computers

MDPI

Article

Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard

Md. Shohidul Islam [1,*], Mohamed Ariff Bin Ameedeen [1], Md. Arafatur Rahman [2,*], Husnul Ajra [1] and Zahian Binti Ismail [1]

[1] Faculty of Computing, Universiti Malaysia Pahang, Kuantan 26600, Malaysia
[2] School of Engineering, Computing & Mathematical Sciences, University of Wolverhampton, Birmingham WV1 1LY, UK
* Correspondence: msi.ice.ru@gmail.com (M.S.I.); arafatur.rahman@wlv.ac.uk (M.A.R.)

Abstract: The pervasiveness of healthcare data to create better healthcare facilities and opportunities is one of the most-imperative parts of human life that offers radical advancements in healthcare services practiced through the blockchain-based management, analysis, storage, and sharing of health-related big data. Researchers can accelerate the challenges of developing a secure, scalable, and accessible dynamic healthcare infrastructure by the extensive data exchange required through individual microservices of blockchain-based privacy-preserving health data management ledgers in Healthcare Industry 4.0. Conducting secure and privacy-preserving platforms through primitive cryptographic algorithms is risky and can be a serious concern as the need to authenticate and store sensitive health data automatically are increasingly high. To achieve interoperability, security, efficiency, scalability, availability, and accountability among healthcare providers in heterogeneous networks, this paper proposes a blockchain-enabled decentralized, trustworthy privacy-preserving platform in the healthcare industry. In the healthcare-chain system, blockchain provides an appreciated secure environment for the privacy-preserving health data management ledger through hash processing, which updates high data security, storage immutability, and authentication functionality with an integrated attribute signature in accessing prescribed health block data. This article describes a new secure data retention design, prescribed evidence collection, and evaluation mechanism with integrity–confidentiality–availability to enforce the data access control policies for transactions of healthcare microservices. This scheme revealed the optimal performance in terms of mining health data size, average response time, transaction latency, and throughput for secured block transactions in blockchain networks.

Keywords: blockchain; data transaction; healthcare; Industry 4.0; trustworthy

Citation: Islam, M.S.; Ameedeen, M.A.B.; Rahman, M.A.; Ajra, H.; Ismail, Z.B. Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard. *Computers* **2023**, *12*, 46. https://doi.org/10.3390/computers12020046

Academic Editor: Paolo Bellavista

Received: 26 January 2023
Revised: 17 February 2023
Accepted: 19 February 2023
Published: 20 February 2023

1. Introduction

Blockchain technology has been considered more adaptable than other technologies because of its secure and amiable construction in recent years with the increasing demand for digital data protection in any domain. Thus, a cyber safeguard scheme based on blockchain technology can offer a highly secured health data ledger to healthcare providers in integrated domain environments [1]. Achieving data transactions' interoperability and smart services in many of the healthcare industries is a major challenge currently. Existing systems for managing healthcare records are suffering from data transfer delays, asset theft, record duplication, eavesdropping, and so on [2]. Besides, stored data in an external server are sensitive to healthcare management for data access and their security [3]. A new model for patient care needs to be developed by incorporating patient data and various diagnostic data into a blockchain-enabled decentralized Trust System 4.0 for smart healthcare. The main goal of this research work was to design a decentralized, trustworthy system for

scalable healthcare data management by exploiting blockchain technology. In Figure 1, a functional sketch is shown of how to explore the matter of data transactions in our proposed healthcare system. Here, the basic scenarios of the healthcare system are mentioned that can accomplish the health data transactions to ensure security, scalability, confidentiality, and integrity. Healthcare data can be kept in the blockchain and accessed by authorized health prescribers. Industry 4.0 is capable of synchronizing many of the latest technologies, blockchain technology being one of them. Therefore, here, in Industry 4.0, blockchain technology and health records can be synchronized to make them accessible.

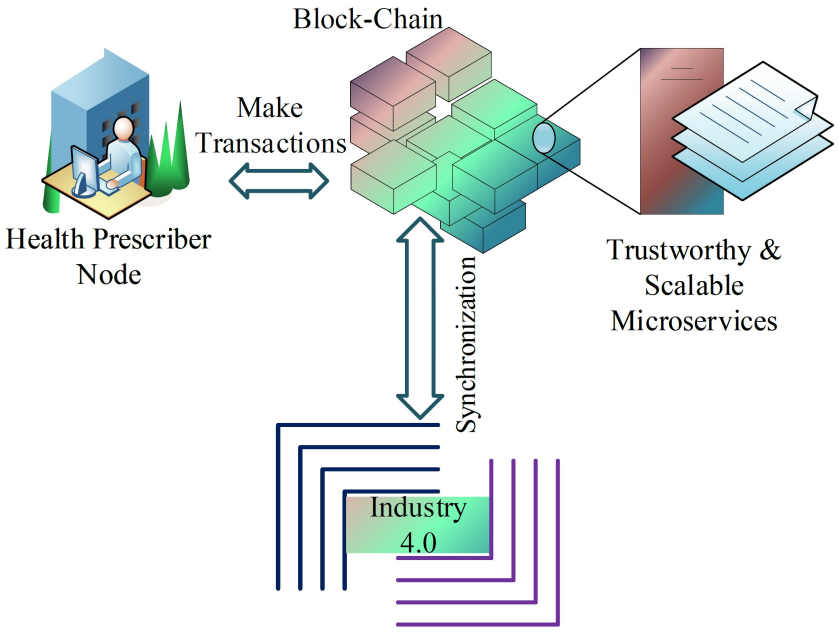


Figure 1. Basic scenarios of a healthcare system.

Investigating existing challenges for secure data transfer [4,5] by incorporating trustworthy and scalable features, blockchain-enabled Healthcare Management Industry 4.0 offers a radical improvement in healthcare services for secured data transactions. The development of blockchain-based [6,7] Healthcare Industry 4.0 in a decentralized network for accessing healthcare records provides significant security to operate periodic medical data sensing, integration, data transmission, data sharing, and data storage. In modern times, healthcare providers in the health clinic industry are concerned about the privacy of their sensitive health records, such as prescribed data, test reports, vaccination information, mental or physical disorders, and so on, which are being stored in different ledgers to achieve the desired results for various purposes. Blockchain is one of the most-promising mechanisms that can improve the security features of a decentralized healthcare system [8] through a structure of blocks connected by the strength of the hashing function.

In this context, this study proposes a blockchain-based healthcare model that ensures interoperable prescribed record retentions and patient data sharing using the hash key, stops information obstructing, and increases data transfer efficiency [9]. This platform accomplishes the whole process of storing health information collected by healthcare providers such as doctors, physiotherapists, health examination and screening specialists, nutritionists, and dieticians with privacy, integrity, and security [10]. The engagement of cryptographic hash keys, DER, PEM, and AES in blockchain technology is crucial to make strong encoding procedures by ensuring security signature codes for secure transactions in this type of proposed healthcare environment. The system is designed to provide trustworthy and scalable secure data transactions by controlling health microservices, whose main goal is to ensure maximum availability and integrity through the arrangement of lightweight computational data blocks. In implementing this design, improving the performance of secure data transaction throughput and latency will increase the acceptability of

the scalable healthcare management industry. Thus, this system can store and protect any type of healthcare records with privacy, as well as providing better consent than existing health services.

We refer to such a proposed design for performing the entire process of achieving the privacy and security of health records as the healthcare-chain. In this case, each healthcare provider is considered a different node in a network to access specific human health data from the healthcare blockchain. To recap, this paper contributes explicitly to the following to handle secure data transactions and data retention:

1. We propose an immune healthcare management model that ensures health data privacy preservation by exploiting the techniques of blockchain technology.
2. We assimilated the trustworthy and scalable features into the healthcare-chain framework, which guarantees a secure and cryptographic healthcare environment, including health microservices.
3. We present three algorithms to utilize data block hashes in the proposed framework for secure data transfer to ensure confidentiality, availability, and integrity as cyber safeguards.
4. In the thorough analysis and investigation setup, we validated the proposed proposition by estimating the performance of a blockchain-enabled decentralized, trustworthy system.

