electronics

MDPI

Article

Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain

Aitizaz Ali [1], Hasliza A. Rahim [2,3], Muhammad Fermi Pasha [4], Rafael Dowsley [5], Mehedi Masud [6,*], Jehad Ali [7,8,*] 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 (ACE) Centre of Excellence, Universiti Malaysia Perlis, Kangar 01000, Malaysia; haslizarahim@unimap.edu.my
3 Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis, Perlis 02600, Malaysia
4 Department of Software Systems and Security, School of IT, Monash University, Subang Jaya 47500, Malaysia; Muhammad.FermiPasha@monash.edu
5 Department of Software Systems and Cyber-Security, School of IT, Monash University, Clayton, VIC 3168, Australia; rafael.dowsley@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 Computer Engineering, Ajou University, Suwon 16499, Korea
8 Department of AI Convergence Network, Ajou University, Suwon 16499, Korea
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: mmasud@tu.edu.sa (M.M.); jehadali@ajou.ac.kr (J.A.)

Citation: 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. *Electronics* **2021**, *10*, 2034. https://doi.org/10.3390/electronics10162034

Academic Editor: Gongping Yang

Received: 7 July 2021
Accepted: 18 August 2021
Published: 23 August 2021

Abstract: According to the security breach level index, millions of records are stolen worldwide on every single day. Personal health records are the most targeted records on the internet, and they are considered sensitive, and valuable. Security and privacy are the most important parameters of cryptography and encryption. They reduce the availability of data on patients and healthcare to the appropriate personnel and ultimately lead to a barrier in the transfer of healthcare into a digital health system. Using a permission blockchain to share healthcare data can reduce security and privacy issues. According to the literature, most healthcare systems rely on a centralized system, which is more prone to security vulnerabilities. The existing blockchain-based healthcare schemes provide only a data-sharing framework, but they lack security and privacy. To cope with these kinds of security issues, we have designed a novel security algorithm that provides security as well as privacy with much better efficiency and a lower cost. Hence, in this research, we have proposed a patient healthcare framework that provides greater security, reliability, and authentication compared to existing blockchain-based access control.

Keywords: security; digital healthcare solution; blockchain; smart city; reliability; privacy

1. Introduction

Security and privacy are critical factors of efficient access control models for healthcare systems. More importantly, the internet affects humans' lifestyles and methods of communication, including their professional lives and social connections. The Internet of Things (IoT) is the use of tiny sensor-based devices that integrate physical and virtual domains. The application of blockchain-based frameworks provides tamper-proof and more decentralized communication among nodes. Blockchain is also called a distributed and immutable ledger [1]. Hence, it provides applications and services, functionality, management, and on-demand access [2]. However, the recommendations and implementations of networking devices and other things are still growing. Hence, most industries are shifting towards the IoT and the adaption of blockchain technologies [3,4].

Moreover, security and privacy challenges are crucial for blockchain-based models, especially systems that use the integration of healthcare systems. Security breaches consist of denial-of-service (DoS), structured query language (SQL) injection, spoofing, eavesdropping, and replay attacks, which are challenging for IoT-based systems. Such attacks affect security applications and their authorization, authenticity, and privacy. Therefore, it is very important to address these issues and to provide a novel design framework that can provide security to IoT devices that leverage blockchain applications. It is evident that weak security at any node can lead to access to patient health records. An electronic health record (*EHR*) is regarded as the most important and sensitive type of data because it consists of a lot of sensitive information related to patients and diagnoses. However, the advancement and progress in digital healthcare systems has caused *EHR* data to become more vulnerable to breaches [5]; hence, security and privacy must play an important role in the case of decentralization and trust [6].

However, a very important aspect of IoT may provide more security and applications to diverse users [7]. Due to the ease of access to the internet and the increase in smart communication among people, objects, data, and processes, the exponential growth in the number of connected devices throughout the globe resulted in billions being recorded in the year 2020 [8]. Therefore, the security challenges of IoT applications are the basic requirements for dealing with such issues. Consequently, there has been an improvement in their intricacies, as the great complexity of devices provides less security in the performance of access control. Access control is the basic security tool for *EHR* data from any source. Therefore, it is compulsory to design access control policies for *EHR* and *PHR* [9]. A blockchain-based digital healthcare framework, which is also called Hyperledger Fabric, is used for the development of patient health record (*PHR*) systems. Security, privacy, and cross-domain authorization are factors that influence patient health records around the world. According to the security breach level index, every single day, million of records are stolen online [10]. These issues need to be explored by researchers in order to investigate the security and privacy challenges related to the use of blockchain for *PHR*.

In a digital healthcare system, a cross-domain organization approach can provide facilities to clinicians and patients for accessing data that are distributed among different domains. On the other hand, accessing data through a cross-domain organization requires more security and flexible authorization policies. A policy defines rules and strict conditions for the attributes of participants and data. Moreover, data can be encrypted by using cryptographic techniques. In the literature, the encryption techniques used by the researchers are based on ring signatures and group signatures. These encryption techniques have specific applications for predefined access control models, e.g., role-based access control (RBAC), access control list (ACL), discretionary access control list (DAC), and trust-based access control (TBAC). In our proposed framework, we will use an attribute-based signature (ABS) with an ABAC access control model to encrypt data. We will use the model of Sahai and Water [11] as a benchmark for our access control model, which is completely based on ABAC.

Our main contribution in this research comprises the identification of security issues regarding the IoT and an investigation of a blockchain-based framework to overcome these issues. Our second contribution is the design of a novel algorithm for a blockchain-based IoT network in order to access electronic health records securely. Our third contribution is a novel blockchain-based framework for reading, applying, returning, and adding electronic health records using private and public blockchains.

The rest of the article is organized as follows. Section 2 describes the literature review. In Section 3, we explain the methodology of our proposed work. Section 4 describes the flow of transactions in our proposed framework, and in Section 5, we explain the proposed algorithms. Section 6 provides the dataset and the types of data that we used. Section 7 explains the experimental setup and analysis. In Section 8, we provide a detailed discussion of our results. Finally, in Section 9, we conclude our study and describe future work.

Our Contributions

Our contributions in this research paper include a secure and flexible access control based on a ring signature. Our proposed method provides more security and privacy by leveraging novel smart contract and encryption algorithms. Moreover, we used a ring signature to encrypt and decrypt data. Once a user signs a message with a ring signature, only the selected and authenticated users can decrypt it. In addition, the user does not know the identity of the signer, and this feature helps in keeping the privacy of the users in the blockchain. Moreover, this protects users from active collusion attacks. Therefore, we used an attributed-based fine-grained access control mechanism that provides more security, as only users who have the required access rights can access the data. If a user does not meet the security criteria, their request is denied.

2. Literature Review

The tremendous growth in the number of IoT devices and their impacts on social life have created a protected, open, and unique environment in which patient health records can be securely accessed. The models for IoT necessitate the utilization of a central cloud server, which results in a single point of failure (SPOF) [12]. In order to provide solutions to such problems for sensor-based medical devices, blockchain is considered as one of the best tools and platforms for a decentralized environment. The innovation of blockchain is a huge advancement in the IoT security field [12]. The applications of blockchain technology start from its decentralization, trust, and distributed nature from diverse points of view. The use of blockchain with IoT devices provides more a secure environment that is not dependent on a single trusting authority. During the development of IoT frameworks, there are more possibilities to have an expanded number of cooperating gadgets or things in them. These expanded numbers of gadgets attempt to communicate with each other by using Internet as a medium. This would result in numerous obstacles because most of the gathered data are kept in the focal servers of IoT systems. Therefore, in the literature, researchers have tried to cope with these issues.

Ali et al. [1] proposed a system based on a patient monitoring system and an interference-aware system for the IoT. The authors also provided a comparative analysis with the benchmark models and traditional central-authority-dependent models, which rely on a central authority node. The authors also proposed a lightweight ring-signature-based consensus algorithm for a sensor-based blockchain network. Ali et al. also proposed the idea of a decentralized medical-data-sharing scheme for cross-domain use with the Hyperledger Fabric platform. The authors provided many details about the application of this blockchain tool in an IoT-based environment and peer-to-peer networks. They also designed a P2P-based record-sharing protocol that supports smart-contract-based access control polices. The authors of [13] highlighted recent issues and developed an access control policy for digital medical records through a fine-grained access control system. A novel architecture was designed by authors in the literature to secure electronic healthcare records based on a distributed ledger technology and also improved the interoperability of health records between different organizations [14]. However, the authors also provided a performance evaluation by using a blockchain tool and proposed some endorsement policies. In [15], the authors explored the performance metrics of the Hyperledger Fabric framework. Some researchers provided optimization of security and performance by using a blockchain platform with sensor-based networks. The authors of these research works provided a complete justification for enhanced performance with minimal computation time. Last but not least, the authors of [16] devised a searchable encryption scheme for electronic healthcare records using blockchain. They designed an algorithm for indexing healthcare records and a two-part evaluation scheme.

Dwivedi et al. [14] proposed a peer-to-peer network in order to improve privacy and security when connecting remote medical sensors and devices. The authors designed a framework of modified blockchain models while considering IoT sensor devices. In summary, the contributions of the authors were the resolution of the issues of using a blockchain

with sensors. Irving et al. [17] designed a method for using a blockchain in a doctor-and-patient setup and for booking for patients. Srivastava et al. [3] proposed a modified blockchain based on directed acyclic graphs, which were proposed by Zohar and Somplisnky [18]. However, the transaction protocol was for a private blockchain, and the author also provided a comparative analysis between private and public blockchains. The main contribution of this research design was the provision of solution to some types of security breaches. The authors attained a better efficiency and scalability. Yazdinejad et al. [19] presented a blockchain-based framework for software-defined networking (SDN) [20,21]. These works have provided a road map to 5G technology, and they reduced the execution time and the delay for re-authentication in 5G and advanced networks [22].

2.1. Smart Cities

Over the last decade, the applications of technology and IoT have brought improvements to human life and social activities. Various fields, such as weather prediction, geographical changes, and resource utilization, are managed smartly now. According to recent reports and a survey on IoT [22], it is predicted that by 2050, most devices will be connected through the IoT and sensor networks, which will be known as the Internet of Energies. For future purposes, more and more researchers are analyzing and planning resource utilization in a more intelligent manner, especially for IoT models because IoT devices are run with battery power. Smart cities have been implemented and designed in developed countries, and they have shown the best results for human life and healthy lifestyles, especially in noise-free environments [23]. Rathore, Kwon [24] designed a peer-to-peer network and proposed a security protocol for software-defined networking (SDN) using blockchain technology for IoT applications in smart cities. The authors integrated IoT devices and blockchain in different scenarios, such as SDN or mobile edge and fog computing [23]. In the case of SDN [25], the authors provided and deployed a prototype for their proposed framework [26]. In their research, the authors of [27] explored the maximum utilization of blockchain technology to provide a solution to the IoT security challenges in a 5G cell framework. The research mainly focused on a multi-layer security framework for an IoT arrangement that was dependent on blockchain [26]. The proposed framework supported the relatively real sending of the blockchain applications through the integration of the IoT network into a multi-layer decentralized framework [28]. The authors used machine learning techniques and a classification algorithm to classify the users who did not have access to the *EHR* data through the blockchain. The high security and believable confirmation of the blockchain technology provided a validation system for clustering the correspondence of heads with one another and a base solution through a neighborhood blockchain [29].

