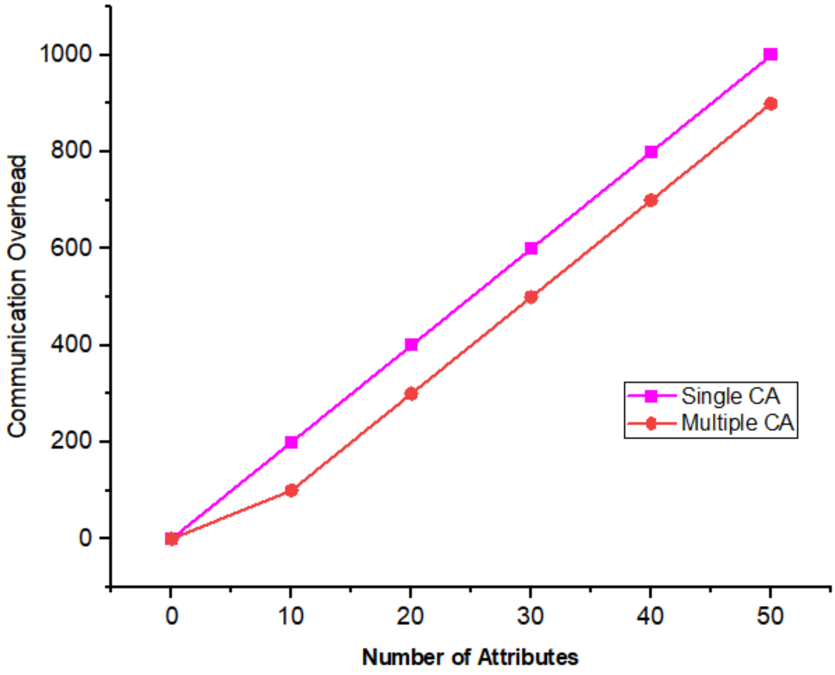


Figure 13. Evaluation results of number of evaluations vs. confirmation time.

Figure 15 shows the detailed information about the number of group of policies and the EHR sent per second. The x-axis denotes the group of access control policies, while the y-axis shows the EHR, which is sent per second. We did comparative analysis with our proposed framework and benchmark model, that is, medrec based on number of transactions for the same number of policies. It is evident from the graph that the proposed framework surpasses medrec for the same policies. In Figure 16, the comparison is carried out on the basis of number of nodes and response time. From Figure 16, it is clear that the greater the response time, the less efficient the model for the same number of nodes will be. It is evident from Figure 16 that our proposed framework takes less response time in order to transfer the electronic health records. We carried out the experiment for the same number of nodes hence our technique response in a very short time as compared to the benchmark model, which takes more time. The main reason for our technique is that we are using stream based data whereas the benchmark models have used block data. In order to check the integrity of packets, only the last bit of the stream is required to check for the integrity. Hence, for n bit of stream the complexity will be equal to $b-1$.

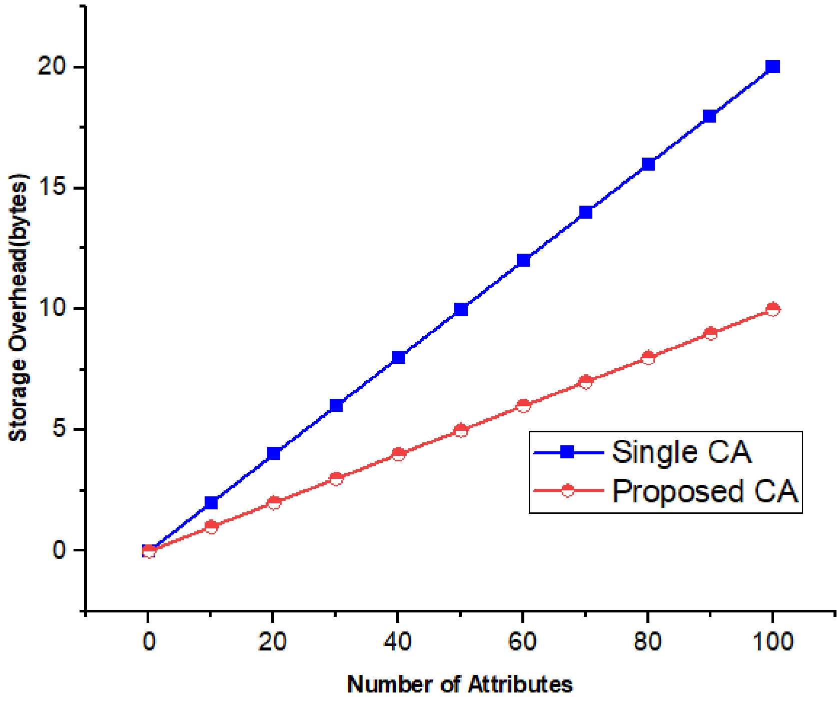


Figure 14. Comparative Analysis of Single CA versus our Proposed method(Multiple CA).

