applied sciences

MDPI

Article

Secure Healthcare Record Sharing Mechanism with Blockchain

Ghulam Qadar Butt [1], Toqeer Ali Sayed [2], Rabia Riaz [1], Sanam Shahla Rizvi [3] and Anand Paul [4,*]

[1] Department of CS&IT, University of Azad Jammu and Kashmir, Muzaffarabad 13100, Pakistan; ghulamqadir90@gmail.com (G.Q.B.); rabia.riaz@ajku.edu.pk (R.R.)
[2] Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia; toqeer@iu.edu.sa
[3] Raptor Interactive (Pty) Ltd., Eco Boulevard, Witch Hazel Ave, Gauteng 0157, South Africa; sanam.shahla@raptorinteractive.com
[4] School of Computer Science and Engineering, Kyungpook National University, Daegu 37224, Korea
* Correspondence: paul.editor@gmail.com

Abstract: The transfer of information is a demanding issue, particularly due to the presence of a large number of eavesdroppers on communication channels. Sharing medical service records between different clinical jobs is a basic and testing research topic. The particular characteristics of blockchains have attracted a large amount of attention and resulted in revolutionary changes to various business applications, including medical care. A blockchain is based on a distributed ledger, which tends to improve cyber security. A number of proposals have been made with respect to the sharing of basic medical records using a blockchain without needing earlier information or the trust of patients. Specialist service providers and insurance agencies are not secure against data breaches. The safe sharing of clinical records between different countries, to ensure an incorporated and universal medical service, is also a significant issue for patients who travel. The medical data of patients normally reside on different healthcare units around the world, thus raising many concerns. Firstly, a patient's history of treatment by different physicians is not accessible to the doctor in a single location. Secondly, it is very difficult to secure widespread data residing in different locations. This study proposed record sharing in a chain-like structure, in which every record is globally connected to the others, based on a blockchain under the suggestions and recommendations of the HL7 standards. This study focused on making medical data available, especially of patients who travel in different countries, for a specific period of time after validating the required authentication. Authorization and authentication are performed on the Shibboleth identity management system with the involvement of patient in the sanction process, thereby revealing the patient data for the specific period of time. The proposed approach improves the performance with respect to other record sharing systems, e.g., it reduces the time to read, write, delete, and revoke a record by a noticeable margin. The proposed system takes around three seconds to upload and 7.5 s to download 250 Mb of data, which can contain up to sixteen documents, over a stable network connection. The system has a latency of 413.76 ms when retrieving 100 records, compared to 447.9 and 459.3 ms in previous systems. Thus, the proposed system improved the performance and ensured seclusion by using a blockchain.

Keywords: blockchain; cyber-security; medical services; cyber-attacks; data communication; distributed ledger; identity management; RAFT; HL7; electronic health record; Hyperledger Composer

check for updates

Citation: Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure Healthcare Record Sharing Mechanism with Blockchain. *Appl. Sci.* **2022**, *12*, 2307. https://doi.org/10.3390/app12052307

Academic Editors: Suhuai Luo and Kamran Shaukat

Received: 18 January 2022
Accepted: 15 February 2022
Published: 23 February 2022

1. Introduction

There are numerous methods of data communication, each having specific advantages and disadvantages, for which security and privacy are an important concern. In the case of medical data availability, the trust required to provide information, transparency, and access control are important factors, because malicious individuals such as hackers are constantly improving their techniques, with a focus on identifying loopholes in the data transmission process.

Health is the basis of a happy life, and humans are now the beneficiaries of technical advances in the clinical industry [1]. An electronic health record (EHR) is the computerization of a patient's medical history, e.g., test reports and doctor prescriptions. The EHR enables the digital sharing of data with medical officers in any global location. Creating an EHR over the internet ensures that patient information is instantly available to any hospital around the world, when needed, regardless of the hospital that created it. Many EHR systems exist around the world, each with its own specifications. Sharing of information between different EHR systems requires mutual co-ordination, which is achieved through the use of standards [2]. An EHR system must both meet communication standards and be suitable for data models for inter-EHR system communications.

The Internet of Things (IoT) has embraced the blockchain to enhance its security, privacy, and monitoring [3,4]. Many IoT platforms use a blockchain as a distributed ledger to save their data. A number of blockchain architectures exist because each blockchain network needs to follow an architecture to perform transactions in the network. Similarly, platforms exist that use the IoT, blockchains, and the cloud collectively [3]. The research undertaken to date has led to the ecosystem shown in Figure 1. The IoT is shown as a platform in the first layer of the ecosystem.

The blockchain has addressed a number of complications in healthcare; for example, the secure transfer of information between different entities [5], efficiency enhancement due to low-cost transactions, and the restriction of access to information to the individuals concerned [6]. Many blockchain platforms are used in healthcare, and choosing an appropriate platform is a subject of debate within the industry [7–9]. The ecosystem in Figure 1 shows the latest electronic health record sharing mechanisms in its application layer. Trusted authorities are the backbone of the digital economy, and verify the legitimacy of the receiver in a transaction. The inclusion of a third party increases the risk of data being misused, compromised, and hacked [10]. The blockchain address this issue via the use of a distributed ledger and consensus [11,12]. The blockchain has a promising future in the modern world, in which many activities are undertaken online, especially in regard to businesses and commerce [13].

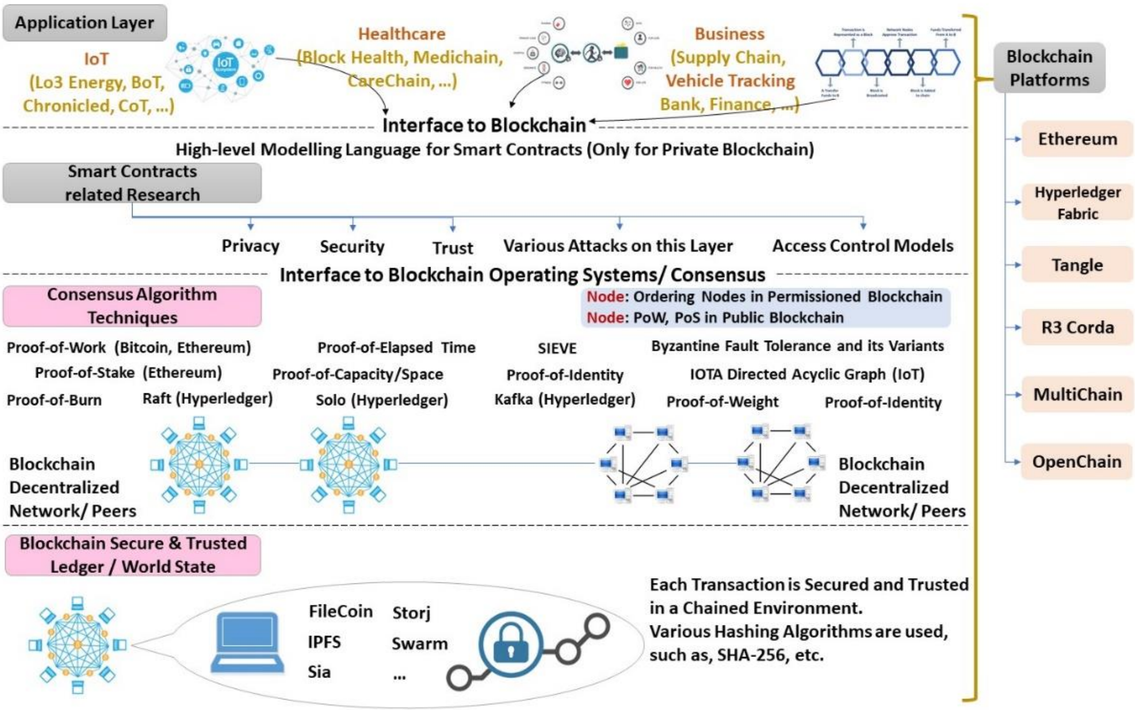

Application Layer
IoT
(Lo3 Energy, BoT, Chronicled, CoT, ...)
IoT
Healthcare
(Block Health, Medichain, CareChain, ...)
Business
(Supply Chain, Vehicle Tracking Bank, Finance, ...)
Interface to Blockchain
High-level Modelling Language for Smart Contracts (Only for Private Blockchain)
Smart Contracts related Research
Privacy
Security
Trust
Various Attacks on this Layer
Access Control Models
Interface to Blockchain Operating Systems/ Consensus
Consensus Algorithm Techniques
Node: Ordering Nodes in Permissioned Blockchain
Node: PoW, PoS in Public Blockchain
Proof-of-Work (Bitcoin, Ethereum)
Proof-of-Elapsed Time
SIEVE
Byzantine Fault Tolerance and its Variants
Proof-of-Stake (Ethereum)
Proof-of-Capacity/Space
Proof-of-Identity
IOTA Directed Acyclic Graph (IoT)
Proof-of-Burn
Raft (Hyperledger)
Solo (Hyperledger)
Kafka (Hyperledger)
Proof-of-Weight
Proof-of-Identity
Blockchain Decentralized Network/ Peers
Blockchain Decentralized Network/ Peers
Blockchain Secure & Trusted Ledger / World State
FileCoin
Storj
IPFS
Swarm
Sia
...
Each Transaction is Secured and Trusted in a Chained Environment.
Various Hashing Algorithms are used, such as, SHA-256, etc.
Blockchain Platforms
Ethereum
Hyperledger Fabric
Tangle
R3 Corda
MultiChain
OpenChain

Figure 1. Working of the blockchain (by same author [14]).