The remainder of this article is organized as follows. In Section 2, the overall preliminary knowledge to design blockchain-based trustworthy systems is introduced. In Section 3, we provide the state-of-the-art closely related to blockchain-based works and the problem formulation. Section 4 describes the overall approach to the healthcare-chain model. Next, the experimental setup and performance evaluation of the proposed framework are given in Section 5. Finally, Section 6 gives the concluding remarks of this work.

2. Preliminary Background Related to Prototype Development

In this section, we introduce the preliminary knowledge for designing a blockchain-based immune healthcare management solution, including the relevant security requirements of data retention.

2.1. Blockchain-Based Healthcare

Blockchain is the cryptographic data chaining name for a digital ledger or immutable record in which previous blocks are linked to form a long chain, allowing blockchain-based healthcare to store and transfer human health information securely. A unique transaction framework can be employed to store encrypted healthcare data in a healthcare application network based on the blockchain. For controlling digital data in the healthcare sector, its blockchain-based applications have the potential to solve current interoperability issues [11]. In this case, this system ensures safe data transactions among users such as medical controllers, doctors, patients, and other medical entities over the network. The healthcare blockchain enhances data authentication, transparency, and legitimacy, which influence the quality of the data, the cost, and the significance of providing healthcare within the system.

2.2. Decentralized Trustworthy and Scalable Healthcare Management

Trustworthiness and scalability are cryptographic security qualities inherent in blockchain technology for healthcare management to maintain anonymous and trusted significant transactions based on decentralized and consensus principles. In particular, the usage of blockchain in the healthcare industry is rising exponentially for the privacy and protection [12] of health records, where the healthcare system employs blockchain-driven features such as CIA, interoperability, compatibility, and verifiability for secure data access [13]. Blockchain-based healthcare ensures the decentralization of information across any network to control the entire process, including its features, and solve security-related issues. Exchanging trustworthy data of this system in a blockchain network comprises

decentralization, being tamper-proof, and traceability. Healthcare data transactions can be scalable and trustworthy by ensuring security, confidentiality, integrity, and privacy with maximum data availability in the system.

2.3. Healthcare Industry 4.0

Healthcare developers for human health indicators are driving unprecedented progress in the healthcare environment through smart data transactions based on digital cyber–physical security, artificial intelligence, information networks, and the connection of virtual objects with real objects in the Fourth Industrial Revolution or Industry 4.0 management [14]. It has created a promising new concept from Industry 4.0 for the best healthcare practices by bringing together the expected areas of the healthcare sector. Massive data handling requirements in the Healthcare Management Industry 4.0 engage in a variety of data transaction activities such as scalability, resilience, confidentiality, integrity, and trustworthiness [15]. The contemporary emergence of Industry 4.0 has stimulated the evolution of a powerful information platform that is revolutionizing data processing across healthcare organizations worldwide. As an ongoing industrial revolution, Industry 4.0 could present state-of-the-art technology for accessing well-processed real-time data in healthcare systems. Moreover, blockchain-based healthcare systems can be configured for Industry 4.0 in terms of interactions with global organizations such as the World Health Organization (WHO). As an emerging technology in Industry 4.0, blockchain has paved the way for a transition in the healthcare sector. In this regard, blockchain helps prevent the misuse of health data through secure data transactions in the healthcare sector, which accelerates the Industry 4.0 definition.

3. State-of-the-Art

3.1. Review of Existing Works

The studies of this research provide a similar state-of-the-art in the existing work from the most-relevant articles based on blockchain-enabled healthcare. In [16], the authors presented a healthcare architecture named FogChain using blockchain technologies and Fog computing for the IoT. In this context, the authors improved the response time for registering personal health records in the IoT. Mahajan et al. [17] designed an architecture for Healthcare 4.0-assisted health data repository processing and sharing in cloud service providers using blockchain technologies. Taylor et al. [18] proposed a patient-centric and interoperable prescription system called VigilRx that uses smart contracts and blockchain to handle prescriptions with ensuring records. Mubarakali et al. [19] introduced efficient and secure health data transaction exploiting the blockchain using the SEHRTB algorithm for medical record transactions in the blockchain.

Abdellatif et al. [20] proposed a secure and intelligent healthcare system called ssHealth that is supported by blockchain and edge computing technologies. This system allows secure medical record exchange and controls medical data-sharing services among local healthcare entities. Jeet et al. [21] designed a secure model for IoT healthcare systems using the concept of encrypted blockchain technology. This system can encrypt the secret data of patients under block-based data encoding over a cloud server. Dantu et al. [22] described an exploratory investigation of the Internet of Things (IoT) in medicare by mainly focusing on the technical aspects dominated by data security and privacy concerns. Al-Aswad et al. [23] introduced the blockchain-based zero knowledge proof (BZKP) benchmark to improve medicare safety in an IoT-based smart city in Bahrain. This design interconnects the public health supervision organizations that ensure patients' prior authorization and protect patient confidentiality on any entrance to their records, together with their health grade, as well as to mitigate COVID-19 risks. Shynu et al. [24] presented a protected healthcare application based on blockchain technology in Fog computing for disease prediction regarding diabetes and cardiac diseases. In this system, the patient health records are accumulated from Fog network nodes and reserved in the blockchain, and the authors evaluated the execution of their suggested work. Dai et al. [25] described

the Internet of Medical Things (IoMT) enabled by blockchain to manage the privacy and security concerns of IoMT schemes where there is an integrated blockchain and the IoMT.

We exhibit the comparison of the functionalities of some existing related works in Table 1. In this table, by differentiating them as specified (✓) and not specified (×), some different functionalities such as crypto algorithms, scalability, availability, confidentiality, and integrity are mentioned. Hence, we can make an optimistic determination to overcome the constraints of existing relevant schemes for data transactions with confidentiality, integrity, availability, and scalability.

Table 1. The functionalities' comparison of some existing related works.

Ref.	Scheme	Crypto Algorithm	Confidentiality	Integrity	Availability	Scalability
[26]	Secrete sharing	✓	✓	×	✓	✓
[27]	SHAREChain	×	✓	✓	×	×
[28]	Distributed computing	✓	✓	×	✓	✓
[29]	Electronic health record	×	✓	✓	×	×
[30]	Storage allocation	✓	×	×	✓	✓
[31]	Personal health records sharing	✓	✓	✓	×	×
[32]	Attribute-based encryption	✓	✓	✓	×	×
[33]	Healthcare data protection	×	×	✓	×	×
[34]	Distributed storage	✓	✓	×	✓	✓
[35]	Secure electronic health record	✓	✓	✓	×	×

3.2. Problem Formulation in Existing Literature

Recently, some researchers have worked on data security in the health sectors, and we tried to study some existing works [27,35]. However, due to conceptual issues such as a lack of data security, trustworthy transactions, scalability, etc., the application of many types of technology in digital transactions in the healthcare industry is relatively slow. Many researchers have attempted to involve blockchain technology in the health sector to find realistic solutions to healthcare challenges, but the progress of the digital health system has been disappointingly slow, and its use has been limited from reaching a full launch. Ensuring fine-grained access control is critical during health record sharing in blockchain-based decentralized distributed systems [31,33], including data integrity and privacy. However, it is necessary to use blockchain-based encryption techniques in health record protection to overcome the data scalability and availability barriers in such systems. It is very relevant to include cryptographic mechanisms to make the storage of expected healthcare data and participant transactions safe and reliable within the system.

In the relevant context, the complexity of healthcare or service coordination is increasing due to the use of primitive technology to transfer health records [32]. Still, in many cases, health industries or healthcare providers in a country use legacy systems and paper-based health records to retrieve and transfer health data, which could damage or endanger public health records. In this case, the interaction between the healthcare recipient and the healthcare consultant is very important and time-consuming in the existing system, where if the prescription paper or certificate is lost or damaged, the healthcare recipient will have to go to the healthcare consultant again.