The idea of a power grid system using blockchain was proposed in [30,31]. It was observed and justified that blockchain technology will be more useful in the utilization of available power and resources through its decentralized nature [32]. Using blockchain can provide more efficiency and security. In the literature related to blockchain, some researchers proposed the idea of integrating electronic technologies, such as an inverter with blockchain, which can be more helpful in smart cities by providing efficiency and a low cost [26]. This is proof that blockchain can provide better solutions to solar-system-based power grids [33].

2.2. Smart Healthcare

Recently, the blockchain-based IoT has provided more security and ease of management for sensor data, which has led to more advancement in the IoT field [34,35]. One great application is the integration of blockchain into the healthcare domain. Using blockchain, patients and doctors can access electronic health records in a secure manner. A doctor can add an *EHR* to the blockchain for a patient, and it can also be provided for future usage. Medical sensors are used in such applications to gather sensor data [36]. Most developed countries, such as China, the USA, and the UK, are integrating blockchain with

their digital healthcare systems because, it helps in the transformation from a traditional medical system towards a digital healthcare system.

2.3. Smart Homes

Smart homes play a vital role in human life and in social economics [37]. Smart homes are important applications of the IoT and sensor networks [38]. Blockchain-based sensor networks and smart cities can be applied for improvements in smart homes [39]. In the following literature, these applications were discussed. An IoT-based sensor network consisting of distributed but connected sensors that broadcasted data to the connected nodes, which was called a cluster head, was presented in [15]. Blockchain has gained great importance in various fields, but there are security issues. Moreover, there are challenges related to access control and performance. In an IoT-based network, data are verified through a centralized system that manages the security of the data. According to the security breach level index, millions of peoples' data are stolen worldwide [40]. DoS attacks, device spoofing, and Byzantine fault tolerance are some of the most prominent security breaches related to sensors and IoT-based networks. In this paper, we provided the security challenges related to sensor networks and the application of blockchain technology with integrated sensor networks [40]. We designed a novel smart-contract-based algorithm that checks the security of the users, and if the requested users have enough rights, then access is granted; otherwise, it is denied. In this research, we replaced the central authority of the network, as the blockchain technology was integrated as a backbone of the IoT and sensor network in order to obtain the optimum privacy and cope with security issues [41]. Blockchain technology plays a vital role in present technologies; most significantly, in the IoT, it improves a network by consolidating various sorts of sensors and things to produce connections among things without human involvement [42]. Frequently, the devices of the IoT have restricted network storage, capacities, and computing processors. Therefore, they have more opportunities to be attacked. The reliability, security, and privacy of data are three basic issues in the field of IoT security [43]. The blockchain-technology-based IoT supports flexible access control policies for users who want to securely access data from the IoT. Blockchain is an important technology for the administration and storage of the metadata of patients, smart healthcare, and clinician data [36]. Recently, blockchain technology has been used to increase the applications of IoT technology. The reason is that blockchain technology contains numerous aspects that can improve the security of IoT devices, which are restricted by limited resources [44,45]. Dorri, Kanhere [37] designed a lightweight scalable blockchain (LSB) framework for IoT industries. They integrated the application of a lightweight consensus mechanism in the IoT and smart homes [14].

2.4. Smart Government

The IoT has widespread use in smart governments to ease the maintenance of policies; hence, people can easily approach the available facilities provided by the government [46]. One application that has been implemented regarding this aspect is the improvement of smart services and reaching vital destinations [47]. Nowadays, there are many applications in this filed of research. For example, this provides easiness to the administration of government polices and rules [48]. First, the privacy rights of patients correspond to the access rights of materials. Doctors or professionals who have access to read a patient's data are granted access to the patient's health records. Using an attribute-based access control policy corresponds to a patient privacy information system or healthcare system, and the PHR access behavior corresponds to the application of patient privacy. A user's interaction with a healthcare system and the behavior returned by our proposed framework ultimately correspond to a patient privacy return action. Moreover, reading access corresponds to the action of reading the patient's private data [44]. Similarly, private patient data must be read after using the access control and security policy that were designed. The patient privacy copyright records are applied for and returned in the smart contract system, which comprises four sub-modules in the proposed system, i.e., (1) the

patient module, (2) the private blockchain module, (3) the proposed smart contract module, and the (4) healthcare module. The comprehensive patient query subsystem provides management related to patient privacy copyright records and serves functions for querying and linking various systems. The blockchain subsystem includes a private blockchain for doctors and the healthcare system with patient privacy. Table 1 shows a comparative analysis of the benchmark models.

Table 1. Analysis of the benchmark models.

Benchmark Models	Access Control	Performance
Medrec [49]	NO	Medium
Medblock [50]	NO	Low
Medchain [51]	NO	Low

2.5. Research Gap

The existing blockchain-based frameworks, i.e., Medrec [49], Medblock [50], and Medchain [51], use blockchain for data storage. These existing techniques only focus on the storage of data. The issue with the existing approaches is that they do not provide security and privacy for users by using encryption techniques. Moreover, the computational cost of these approaches is very high due to the encryption techniques used for their implementation, and the transactions are delayed. Hence, in this paper, we provide a novel security and privacy mechanism, a ring-signature-based flexible access control framework, which provides anonymity and flexibility to its users. Moreover, our proposed framework provides access to users based on their attributes.

3. Proposed Methodology

In this section, we explain our proposed scheme. We propose and design a patient query sub-module that consists of a private blockchain sub-module, a healthcare smart contract sub-module, and a healthcare database sub-module. In our proposed framework, the patient sub-module plays a very important role and provides assistance to users for accessing patient privacy copyright records. Moreover, it serves functions for querying and linking various systems. The blockchain subsystem includes a private blockchain for doctors and healthcare systems with patient privacy. Figure 1 shows the sub-module of the the proposed healthcare module. In Figure 1, we describe the detailed structure of the sub-module of the system, which operates according to the following steps. **Step 1.** In our proposed framework, the user first logs into the system through a blockchain application programming interface (API), and then requests the desired patient health record. **Step 2.** In this step, the smart contract is triggered for the privacy check. This smart contract will check for the security and access control rights. If the applicant making the request has authorized user rights, then they are provided with access to a specific PHR; otherwise, access is denied. **Step 3.** In this step, the contract confirms that the users have eligible privacy and access control rights, and the PHR is provided to the user. **Step 4.** In this step, the authorization level is checked according to the access control policy for each participant. This depends upon the users' access control rights; a user can read, write, delete, add, or update. **Step 5.** In this step, the smart contract monitors the behavior of a patient and records the session and interaction.

Figure 2 shows the return process of the sub-module of the framework. In the following, we explain it step by step.

Step 1. In this step, the participant first logs into our proposed system and then searches for the desired patient privacy record.

Step 2. In this step, the smart contract is triggered in order to check the privacy and access rights. The smart contract checks if the session is overdue; if it is overdue, then it is returned to the return sub-module for privacy updates.

Step 3. In this step, the smart contract updates the PHR and modifies it.

Step 4. Then, the returning smart contract performs recalculations, updates the latest status for the PHR, and maintains its privacy.

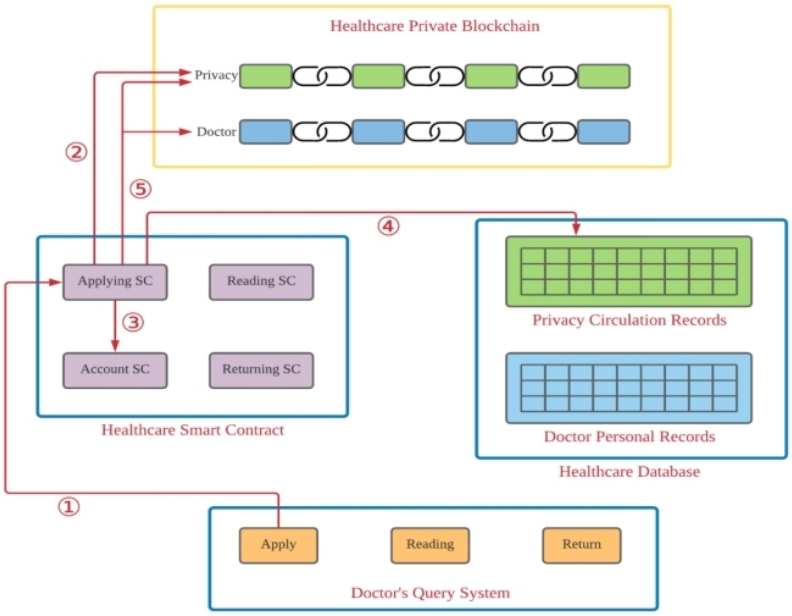

Figure 1. Data flow of the proposed healthcare application subsystem.

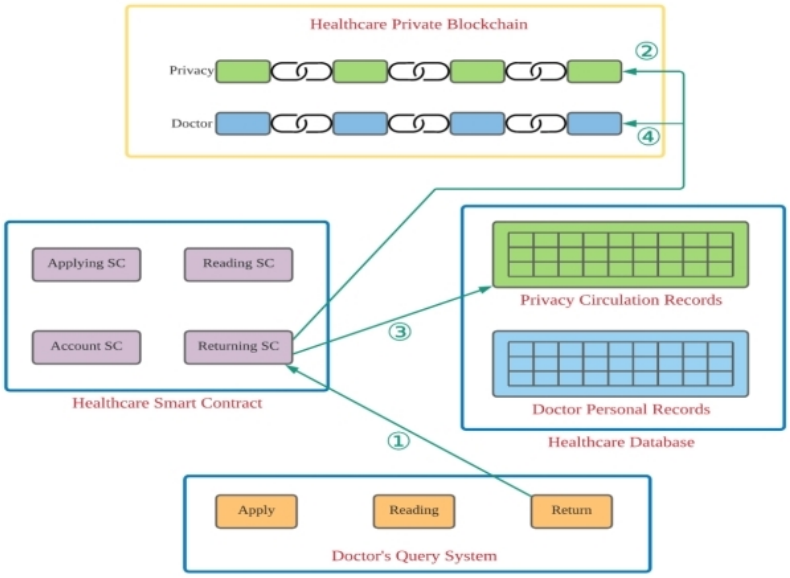

Figure 2. Proposed privacy check using the cross-domain module.