The current research provides, first, a complete design of a framework that integrates global healthcare record systems. This solution is helpful for patients who travel regularly to other countries and, in the case of an emergency, are unable to provide their health history from their home healthcare system. Second, a prototype implementation of a health system is provided over a blockchain and remotely retrieves the records of a remote patient. Third, a general performance analysis was performed over the permissioned blockchain. The transaction analysis shown in the Results and Evaluations Section clearly shows the advantages of this study compared to other similar systems.

The proposal presented in this study enhances the security of the communication of patient data with the use of a blockchain, and lowers the burden on systems via the use of identity management. According to our findings, no previous study has used Shibboleth identity management with a blockchain for the transfer of health-related information to create a global system with proper implementation. In this study, the RAFT algorithm, Hyperledger Fabric, and identity management were used to create a low-burden system for medical record sharing. The results clearly show the dominance of the proposed system with respect to the current EHR systems.

2. Background

The world of Information Technology (IT) has revolutionized methods of dealing with data in various sectors. In particular, healthcare services have become more approachable, flexible, and efficient. An EHR can efficiently keep and transfer the medical documents of a patient, and be used to maintain a detailed patient history. However, the diversity of file formats used by various EHR systems results in issues relating to interoperability, scattering, and security. This study introduces a blockchain to resolve these issues.

2.1. Blockchain

A blockchain is a chain of blocks, often called a distributed ledger, without any ownership. The idea was presented initially by Satoshi Nakamoto in the creation of a cryptocurrency. A blockchain appears as a distributed ledger and has no sovereignty; that is, no individual or organization can dictate the interchange and access of information [15]. The term "distributed ledger" means that data is stored at multiple locations, and is not maintained or owned by a single entity. Thus, any change in the network is replicated on every node in the system, as if every node has the original document [16]. The same ledger is distributed to all nodes, so it is almost impossible to make malicious changes. The ledger stores information in the form of blocks, each of which has header and data sections. The data section stores the transactions, whereas the header sections contain the block metadata. Every header contains hashes of the current and previous blocks.

2.1.1. Types of Blockchain

Blockchains can be divided into two main categories, private and public, with are characterized by huge difference depending on need of the technology. Private blockchains control access and do not allow the general public to have unauthorized access to the network. A node must be authorized by all other nodes before it is provided access [17], but any transaction in the network is visible to all of the authorized nodes of the network. Private blockchains do not have a proof of work or mining, which is in contrast to the operation of a public blockchain. Hyperledger Fabric and Quorum are examples of private blockchains [18].

A public blockchain is open to all, and each node can read and utilize the blockchain to perform any transaction without a central register. In public blockchains, it is optional for each node in the network to validate a modification. Ethereum is an example of an open-source public blockchain. Ethereum uses the Solidity language to create its smart contracts [19], which was created by the Ethereum community. Bitcoin is a cryptocurrency based on a public blockchain, which takes much longer to complete a transaction compared to a private blockchain. According to the official information about the Bitcoin cryptocurrency, it may take up to ten minutes for a transaction to complete [20].

Another type of blockchain exists that combine the benefits of both public and private blockchain properties. Known as the Consortium blockchain, a group of individuals control the network while maintaining the efficiency and privacy of the blockchain.

2.1.2. Blockchain Working

The working of a blockchain can be understood using the scenario in Figure 2, in which a node of the network wants to enter a record in the blockchain network. This request is broadcast to the network, validated by a defined algorithm of the network, and permanently added to the network. This new record becomes unmodifiable after verification of the block [21].

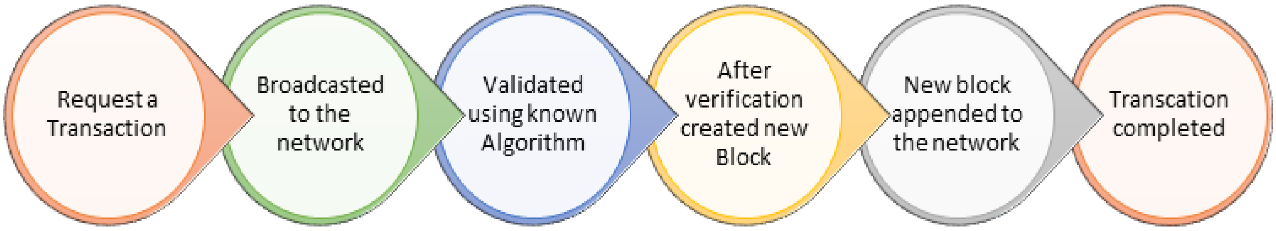

Request a Transaction
Broadcasted to the network
Validated using known Algorithm
After verification created new Block
New block appended to the network
Transcation completed

Figure 2. Working of a blockchain.

2.2. Communication

Communication is the process of transferring information from one place to another [22]. Every communication must consist of a sender, a message, and a receiver. The sender and receiver can be a person or a computerized device, whereas the message can be text, audio, video, voice, or other formats. Accuracy, effectiveness, security, and unambiguity are the main concerns of all communication, and are sometimes hard to achieve. In the case of modern communication, where the sender and receiver can be in different locations around the world, the main concern is ensuring that information is transferred correctly to the receiver, without others listening to the communication during the process.

Significant technological improvements have been made, especially in the field of communication, allowing a receiver to receive information from the sender in seconds. At the same time, threats to communication have also increased. Modern communication requires the inclusion of a form of encryption to minimize the chances of hacking during the communication process [23]. Figure 3 shows the complete communication process. The center of all communication is the message to be transferred, and efforts are made to maintain its integrity. Different forms of security protocols are followed to achieve the security and integrity of the communication, depending on the type of message and the medium through which it will be transferred.

In the system under study, patients, health personal, and service providers are considered users; all of these roles have different levels of authorization. Patients may wish to share their clinical information with other doctors, laboratories, insurance companies, or research centers. Health personal are requesters of the service, e.g., a doctor asking a patient for their previous medical data. Service providers manage the client's data, and are also known as administrators.

Communication Menaces

There are numerous ways a communication can be compromised, and all three components of communication (sender, receiver, and message) can be victims of an attack by hackers. Some common attacks and their possible solutions are described in [24]. Session hijacking aims to attain unauthorized access to any communication [25], and is also referred to as a man in the middle attack (MIMA). In session hijacking, the hijacker pretends to be the legitimate sender or receiver while bypassing the actual legitimate connection. This type of attack is used to steal information, to listen to conversations, and for spying. Session hijacking can be performed by sniffing the network, using a brute force attack (BFA), or using cross-site scripting (XSS) [26]. Session hijacking can be minimized in a network by using a secure socket shell (SSH), https (the secure mode of a website), or a complex session ID [27].

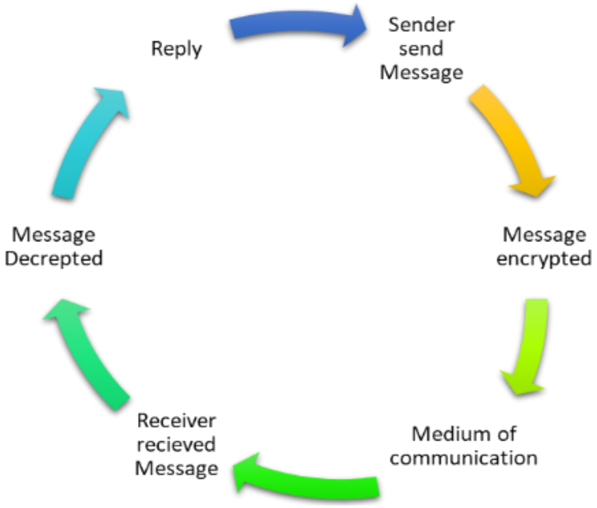


Figure 3. Secure communication process.

Bots (originating from "robot") are software applications over the Internet working on automated tasks. A combination of bots can form a botnet, which can propagate and organize itself to compromise the system of communication. The bots have the ability to install worms that can harm the system by replicating themselves, and also install backdoors that can bypass the authentication and encryption in the system [28]. Bots also cause a denial of service (DoS), and its advanced form, a distributed denial of service (DDoS), which can take a network or system artificially offline. Such challenges and their remedies are discussed in [29]. In probing DNS caches, the IP address of the system accessing the network is checked in a local DNS server, and only IP addressed present in the local DNS server are allowed [30]. Malware (from "malicious software") is a computer program created with the intention of damaging a system or network. There are numerous types of malware, which are intended to have different behaviors; a list is provided in [31]. Data acquisition malware takes data from the victim; honeypots and spam-traps are existing examples. Anti-virus programs can detect data acquisition malware. Behavior monitoring malware aims to monitor changes in the system state and sends the collected data to the attacker, which can be utilized for malicious purposes. These types of malware are identified by updated antivirus software. Account harvesting malware takes users' credentials from a database, search engine, webpage, or any online system, using a computer program. These attacks can be reduced by using a strong password policy, using different passwords for different systems or websites, and by locking accounts after a certain number of failed attempts. The authors in [32] created a penetration testing methodology to secure networks from these attacks.

A Trojan horse is a social engineering method that deceives a user about its true intention, and installs a backdoor that remotely controls the victim's computer, to alter or delete the victim's data [33]. A Trojan horse attack can be avoided by taking extra care when browsing the Internet [34], e.g., use only trusted software, never open mail from unknown senders, do not surf untrusted sites, install authorized antivirus software, and use a firewall to protect against unknown attackers. Packet sniffing targets the transmission medium; all of the communication packets between two participants of a network are captured and analyzed using specialized software. This type of attack can be countered by using a trusted medium of communication, never allowing unauthorized persons near the server, and only permitting trusted computers to access the network. Port scanning regularly scans a system's ports to identify an open port for malicious purposes [35]. An open, compromised port can be catastrophic for any system, and can allow a hacker to access the system's data. This attack can be avoided by disabling the port scanning of the system. A Byzantine attack compromises mobile networks, and involves the hacking of one of the devices on the network due to the leakage of information or credentials, which allows that device to act as a legitimate device. This type of attack is very difficult to identify, but can be minimized by continuous monitoring of the behavior of every device on the network and blocking devices that act abnormally [36]. The threats to a network can be detected using specialized software [37], and incorporating techniques to detect malware, spyware, and other undesired applications on the network.