In this research work, we explored how to improve data security, privacy, trusted transactions, and scalability by applying blockchain technology, considering the existing working situations in the field of digital healthcare. We tried to make a realistic and vital assessment of how the information in each healthcare department can be stored and made available to all people outside. Blockchain data transacted within a healthcare network or service affect the importance of providing healthcare within the system by determining the cost of healthcare and the data quality and validity, which is transparent to the data healthcare consumers. It was analyzed as a functional sketch of how to explore the problem of data transactions in the healthcare system.

4. Methodology of Healthcare-Chain Model

This section describes the effectual design view and methods of the proposed blockchain-enabled decentralized, trustworthy healthcare systems and their constructive functions. This work presents a blockchain-based privacy–integrity–availability–security-supported healthcare management industry standard, named the healthcare-chain model, that meets the goal of implementing a new versatile, high-performance framework for securely collecting, handling, and storing human health records. In this section, we discuss the functions and activities used in the trustworthy healthcare-chain system, which is shown in Figure 2. In this framework, the blockchain-enabled healthcare system can be synchronized with Industry 4.0 by addressing the potentially unique features of emerging blockchain technology. The proposed work offers a radical development in healthcare resources for secured health data transactions. Here are the most-important benefits of the blockchain-based module that prove useful for the management of data sharing, data transmission, and data storage in the healthcare industry. The proposed system provides secured, immutable, and scalable data transactions, as well as indicates the strategies for the quality of e-health services. It potentially processes real-time health data, ensuring remote access to low-cost healthcare industry services.

However, blockchain technology supports establishing trust and reliability in various potential use cases or scenarios for digital health records in the healthcare sector. The use case of blockchain-based secure data storage and transactions or sharing is fully encouraging the improvement of the healthcare system in our proposed decentralized distributed system. In this virtual era, blockchain protects the storage and transfer of sensitive healthcare data with strong security, and healthcare consumers feel secure. The immutability, integrity, and scalability features of this technology make the secure storage and accessibility of life's most-sensitive data more reliable for healthcare customers and doctors. Based on this sensitive data for secure data sharing or transactions, consultants can provide more specific and authentic treatment to healthcare customers.

4.1. Overview of Blockchain-Based Healthcare Architecture

The design and development of this work fulfill the originality and innovativeness of competitive research according to similar supported studies for secure block data transactions in the heterogeneous network. This module incorporates trustworthy and scalable features according to the transactions of health services. Health data providers participate in this system to process data access and privacy preservation through consensus mechanisms and digital transaction signatures to generate new information ledger policies. In several cases of this architecture, the key design approach and views are presented as follows.

4.1.1. Healthcare Provider Responses and Activities

In the scope of this work, the registered users of the healthcare system may participate in the blockchain consensus protocols for their confidential and immutable data transactions and accomplish health record management. The proposed model uses smart hash contracts for compliance in each block of the blockchain platform to maintain the integrity of health organization data. This model will play a new role in making healthcare accessible to the healthcare recipient and the healthcare consultant using a modern web application by completing the necessary procedures. Healthcare data collected by healthcare consultants are reserved on the blockchain and used as storage on this platform. Only authorized healthcare consultants are able to connect health data transactions to the blockchain in this application, but there is no permission for unauthorized consultants or third parties.

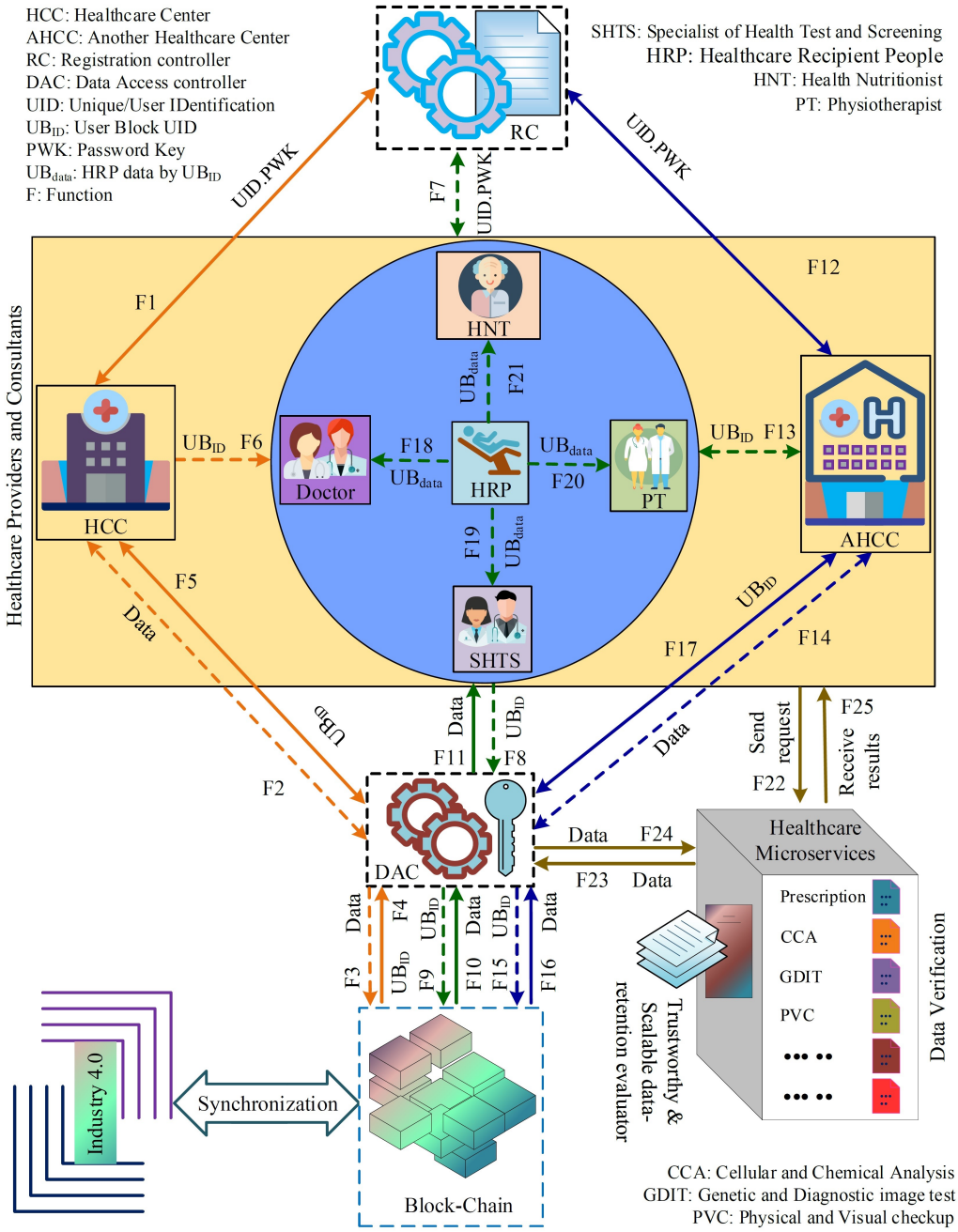


Figure 2. Trustworthy healthcare-chain model.

Healthcare providers such as doctors (DTR), physiotherapists (PT), health nutritionists (HNT), and health examination and screening specialists (SHTS) are governed by the healthcare center (HCC) or another HCC (AHCC) through registration. The actions of healthcare providers with the platform are shown in Table 2. All the HCC's authorized consultants are the original data providers and generators of healthcare services within the blockchain of this system. As a core functionality without sharing any information with strangers, the consultants of the HCC produce or update human health records through their transaction signatures with their own secret keys generated by the system. Health consultants access digital healthcare information using public keys from blockchain-based health ledgers of their own HCC when they need to know about a person's health. The AHCC's health consultants are important data recipients of healthcare information secured on the blockchain. The AHCC's health consultants can only view and verify healthcare records from the blockchain ledger with the permission of the HCC's registered healthcare

consultant or provider if they need to know a person's past health history. They are not able to add or modify any data in existing healthcare records.

Table 2. The actions of healthcare providers with the platform.