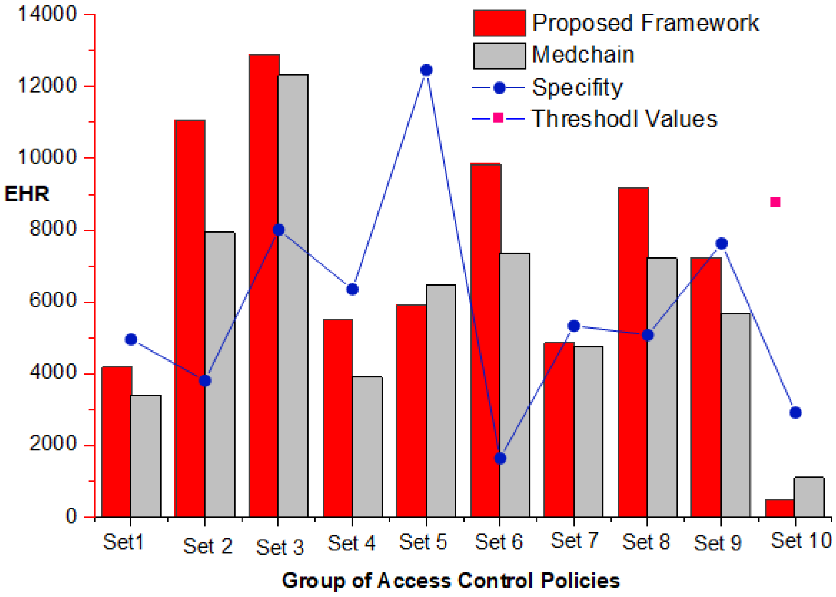


Figure 15. Comparative analysis of group of policies versus EHR.

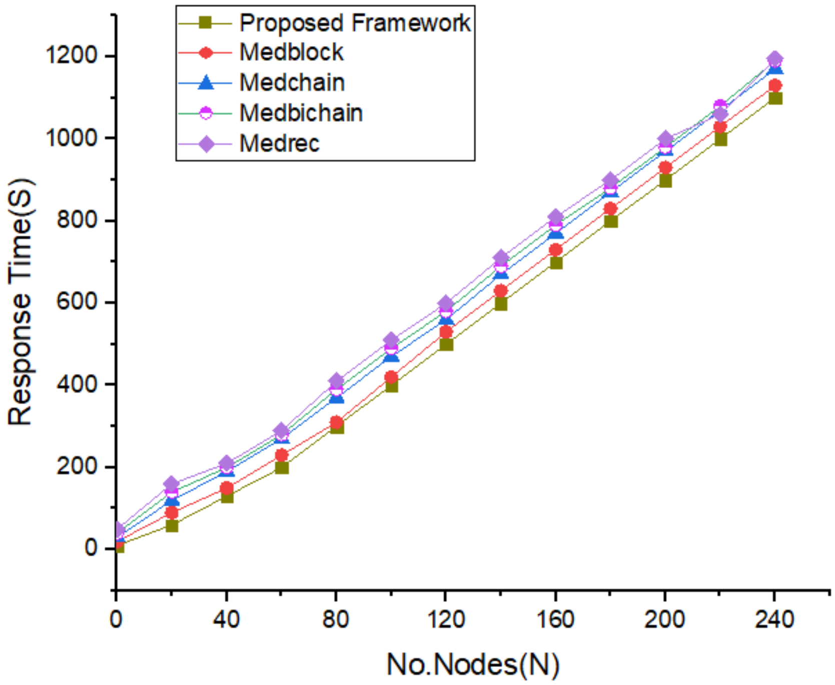


Figure 16. Analysis of similar events or experiment versus the average gas consumption used.

7. Conclusions

In this paper, we have proposed a blockchain based framework using the hyperledger fabric based certificate authority. We have configured two CAs for each organization. Moreover, we performed our experiments for one, two, three and four organizations, and for cross-domain based multiple certificate authority. More and more, we have used hyperledger fabric as our experimental tool to implement our algorithms and smart contracts. Finally, we evaluated our data using PHYCHARM and Oigionlab Pro. We compared our proposed framework with the benchmark models using specific criteria in a tabular form. From the analysis, it is validated that our proposed framework provided better throughput and security, which is justified by the simulations and comparative analysis with the benchmark models. Our proposed framework provides improved security, resistance to replay and collusion attacks. Furthermore, to the best of our knowledge, we proposed a novel idea about multiple certificate authorities in healthcare systems using cross-domain or cross-organization, which makes our research more novel and provides contributions towards access control as well as security in blockchain based platforms. In the future, we are planning to deploy the prototype in the healthcare system, especially in Malaysia. Moreover, we also plan to use machine learning techniques to take and trace the behavior of users requesting personal or electronic heart records, so that the users can be further classified into groups based on their interactions and behavior.

Author Contributions: Conceptualization, A.A.; data curation, A.A.; formal analysis, A.A., H.A.R., M.F.P., J.A. and M.M.; investigation, J.A., M.B.; methodology, A.A.; project administration, A.U.R. and J.A.; resources, M.F.P. and M.B.; software, A.A.; supervision, H.A.R., J.A. and M.M.; validation, M.B.; visualization, A.A.; writing—original draft, A.A., J.A. and M.F.P.; writing—review and editing, A.A., M.B., M.M. and J.A.; proofreading and writing the paper script in overleaf, C.C. All authors have read and agreed to the published version of the manuscript.