Next, we explain the reading sub-module of our proposed system. The reading process is shown in Figure 3, and it acts according to the following steps.

Step 1. Participants first log into our proposed framework and then search for their desired PHR.

Step 2. When the smart contract for reading is triggered, it checks the privacy.

Step 3. Our proposed smart contract verifies the reading platform for privacy purposes. Then, after checking the privacy and access control rights, participants are informed that they can read the information.

Step 4. In this step, the smart contract will regularly check whether or not the usage period is still valid.

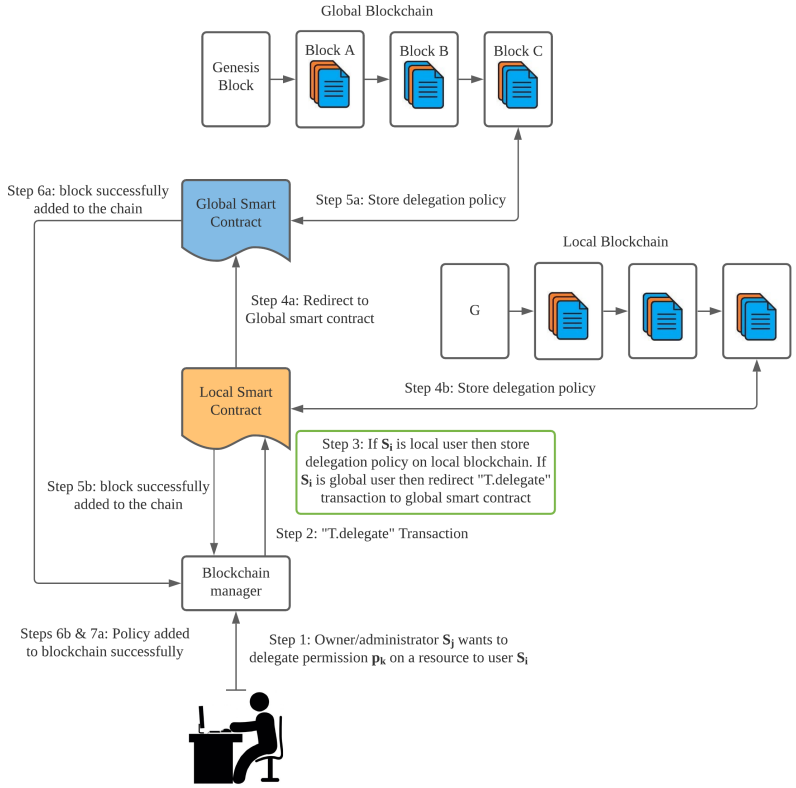

Figure 3. System architecture.

In the next sub-module, the participant checks the privacy record during the loan period. The participant can try to connect to the healthcare reading platform at any time to read the requested documents. The reading processes are explained in Figure 3, and they use the following steps.

Step 1. Users first try to log into the system and search for the desired health records.

Step 2. The smart contract for reading is activated; it will first check the private blockchain of the healthcare system to verify the participant's access rights.

Step 3. The reading smart contract checks the reading platform. Then, the private blockchain is connected for reading.

Step 4. During the reading process, the smart contract regularly verifies whether or not the time limit has been reached. This is clearly described in Figure 3.

System Architecture

Figure 3 shows the system architecture, which consists of a user interface, local domain, and public domain. We can also call these a local blockchain and a global blockchain. Our proposed system architecture consists of three layers. We call this a three-layer internet topology. The first layer is the user layer, the second layer is the local domain, and the third layer is called the global domain. If a user wants to store polices in the blockchain, the smart contract is triggered according to the request. The initial block in the blockchain is known as the Genesis block. It has no previous hash address. Its hash address is considered to be zero. If the user wants to store access control policies in the local domain, then the local smart contract is triggered, and the local smart contract adds a new block in the local domain to store it. Otherwise, the global smart contract is triggered to add a new block in the global domain and store the policies.

4. Flow of Transactions Using the Proposed Framework

In Figure 4, we show the transaction flow architecture for our proposed model. In this architecture, we have labeled each transaction with the label of T_n and the responses with R_n; the person who endorses the transactions is represented by E. P represents the peers,

which are the numbers of connected nodes on a common channel C. We represent the blockchain network with N. The Orderer nodes are denoted by O; these are the nodes that assign public and private keys to the certificate authority (CA). We have labeled the block as B in our proposed architecture.

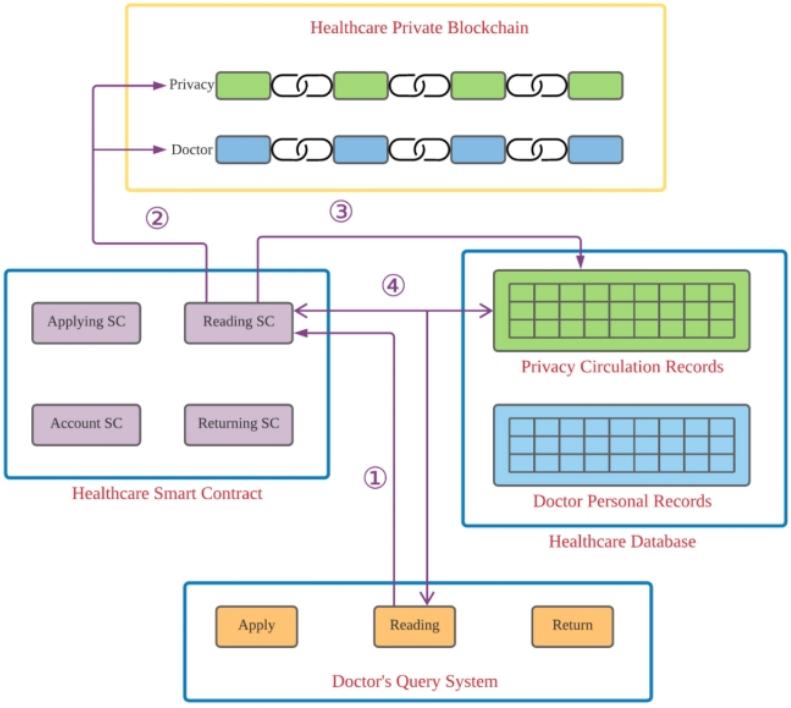

Figure 4. Proposed blockchain-based access control framework.

In Figure 5, we describe the transaction validation architecture. In this figure, we provide the details of how our proposed framework validates transactions in order to provide secure access control by using attributes and smart contracts. We can clearly observe in Figure 5 that there are two peer nodes, which are represented by P, and each node transfers a set of transactions in the form of a block. Each block consists of valuable information, such as a hash address, the number of transactions, the endorsement mechanism, a signature, and hash techniques. The mechanism that we use to design a cross-domain blockchain-based framework for healthcare systems and to evaluate the improvements is illustrated in Figure 6.

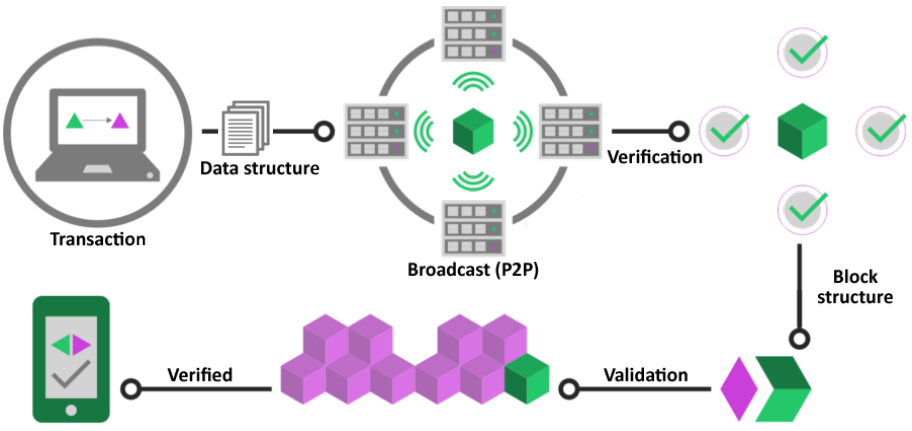

Figure 5. Proposed topology for the blockchain and the IoT.

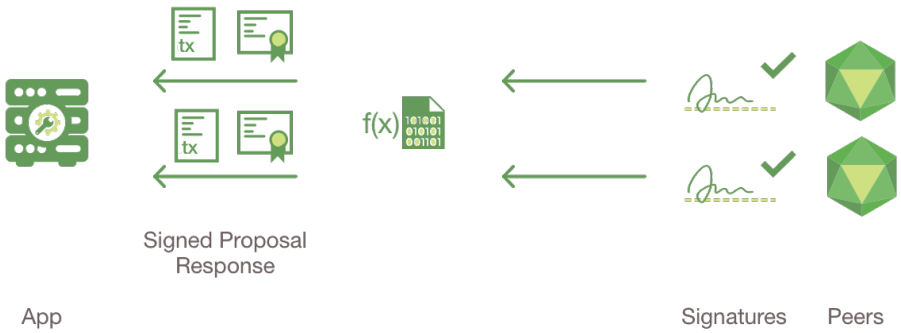

Figure 6. Proposed structure and flow of transactions through our proposed topology.

5. Proposed Algorithms

Our proposed *PHR* access control system has four types of users. These users mainly consist of administrators (*Admin*), patients (*Pt*), clinicians (*Cl*), and lab staff (*Ls*). The details of the execution of the administrative part in our proposed framework are presented in Algorithm 1. This part consists of enrollment certificates (*EC*). The certification authority is responsible for the enrollment certificates. The administrative module can access the system with exclusive rights. The administrative part can read, write, update, and revoke any participants. If the physician, patients, or laboratory staff provide valid attributes, then the administrator has the right to issue a relevant *ID* to each participant (authorized user) to provide access to the proposed framework. If a user's behavior is found to be wrong, then the administrator has the right to remove that participant from the Hyperledger blockchain network with a remark. We illustrate all the notations with explanations in Table 2.

Algorithm 2 describes the workings of the patient sub-module. To log into a patient node, the procedure is to request a private key from an administrator. After access to the blockchain network is granted, the patient can read, write, and revoke access to the *PHR*. In this algorithm, the module uses its attributes as the key to identifying an authorized user as a patient. In the following algorithm, *CID* stands for the clinician *id*, *BN* stands for the blockchain network, and U^{Name} stands for the username.

We designed new algorithms, i.e., Algorithms 3 and 4, for the encryption and access control policies. We used a ring signature in order to encrypt the *PHR*. Our access control policies are based on attributes and identities. If a user meets both the identity and attribute requirements, then he/she is granted access; otherwise, access is denied. This is clearly mentioned in Algorithms 3 and 4.

Authentication Mechanism

We proposed our own authentication method where we used a ring signature mechanism. An entity to be authenticated needs to prove its claimed attributes by declaring that it is eligible and its corresponding private signature key.