Healthcare Providers	Actions
DTR	The corresponding DTR may store the health records of the desired healthcare recipients in this system. He/she may view or share a person's past health history as necessary to make decisions and may keep the data in the system accordingly.
PT	The respective PT may store the physiotherapy-related health data of the expected recipients in this system. He/she may also view or share a recipient's past health history as needed and preserve it.
HNT	The concerned HNT may store the health data of the expected recipients to make positive nutritional habits in this system. He/she may also view or share the recipient's history of past nutritional habits as needed and store new data accordingly.
SHTS	The accredited SHTS may store the health examination and screening results of the expected recipients in this system.
HCC	The HCC governs healthcare providers and allows them to use this system. it cannot store health data.
AHCC	The AHCC may allow its registered healthcare providers to view and verify healthcare records from the blockchain subject to the HCC's permission. It is not able to add any data to the existing health history.

4.1.2. Registration Control Process of Consultants

In this platform, accredited healthcare providers or consultants are allowed to generate their personal unique user identities through the registration controller using their own public keys to provide the prescribed health data. Human care providers collect, share, and access health information through a registration process in this healthcare web application. Precisely, when a provider or consultant in the healthcare system applies to register by this design, he/she checks the validity of those applicants' skills and competency records, then he/she securely generates his/her individual unique/user identification (UID) with the password key (PWK). For secure registration, PWK generation is designed based on a password-hashing function called bcrypt to create the user's best crypto-secret key. All human healthcare records are generated based on SHA-256 for faster processing at a lower cost in the blockchain.

4.1.3. Controlling Access to Health Information

The access control module to health information of the trustworthy healthcare-chain model is designed to allow accredited healthcare providers or consultants to access human health data on the blockchain. The access control module of this platform is governed through the HCC or the AHCC from the healthcare sector side and the blockchain from the technology side to access the health data. Various hubs of the healthcare industry, through healthcare providers or consultants, are able to connect to this blockchain-based platform and have the benefit of accessing secure information. All interaction methods, such as adding, storing, viewing, and sharing the collected human health records, are implemented in accordance with the principles of ensuring the availability, confidentiality, usability, integrity, and security of information by participants in the public healthcare-chain model.

4.1.4. Digital Human Healthcare Ledger

One of the key components of this blockchain-based healthcare system is the digital human healthcare ledger, where health consultants on the platform participate in a peer-to-peer blockchain ledger and manage all transactions. It is particularly designed to securely store health data transaction records in the blockchain under perfect integrity, usability, and confidentiality. In addition, this module is built on the blockchain RSA encryption

technique, where health data transactions are cross-referenced by the SHA-256 hash of a block, and the transaction signature method is used to ensure the authenticity. The entire process of adding new and previous block data is performed based on the PoW consensus mechanism to ensure security through health block mining for transactions. Each block contains health data related to valid transactions, previous block hashes, and timestamps, which are capable of being stored in the blockchain-enabled healthcare ledger. Using this platform, each accredited health provider stores, shares, or accesses relevant records from the blockchain ledger when required.

4.2. Health Data Retention Mechanism with Analysis

The data retention evaluator is incorporated into the healthcare-chain system to analyze healthcare processes with reliability and scalability. The blockchain-based healthcare industry exploiting validation techniques stimulates automatic data retention analysis to process human healthcare services, such as prescriptions, cellular and chemical analysis (CCA), genetic and diagnostic image tests (GDITs), physical and visual checkups (PVC), etc. The activities of the proposed approach involving designated healthcare providers or consultants occur consecutively through the approach of collecting, transmitting, storing, and receiving health data in the healthcare-chain. Three types of users, such as the HCC, the AHCC, and healthcare workers or consultants, work in the proposed system to allow access to health data on the healthcare blockchain. An authorized consultant uses a client node to encrypt healthcare data with a designated user public key in this system using key encryption techniques. Encrypted healthcare data are hashed using SHA-256 on blockchain nodes via the DAC module, and the value is implanted inside a block for the mining process. Private blockchain miners successfully start mining over this block to add it to the healthcare-chain. Authorized consultants must decrypt the health data to view their transactions using signature key techniques. Permitted consultants can view or share the health data from the blockchain if the health data block's hash matches the sender's encrypted hash. As depicted in the prototype of Figure 2, the technique of healthcare data transaction activities is briefly introduced as follows.

F1, F7, and F12: Accredited healthcare providers need to assign the UID and PWK through the registration controller (RC) to use the healthcare-chain system. Once the registration process is authenticated, they can send requests directly to the Healthcare-Chain to reserve and access healthcare through client nodes. Otherwise, they will not be allowed in this system.

F2 and F14: Once the registration authentication process of the HCC or AHCC's healthcare provider is accomplished, they can individually request to send human healthcare data to the DAC. The healthcare data sent will be encrypted for security purposes. In another case, the HCC or AHCC can request to forward the healthcare data to each other's through the DAC, and they can view the corresponding data after decryption.

F5 and F17: The healthcare providers of the HCC or AHCC will receive their respective UB_{ID} from the DAC and reserve it in the healthcare ledger for acknowledgment. In another case, the HCC or AHCC can request to view each other's healthcare data on the DAC using their respective UB_{ID}.

F3 and F16: Encrypted health records with the signature key will be shipped to the healthcare-chain ledger by the DAC for storing purposes, which are immutable. In another case, when the healthcare data are to be viewed or shared by the HCC or AHCC, the stored data will be sent to the DAC in encrypted form.

F4 and F15: The healthcare user identification and password key data are stored in healthcare-chain ledger blocks. A unique block identity UB_{ID} will be generated for the request of the HCC or AHCC's healthcare provider, and the DAC will receive this UB_{ID}. In another case, if healthcare users want to view or share healthcare data, they can directly request the healthcare-chain ledger to match their respective identities with the stored unique block identity UB_{ID}.

F6 and F13: Accredited healthcare consultants such as the DTR, PT, HNT, and SHTS can request the HCC or AHCC to make their respective identity UB_{ID}. They can collect or access healthcare block data using their respective identity. In another case, consultants can gain permission from the HCC or AHCC to view or share the healthcare data for a particular time through the unique healthcare identity of the desired healthcare recipient people (HRP).
F8: Once the respective identity process is authenticated, an accredited healthcare consultant can send a request to the DAC to obtain his/her identity UB_{ID} from the healthcare-chain ledger.
F9: The DAC will interact with the blockchain to assign the generated corresponding consultant identity UB_{ID}. A consultant can also send an instruction to the healthcare-chain ledger to match the respective identity with the stored identity UB_{ID} through the DAC.
F10: When the concerned consultant wants to view or update the data of the desired HRP, the healthcare-chain system will securely explore and authenticate the HRP's data on the blockchain with the UB_{ID} as the respective reference and put it back into the DAC.
F11: The DAC will send the encrypted healthcare data of the desired HRP to the corresponding consultant after authentication, and they can view or update that data as needed.
F18, F19, F20, and F21: The corresponding consultant will only collect the healthcare data, UB_{data}, including the respective identity of the HRP, for storage purposes on the blockchain. Regardless, due to the possibility of the misuse of health data, the HRP will not obtain any permission for the prescribed data view.
F22: Healthcare providers and consultants as users can submit their requests for health service access to the trustworthy and scalable data retention evaluator for authentic data verification.
F23: The authentic data evaluator of this system will interact with the DAC for the health service access verification to accomplish the user requests.
F24: The DAC will allow a data retention evaluator once data verification techniques ensure secure data access.
F25: The data retention evaluator will send feedback to the healthcare providers and consultants regarding their requests for the healthcare receipt.

4.3. Trustworthy and Secure Healthcare Policy

If health information is processed, stored, or transmitted entirely through blockchain technology in a secure healthcare system, the system can be trusted and scalable while ensuring the high performance of data privacy, integrity, and availability. In this system, the main strategy of decentralized entities is to gain legitimacy to store health data resources by controlling decision-making activities or transferring health data to the blockchain without the risk of an intermediary. A detailed description of the secure data transaction policy in the proposed healthcare system is adequately represented in Figure 3 through the health data block generating process.

Healthcare providers or consultants as users can participate and confirm transactions on this platform without the need for a central clearing authority. Through all transactions within the blockchain across a peer-to-peer network, prescribed health data are packaged into blocks, which connect to construct a chain accompanied by other blocks of identical information.