2.3. Health Level Seven (HL7)

Standards are commonly needed, and HL7 is a well-known organization that creates standards. The exchange of clinical data is only possible between EHR systems if the systems are built on common standards during development; an example is the identification of the mandatory fields of patient information or tests. The global use of HL7 in clinical environments has streamlined the healthcare practice. According to its official website, HL7 has more than 1600 members in more than 50 countries, including corporate members, stakeholders, medicine companies, drug vendors, and suppliers

Health care is also a major initiative of some of the biggest global industries. In recent years, the health care industry has improved significantly, further advanced by inventions in the IoT. However, the communication of IoT and medical data is contentious issue. Although electronic health record (EHR) systems are able to manage the global needs of health-related industries, the security of medical data is a matter of concern. A lightweight and efficient mechanism is needed in the EHR system for the secure transfer of medical data on the basis of standards. This study follows the standards of HL7, one of the leading organizations in the creation of standards in the medical field, to create a robust, expandable, and reliable system for medical data communication.

2.4. Hyperledger Fabric

IBM's Hyperledger Fabric is a primary private blockchain platform for creating and maintaining distributed systems using modular consensus to follow a customized trust model. Fabric applications are written in general purpose languages including Java, Go, and node.js, whereas the smart contract is written in a domain-specific language. Hyperledger Fabric provides greater flexibility and an entirely different blockchain design that deals efficiently with the exhaustion of resources, attacks, and non-determinism [38]. Hyperledger Fabric is written in the Go language, which consists of endorsers, committers, a ledger, a database, and gossip. Endorsers are the peers in favor of transaction or chaincode execution. Committers are the peers that validate the proper configuration and verify the transaction according to the endorsement policy. The ledger consists of a transaction manger and a block store, to verify other transactions and to update the ledger. Gossip checks for ledger failures and maintains the correctness and efficiency of the whole system [39].

Hyperledger Fabric has two main components i.e., chaincode and the endorsement policy. Chaincode is a smart contract that lies at the heart of all the applications in Fabric and runs in the execution phase. It runs separately from Fabric code in a separate container called a Docker container. It stores data in CouchDB through a key-value that can be 'get' or 'put' to read or write transactions in the database. The endorsement policy runs validation and behaves as a protocol of the transaction validation, and cannot be altered by any non-trusted application. An endorsement policy enables chaincode to select the endorser of a transaction. Transactions are initiated by the clients using a chaincode function, who then digitally sign it and send it to the channel. All the peers check the authenticity, structure, and authorization of newly created transactions, via a number of checks that must be verified by the peers. If the peers verify all of the checks, the transaction is executed and the response value is stored in the key-value store.

All endorsements sent by the peers are gathered by the client and matched with the endorsement policy requirements. After gathering the required endorsements, resources are provided in the case of a read request. In the case of a write request, then all of the endorsements are collected and forwarded to an ordering service for the addition of the transaction. The ordering service sends all of the transactions, with their endorsement, to all peers on the same channel, where each channel contains all of the nodes communicating with each other and sharing information with each other over a blockchain network. The peers on the channel verify each of the transactions according to the endorsement fulfillment policy, which contains the smart contract agreement between all the stakeholders. On successful verification, the block is added to the ledger, but all of the endorsing peers have to commit the transaction.

2.5. Consensus Algorithm for Decentralized Trust Management

In the consensus algorithm, all of the nodes of the blockchain network reach an agreement regarding the latest state of the ledger. This consensus stabilizes the blockchain network and maintains the trust of the peers on the distributed network. There are different types of consensus algorithms, some of which are described here.

2.5.1. Proof-of-Work

This is the most famous consensus algorithm, and was initially used by Bitcoin, in which the miner has to solve a complex mathematical puzzle, thus requiring huge computing power. Among all of the peers, the peer that solves the puzzle first can mine a new block in the network.

2.5.2. Byzantine Fault Tolerant (BFT)

BFT introduced voting into the consensus, in which every node has to vote and must come to an agreement about the network's current condition. All the nodes in the network collectively define the blockchain ledger, which is divided into clusters on each node using Kafka. Maximum nodes in the network must participate in the process of voting for a decision in order to minimize the errors in the network. The most important benefit of using this algorithm in a network is that it maintains the network integrity, and will not crash, even if all nodes are not included in the voting process.

2.5.3. Proof-of-Stake

This is a simple algorithm based on the stake a node has in the form of Bitcoin. In contrast to proof-of-work, it does not require high processing power and can be mined with the minimum resources. The node can mine the block according to the percentage of Bitcoin it has, e.g., if a node has 5% of the Bitcoin, then it can mine 5% of the proof-of-stake blocks. Proof-of-stake provides maximum security against network attacks.

2.5.4. Proof-of-Capacity

Proof-of-capacity is the best alternative to proof-of-work and proof-of-stake. In proof-of-capacity, rather than using data centers for mining or the utilization of Bitcoins, free hard disk space is used in the consensus. The node with the maximum free hard disk space has a high probability of being chosen to mine the next block and to win a reward in the shape of a block.

2.5.5. Paxos

The Paxos algorithm is used to reach a consensus in a group of distributed computers. A node or group of nodes choses a value from a number of available choices, and sends it to the network as a broadcast. A consensus is reached when a majority of the nodes agrees on a chosen value. In the case of disagreement, an automated process terminates the consensus. Paxos is efficient in term of resource utilization as it will terminate the consensus instead of being endlessly blocked.

2.5.6. RAFT

RAFT is commonly used due its fault-tolerant nature, simplicity, and efficiency in distributed systems. In RAFT, the network is divided into three types of nodes: leader, candidates, and followers. In this algorithm, every new node must be added to the leader, which is also responsible for maintaining the log in the network, and the algorithm clones it in the network. In the case of a transaction, the leader broadcasts the write request to the followers and verifies its response. On confirmation from all of the nodes, the new transaction is added. A candidate is a node who wants to become a leader, and the leader is chosen on the basis of the votes of the followers. The candidate having the maximum number of followers will become the leader and the previous leader becomes a follower because it lost its majority. Figure 4 explains the complete process of the algorithm.

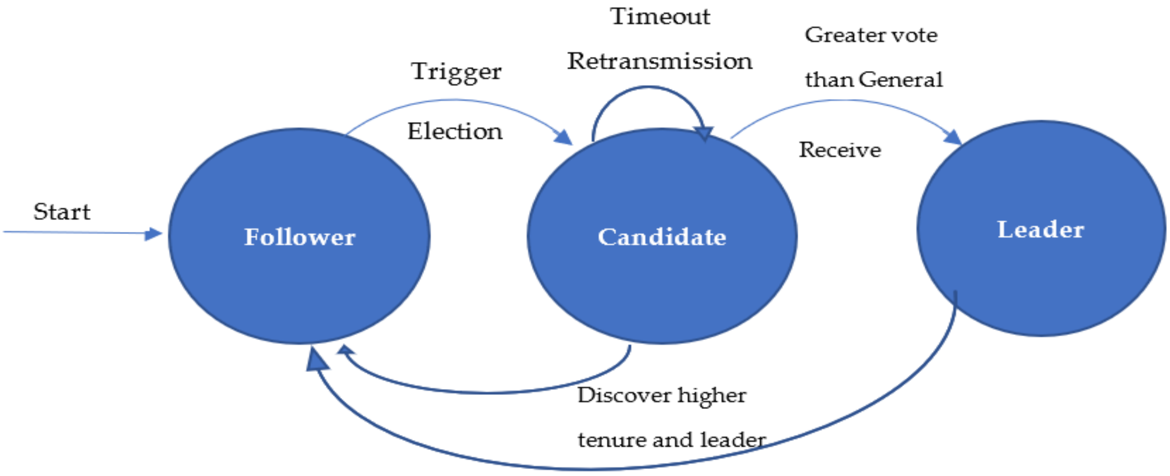


Figure 4. Working of the RAFT consensus.

2.6. Identity Management

Identity management is the task of creating and maintaining user identities. This task recognizes the individuals in a company, network, or country, and controls their access to the assets [40]. Most companies use identity management to lower the burden of data storage because it is not economical to save the record of a user who visited the company only once. An identity provider also enables the option of single sign-on (SSO) for users who want to access the system only once. The current study uses Shibboleth identity management because it is easy to configure and is free to use for study purposes.

Shibboleth is an open-source, multinational, federated identity management architecture [41]. The main concerns of identity management relate to the identity provider (IdP), service provider (SP), and the communication between them [42]. Shibboleth identity management uses Security Assertion Markup Language (SAML) for information transmission between the IdP and SP. Shibboleth identity management also permits the SP to manage their shared users' profile data. It also supports local single sign-on (SSO) and organizational level SSO, for inter-individual and inter-organizational communication, respectively. Users must follow the required procedure to receive the service from Shibboleth identity management. First, the user asks the SP for the service. This request is then forwarded to the IdP by the SP, and the IdP asks for user authentication. The IdP validates the response from the user. After validation, the IdP asks the SP to include the request of the user and provide the user with the service that it demanded [43].