(1) Unilateral authentication: Only one pass is needed in unilateral authentication, where only one of the two communicating entities is authenticated by others. A simplified authentication mechanism is shown in Figure 4. In the unilateral authentication mechanism, the authentication process is initiated by the claimant e_i, and it is authenticated by the verifier e_j. The form of $Token_{i,j}$ is: $Token_{i,j}$= $N_i||ID_i||T$ ext$||s_{ki}(N_i||ID_i||T_{ext})$, where $s_{k,i}$(X) indicates the signing on the message X using the private signature key s_{ki} of claimant e_i.

N_i is a non-repeating random number that is used to prevent valid authentication information from being accepted at a later time. T_{ext} is not a necessary data field for authentication, but it can be added for other purposes. Claimant e_i initiates the authentication process by sending $Token_{i,j}$ to the verifier e_j. Upon receiving $Token_{i,j}$, the verifier e_j first ensures that it possesses a valid public key of the claimant e_i. Then, the verifier e_j verifies $Token_{i,j}$ by generating a signature on the unsigned message through a further comparison with the signature received in $Token_{i,j}$.

(2) Mutual authentication: When two participants are mutually authenticated by each other, one more inverse pass is involved, as described in the algorithm and the mathematical equation. The form of $Token_{j,i}$ is: $Token_{j,i} = N_j \,||\, ID_j \,||\, \text{Text} \,||\, ss_{k,j}\,(N_j \,||\, ID_j \,||\, \text{Text})$. After e_i is authenticated by e_j , the two parties exchange their roles with each other, which means that e_i becomes the verifier and e_j becomes the claimant. e_j initializes another round of the authentication process and sends $Token_{j,i}$ to the verifier e_i. Upon receiving $Token_{j,i}$, the verifier e_i first ensures that it posses a valid public key from e_j. Then, the verifier e_i verifies $Token_{j,i}$ by generating a signature on the unsigned message and further compares it with the signature received in $Token_{j,i}$.

Algorithm 1: Admin Node

$I \leftarrow 100$
if $C_{ID} \leftarrow Valid$ **then**
  Add $CID \leftarrow Blockchain$
else
  Add(BN , CID)
  Grant access (CID, $UName$, PK)
end if

Algorithm 2: Patient Node

Input: ID and key requested from $N - admin$
Output: Get access to PHL transactions
Initialization: PHL should be a valid node. PHL can read/write/grant/revoke EHR records.
procedure Patient($P - ID$)
while (True) **do**
  if $(P - ID = B - N)$ **then**
    if (PHR does not exist $B - N$) **then**
      Create$_{records}$ (P_{ID}, $PREC_I$, B_N)
    else
      Update$_{records}$ (P_{ID}, $PREC_I$, B_N)
      Read$_{records}$ (P_{ID}, PHR, C_{ID}, L_{ID}, B_N)
    end if
  else
    Not$_{exist}$(P_{ID})
  end if
  if (Visit (P_{ID}, C_{ID}, L_{ID}, B_N)) **then**
    P_{ID} = Medrecord (P_{ID})
    if $(P - ID\ PHR\ (B_N))$ **then**
      Grant records $(P_{ID}, C_{ID}, L_{ID}, B_N)$
    else
      (C_{ID}, L_{ID}) $\leftarrow$ NOTIFY("Medical record does not exist")
    end if
    if (P_{ID} C_{ID}, L_{ID} Treatment-Completed (P_{ID})) **then**
      Revoke$_{records}$ (P_{ID}, $PREC_I$, $C - ID$, L_{ID}, B_N)
    else
      (C_{ID}, L_{ID}) $\leftarrow$ NOTIFY ("$P - ID$ voluntary revoke P-ID")
      Revoke$_{records}$ (P_{ID}, $PREC_I$, C_{ID}, L_{ID}, B_N)
    end if
  else
    Not Visit
  end if
end while end procedure

Algorithm 3: Attribute-Based Identification Algorithm

1: Input: Public Key
2: Output: Verification result: succeed or fail.
3: Generate a random integer $r \in [1, N-1]$
4: Compute $w = g^r$ in G_T and convert the data type of w into a bit string
5: Compute integer $h = H2(M||w, N)$
6: Compute integer $l = (r-h) mod N$; if l = 0, go to step (2);
7: Compute element $S = [l]ske$ in G_1
8: Convert the data type of h and S into a byte string, and output (h, S) as the signature on message M

Algorithm 4: Attribute-Based Signing Algorithm

1: Input: Master public signature key (Ppubs) of domain, system parameters of domain, message (M0), e's identity (IDe), and digital signature (h0, S0)
2: Output: Verification result: succeed or fail.
3: : Convert the data type of h0 into an integer; if h0 $\in [1, N-1]$ does not hold, the verification fails;
4: : Compute element t = g h0 in GT;
5: Compute integer h = H2(M | | w, N)
6: Compute integer l = (r − h) mod N; if l = 0, go to step 2
7: Compute integer h1 = H1(IDe | | hid, N)
8: Compute element P = [h1]P2 + Ppubs in G2
9: Compute element u = e(S0, P) in GT
10: Compute element w0 = u • t in GT , converts the data type of w0 into a bit string
11: Compute integer h2 = H2(M0 | | w0, N). If h2 = h0 holds, the verification succeeds. Otherwise, the verification fails

Table 2. Notations and their explanation.

S.NO	Parameters	Details
1	BN	Blockchain Network
2	C_{ID}	Clinician ID
3	LID	Lab ID
4	PHR	Patient Health Record
5	R^s	Ring Signature
6	U^{Name}	Username
7	P^K	Private Key
8	r	Integer
9	N	Number of Nodes
10	G	Bilinear Order Group
11	P^1	Generator of Additive Group 1
12	P^2	Generator of Additive Group 2
13	id	Bilinear Identifier
14	H	Homomorphic Encryption
15	k	Degree of Signature
16	$G1$	Group 1 of Bilinear Pair
17	$G2$	Group 2 of Bilinear Pair
18	r	Number of Rounds
19	h	Digital Signature
20	W_o	Random Weight
21	S	Signature
22	T_{id}	Token

Table 2. *Cont.*

S.NO	Parameters	Details
23	P_K	Public Key
24	Mod	Modulus
25	D_e	Decryption
26	E_T	Transmission Energy
27	P^T	Transmission Power
28	p	Probability
29	$Elec$	Node Election
30	$SM1$	Modular Signature

6. Data Type and Sub-Module of Our Proposed Framework

The data for our proposed framework are intended to be patient health records (PHR). PHR can be divided into three classes: PHR privacy attributes, explicit id, and $quasi - id$. Explicit id is normally used as a patient's identifying information that indicates the patient, such as an ID number, name, and cell number. Similarly, the $Q - ID$ provides the patient's bio-data and home address, as well as their age, date of birth, and office address. Privacy-related information refers to a patient's sensitive attributes, which include types of illness and the patient's income or resources. To publish the patient's health data and to maintain their 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 will provide a novel technological approach that includes anonymity, diversity, and confidence. Figure 7 shows the Block header and sequence of transactions leveraging CA.

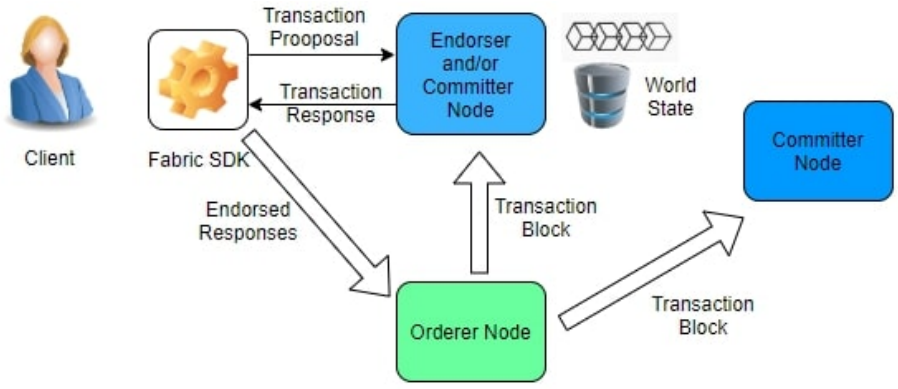

Figure 7. Block header and transaction sequence using CA.

7. Proposed Approach to the Experimental Setup and Analysis

The step-by-step procedure is described below. We first identify the features that affect the performance of a cross-domain framework in a healthcare system. We then pre-process and elaborate these features. We have developed a novel algorithm for a cross-domain blockchain-based framework and a clustering mechanism to be used for performance improvements. An experimental evaluation of the security and performance with the highest number of rounds is conducted by using a novel smart contract. The experimental evaluation is conducted by using the three-layer internet topology. To allow multiple sensors to be placed, the topology is partitioned into several domains; the sensors are placed using an effective sensor placement algorithm and by using smart contracts such that the delay between the blocks and transactions is minimal. The performance results of the proposed approach are compared with those of the benchmark schemes by using blockchain tools, Matlab, and Pycharm.

Figures 5 and 6 represent the configuration and background of our proposed blockchain. We implemented our proposed blockchain by using a Hyperledger Fabric component and

the Docker tool. The code was edited with chaincode, and we performed our analysis with the Spyder IDE tools.

7.1. Computational Overhead

We evaluated the communication cost by using mathematical modeling; through simulations, we evaluated all of the operations.

Theoretical analysis: We deployed our framework in a key-generation system and used sensors for every domain. Our main objective was to achieve authentication and authorization. In our proposed framework, each node and entity executed the various cryptographic operations that were involved in the system. We summarized the most time-consuming operations performed in Medrec. To evaluate the computational overhead, we counted the cryptographic operations using the $G1/G2$ addition operations, exponentiation in GT, and bi-linear pairing, which are denoted by $PA1/PA2, SM1/SM2/SMT/SMr1, ExpT$, and BP, respectively. The rest of the operations, such as hash operations, integer addition, and multiplication, took little time in our tests, so they were not considered here. The numbers of time-consuming cryptographic operations are provided in the simulations results. It should be noted that the operations were not simply added up when combining the authentication and key negotiation. We used two signing and verification algorithms for authentication and authorization. Moreover, we used a ring signature to provide encryption and decryption due to its lightweight features and because it provides anonymity for the signer. More and more, we used different sizes for the messages in order to check and evaluate the variations in the proposed algorithms.