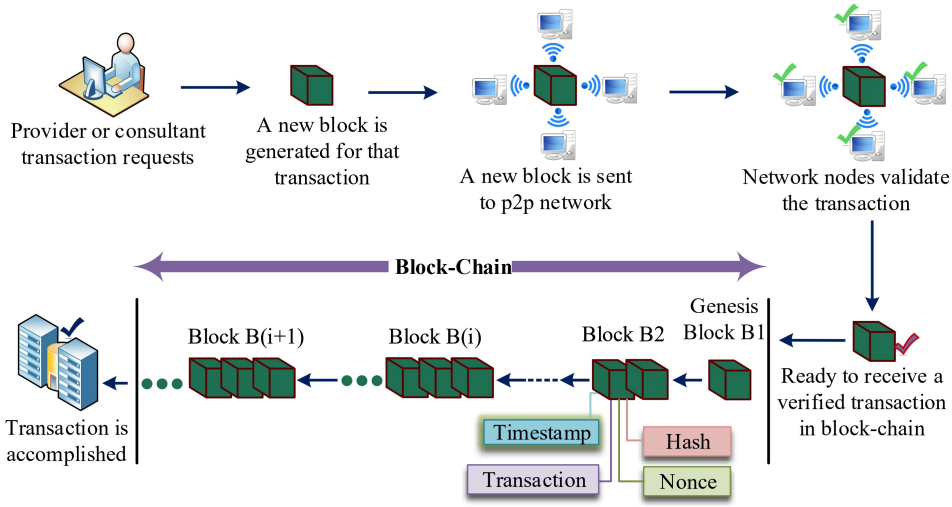


Figure 3. Secure data transaction policy in a healthcare system.

Healthcare transaction records are guided as blocks in the blockchain, and healthcare providers or consultants represent data access transactions as network participants. Participants in this system establish a signed transaction when exchanging health information of healthcare recipients using their private keys at a timestamp. The hash value h_{256} of the block links to the nonce, which is used to identify the data in the particular block. In accordance with the blockchain engineer, B_1 is the initial or first block in the blockchain system that should be NULL in value for all periods as genesis block. A nonce is a 32-bit whole number rendered by the proof-of-work process to miner nodes when a block is created. A digitized timestamp is used to store the system time for each digital healthcare data transaction when each block is completed.

The defined notation (DN) and description of related primitives for Algorithms 1–3 are exhibited in Table 3. A public key, K_{pub}, and secret key, K_{pri}, pair is generated and kept in the healthcare ledger, which is used for health data transmitting, shown in Algorithm 1. In this case, the cryptography RSA process is employed to encrypt or decrypt the health record, and a transaction signature is generated using the private key to maintain authentication. The processing block's hash for healthcare transactions is presented in Algorithm 2. The hash function is used for cryptographic block transactions in the blockchain. Here, the given health data are digested to the hash-256 value. In this case, the data block transaction is assembled with a combination of the timestamp, hash value, and nonce, which are important for data immutability and security. Algorithm 3 presents the procedure of publishing health block data in the healthcare blockchain. A new node is allowed to be added to this system for data transactions on the blockchain. Here, the transactional signature method is used to verify the digital signature of the transactions. Health transaction blocks are hashed using the SHA-256 process as a valid proof technique to validate the data, and and PoW function is used to check the validity of mining necessities. The transactional chain function performs validation checks for successful blockchain operation. The system then broadcasts the health block data through the transaction function on the healthcare blockchain. The following aspects are discussed to maintain the continuity of reliable and safe healthcare policy in the mentioned algorithms.

Table 3. Summary of related primitives.

DN	Description	DN	Description
BC	Blockchain	D_{Hr}	Healthcare recipient information
K_{pub}	Public key	D_{ph}	Prescribed health information
K_{pri}	Private key	D_T	Health data transactions
HC	Healthcare	P_HC	Healthcare provider
H	Hash	$Sign_T$	Transaction signature
H_l	Last hash	$Sign_{TD}$	Transaction digital signature
$chain$	Keep all blocks	S_{node}	Nodes of current block
$genesis$	Initial block	$path$	Transaction route
$Netloc$	Network address	TRX	Transmitted data into current block
$block_N$	Number of block	Est_s	Estimation of encoded string value
m	Prime numbers	$block_s$	String of block

Algorithm 1 Key management and data transmitting to HC-chain system by health provider.

Procedure setup(Initialization, dictionary, signature)
Initialization of variables: K_{pub}, K_{pri}, D_{Hr}, D_{ph}
$D \leftarrow raw(D_{Hr}, D_{ph})$
function orderedDictionary()
if $Key == K_{pub}$ **then**
    Collects D_T except sender's K_{pri}
    return D_T
else
    Denied to preserve D_T
end if
end function
function signatureOfTrnsaction(D)
if P_{HC} wishes D_T over BC **then**
    $D_T \leftarrow$ Performs D_T except healthcare sender's K_{pri}
    $K_{pri} \leftarrow$ Generate hexadecimal imported key(sender's K_{pri}) with RSA
    $Sign_T \leftarrow$ Generate crypto-sign of sender's K_{pri}
    $H \leftarrow$ Compute hash of encoded (D_T)
    Decode $Sign_{TD}$ using H and $Sign_T$
    return $Sign_{TD}$ for D_T
else
    Denied to generate $Sign_{TD}$
end if
end function
function keyGeneration
$RNG \leftarrow$ Generate random(crypto key value)
$K_{pri} \leftarrow$ Perform random(RSA(1024, RNG))
$K_{pub} \leftarrow K_{pri} \cdot K_{pub}(m)$
Decode hexadecimal K_{pri}, K_{pub} by PEM, ASCII
Get generated K_{pri}, K_{pub}
end function
function performHealthRecord Transaction
if D_T == $Sign_T$ of health record **then**
    P_{HC} access D_T with K_{pub} except sender's K_{pri}
else
    No access
end if
end function

Algorithm 2 Processing block's hash for transactions.

Procedure setup of block's hash strategy
function generateBlock
Assign in *block*:: $block_N$, $timestamp$, $transactions$, $nonce$, H_{pre};
if $block_N = length(chain) + 1$ **then**
  Add a new *block* in *BC*;
  Reset list for current *transactions*;
  Append *block* to *chain*;
else
  do nothing;
end if
end function
function hash(block)
if $block_{st} \leftarrow$ encoded *block* as a json file **then**
  $h_{256} \leftarrow$ SHA-256 H of a *block*;
  update $block_{st}$ with h_{256};
  return hex h_{256};
else
  get inconsistent hash;
end if
end function
processing blocks move forward to the blockchain

Algorithm 3 Publishing health block data in HC blockchain.

Procedure setup of blockchain strategy
Initialize parameters:: *chain*, $TRXs$, S_{node}, *genesis*
function registerNode
if holds *Netloc* with containing *path* **then**
  urlparse(node-url).*Netloc* and urlparse(S_{node}).*path*;
  Allow to add a new node to S_{node};
else
  Not allow to add for invalid node;
end if
end function
function verifySignature
$K_{pub} \leftarrow$ hex imported sender's K_{pub} with RSA;
if verifier = PKCS1.new(K_{pub}) **then**
  h = Hash encoded $TRXs$;
  verify(h, hex $Sign_T$) by verifier;
else
  verify nothing;
end if
end function
function validProof
Est_s = Encoded string($TRX + H_l + nonce$);
$h_{256} \leftarrow$ get SHA-256 H of a *block*;
$h_{256}(Est) \leftarrow$ Update E_s value with hex and h_{256};
TRXs $h_{256}(Est)$ satisfy the mining conditions;
end function
function PoW