3. Related Work

A blockchain solution for healthcare record sharing, based on Hyperledger Caliper, was proposed in [44]. Another study [45] focused on encryption schemes for sharing of records using a blockchain over cloud services; confusion and anonymity techniques were proposed for encryption of data in the presented model. A Bayesian model for monitoring activities was used in [46], which are then stored on a blockchain network without any consensus algorithm; here, the scheme merely focuses on creating a smart home and collecting data from different modules. Another paper on medical data communication with a blockchain for a cloud-based network mainly discusses security and encryption techniques [47]. A blockchain network based on Hyperledger Caliper intended for small businesses was proposed in [48]. The most recent related work is presented in [49], but this study is limited only to creating a data bank of the medical records and securing it using blockchain technology. Another blockchain-based solution for heath record sharing was proposed in [50]; however, it lacks encryption techniques and the cloud-based structure is not fit for some organizations.

An interesting study regarding the topic of discussion was presented in [51]; however, due to the use of mutable storage, the response time was slower than that of the proposed scheme. The research in [52] summarized some of the main studies related to blockchain and health, and also drew a comparison between these systems. However, it did not provide an implementation of their findings, and only compared the existing systems at the current time. Another system created under the blockchain umbrella was presented in [53]. This is an efficient system based on Hyperledger Fabric; although it has some similarities with our system, the study was not related to healthcare, and its results were inferior to those of the system presented in the current study. Ref. [54] presents a state-of-the-art network for sharing information, with the inclusion of identity management; however, this study is difficult to implement due to the much higher production cost. Another significant study in the field of secure transfer of information in health is presented in [55]. In this research, the authors propose a new model for information interchange between IoT devices using a blockchain network and the efficiency of a 5G network. Although the study showed promise, it is currently only a proposal and no implementation plan has yet been designed. A blockchain technology for communication in health applications due to the privacy and security provided by the blockchain was proposed in [56]. The study also proposes the use of cloud technology with Fabric, but the study does not provide an idea of how to implement it in the real world. All the studies presented above are either just proposals and are not yet implemented, or have lower efficiency than the system under study, due to the different limitations discussed above. Some also have a higher cost, are difficult to implement, or use cloud technology with the blockchain.

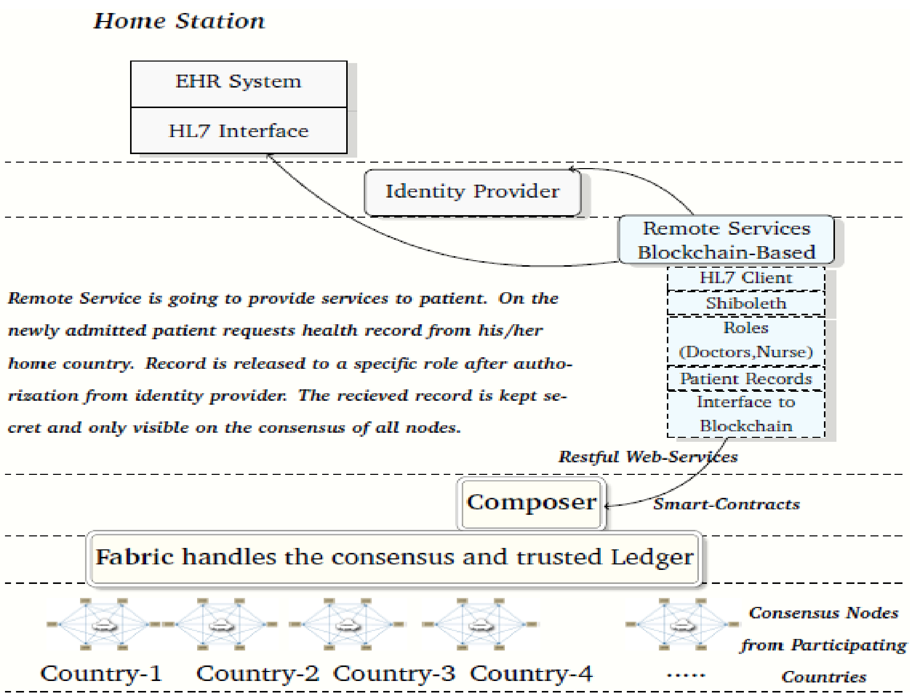
4. Proposed Solution

A blockchain is a distributed ledger with built-in security and privacy features, and can be used in communication by storing messages in chains of blocks for transmission, thus reducing many of the attacks that may occur during the secure communication. Applications related to financial transactions and users' personal data require strict access control. An audit is also required of who accessed the data, the time at which they accessed it, and the length of time for which they had access. All of these issues can be resolved using a blockchain's built-in feature; that is, once a transaction is confirmed in the blockchain, it is almost impossible to modify it in verifiable way [57]. The peer-to-peer nature of a blockchain makes it highly fault tolerant, because each node has the same copy as that of the other nodes, and it is difficult to alter all of these copies. In a system attack, the intruder is unable to change anything meaningful, and can be easily identified due to the log management of the blockchain.

A consensus is also required from all the participating nodes in order to perform a transaction or communication in a network. The use of the consensus reduces the effects of DoS or DDoS attacks, and makes it difficult to add malware to the blockchain network. Cryptography is also a built-in feature of blockchain, because every transaction in a network is communicated or stored in the form of a hash [58]. Each blockchain network uses a specialized hashing algorithm that is very difficult to crack. Thus, if an eavesdropper listens to a communication or has access to a transaction through packet sniffing, they cannot make use of it because it cannot be decrypted [59]. A blockchain network is not located at a single location, nor is it owned. This decentralized nature of a blockchain makes it resistant to port scanning attacks and also prevents the network from being destroyed. Due to the decentralized nature of a blockchain, the system availability is much higher than that of traditional systems. All of these features were the inspiration for the use of a blockchain in this study.

4.1. System Architecture of Proposed Model

The system under study uses an innovative architecture for medical data communications with the use of a blockchain, as shown in Figure 5. The suggested design consists of a service provider in a home station, a Shibboleth identity provider, and a blockchain ledger. The service provider must be registered in the home station, and provides the information to remote stations when required. The home station properly investigates the information, and only provides the information after verifying the role and authentication level of the medical person demanding the information. The home station prohibits access to the information if the request is not appropriate to the level of the role asking for the information.



Remote Service is going to provide services to patient. On the newly admitted patient requests health record from his/her home country. Record is released to a specific role after authorization from identity provider. The recieved record is kept secret and only visible on the consensus of all nodes.

Figure 5. Proposed architecture.

In this study, Shibboleth federated identity management was included as the service provider due to its open-source nature and its adaptability in the domain. Using Shibboleth, each medical person is given a unique id and is authorized according to their role. Depending on their role, it is decided whether the healthcare personal should be given SSO or complete login credentials for that role, and for how long these credentials remain active for the particular medical person.

The blockchain maintains all records using CouchDB, according to the standards provided by HL7, thus ensuring the interoperability between different systems. This study used a permission blockchain, so no proof-of-work concept is required; rather, consensus is achieved using an automated procedure to maintain the efficiency of the system. A well-known Hyperledger algorithm, RAFT, was used as the consensus algorithm. RAFT is a fault-tolerant and easily understandable consensus algorithm that enables clients to create distributed systems as a single system. Randomized election, log replication, fault tolerance, and ease of use are the distinguishing properties that motivated the use of RAFT in this study.

4.2. Working Procedure

The client must by registered on the home station (HS) to be eligible to receive the services of the system. Algorithm 1 shows the working procedure for the registration of a client on the HS, in the case in which a patient traveled to a remote station (RS) and required their medical history from their home station. The client needs to open the interface provided by the identity provider corresponding to the HS through a web application, arranged by the patient's own country. Due to the security and sensitivity of healthcare data, the HS does not deliver sensitive information to a non-approved user; however, the HS asks the login credentials to be entered; the system then follows the procedure for authentication as shown in Algorithm 2. It first checks if the client has blockchain network access, and then asks for the client's login credentials. After a successful login, all of the relevant IdPs are displayed, which are authenticated by the HS.

Algorithm 1: Create_Contract: Algorithm that create a smart contract in blockchain network

```
Input: BlockchainAddress Ba, Timestamp Ts, HomeStation Hs, Client Ct,
Terms&Conditions Tc
Output: Bool
if Ct exist then
return false
else if Ct agrees on Tc then
    mapping Ct to Ba
    add it to ledger of Hs with Ts
return true
```

A blockchain intermediary node is used to save the transactions on the blockchain network. The correspondence between the remote station and the home station is transmitted through this node, which is also associated with the blockchain through Hyperledger Composer. Figure 6 shows the complete working process in a sequence diagram. The Shibboleth identity provider provides the complete list of IdPs for their roles. This is also provided to all of the registered home stations, and these IDs are shared through a signed XML document for security purposes. The HS diverts the solicitations to the Shibboleth for approval of the mentioned job. The web application demands credentials, which are given by the respective IdP, and the HS requires the IdPs to be approved, regardless of their actions or their designation. All of the authentication and security are maintained by the IdP, and the service provider then diverts the resources to the HS, in addition to the approval tokens delivered by the IdP.