7.2. Equation for the Number of Rounds and Transmissions

In these equations, we describe the energy transmitted by each sensor Et in the communication process. However, they also describe the residual energy of the transmitter. ERx describes the receiver node's energy. K is the constant. d denotes the diameter of the network or the distance between the nodes.

$$ETx(k,d) = ETx - Elec(k) + ETx - amp(k,d), \tag{1}$$

$$ERx(k,d) = ERx - Elec(k), \tag{2}$$

$$ERx(k) = Eelec * k. \tag{3}$$

$$P^L(f) \propto f^k, \tag{4}$$

$$P^L(f,d) = PLo + 10nlog10d/do + X\sigma. \tag{5}$$

$$P^Lo = 10log10. \tag{6}$$

$$(4\pi df)c^2, \tag{7}$$

8. Results and Discussion

We implemented our proposed smart contract and access control policies using Node.js and the Postman web API. Similarly, we tested our simulations for concurrent requests of m with $N = 50$, 200, 400, 600, and 800 nodes. We kept the total number of requests to 800 and the total number of policies to 1100. For our initial simulation, we tested the results for 250 nodes.

Figure 8 shows the simulation results when the average authentication time took 240 ms. We set the time for authorization to 30 ms, and the "access control policy" took 120 ms. We also observed that our proposed policy for the delegation and revocation took 87 ms. With our proposed method and in the experiments, we achieved significant improvements by running the simulations from 200 to 800 rounds, respectively. The results are shown in Figures 8 and 9, respectively. We also tested the proposed policies that were mentioned earlier for the number of rounds, which ranged from $N = 50$ to 800 clients. The results show that the throughput of the proposed framework increased with an increase

in the number of concurrent requests. Our proposed method provides an efficient access control policy as compared to the other existing benchmark methods.

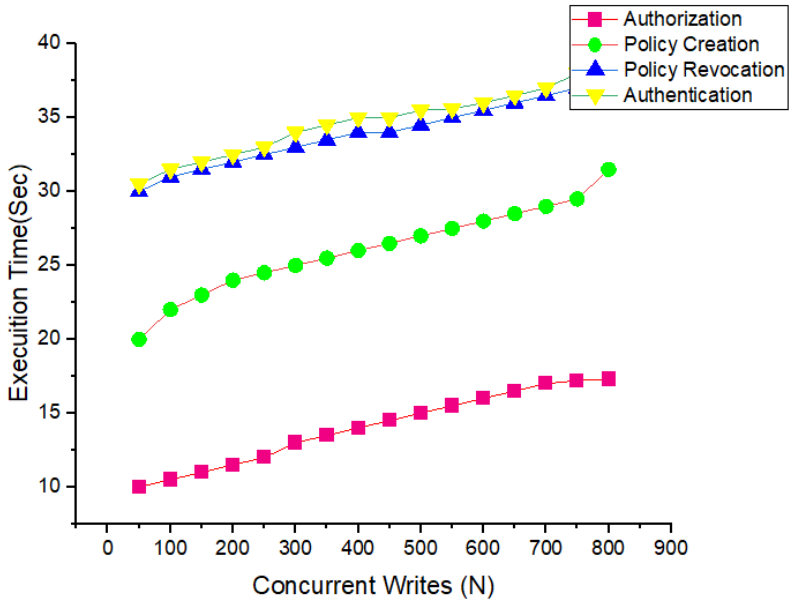

Figure 8. Simulation results of our proposed policies for access control.

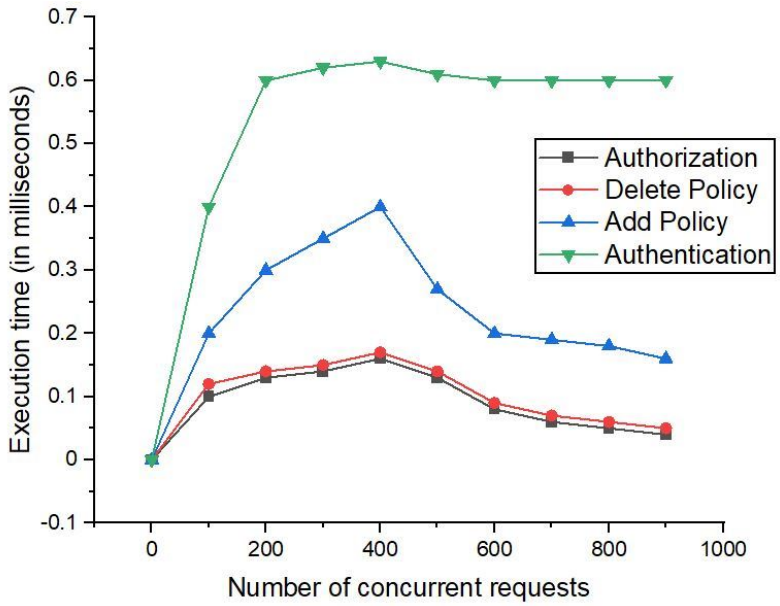

Figure 9. Simulation Results of our proposed policies for access control.

Figures 8 and 9 show that the execution time of user authentication and policy creation was not affected much by the increase in the number of policies. However, the user authorization time and policy revocation time increased due to the increase in the time required to search for a specific policy in a long chain of policies. We also performed experiments for the user authentication, authorization, and delegation policies. We further divided our policies into creation and revocation operations. We evaluated our experiments for the same requests and ran the simulations from $N = 0$ to 4000 concurrent requests. N shows the total number of concurrent requests. The total number of delegation policies was kept constant, i.e., $p = 1000$. Initially, 500 concurrent virtual client requests were tested. The average authentication time took 240 ms, the authorization time took 30 ms, the

"delegation policy" creation time took 120 ms, and the "delegation policy" revocation time took 87 ms. Then, the experiment was repeated for $n = 200$, 400, 600, and 800, as shown in Figure 9.

Figures 10 and 11 describe the encryption and decryption time taken for different formats of electronic health records. From Figure 10, it is clear that the increase is not significant if we increase the file size to 864 kb, while more time is taken if the *EHR* size increases to 4329 MB. Taking the encryption time into account, we used the ring signature for the encryption and decryption, which was shown to take less time compared to the group signature and traditional signature methods. Moreover, we also conducted an analysis of the encryption and decryption time for three different formats—Malay, English, and Urdu. It took much less time if the file was in the Malay language. However, the average encryption and decryption time for these three formats remained the same when using the ring signature.

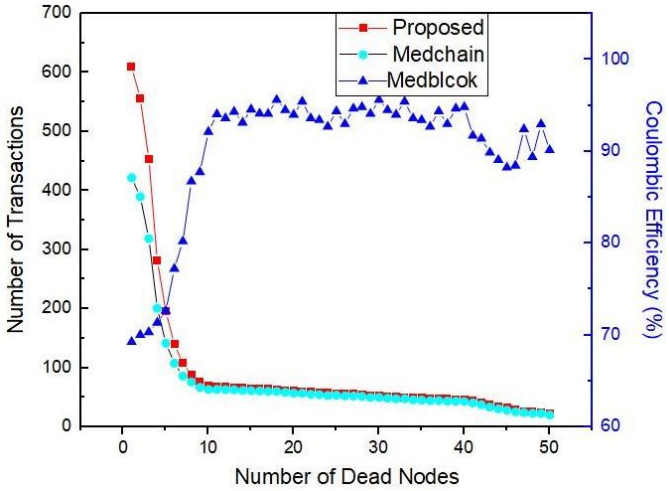

Figure 10. Number of dead nodes versus number of rounds for our proposed framework and benchmark models [50,51].

In Figure 12, we provide an experimental analysis of the number of evaluation reports for the executions carried out for each evaluation request. We kept the number of evaluation requests between 10 and 90. In Figure 13, we provide the simulation results for the amount of throughput with respect to the number of evaluation requests and number of blocks transferred. Figure 13 presents the simulation results for the execution throughput for 20 matched evaluation requests. Figure 13 shows that, for 10 and 30 evaluations, the percentage of confirmed transactions was same, and this proved that our proposed framework provides high throughput in the cases of 10, 30, and 50 evaluation requests under cross-domain conditions. It can also be observed that our proposed framework has some limitations at the initial stage, i.e., for large numbers of evaluation requests the throughput is affected more, as shown by the yellow line.

Figure 10 presents the number of dead nodes and the number of rounds for our proposed framework. We ran our simulations for 2500 rounds, and the number of dead nodes reached 100. In this case of sensors deployed in a healthcare system, we can see that our proposed smart contracts provide better efficiency because we observed that for 100 sensor nodes, the number of rounds can reach 1200.

We also evaluated our proposed framework for the number of packets sent to the base station and the number of rounds. The X-axis represents the number of rounds (N), and the Y-axis represents the number of packets sent to the cluster head. It is very clear in Figure 11 that with 2500 rounds, the number of packets sent is 8000. This shows the greater efficiency compared to the benchmark models in the literature.

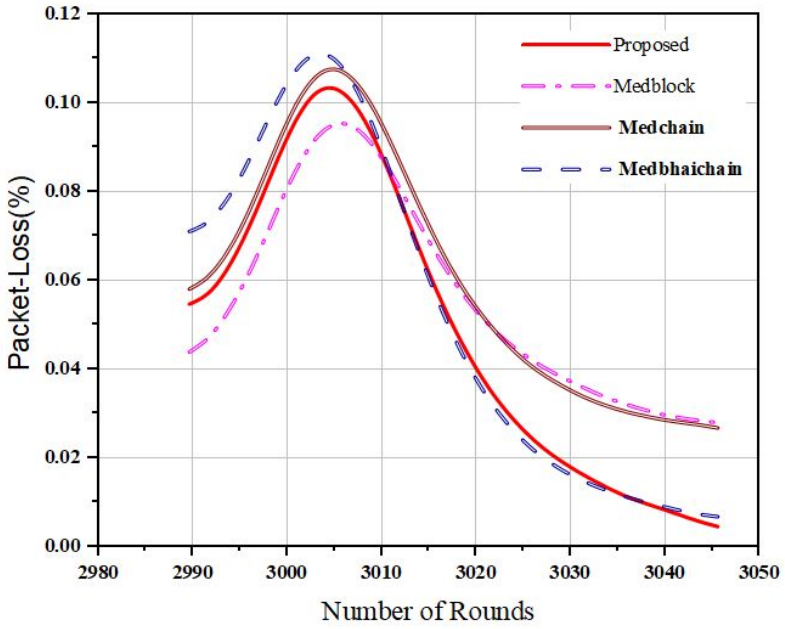

Figure 11. Number of packets sent to the BS versus the number of rounds (0, 2500); comparison with the benchmark models [50,51].