Algorithm 3 *Cont.*

$block_l \leftarrow$ get last value of chain list;
$H_l \leftarrow H(block_l)$ and $nonce \leftarrow 0$;
while validProof(TRXs, H_l, nonce) is false **do**
  $nonce+ = 1$;
  return *nonce*;
end while
end function
function validChain
while length(chain) > current index of *block* list **do**
  $block = chain[currentindex]$;
  if $block[H_{pre}]$ matches $H(block_l)$ **then**
    Elements of D_T is successful;
  else
    validProof(Elements of D_T) is not correct
    return unsuccessful operation;
    current index $+ = 1$;
  end if
end while
end function
function newTransaction
$TRX_{new} \leftarrow$ collect K_{pub}, signature, $raw(D_{Hr}, D_{ph})$
if sender's K_{pub} == mining sender's value **then**
  append TRX_{new} to TRXs(pending list);
  return $length(chain) + 1$;
else if signature verification is performed **then**
  append TRX_{new} to TRXs(pending list);
  return $length(chain) + 1$;
else
  return inconsistent TRX;
end if
end function
get block D_T, chain and mining BC by connected nodes

4.3.1. Privacy

In the proposed healthcare-chain framework, blockchain guarantees health data storage and protects data privacy by providing access to fair participants in a trustless environment. In this case, confidentiality appraisals defend published data from unrecognized credentials and wrongdoing. This process uses RSA and SHA-256 to ensure data privacy while protecting health data storage access on the network by overcoming digital risks. With this cryptosystem, healthcare data can be encrypted with public keys, and encrypted health data are decrypted by matching participants' private keys. This approach uses such cryptosystems with raw health data and incorporates trust and anonymity to ensure the ultimate right to privacy.

4.3.2. Integrity

Healthcare providers or consultants who participate in the blockchain platform and add healthcare data to the blockchain once cannot completely delete or modify the data later on. The ethical behavior of integrity prevents unauthorized parties from altering health information and accomplishing unrecognized transactions. In this scheme, the hash function is used to ensure that no one can change the health data of the transaction. Here, SHA-256 and PEM are two methods used to maintain data security. Typically, a key component of blockchain technology for data integrity is the Markel tree, which is verified through a cryptographic hash function. In the block-to-block hashing approach, the hash of the previous block must be found in all data blocks within the blockchain

to conserve chain integrity. Integrity guarantees healthcare data transactions without any content tampering or alteration by holding hash values, genesis blocks, nonces, and timestamps in the blockchain. A consensus protocol named proof-of-work is used to ensure the integrity of new blocks of health data added to verify transactions on the proposed healthcare blockchain in a more decentralized way.

4.3.3. Availability

The availability arrangement provides timely data in blockchain storage without allowing interrupted access to the proposed distributed healthcare process. The process uses blockchain technology to provide secure authentication and access to healthcare data in a decentralized manner to achieve high maximum availability. Healthcare providers or consultants connect to the healthcare-chain through the DAC process to send, store, and receive data. In this case, all transactional healthcare data demand generated within a given period can be witnessed by all access levels of the blockchain network. In addition, the blockchain network ensures security and compliance by creating independent streamlined access to HCC and AHCC users using public and private keys, including forming a data transaction signature. Data availability does not include such data on transactions that have been accomplished in the system but not published in the blockchain. User nodes can observe new block generation in this module to ensure that all healthcare records in the block have been published to the blockchain. Thus, data availability guarantees readily available information to healthcare users while maintaining system security.

4.3.4. Scalability

Scalability generally refers to the ability of a network to process many data transactions or how quickly they can be processed. Scalability is the performance of blockchain networks that can sustain significant transactions based on consensus and decentralized principles in healthcare management. In this case, the consensus PoW function of the blockchain system will automatically adjust the number of nodes taking into account new participants in the network and make the data transactions scalable. Blockchain is capable of maintaining the scalable performance of secure data access with increased transaction load across the platform's networks.

4.3.5. Interoperability

Interoperability, as one of the features of blockchain, enables distinctive and promising data transactions or records in this healthcare system. The proposed distributed healthcare system enables secure data exchange between two or more interoperable blockchains using the PoW consensus protocol. In this case, this application can ensure data security without the necessary cooperation of third parties for digital healthcare transactions. Healthcare providers or consultants connect to the healthcare-chain ledger through the DAC process to share, view, and receive data from other healthcare blockchains.

4.3.6. Accountability and Efficiency

Accountability for data transactions can be an important assessment to ensure secure health services in decentralized delivery systems through consultants. The presented platform for storing and sharing prescribed health information executes accountability through blockchain, digital signature, and key pair techniques. In this case, accountability is acknowledged by calculating the transaction, timestamp, hash value, and nonce within the health blockchain record. Moreover, these processes support achieving the efficiency of secure data transactions in completing transactions on the blockchain.

4.4. Novelty of Proposed Scheme

The novelties of the propounded scheme are listed below on the basis of the significance and technical quality of modern healthcare against existing works:

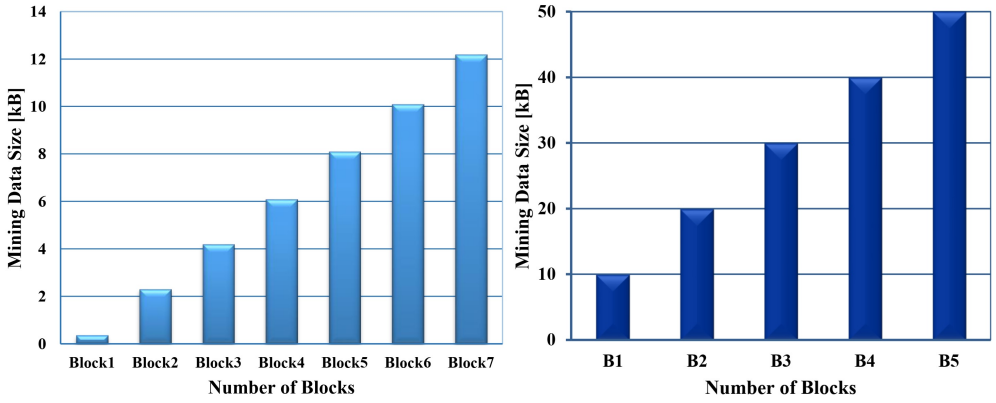
- This research work supported by blockchain can meet the terms with future technology of modern data retention and transfer in healthcare in the virtual world.
- The proposed framework provides the protection of legal rights and intellectual property of human healthcare data as cryptographic blocks.
- This work encourages innovative efforts to elevate the health sector by further developing the current trend of data transfer systems with privacy and security in the healthcare enterprise through such blockchain-based technology.
- The participation of block hash keys and the consensus process to allow secure, distributed controlled access within the healthcare-chain model helps in maintaining the integrity, scalability, authentication, and immutability of health information in the proposed scheme.

5. Experimental Setup and Performance Evaluation

This section gives the performance evaluation of the proposed blockchain-enabled decentralized, trustworthy scheme for the healthcare industry regarding data access execution with cyber safeguards. The proposed framework discusses the assessment and analysis of consequences related to system efficiency to achieve healthcare data privacy and security purposes. Here, the experimental setup and qualitative investigation were conducted to explore healthcare providers' and consultants' perceptions of managing human health data using blockchain technology.

We arranged a protocol evaluation setting for the scheme demonstration and investigation using an Intel(R) Pentium(R) Silver N5000, CPU-1.10GHz laptop, with 4 GB RAM, x64-based processor, 64-bit operating system, and Windows 10. In the protocol evaluation setting system, analyses and investigations were performed with the assumptions underlying the operation of the healthcare project, where the user node, blockchain node, data access provider, or consultant with a unique profiling UID were embedded to control the healthcare facilities. We used Python 3.9.0 (64-bit) and Flask 1.1.1 to develop the proposed framework and Werkzeug/0.16.0 as the web server gateway interface. The user node represents the healthcare provider or consultant of the HCC or AHCC and issues data transactions through the verification of endorser peers. After obtaining valid transactions, the user receives the transaction signature and sends it to the blockchain node. This node performs the consensus rules of PoW, and the timestamp is set in the expected transactions. Performing data transactions is advertised by the healthcare-chain platform for the miner selection and confirmation on the blockchain. Then, miners start to process healthcare data transactions in the blockchain.