Algorithm 2: Access_Request: Algorithm shows how a client access its data on network

```
Input: BlockchainAddress Ba, Client Ct, Credentials Cd
Output: Bool
if Ct is not Ba then
throw;
end
if Cd ≥ Approved then
return true
else
return false
```

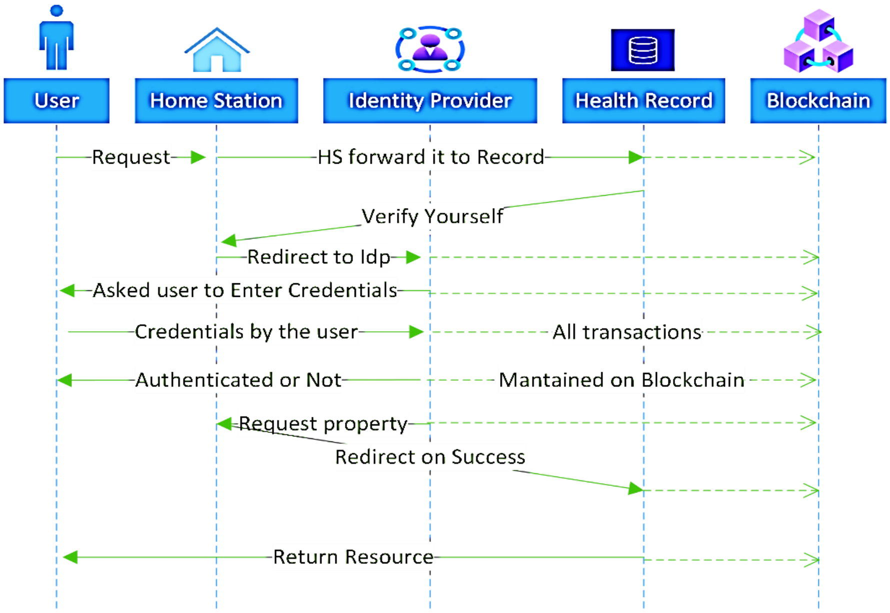


Figure 6. Proposed system's sequence diagram.

The HS approves the metadata, utilizing the protocols related to the security of the system, and delivers the clinical data in normalized form. The proposed design is based on the HL7 standards, which are presently used in numerous countries, because very little effort is required for their integration into the system. The proposed strategy safeguards the privacy of the entities utilizing the clinical data. It also recognizes the privilege of the patient to acquire the information about these elements, and makes it feasible and scalable for the HS. The distributed deployment and modular architecture lower the deployment burden for all parties involved in the process, and results in a steady change to the new system.

Algorithm 3 shows how patients and health personnel access the network. The access given to the user (patients) depends on their registration on the network, whereas the heath personnel access is subject to the person's role and the time required to access a document. Creating transactions in the network is restricted only to the specific authorized health personnel, and each access to the network by authorized personnel is stored, such as in a log book in the blockchain.

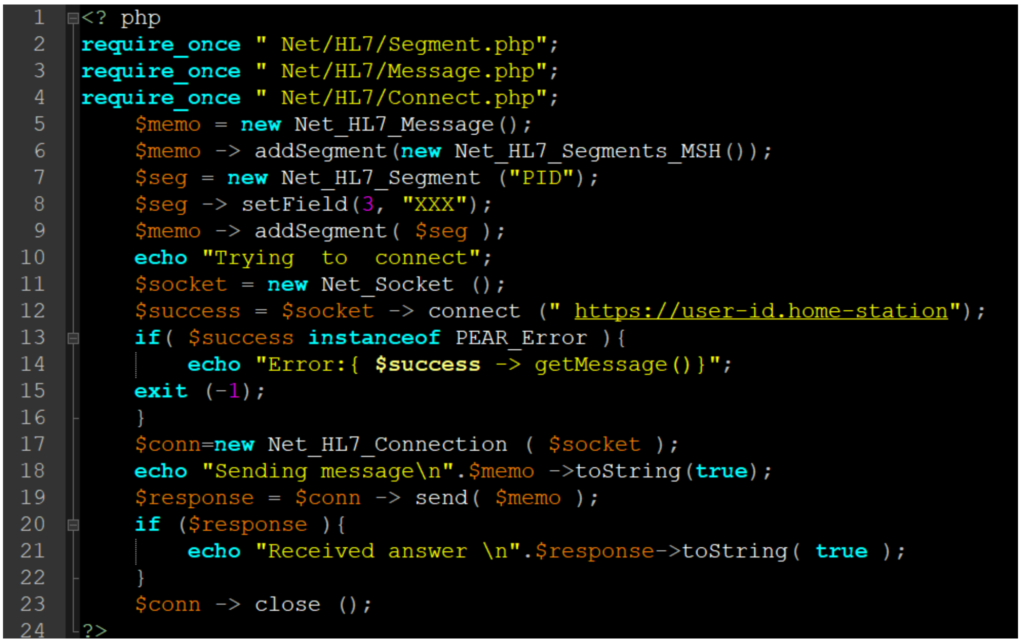
4.3. Implementation

This study was built on three basic modules, namely, the blockchain, Shibboleth, and HL7. The user identity, such as a CNIC or passport number, is required by the client to fetch his home station information to create a URL to communicate with the HL7 server. Net-HL7 was used in this study, with the help of a PHP parser through the PEAR extension. Figure 7 shows the code snippet of the interaction with the HL7 server.

When the client requests patient records from the remote HL7 server, the client connected with the network is redirected to the second module, Shibboleth, for authentication, and the Shibboleth module receives authentication from HL7 client. This blockchain network records all of the transactions during the process. The network communication work using the Apache shibd daemon and its source is located at httpd.conf(/etc/apache2/httpd.conf) on Apache, which redirects each web request to the mod shib. The communication between IdP and shibd uses Security Assertion Markup Language (SAML), and SSL is also implied to ensure security. During the execution, the service provider trusts the authentication of IdP and creates an authentication assertion as a response of authenticity. The Federated Identity Authentication (FIA) system is used by the Shibboleth for the consensus. When a remote station wants to access the information from the home station using HL7 standards, the FIA registers the remote station with a unique id. Figure 8 shows SAML snippets when a remote station wants to access the information from the home station

Algorithm 3: Blockchain Network Access and Registration

```
Procedure: BlockchainNetworkAccessRegistration
Requirements from Health Personnel for Patient Data Access: 1. Personnel Role Pr,
        2. Required Time Rt, Credentials for the Blockchain Network access CrBN
Patient Pt, ViewNetwork Vn, HealthPersonnel Hp, CreateTransactions Ct,
BroadcastToNetwrok BtN, AskForAuthorization AFA, Terms and Conditions Tc, Smart
Contract SC, BlockchainNetwork BN, PatientUniqueId PuId,
If Pt registered then {
    Vn ();
    If Hp authorized Pt data then {
        Vn ();
        If Hp authorized to Ct then {
            Ct (); BtN ();
        }
    }
    Else { AFA ();
        If Hp AFA then {
            If (Pr, Rt ==true) {return CrBN;}
    }
}
Else {
    If Patient agrees on Tc then {
    Create SC ();
    BtN ();
        If BN approves then {Return PuId;}
        Else {Request denied}
    }
}
```

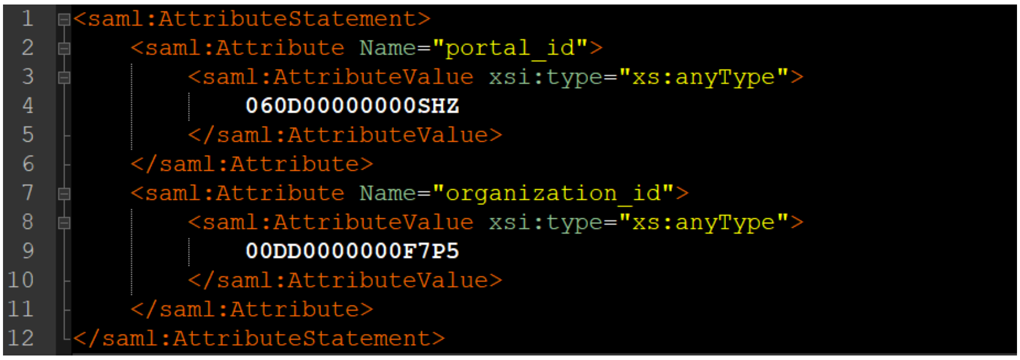


```php
<? php
require_once " Net/HL7/Segment.php";
require_once " Net/HL7/Message.php";
require_once " Net/HL7/Connect.php";
    $memo = new Net_HL7_Message();
    $memo -> addSegment(new Net_HL7_Segments_MSH());
    $seg = new Net_HL7_Segment ("PID");
    $seg -> setField(3, "XXX");
    $memo -> addSegment( $seg );
    echo "Trying  to  connect";
    $socket = new Net_Socket ();
    $success = $socket -> connect (" https://user-id.home-station");
    if( $success instanceof PEAR_Error ){
        echo "Error:{ $success -> getMessage()}";
    exit (-1);
    }
    $conn=new Net_HL7_Connection ( $socket );
    echo "Sending message\n".$memo ->toString(true);
    $response = $conn -> send( $memo );
    if ($response ){
        echo "Received answer \n".$response->toString( true );
    }
    $conn -> close ();
?>
```

Figure 7. Interaction with HL7 server.

The complete implementation process of this study is shown in Figure 9. Hyperledger Composer uses a business application model (BNA) for data manipulation, in which every response received or dispatch is registered against the unique id of each user. In this study, the BNA append-only mode was used to document all of the transactions on the blockchain.