Funding: Taif University Researchers Supporting Project number (TURSP-2020/239), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank for the support from Taif University Researchers Supporting Project number (TURSP-2020/239), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ali, A.; Ejaz, A.; Jabbar, M.; Hameed, K.; Mushtaq, Z.; Akhter, T.; Haider, A. Performance analysis of AF, DF and DtF relaying techniques for enhanced cooperative communication. In Proceedings of the 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, 24–26 August 2016; pp. 594–599.
2. Mushtaq, Z.; Sani, S.S.; Hamed, K.; Ali, A. Automatic Agricultural Land Irrigation System by Fuzzy Logic. In Proceedings of the 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), Beijing, China, 8–10 July 2016; pp. 871–875.
3. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
4. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
5. Hasnain, M.; Pasha, M.F.; Ghani, I.; Mehboob, B.; Imran, M.; Ali, A. *Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis*; IEEE Access: Piscataway, NJ, USA, 2019; Volume 8, pp. 53649–53665.
6. Sharma, A.; Tomar, R.S.; Chilamkurti, N.; Kim, B.-G. Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare. *J. Electron.* **2020**, *9*, 1609. [CrossRef]
7. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. *J. Electron.* **2021**, *10*, 2034. [CrossRef]
8. Ali, A.; Naveed, M.; Mehboob, M.; Irshad, H.; Anwar, P. An interference aware multi-channel MAC protocol for WASN. In Proceedings of the 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, Pakistan, 5–7 April 2017.
9. Ali, A.; Mehboob, M. Comparative Analysis of Selected Routing Protocols for WLAN Based Wireless Sensor Networks (WSNs). In Proceedings of the 2nd International Multi-Disciplinary Conference, Oxford, UK, 5–7 September 2018; Volume 19, p. 20.
10. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems-a survey of scheduling algorithms. In Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China, 2–5 August 2016; Volume 1.
11. Khan, F.A.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *J. Sustain. Cities Soc.* **2020**, *55*, 102018.
12. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *J. Sustain. Cities Soc.* **2020**, *55*, 10–18. [CrossRef] [PubMed]
13. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. A blockchain based privacy-preserving data sharing for electronic medical records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018.
14. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient privacy-preserving machine learning for blockchain network. *J. IEEE Access* **2019**, *7*, 136481–136495. [CrossRef]
15. Jiang, S.; Cao, J.; McCann, J.A.; Yang, Y.; Liu, Y.; Wang, X.; Deng, Y. Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410.
16. Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 1178–1187.
17. Chakraborty, S.; Aich, S.; Kim, H.-C. A secure healthcare system design framework using blockchain technology. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 17–20 February 2019; pp. 260–264.
18. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *J. Comput. Secur.* **2020**, *88*, 101–629. [CrossRef]
19. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (Smartcomp), Taormina, Italy, 18–20 June 2018; pp. 49–56.
20. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based packing of industrial IoT data in permissioned blockchains. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7639–7649. [CrossRef]
21. Dorri, A.; Kanhere, S.; Jurdak, R.S.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
22. Lazaroiu, C.; Roscia, M. Smart district through IoT and blockchain. In Proceedings of the 2017 IEEE 6th International Conference on Renewable Energy Research and Applications, San Diego, CA, USA, 5–8 November 2017; pp. 454–461.

23. Lacity, M.C. Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *J. Mis Q. Exec.* **2018**, *17*, 3.
24. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
25. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* **2021**, *21*, 772. [CrossRef] [PubMed]
26. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Alvin Yau, K.-L.; Ji, Y. Blockchain for vehicular Internet of Things: Recent advances and open issues. *Sensors* **2020**, *20*, 5079. [CrossRef] [PubMed]
27. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy. *J. IEEE Cloud Comput.* **2018**, *5*, 31–37.
28. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *15*, 1398–1411. [CrossRef] [PubMed]
29. Kim, T.M.; Lee, S.-J.; Chang, D.-J.; Koo, J.; Kim, T.; Yoon, K.-H.; Choi, I.-Y. DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. *J. Appl. Sci.* **2021**, *11*, 1612. [CrossRef]
30. Hang, L.; Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228. [CrossRef] [PubMed]
31. Figorilli, S.; Antonucci, F.; Costa, C.; Pallottino, F.; Raso, L.; Castiglione, M.; Pinci, E.; Del Vecchio, D.; Colle, G.; Proto, A.R.; et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain. *Sensors* **2018**, *18*, 3133. [CrossRef] [PubMed]
32. Zhu, X.; Badr, Y. Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors* **2018**, *18*, 4215. [CrossRef]
33. Jia, X.; Hu, N.; Su, S.; Yin, S.; Zhao, Y.; Cheng, X.; Zhang, C. IRBA: An identity-based cross-domain authentication scheme for the internet of things. *J. Electron.* **2020**, *9*, 634. [CrossRef]