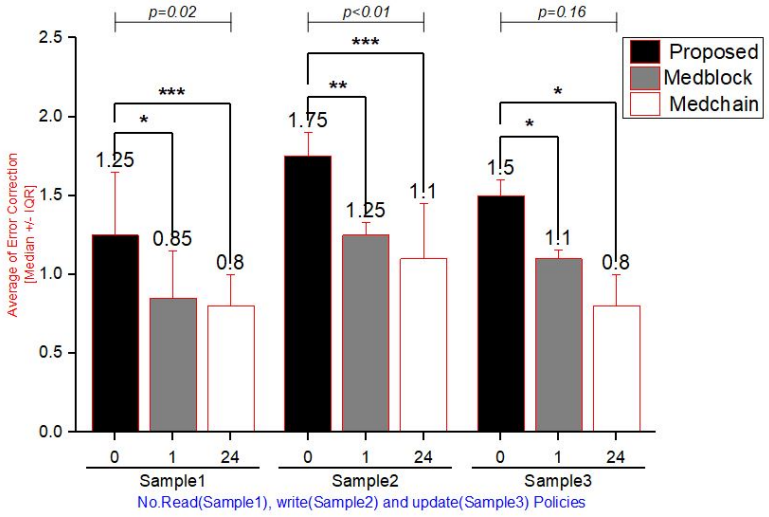

Figure 12. Comparative analysis of the number of various access control policies and a comparison with the benchmark models [50,51].

Figure 12 presents the number of rounds and the number of packets sent to the cluster head (CH) when using medical sensors to gather patient data through the blockchain. We ran our transactions with up to 2500 rounds and evaluated the performance of our proposed system; we found that our system performed efficiently for the maximum number of rounds by sending PHR and EHR to the cluster heads.

In Figure 13, we provide a comparative analysis our proposed framework with the benchmark models when embedded with medical sensors. The benchmark models taken in this case are Medrec and Medblock, which are blockchain-based technologies. From these simulations, we can see that the number of dead nodes in the case of our proposed framework is less than those of the benchmark models. For the same number of dead nodes, our proposed framework delivers more transactions. Hence, this justifies that our proposed approach is more efficient in terms of throughput.

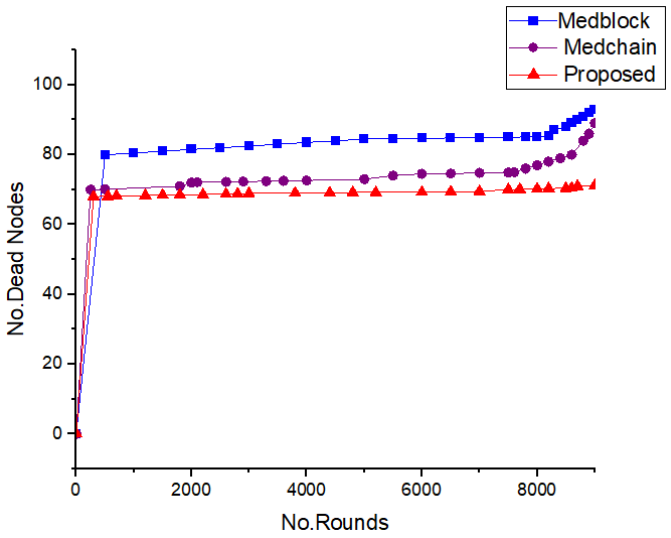

Figure 13. Comparative analysis of our proposed framework vs. the benchmark models [50,51] considering the attributes of dead nodes versus the total number of rounds (0, 9000).

Figure 14 provides the simulation results for the number of live sensor nodes based on our proposed framework and the benchmark models. It is evident from Figure 18 that, for the same delay and transaction endorsement time, the number of live nodes is greater than those of the benchmark models. With this comparative analysis, it is proved that our proposed approach is better than the benchmark models for the use of blockchain for PHR.

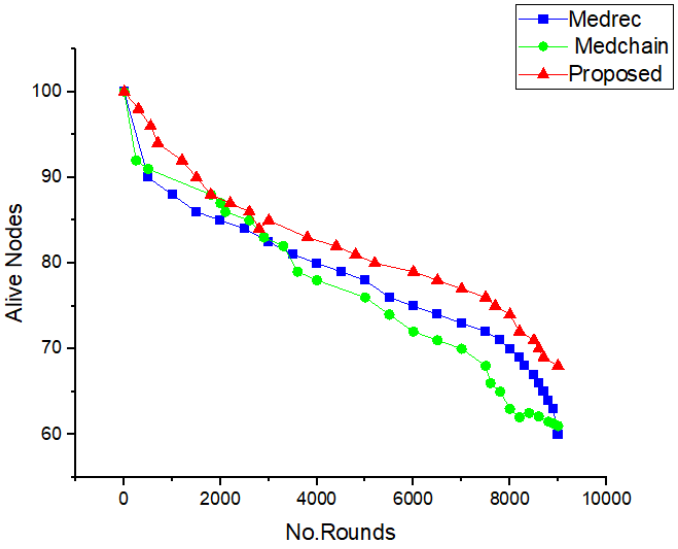

Figure 14. Comparative analysis of live nodes vs. the total number of rounds with the benchmark models (Medrec [49], Medbloc [51]) (0, 9000).

Figure 15 provides a classification of users interactions with our proposed method. We used machine learning techniques, such as K-nearest neighbors (KNN), to classify users according to their behaviors and interactions. We set a threshold value of trust, which was 1.0, and if a user's interaction with the system is good enough, then the system would provide a value of 1; otherwise, this would be 0.5 or 1. We divided the participants into three major groups based on the classification of their interactions. This provided more security and alerts regarding trust and access to the PHR. For the number of rounds and cluster head selection, we used the following equations:

$$Eelec = 50 \text{ nj/bit.} \quad (8)$$

$$Eamp = 100 \text{ pj/bit/m}^2. \tag{9}$$

$$EDA = 50 \text{ nj/bit}. \tag{10}$$

$$do = r\sqrt{fx/e^m p}. \tag{11}$$

The mathematical model above consists of four equation, and it describes the cluster head selection based on the remaining energy from the live nodes. We used the following KNN technique to classify the users into different groups.

$$ED = \sqrt{(x_2 - x_1)^2}. \tag{12}$$

Here, in the euclidean distance equation, which is denoted by ED, x_1 and x_2 represent the two groups of datasets.

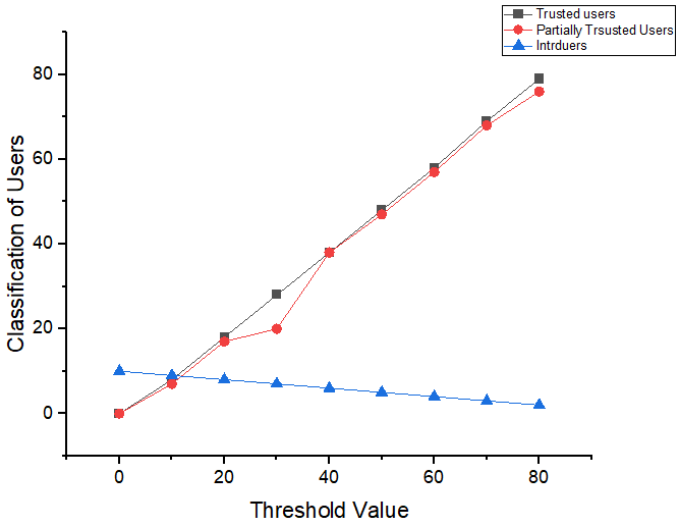

Figure 15. Using machine learning techniques to classify users' trust according to their behaviors and interactions.

In Figure 16, we present a comparative analysis of our proposed scheme with respect to the benchmark models. In Figure 16a, we present a comparison of our proposed framework and the benchmark models in terms of the number of dead nodes and the time for execution taken by each framework for various policies and transactions. It can be easily observed that our proposed framework performs better than the benchmark models [49,50]. Moreover Figure 16b shows the simulation results for the number of dead nodes and the time for execution taken by each framework for concurrent access control policies. The greater the number of live nodes is, the greater the efficiency of the framework will be. In addition, in Figure 16c, we show our comparative analysis based on the number of packets sent versus the execution time for each sent packet. From Figure 16c, it is evident that our proposed framework has significant improvements over the benchmark models [49,51]. The equations for the number of dead and live nodes are as follows:

$$E_{ADV} = E_o(1 + \alpha). \tag{13}$$

$$E_{INT} = E_o(1 + \mu). \tag{14}$$

$$nb(1 + \alpha), \tag{15}$$

So, the energy of all nodes in the blockchain-based network will be equal:

$$nb(1 + \alpha), nE_o(1 - m - bn), andnmE_o(1 + \alpha). \tag{16}$$

In the above equation, E represents the energy and Adv represents the advance nodes' energy. Int represents the intermediate nodes' energy, whereas n represents the normal nodes.

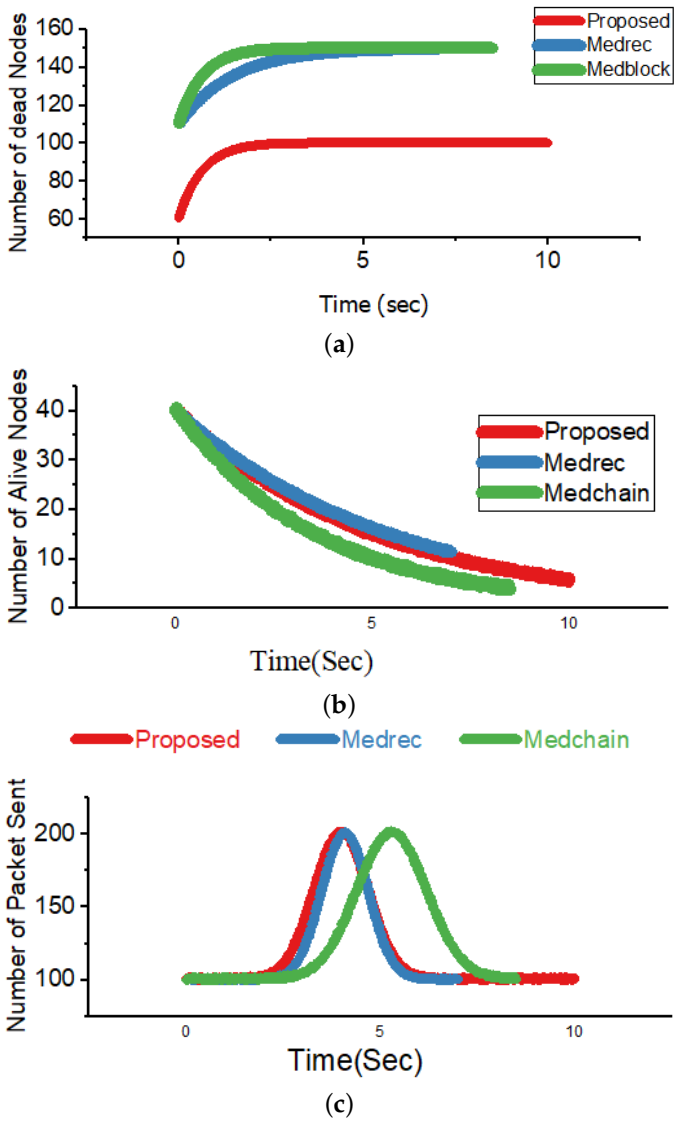

Figure 16. Comparison of our proposed method with the benchmark models [49–51] in terms of: (**a**) the number of dead nodes, (**b**) number of live nodes, and (**c**) number of packets sent.