The authorized persons from each organization can view this ledger via an interface, and the ledger can also be used to track or audit any transaction.



```
<saml:AttributeStatement>
    <saml:Attribute Name="portal_id">
        <saml:AttributeValue xsi:type="xs:anyType">
            060D00000000SHZ
        </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="organization_id">
        <saml:AttributeValue xsi:type="xs:anyType">
            00DD0000000F7P5
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Figure 8. SAML code for information access.

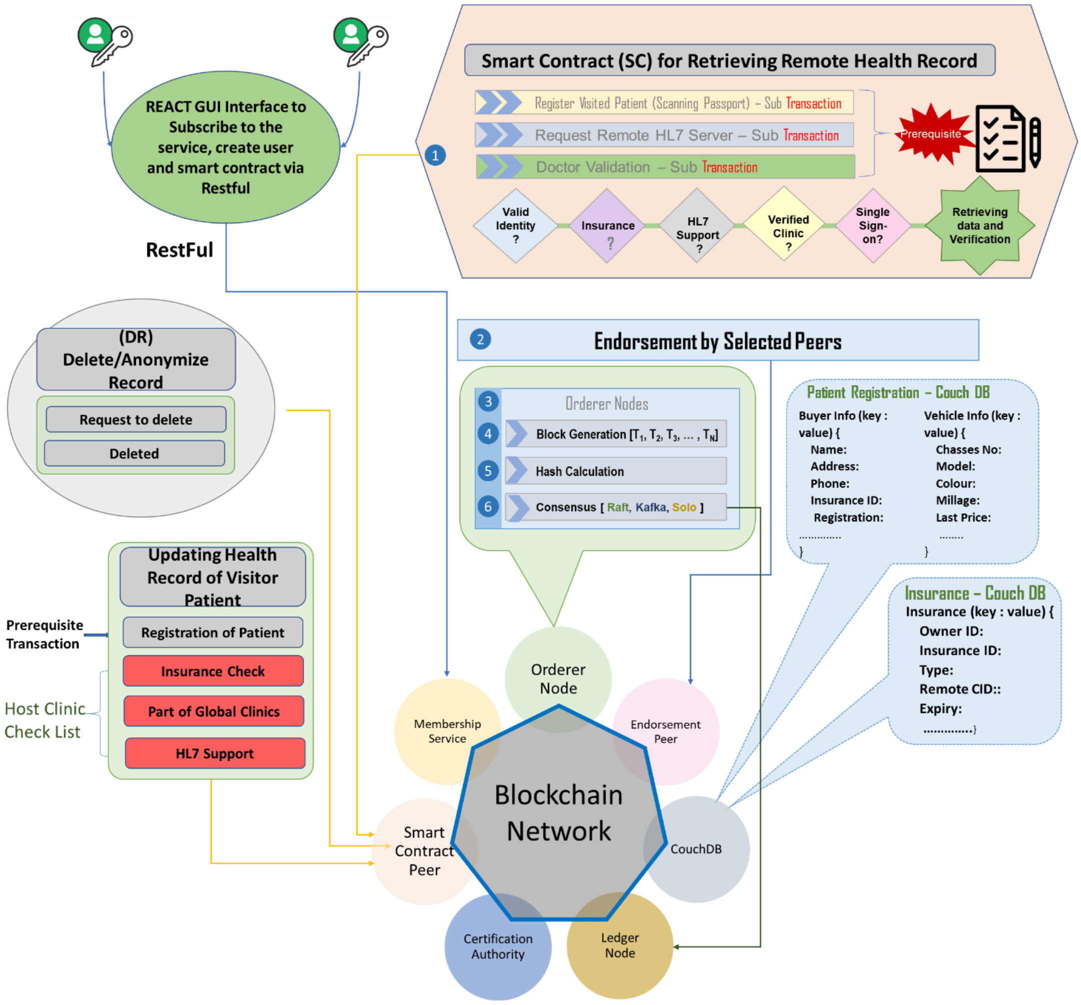

REACT GUI Interface to Subscribe to the service, create user and smart contract via Restful
RestFul
Smart Contract (SC) for Retrieving Remote Health Record
Register Visited Patient (Scanning Passport) – Sub Transaction
Request Remote HL7 Server – Sub Transaction
Doctor Validation – Sub Transaction
Prerequisite
1
Valid Identity ?
Insurance ?
HL7 Support ?
Verified Clinic ?
Single Sign-on?
Retrieving data and Verification
(DR) Delete/Anonymize Record
Request to delete
Deleted
2
Endorsement by Selected Peers
3
Orderer Nodes
4
Block Generation [T_1, T_2, T_3, … , T_N]
5
Hash Calculation
6
Consensus [Raft, Kafka, Solo]
Patient Registration – Couch DB
Buyer Info (key : value) {
Name:
Address:
Phone:
Insurance ID:
Registration:
…………..
}
Vehicle Info (key : value) {
Chasses No:
Model:
Colour:
Millage:
Last Price:
……..
}
Insurance – Couch DB
Insurance (key : value) {
Owner ID:
Insurance ID:
Type:
Remote CID::
Expiry:
…………..}
Updating Health Record of Visitor Patient
Prerequisite Transaction
Registration of Patient
Host Clinic Check List
Insurance Check
Part of Global Clinics
HL7 Support
Orderer Node
Membership Service
Endorsement Peer
Blockchain Network
Smart Contract Peer
CouchDB
Certification Authority
Ledger Node

Figure 9. Complete implementation diagram.

5. Results and Evaluations

All of the results obtained below were generated using the system specification shown in Table 1.

Table 1. Specification of the environment.

Specification	Value
CPU	Dell server (intel 3.4 quad-core i7)
Memory	32 GB
Network Bandwidth	4 Mb CIR
Concurrent blockchain nodes	20

The use of the blockchain in the communication process protects the medical data by encrypting it using asymmetric cryptography. It also improves the efficiency in terms of the total cost of the system for storage and document access. The comparison of this study with other EHR systems shows that the document access and retrieval time is faster in the proposed approach compared to that in the other systems. Table 2 summarizes the comparison between the system under study and other existing systems. The data in Table 2 clearly indicate the superiority of the system under study with respect to the existing alternatives ([50,51,60,61]). The alternative approaches are either centralized or semi-centralized. This is in contrast to the system under study, which is based on a decentralized network, thus making it durable and coherent in terms of availability and access.

Table 2. Comparison between existing frameworks and the proposed system.

Schemes	[60]	[50]	[61]	[51]	Proposed System
Source Data	Yes	Yes	Yes	Yes	Yes
Data Storage Type	PACS	Cloud Server	Dedicated	Mutable P2P	Immutable Storage
Tamper Proof	No	Yes	Yes	Yes	Yes
Encryption Type	Not Mentioned	Not Mentioned	Symmetric	Asymmetric	Asymmetric
Database Sharing	PACS	Blockchain	Blockchain	Blockchain	Blockchain
Smart Contract	No	Yes	No	No	Yes
Attack Resilience	No	No	No	No	Yes
Database Type	Centralized	Centralized	Centralized	Semi-Centralized	De-Centralized

The storage type used by [51] is a mutable peer-to-peer storage network with manual entry by the health personal, and [60] uses picture archiving and communication systems (PACS). As a result of their respective approaches, both of these systems are vulnerable to data attacks by hackers, and to anomalies created due to the duplication of data. The proposed system is superior due to its use of an immutable blockchain technology and hashes to store data, which removes the probability of data duplication. The proposed system provides users full command of their information with greater security, clarity, and integrity. Due to the use of a blockchain, the proposed system's transactions are not prone to deletion and information can be easily recovered in the case of a node failure. Encryption and decryption on all the comparative systems are performed manually, which can cause data issues. In contrast, the proposed system utilizes the advantages of the built-in features of the blockchain technology for encryption and decryption. Protection of documents after decryption is also an issue, which is resolved in this system with the use of digital signatures.

The proposed system also provides a great deal of resilience against cyber-attacks, thus improving the overall security of the system. This resilience is not provided by any of the comparative approaches. The proposed system is based on encryption and each transaction is encrypted prior to transfer. Due to the use of asymmetric encryption and immutable storage, the proposed system is secure and transaction alteration is almost impossible due to the presence of the distributed ledger, which protects it from alterations. Due to the fault tolerance of RAFT, the consensus algorithm used in this study, the system is robust and reduces the downtime of the network.

5.1. Performance Analysis

The performance of the blockchain network can be measured by analyzing the running time with the variation in the number of orderers and peers. The running time is short for a small network with few orderers and peers. Table 3 shows the running time with a different number of orderers and peers in Hyperledger Fabric. The results are based on the average of thirty different running times, using the same number of orderers and peers in a network. The results were gathered by ensuring that the overhead of other applications does not alter the performance of the block in the network; this was achieved by using Hyperledger Fabric to create the block in the permissioned blockchain network. Figures 10 and 11, respectively, show the time taken to upload and download the medical documents using the proposed system.

Table 3. Performance analysis of block creation.

Peers	Orderers	Running Time
3	1	3.8 s
3	2	3.9 s
5	1	4.7 s
5	2	4.7 s
7	1	5.2 s
7	2	5.3 s

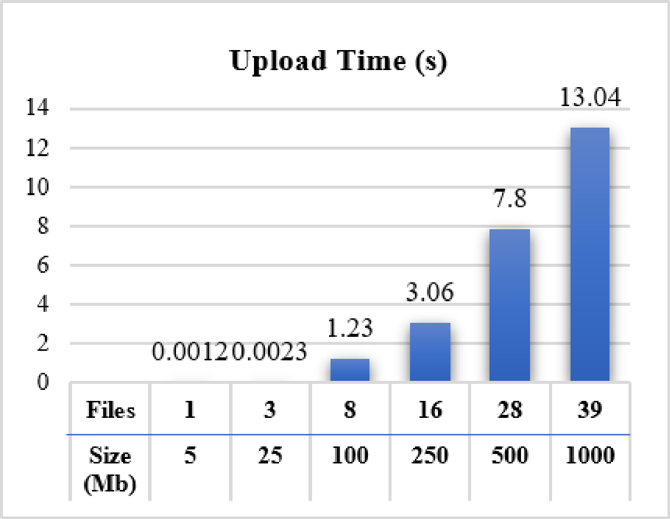


Figure 10. Uploading performance in seconds.

The variation in the graph shows a gradual increase in the time required for uploading and downloading documents (i.e., a receipt, body scan, prescription, X-ray, etc.). In the proposed system, the system takes around three seconds to upload 250 Mb of data, which can contain up to sixteen documents, over a stable network connection with reasonable bandwidth.

The uploading time increases with the increase in the file size, and it takes 7.8 s to upload a file of 500 Mb. All these results were gathered using a virtual machine with the Ubuntu 16.4 operating system, with no other application software installed except the recommended software for the proposed system. The downloading time also shows a gradual increase. As shown in Figure 11, it takes almost three and a half seconds to download a file of 100 Mb, and 26.34 s to download a file of 1000 Mb, over a stable internet connection with reasonable bandwidth.