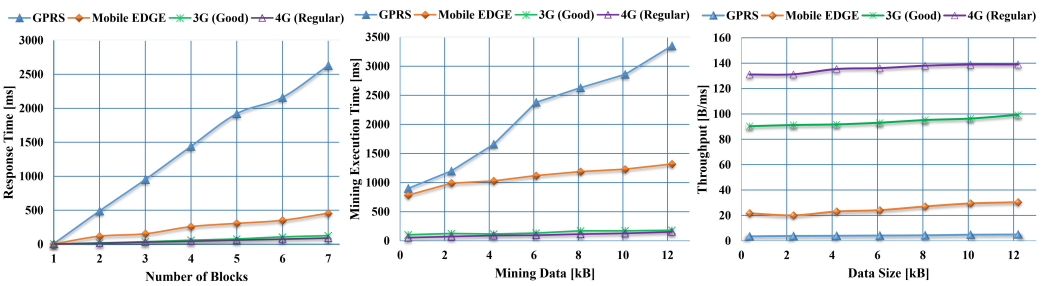
Consequently, the proposed scheme adopts the trustworthy system model using a blockchain network of healthcare data processing. To figure out the data transaction responses of the proposed healthcare-chain scheme, we assembled our environment with Google Chrome/Version 104.0.5112.79 (64-bit) and the DevTools network. In this architecture, the blockchain stores healthcare data in terms of the executing user access permissions, and we measured the processed block data size to evaluate the performance of the interaction between the HCC or AHCC and the blockchain. The mining data sizes in kilobytes (kB) for each block were received 0.36 kB, 2.3 kB, 4.2 kB, 6.1 kB, 8.1 kB, 10.1 kB, and 12.2 kB in this system, where the system metrics or parameters were evaluated through GPRS, mobile EDGE, 3G (Good), and 4G (Regular) networks. Figure 4a shows different mining data sizes concerning different numbers of blocks in the healthcare-chain system.



(**a**) (**b**)

Figure 4. Block transaction data size for different evaluation cases: (**a**) healthcare-chain by different networks and (**b**) for an analogy of the healthcare-chain and educhain.

Figure 5a describes the average response time in milliseconds of block transactions in the healthcare-chain system across the GPRS, mobile EDGE, 3G (Good), and 4G (Regular) networks. The response time for each block transaction on different networks was the time required to process and post a single data block to the blockchain. In this case, block data in different networks showed variation in duration under transfer. This setting demonstrates an approximately graphical relationship between block generation and response time to group the published block transactions into the blockchain. In terms of the other networks, the corresponding block transaction response time across the 4G (Regular) network was as expected in the healthcare-chain system.



(**a**) (**b**) (**c**)

Figure 5. Analysis view through the (**a**) response time of block transaction, (**b**) execution time of transaction mining data, and (**c**) throughput of data transaction process in the healthcare-chain by different networks.

Figure 5b depicts the results of the average execution time in milliseconds of each mining data transaction in the healthcare-chain system for the GPRS, mobile EDGE, 3G (Good), and 4G (Regular) networks. To evaluate the scalability of the data transactions, this platform was validated with respect to consensus average execution times for different mining data sizes in the heterogeneous network. According to the results, the test guaranteed the confidentiality and reliability of transactions in our system, where the execution time varied significantly in different networks as the data load increased. In terms of increasing mining healthcare data in the blockchain-based decentralized storage designs, the efficiency of this system on 4G (Regular) clearly supported the transaction preparation execution time compared to others.

Figure 5c exposes the throughput in bytes per millisecond (B/ms) of data transactions over the GPRS, mobile EDGE, 3G (Good), and 4G (Regular) networks in the healthcare-chain system for the scenario of different block data sizes. The proposed scheme evaluated

the size of the data process in terms of increasing the number of data transactions that are consecutively performed to achieve the expected throughput targets on the heterogeneous network. Six experimental datasets with different load accesses from the first block transaction to the last chained transaction were processed to obtain the expected results. According to the demonstration of these results, the interactive activities in this system boosted data throughput in the blockchain and relieved the transaction latency. Moreover, the storage of the data as a blockchain ledger maintained the expected throughput of consistent transactions in the proposed system under the 4G (Regular) network. As the transaction data grew, in this case, we received a balanced average throughput.

Again we conducted mining transactions in this system, and the mining data size in kilobytes (kB) for each block was 10 kB, 20 kB, 30 kB, 40 kB, and 50 kB to evaluate the healthcare-chain and educhain [10] system metrics or parameters. Meanwhile, we define the mining formation size as the transaction data required for the K block. Figure 4b shows different mining data sizes concerning different numbers of blocks in the healthcare-chain system. It is crucial to comprehend how the parameters affect the system's overall performance to evaluate the average publishing time, throughput, and latency of system transactions.

We organized a protocol evaluation setting to demonstrate the performance analysis between our healthcare-chain system and the educhain system of [10] using a client server and blockchain server. Figure 6a describes the average response time in milliseconds (ms) of block transactions, which depended on transaction data sizes, to measure the performance of the healthcare-chain scheme and educhain system. The response time for each block transaction on the network was the time needed to perform and post a single data block to the blockchain. According to the consequences, the first block transaction was initiated from 10 kB and 52.26 ms for the healthcare-chain system and 51.82 ms for the educhain system. The average time kept changing significantly as the size of the data transaction increased. The last block transaction at 50kB of data provided an average time of 241.84 ms for the healthcare-chain and 263.21 ms for the educhain. In this case, the block data for these systems showed a variation in duration under the transfer. This setting demonstrated an approximately graphical relationship between the block generation size and the average time to group the published block transactions into the blockchain. In terms of the educhain network, the corresponding block transaction response time across the healthcare-chain network was as expected in this system.

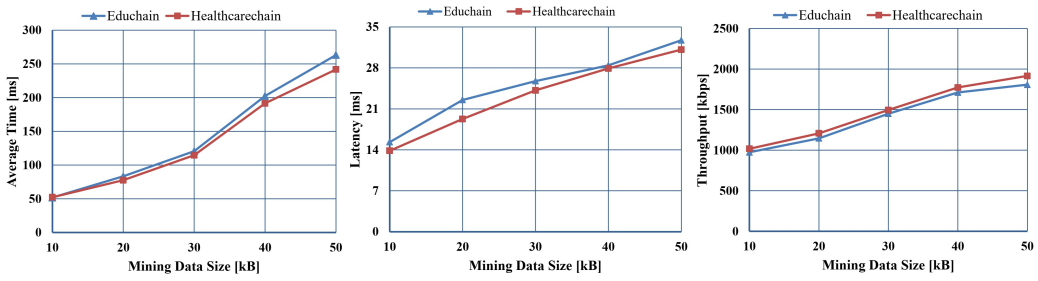


Figure 6. Analogy view through the (**a**) average time of publishing block transaction, (**b**) latency of mining data transaction, and (**c**) throughput of data transaction process for healthcare-chain and educhain system.

According to this work's manifestation, the data size latency was observed in each block transaction under different data load capacities on the individual blockchain servers. Figure 6b depicts the results of the data size latency in milliseconds (ms) of each mining data transaction for the healthcare-chain scheme and educhain design. For the evaluate scalable data transactions, this platform was validated with respect to the consensus average execution times for different mining data sizes in the distributed network. In this case, the latency of 13.84 ms for the healthcare-chain design and 15.32 ms for the

educhain system was obtained for the first block data size of 10kB. However, in line with their respective positions, the respective latency for each subsequent block transaction was observed to increase gradually. At 50kB, both schemes yielded latencies of 31.13 ms for the healthcare-chain and 32.72 ms for the educhain, respectively. According to the results, the test guaranteed the reliability of transactions in our system, where the execution time in the distributed network with the data load increase changed as expected. In terms of increasing healthcare data in the blockchain-based decentralized storage designs, the efficiency of this system on the healthcare-chain clearly supported the transaction preparation execution time compared to the educhain.