In Figure 17, we provide the simulation results for the number of transactions sent versus the number of *PHR* transferred per transaction. From the simulations, it is very clear that the proposed framework provides more efficiency compared to the benchmark model with respect to *PHR*.

In Figure 18, we provide a comparative analysis of the proposed method for different domains while using sensors to monitor health records and share them through a blockchain network. We used medial sensors, such as sensors for the pulse and heartbeat, as well as temperature sensors. Each sensor collected data and sent it to the base station using smart contracts. The smart contracts delivered the transmitted patient data to the BS, and then they were stored in the blockchain ledger. We can easily observe from the simulations that the sending of packets through our proposed framework in the case of medical sensor nodes took less time for confirmation; hence, the throughput was significantly greater than that of the benchmark models.

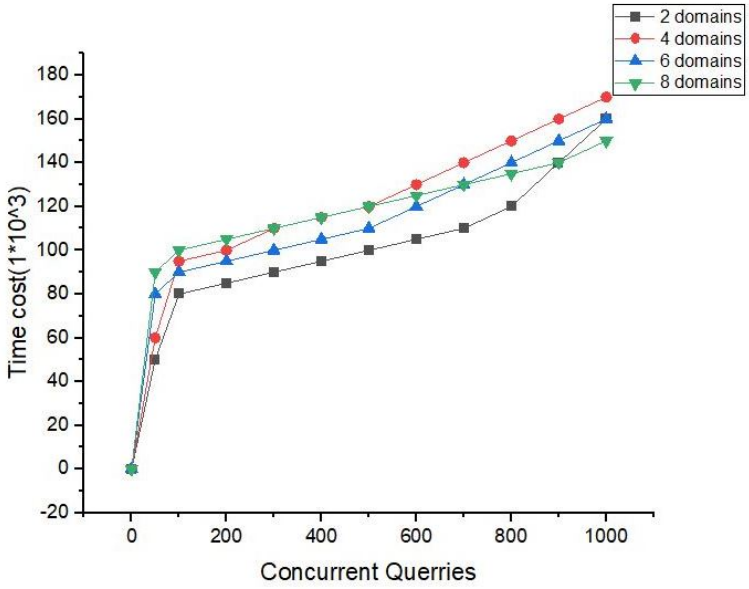

Figure 17. Efficiency analysis of our proposed method in different domains.

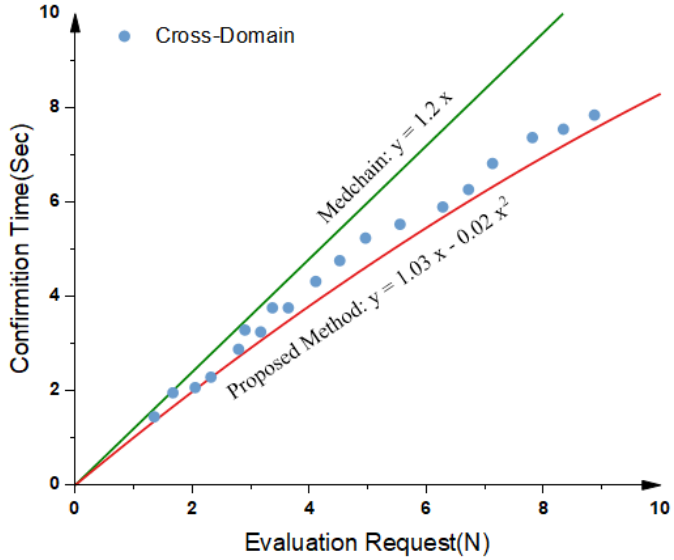

Figure 18. Comparative analysis of the cross-domain module used in our proposed framework.

In Figure 19, we show the intensive simulations and experiments carried out in the cross-domain case. We used different types of domains, and we evaluated the number of query requests versus the time taken. It can be observed that, as we used lightweight encryption techniques with flexible access control policies, the throughput in the cross-domain case was very efficient. From Figure 19, it is very clear that our proposed framework can provide efficient throughput up to 70 domains. Our proposed framework is thus limited to 70 domains. In comparison, Medrec and Medchain can support up to 8 and 10 domains, respectively. Hence, our method surpasses the previous schemes because they can only support 8 to 10 domains. So, in order to provide more security for patients, they can only access data, EHR, or PHR in up to 70 domains.

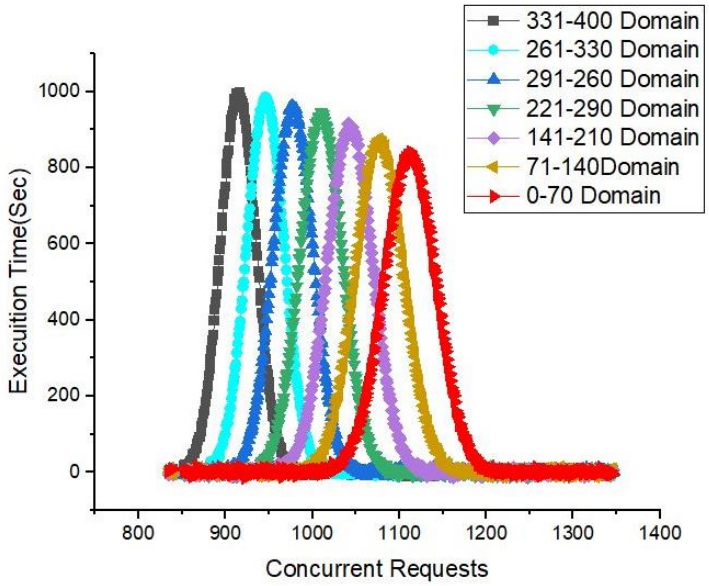

Figure 19. Comparative analysis of the proposed flexible policies for the cross-domain case.

In Figure 20, we provide the cumulative simulations and comparative analyses of our proposed framework and the benchmark models. We used different scenarios and parameters, such as dead nodes, live nodes, sensor energy, and throughput, to evaluate the efficiency and security of the proposed framework. CH selection was performed on a probabilistic basis; each node generated a random number r, which was inclusive of 0 and 1. If the value was less than the threshold value, then it was considered as a cluster head (CH). Threshold formula is given below:

$$Tn = p/1 - p(r, mod(1/p)) \tag{17}$$

$$P_{nrm} = P_i P_t / (1 + (m\alpha + b\mu)), \tag{18}$$

$$P_{int} = P_i P_t (1 + \alpha) / (1 + m\alpha + b\mu), \tag{19}$$

$$n(1 - m - b)p_{nrm} + nbp_{int} + nmp_a d_j = np_i p_t. \tag{20}$$

In these mathematical equations, P represents the power of the sensor node. P_t represents the transmission power through a sensor nodes. N represents the number of nodes. α is a constant value used for the delay in the transactions. In Figure 20, we justify the efficiency and throughput of our proposed framework and the benchmark models [49–51]. The number of rounds in Figure 20 ranges up to 300, and the total number of packets sent is 8000. From Figure 20, it can be observed that by using our proposed framework and the smart contracts that we have proposed, more packets can be sent within the same number of rounds in comparison with the benchmark models [49–51].

Figure 21 represents the simulation results for the comparative analysis of the proposed framework and the benchmark models. We carried out a comparison of the number of rounds and the number of transactions. From Figure 21, it is clear that the number of transactions sent with the proposed method was greater than that with the benchmark models. Through the proposed smart contracts, the delay was comparatively small, and hence, this led to a greater number of transactions with the sink.

Figure 22 shows a comparison based on the number of dead nodes versus the number of rounds. The simulation results show that the number of dead nodes is lower compared to those obtained with Medrec, Medchain, and Medblock. Figure 23 presents the number of rounds and number of live rounds based on simulations. We carried out our experiments for up to 300 rounds, and the value of the number of live nodes reached 5000. From the simulations, it is evident that for a specific number of rounds, the number of live nodes

is greater with the proposed method. Hence, our proposed framework provides more efficiency compared to the benchmark models.

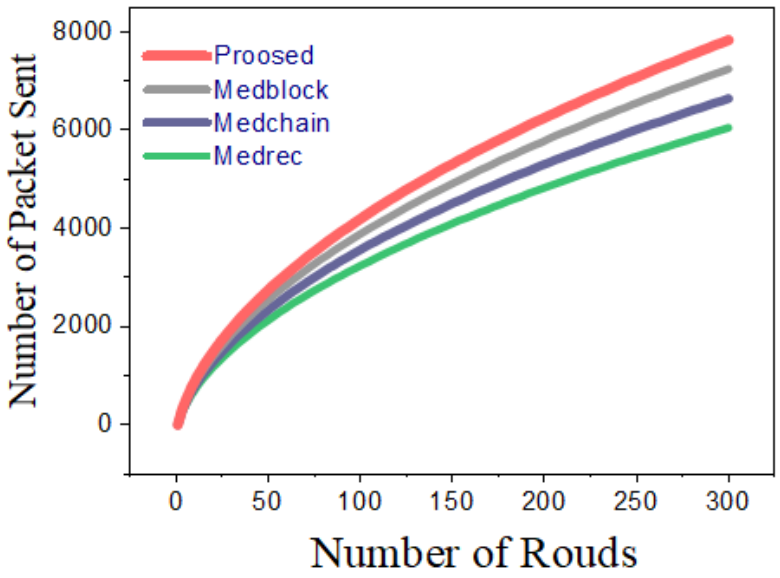

Figure 20. Comparative analysis of the proposed access control policies and the benchmark models (number of rounds versus packets sent) [49–51].

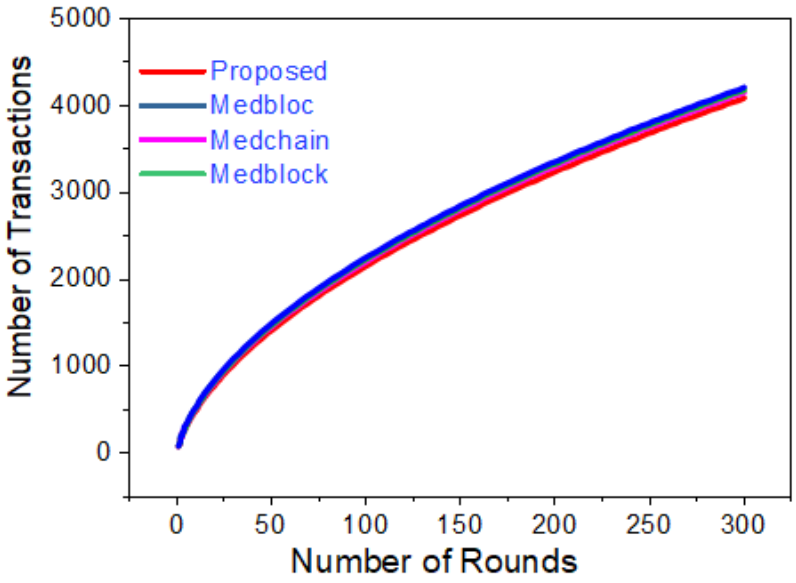

Figure 21. Comparative analysis of the proposed flexible policies for the cross-domain case and the benchmark models [49–51] (number of rounds versus number of transactions).