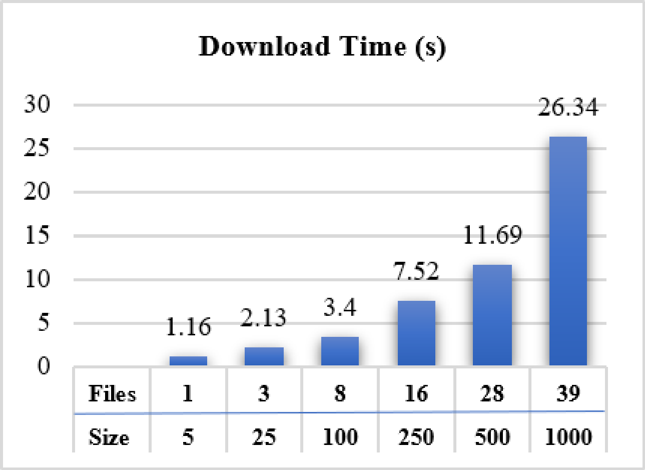


Figure 11. Downloading performance in seconds.

The time required to execute the different policies (read, write, update, delete, and revoke) can be used to analyze system performance. Figure 12 shows comparative analysis of the respective policies introduced in [51,61,62] with the system under study; each comparison is for the execution time of each policy. The experimental results clearly show that the proposed system is superior for almost every type of policy used.

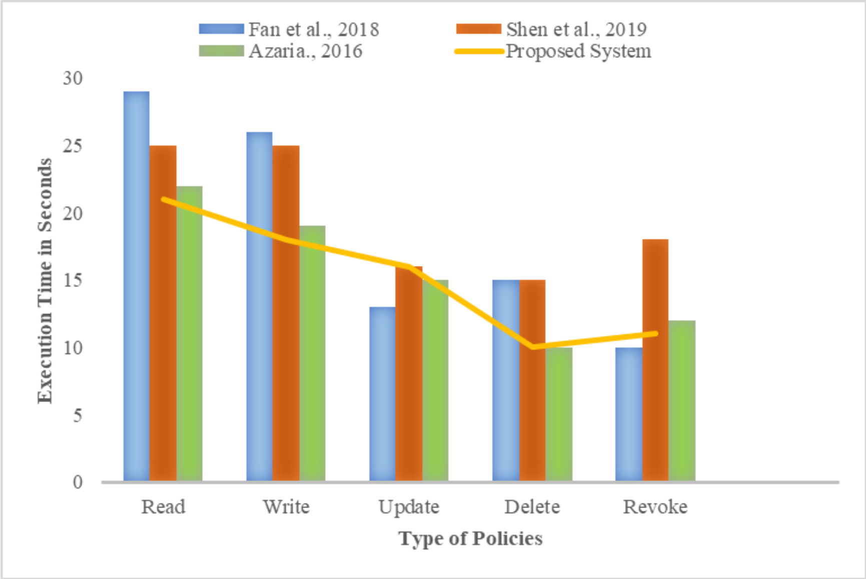


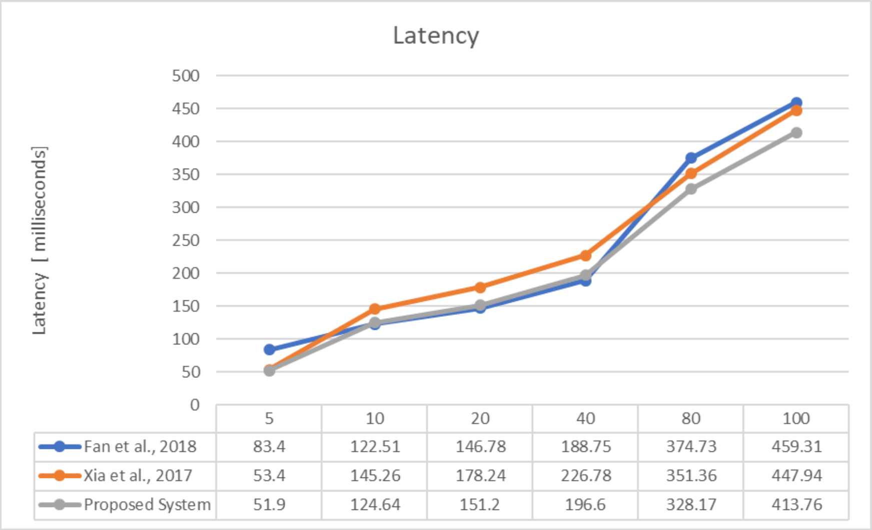
Figure 12. Comparison of policies with respect to execution time.

5.2. Latency Analysis

The delay between the action of a user and the response from the system is known as the latency or the trip time of a data packet. Latency analysis can also be used for performance evaluation; a lower latency means that the system is more responsive and efficient. Figure 13 shows the comparison of the latency of the proposed system with that of [53,54].

5.3. Limitations

As in all systems, benefits are achieved in combination with limitations. In the proposed system, it is difficult to connect current EHR systems that are not created according to the HL7 standards. Furthermore, all of the systems around the world, and every client/patient, must be registered to the network in order to attain the benefits of the network.



	5	10	20	40	80	100
Fan et al., 2018	83.4	122.51	146.78	188.75	374.73	459.31
Xia et al., 2017	53.4	145.26	178.24	226.78	351.36	447.94
Proposed System	51.9	124.64	151.2	196.6	328.17	413.76

Figure 13. Comparison of the delay against the number of requests.

6. Conclusions and Future Work

Although many systems for online record sharing exist, including medical data sharing, most of these are designed either for a specific location, region, or institute, such as a hospital, or do not meet the expected security levels. Most global communications systems are centralized. However, with the advent of the blockchain in cryptocurrency, many fields are attracted toward the idea of decentralization and the benefits provided by customized changes. Blockchain technology has advanced the information technology industry. In this study, a revolutionary blockchain technology was proposed for use in the medical communication field, and a global health record exchange system that is not dependent on the location of the user was created for the transfer of medical data. Using blockchain technology and the Shibboleth federated identity management system, the proposed system performs authentication of the users and the person requiring users' information, under the guidance and support of Health Level Seven standards. The proposed system ensures that a patient is able to provide their medical information to any healthcare worker around the world, without any risk of the data being leaked or hacked.

The system provides appropriate security for all of the stakeholders present in the consensus, and stores each copy of their transaction or data in their home station network. The data shared with the remote country or location is temporary and deleted after a certain period of time or according to the user's requirement; however, every record is maintained in the ledger of the network to maintain the integrity of the data. Blockchain technology is currently penetrating almost every field and shows promise for future applications. However, in this study, it is only used to enable secure data communication in healthcare. In the future, this work can be expanded to add other medical aspects, such as doctors' prescriptions, pharmacy transactions, and vendors' purchases and sales. These additional topics require further research.

Author Contributions: Conceptualization, T.A.S.; Formal analysis, G.Q.B.; Funding acquisition, A.P.; Investigation, G.Q.B.; Methodology, T.A.S.; Project administration, R.R.; Resources, R.R. and S.S.R.; Software, G.Q.B.; Supervision, R.R.; Validation, T.A.S.; Visualization, G.Q.B.; Writing—original draft, G.Q.B. and T.A.S.; Writing—review & editing, R.R., S.S.R. and A.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was supported by the National Research Foundation of Korea (NRF) grants funded by the Korean government under reference number (2020R1A2C1012196).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Special acknowledgement to Junaid Gul for his help and guidance during the research work. We would like to thank HED AJK for the utilization of their servers for testing. We would like to acknowledge the Deanship of research, Islamic University of Madinah for their support in all aspects of completing this research.

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

References

1. Collins, F.S. Exceptional Opportunities in Medical Science: A View from the National Institutes of Health. *JAMA* **2015**, *313*, 131–132. [CrossRef] [PubMed]
2. Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.Á.O.; Toval, A. Security and privacy in electronic health records: A systematic literature review. *J. Biomed. Inform.* **2013**, *46*, 541–562. [CrossRef] [PubMed]
3. Khushi, M.; Shaukat, K.; Alam, T.M.; Hameed, I.A.; Uddin, S.; Luo, S.; Yang, X.; Reyes, M.C. A comparative performance analysis of data resampling methods on imbalance medical data. *IEEE Access* **2021**, *9*, 109960–109975. [CrossRef]
4. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
5. Transaction, C.P. *Blockchain: Opportunities for Health Care*; Technical Report; Deloitte Touche Tohmatsu Ltd.: London, UK, 2018; Volume 1.
6. Ali, T. Z notation formalization of blockchain healthcare document sharing based on crbac. *J. Inf. Commun. Technol. Robot. Appl.* **2018**, *9*, 16–29.
7. TierIon. TierIon: Technology and Products that Reduce the Cost and Complexity of Trust. 2018. Available online: https://tierion.com/ (accessed on 18 September 2018).
8. GEMOS. The Blockchain Operating System. 2018. Available online: https://enterprise.gem.co/ (accessed on 18 September 2018).
9. Brannan, B. Healthcoin-Blockchain-Enabled Platform for Diabetes Prevention. Available online: https://medium.com/blockchain-healthcare-review/healthcoin-blockchain-enabled-platform-for-diabetes-prevention-b3448b34cf36 (accessed on 21 August 2018).
10. Haidar, F.; Kaiser, A.; Lonc, B.; Urien, P.; Denis, R. C-its use cases: Study, extension and classification methodology. In Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, Portugal, 3–6 June 2018.
11. Xu, Y.; Li, Q.; Min, X.; Cui, L.; Xiao, Z.; Kong, L. E-commerce blockchain consensus mechanism for supporting high-throughput and real-time transaction. In Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing, Beijing, China, 10–11 November 2016; pp. 490–496.
12. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of vote: A high performance consensus protocol based on vote mechanism & consortium blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems, Bangkok, Thailand, 18–20 December 2017.
13. Nasir, A.; Shaukat, K.; Khan, K.I.; Hameed, I.A.; Alam, T.M.; Luo, S. What is Core and What Future Holds for Blockchain Technologies and Cryptocurrencies: A Bibliometric Analysis. *IEEE Access* **2020**, *9*, 989–1004. [CrossRef]
14. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]