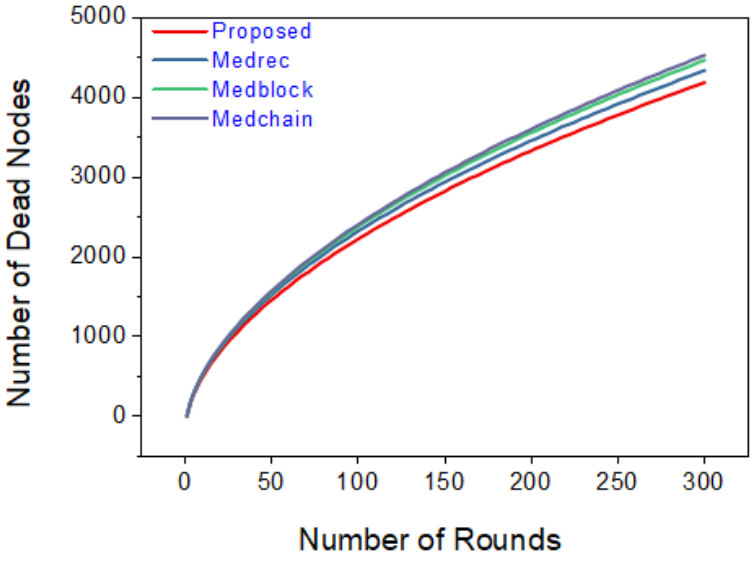

Figure 22. Comparative analysis of the proposed flexible policies for the cross-domain case and the benchmark models [49–51].

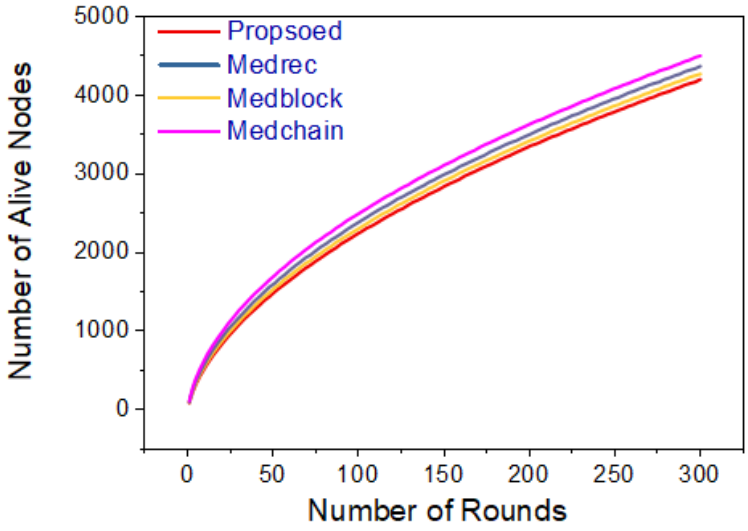

Figure 23. Simulation results based on a comparison of the proposed model with the benchmark flexible policies for cross-domain models [49–51].

9. Conclusions and Future Work

In this research, we proposed a blockchain-based framework using Hyperledger Fabric with flexible access control policies. We used a cross-domain framework for our proposed framework. Moreover, we performed our experiments for one, two, three, and four organizations. We used Hyperledger Fabric as a tool to implement our proposed framework. Moreover, we used two types of software to implement the proposed algorithms, i.e., Hyperledger and the Ethereum tool. To evaluate our experimental data, we used PHYCHARM and Spyder *ID*. From the analysis, it is very clear that our proposed framework provided better throughput and security, which was confirmed by the simulation results. We used the KNN clustering technique to classify the users based on their interactions with the framework. In addition, we divided the users into different clusters based on their trust values and according to the proposed access control algorithms. In order to provide more security, we used a ring signature for encryption and decryption. An efficient access control method integrated with blockchain was implemented in our framework for applications in digital health systems. The proposed system supports and

stores computer-generated data from various clinical devices, which undergo a collection and authentication procedure. The data are aggregated and are correct, which means that they can go unchallenged, are tamper resistant, and are protected in their delivery; this can lead to a reduction of cyber crime. Through this research, the existing issues and problems in the literature on the digital healthcare industry can solved. In the future, we would like to add more fine-grained access control policies in order to access each resource based on these policies.

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

Funding: This research was funded by Taif University Researchers Supporting Project (number TURSP-2020/239), Taif University, Taif, Saudi Arabia.

Acknowledgments: The authors are thankful 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.; 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; pp. 1–9.
2. Arfat, Y.; Shaikh, R.A. A Survey on Secure Routing Protocols in Wireless Sensor Networks. *Int. J. Microw. Wirel. Technol.* **2016**, *6*, 9–19. [CrossRef]
3. 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, Gujrat, Pakistan, 19–20 December 2016; Volume 19, p. 20.
4. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Cross-domain secure data sharing using blockchain for industrial IoT. *J. Parallel Distrib. Comput.* **2021**, *156*, 176–184. [CrossRef]
5. Idrees, S.; Nowostawski, M.; Jameel, R.; Mourya, A. Security Aspects of Blockchain Technology Intended for Industrial Applications. *Electronics* **2021**, *10*, 951. [CrossRef]
6. Sharma, A.; Sarishma; Tomar, R.; Chilamkurti, N.; Kim, B.G. Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare. *Electronics* **2020**, *9*, 1609. [CrossRef]
7. 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 12th International Conference, ICIC 2016, Lanzhou, China, 2–5 August 2016; Volume 1.
8. 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* **2020**, *8*, 53649–53665. [CrossRef]
9. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: 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; pp. 1–6.
10. 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. *Sustain. Cities Soc.* **2020**, *55*, 102018. [CrossRef]
11. Mushtaq, Z.; Sani, S.S.; Hamed, K.; Ali, A.; Belal, S.M.; Naqvi, A.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.
12. Kim, H.; Kim, S.H.; Hwang, J.Y.; Seo, C. Efficient privacy-preserving machine learning for blockchain network. *IEEE Access* **2019**, *7*, 136481–136495. [CrossRef]
13. 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.
14. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
15. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* **2021**, *21*, 772. [CrossRef]
16. Kuo, T.T.; Ohno-Machado, L. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv* **2018**, arXiv:1802.01746.

17. 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.
18. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R.; Aledhari, M. Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2146–2156. [CrossRef]
19. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *8*, 1120–1132. [CrossRef]
20. Ali, J.; Lee, G.M.; Roh, B.H.; Ryu, D.K.; Park, G. Software-defined networking approaches for link failure recovery: A survey. *Sustainability* **2020**, *12*, 4255. [CrossRef]
21. Ali, J.; Roh, B.H. An effective hierarchical control plane for software-defined networks leveraging TOPSIS for end-to-end QoS class-mapping. *IEEE Access* **2020**, *8*, 88990–89006. [CrossRef]
22. Tripathi, G.; Ahad, M.A.; Paiva, S. S2HS-A blockchain based approach for smart healthcare system. *Healthcare* **2020**, *8*, 100391. [CrossRef]
23. Dorri, A.; Kanhere, S.S.; Jurdak, R.; 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.
24. Pourvahab, M.; Ekbatanifard, G. An efficient forensics architecture in software-defined networking-IoT using blockchain technology. *IEEE Access* **2019**, *7*, 99573–99588. [CrossRef]
25. 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 (ICRERA), San Diego, CA, USA, 5–8 November 2017; pp. 454–461.
26. Lacity, M.C. Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *MIS Q. Exec.* **2018**, *17*, 201–222.
27. Devibala, A. A Survey on Security Issues in Iot for Blockchain Healthcare. In Proceedings of the 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 20–22 February 2019; pp. 1–7.
28. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, 12–14 December 2016; pp. 1392–1393.
29. 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]
30. Dabbaghjamanesh, M.; Wang, B.; Mehraeen, S.; Zhang, J.; Kavousi-Fard, A. Networked microgrid security and privacy enhancement by the blockchain-enabled Internet of Things approach. In Proceedings of the 2019 IEEE Green Technologies Conference (GreenTech), Lafayette, LA, USA, 3–5 April 2019; pp. 1–5.
31. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. *Comput. Electr. Eng.* **2021**, *93*, 107209. [CrossRef]
32. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by internet of things. *Trans. Emerg. Telecommun. Technol.* **2014**, *25*, 81–93. [CrossRef]
33. Gretzel, U.; Sigala, M.; Xiang, Z.; Koo, C. Smart tourism: Foundations and developments. *Electron. Mark.* **2015**, *25*, 179–188. [CrossRef]
34. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-based Healthcare. *IEEE Internet Things J.* **2021**. [CrossRef]
35. Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. *IEEE Internet Things J.* **2020**. [CrossRef]
36. Ye, C.; Cao, W.; Chen, S. Security challenges of blockchain in Internet of things: Systematic literature review. *Trans. Emerg. Telecommun. Technol.* **2020**, e4177. [CrossRef]
37. Khare, V.; Khare, C.; Nema, S.; Baredar, P. Renewable energy system paradigm change from trending technology: A review. *Int. J. Sustain. Energy* **2020**, *40*, 1–22.
38. Vermesan, O.; Bacquet, J. *Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution*; River Publishers: Gistrup, Denmark, 2017.
39. Kachali, H.; Storsjö, I.; Haavisto, I.; Kovács, G. Inter-sectoral preparedness and mitigation for networked risks and cascading effects. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 281–291. [CrossRef]
40. 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]
41. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
42. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
43. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]

44. Beebeejaun, A. VAT on foreign digital services in Mauritius; a comparative study with South Africa. *Int. J. Law Manag.* **2020**, *63*, 239–250. [CrossRef]
45. 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.
46. Choo, C.W. *Information Management for the Intelligent Organization: The Art of Scanning the Environment*; Information Today, Inc.: Medford, NJ, USA, 2002.
47. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
48. Bruce, R.R.; Cunard, J.P.; Director, M.D. *From Telecommunications to Electronic Services: A Global Spectrum of Definitions, Boundary Lines, and Structures*; Butterworth-Heinemann: Oxford, UK, 2014.
49. Azaria, A.; Ekbaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016.
50. da Fonseca Ribeiro, M.I.; Vasconcelos, A. MedBlock: Using Blockchain in Health Healthcare Application based on Blockchain and Smart Contracts. In Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020), Prague, Czech Republic, 5–7 May 2020; pp. 156–164.
51. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]