15. Nakamoto Michael, J.; Cohn AL, A.N.; Butcher, J.R. Blockchain technology. *Journal* **2018**, *1*, 35–45.
16. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Econometrica* **2019**, 1–48.
17. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *NISTIR 8202 Blockchain Technology Overview*; National Institute of Standards and Technology, US Department of Commerce: Washington, DC, USA, 2018.
18. Vukolić, M. Rethinking permissioned blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 3–7.
19. Yu, H.; Sun, H.; Wu, D.; Kuo, T.T. Comparison of Smart Contract blockchains for Healthcare Applications. In *AMIA Annual Symposium Proceedings*; American Medical Informatics Association: Bethesda, MD, USA, 2019; Volume 2019, p. 1266.
20. AlTaei, M.; Al Barghuthi, N.B.; Mahmoud, Q.H.; Al Barghuthi, S.; Said, H. Blockchain for UAE Organizations: Insights from CIOs with opportunities and challenges. In Proceedings of the 2018 International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 18–19 November 2018; pp. 157–162.
21. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of blockchain technology: Pros, Cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [CrossRef]
22. Luhmann, N. What is communication? *Commun. Theory* **1992**, *2*, 251–259. [CrossRef]
23. Planer, R.J.; Godfrey-Smith, P. Communication and representation understood as sender–receiver coordination. *Mind Lang.* **2020**, *36*, 750–770. [CrossRef]
24. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
25. Baitha, A.K.; Vinod, S. Session Hijacking and Prevention Technique. *Int. J. Eng. Technol.* **2018**, *7*, 193–198. [CrossRef]

26. Jain, V.; Sahu, D.R.; Tomar, D.S. Session Hijacking: Threat Analysis and Countermeasures. In Proceedings of the International Conference on Futuristic Trends in Computational Analysis and Knowledge Management, Greater Noida, India, 25–27 February 2015.
27. Burgers, W.; Verdult, R.; Eekelen, M.V. *Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials*; Nordic Conference on Secure IT Systems; Springer: Berlin/Heidelberg, Germany, 2013.
28. Liu, J.; Xiao, Y.; Ghaboosi, K.; Deng, H.; Zhang, J. Botnet: Classification, attacks, detection, tracing, and preventive measures. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, 692654. [CrossRef]
29. Shaukat, K.; Alam, T.M.; Hameed, I.A.; Khan, W.A.; Abbas, N.; Luo, S. A Review on Security Challenges in Internet of Things (IoT). In Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC), Portsmouth, UK, 2–4 September 2021; pp. 1–6.
30. Grangeia, L. *Dns Cache Snooping*; Technical Report; Securi Team—Beyond Security: Cupertino, CA, USA, 2004.
31. Rieck, K.; Holz, T.; Willems, C.; Düssel, P.; Laskov, P. Learning and classification of malware behavior. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France, 10–11 July 2008; pp. 108–125.
32. Shaukat, K.; Faisal, A.; Masood, R.; Usman, A.; Shaukat, U. Security quality assurance through penetration testing. In Proceedings of the 2016 19th International Multi-Topic Conference (INMIC), Islamabad, Pakistan, 5–6 December 2016; pp. 1–6.
33. Zhang, X. *The Diagnosis and Prevention of Computer Virus*; China Environmental Science Press: Beijing, China, 2008.
34. Zhu, Z. Study on Computer Trojan Horse Virus and Its Prevention. *Int. J. Eng. Appl. Sci.* **2015**, *2*, 257840.
35. Uma, M.; Padmavathi, G. A Survey on Various Cyber Attacks and their Classification. *IJ Netw. Secur.* **2013**, *15*, 390–396.
36. Awerbuch, B.; Curtmola, R.; Holmer, D.; Nita-Rotaru, C.; Rubens, H. *Mitigating Byzantine Attacks in Ad HocWireless Networks*; Technical Report Version; Department of Computer Science, Johns Hopkins University: Baltimore, MD, USA, 2004.
37. Shaukat, K.; Luo, S.; Chen, S.; Liu, D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 20–21 October 2020; pp. 1–6.
38. Androulaki, A.; Barger, V.; Bortnikov, C.; Cachin, K.; Christidis, A.; De Caro, D.; Enyeart, C.; Ferris, G.; Laventman, Y.; Manevich, S.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, EuroSys'18, Porto, Portugal, 23–26 April 2018; pp. 30:1–30:15.
39. Karp, R.; Schindelhauer, C.; Shenker, S.; Vocking, B. Randomized rumor spreading. In Proceedings of the Symposium on Foundations of Computer Science (FOCS), Redondo Beach, CA, USA, 12–14 November 2000; pp. 565–574.
40. Kumar, V.; Bhardwaj, A. Identity Management Systems. *Int. J. Strateg. Decis. Sci.* **2018**, *9*, 63–78. [CrossRef]
41. Needleman, M. The Shibboleth Authentication/Authorization System. *Ser. Rev.* **2004**, *30*, 252–253. [CrossRef]
42. Dudczak, A.; Helinski, M.; Mazurek, C.; Mielnicki, M.; Werla, M. Extending the Shibboleth identity management model with a networked user profile. In Proceedings of the 2008 1st International Conference on Information Technology, Gdansk, Poland, 18–21 May 2008. [CrossRef]
43. Birrell, E.; Schneider, F.B. Federated identity management systems: A privacy-based characterization. *IEEE Secur. Priv.* **2013**, *11*, 36–48. [CrossRef]
44. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
45. Chen, Y.; Meng, L.; Zhou, H.; Xue, G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6685762. [CrossRef]
46. Khezr, S.; Benlamri, R.; Yassine, A. Blockchain-based Model for Sharing Activities of Daily Living in Healthcare Applications. In Proceedings of the 2020 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; pp. 627–633.
47. Tan, L.; Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 271–281. [CrossRef]
48. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [CrossRef]
49. Lee, J.S.; Chew, C.J.; Liu, J.Y.; Chen, Y.C.; Tsai, K.Y. Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. *J. Inf. Secur. Appl.* **2022**, *65*, 103117. [CrossRef]
50. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
51. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
52. Prokofieva, M.; Miah, S.J. Blockchain in healthcare. *Australas. J. Inf. Syst.* **2019**, *23*. [CrossRef]
53. Syed, T.A.; Siddique, M.S.; Nadeem, A.; Alzahrani, A.; Jan, S.; Khattak MA, K. A novel blockchain-based framework for vehicle life cycle tracking: An end-to-end solution. *IEEE Access* **2020**, *8*, 111042–111063. [CrossRef]
54. Choudhury, O.; Fairoza, N.; Sylla, I.; Das, A. A blockchain framework for managing and monitoring data in multi-site clinical trials. *arXiv* **2019**, arXiv:1902.03975.

55. Srinivasu, P.N.; Bhoi, A.K.; Nayak, S.R.; Bhutta, M.R.; Woźniak, M. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics* **2021**, *10*, 1437. [CrossRef]
56. Clim, A.; Zota, R.D.; Constantinescu, R. Data exchanges based on blockchain in m-Health applications. *Procedia Comput. Sci.* **2019**, *160*, 281–288. [CrossRef]
57. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Paper* **2014**, *151*, 1–32.
58. Schneier, B.; Kelsey, J. Cryptographic Support for Secure Logs on Untrusted Machines. In Proceedings of the USENIX Security Symposium, San Antonio, TX, USA, 26–29 January 1998.
59. Schneier, B.; Kelsey, J. Secure audit logs to support computer forensics. *ACM Trans. Inf. Syst. Secur.* **1999**, *2*, 159–176. [CrossRef]
60. Langer, S.G.; Tellis, W.; Carr, C.; Daly, M.; Erickson, B.J.; Mendelson, D.; Moore, S.; Perry, J.; Shastri, K.; Warnock, M.; et al. The RSNA Image Sharing Network. *J. Digit. Imaging* **2014**, *28*, 53–61. [CrossRef] [PubMed]
61. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 1–11. [CrossRef] [PubMed]
62. 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.