Figure 6c exposes the throughput in kilobits per second (kbps) of the data transactions in the healthcare-chain and educhain systems for the scenario of different block data sizes to the individual blockchain. The proposed scheme evaluated the size of the data process in terms of increasing the number of data transactions that were consecutively performed in achieving the expected throughput targets on the benchmark system. The experimental datasets with different load accesses from the foremost block transaction to the lattermost chained transaction were processed to obtain the expected results. According to the exposition of this benchmark test, the throughput of 1027.52 kbps for the healthcare-chain method and 973.71 kbps for the educhain design was received for the first block data size of 10 kB. At 50 kB, both approaches yielded throughputs of 1915.29 kbps for the healthcare-chain and 1807.11 kbps for the educhain, respectively. According to the demonstration of these results, the interactive activities in this system boosted the data throughput in the blockchain and relieved the transaction latency. Moreover, the storage of data as a blockchain ledger maintained the expected throughput of consistent transactions under the proposed healthcare-chain system.

6. Conclusions

Boosted by the need for secure digitized health data access in Healthcare Management Industry 4.0, we proposed a new framework in a blockchain-enabled decentralized, trustworthy system for secure data management by establishing provider or consultant authentication. In order to overcome the increased risk of storing digital health records in this regard, the proposed work used promising technologies such as blockchain, which ensured transaction signatures with strong keys and provided cyber security. We designed structured mechanisms to support the development and execution of the proposed methodology along with the paradigm specification of the exchange functions of a blockchain-enabled healthcare platform. The system is capable of providing privacy, integrity, availability, and security through healthcare-centric access control for data storage using private keys, public keys, signatures, blockchain, and considerably further lightweight cryptographic primitive techniques. This process was demonstrated using standard metrics such as the transaction data size, response time cost, transit latency, and throughput while publishing health data blocks to present the performances. We found an average time of 241.84 ms, a latency of 31.13 ms, and a throughput of 1915.29 kbps for the 50kB data block transaction for the healthcare-chain system. The results of the mentioned standard metrics showed that the proposed healthcare scheme demonstrated exemplary performance for the healthcare industry, which makes it more promising for secure data transaction and storage than the existing educhain system.

In future work, we can add a part for the prescribed health certificate in this framework where the HCC will issue it to the desired healthcare recipient people through the DAC for the proof copy of the healthcare receipt.

Author Contributions: conceptualization, M.S.I., M.A.R. and M.A.B.A.; methodology, M.S.I. and H.A.; writing—original draft preparation, M.S.I. and H.A.; writing—review and editing, M.A.R., M.A.B.A. and Z.B.I.; supervision, M.A.B.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the University Malaysia Pahang (UMP), Malaysia under the research grant scheme with Reference RDU210310. The authors also extend their appreciation to the University of Wolverhampton for its support.

Data Availability Statement: Data sharing is not applicable to this article.

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

References

1. Akkaoui, R.; Hei, X.; Cheng, W. EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access* **2020**, *8*, 113467–113486. [CrossRef]
2. Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. . 1912828. [CrossRef]
3. Jiang, J.; Zhang, Y.; Zhu, Y.; Dong, X.; Wang, L.; Xiang, Y. DCIV: Decentralized cross-chain data integrity verification with blockchain. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 7988–7999. [CrossRef]
4. Stančić, H.; Bralić, V. Digital archives relying on blockchain: Overcoming the limitations of data immutability. *Computers* **2021**, *10*, 91. [CrossRef]
5. Azrour, M.; Mabrouki, J.; Chaganti, R. New efficient and secured authentication protocol for remote healthcare systems in cloud-iot. *Secur. Commun. Netw.* **2021**, *2021*, *2021*, 5546334. [CrossRef]
6. Singh, M.; Aujla, G.S.; Singh, A.; Kumar, N.; Garg, S. Deep-learning-based blockchain framework for secure software-defined industrial networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 606–616. [CrossRef]
7. Rehman, E.; Khan, M.A.; Soomro, T.R.; Taleb, N.; Afifi, M.A.; Ghazal, T.M. Using blockchain to ensure trust between donor agencies and ngos in under-developed countries. *Computers* **2021**, *10*, 98. [CrossRef]
8. Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1937–1948. [CrossRef]
9. Tan, T.L.; Salam, I.; Singh, M. Blockchain-based healthcare management system with two-side verifiability. *PLoS ONE* **2022**, *17*, e0266916. [CrossRef]
10. Rahman, M.A.; Abuludin, M.S.; Yuan, L.X.; Islam, M.S.; Asyhari, A.T. EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1930–1938. [CrossRef]
11. Alvi, S.T.; Uddin, M.N.; Islam, L.; Ahamed, S. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 6855–6871. [CrossRef]
12. Park, J.; Kim, H.; Kim, G.; Ryou, J. Smart contract data feed framework for privacy-preserving oracle system on blockchain. *Computers* **2020**, *10*, 7. [CrossRef]
13. Athanere, S.; Thakur, R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 1523–1534. [CrossRef]
14. Lin, C.; He, D.; Huang, X.; Choo, K.K.R.; Vasilakos, A.V. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *J. Netw. Comput. Appl.* **2018**, *116*, 42–52. [CrossRef]
15. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
16. Mayer, A.H.; Rodrigues, V.F.; da Costa, C.A.; da Rosa Righi, R.; Roehrs, A.; Antunes, R.S. Fogchain: A fog computing architecture integrating blockchain and Internet of things for personal health records. *IEEE Access* **2021**, *9*, 122723–122737. [CrossRef]
17. Mahajan, H.B.; Rashid, A.S.; Junnarkar, A.A.; Uke, N.; Deshpande, S.D.; Futane, P.R.; Alkhayyat, A.; Alhayani, B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Appl. Nanosci.* **2022**, 1–14. [CrossRef] [PubMed]
18. Taylor, A.; Kugler, A.; Marella, P.B.; Dagher, G.G. VigilRx: A Scalable and Interoperable Prescription Management System Using Blockchain. *IEEE Access* **2022**, *10*, 25973–25986. [CrossRef]
19. Mubarakali, A.; Bose, S.C.; Srinivasan, K.; Elsir, A.; Elsier, O. Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *J. Ambient. Intell. Humaniz. Comput.* **2019**, 1–9. [CrossRef]
20. Abdellatif, A.A.; Al-Marridi, A.Z.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Refaey, A. ssHealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Netw.* **2020**, *34*, 312–319. [CrossRef]
21. Jeet, R.; Kang, S.S.; Safiul Hoque, S.M.; Dugbakie, B.N. Secure Model for IoT Healthcare System under Encrypted Blockchain Framework. *Secur. Commun. Netw.* **2022**, *2022*, 3940849. [CrossRef]
22. Dantu, R.; Dissanayake, I.; Nerur, S. Exploratory analysis of internet of things (IoT) in healthcare: A topic modelling & co-citation approaches. *Inf. Syst. Manag.* **2021**, *38*, 62–78. . [CrossRef]
23. Al-Aswad, H.; El-Medany, W.M.; Balakrishna, C.; Ababneh, N.; Curran, K. BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab J. Basic Appl. Sci.* **2021**, *28*, 154–171. . [CrossRef]
24. Shynu, P.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. *IEEE Access* **2021**, *9*, 45706–45720. [CrossRef]

25. Dai, H.N.; Imran, M.; Haider, N. Blockchain-enabled internet of medical things to combat COVID-19. *IEEE Internet Things Mag.* **2020**, *3*, 52–57. [CrossRef]
26. Yang, H.; Shin, W.; Lee, J. Private information retrieval for secure distributed storage systems. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2953–2964. [CrossRef]
27. Lee, A.R.; Kim, M.G.; Kim, I.K. SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR. In Proceedings of the 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), San Diego, CA, USA, 18–21 November 2019; pp. 1087–1090. . [CrossRef]
28. Yang, H.; Lee, J. Secure distributed computing with straggling servers using polynomial codes. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 141–150. [CrossRef]
29. Chelladurai, U.; Pandian, S. A novel blockchain based electronic health record automation system for healthcare. *J. Ambient. Intell. Humaniz. Comput.* **2022**, *13*, 693–703. [CrossRef]
30. Mohiuddin, I.; Almogren, A.; Al Qurishi, M.; Hassan, M.M.; Al Rassan, I.; Fortino, G. Secure distributed adaptive bin packing algorithm for cloud storage. *Future Gener. Comput. Syst.* **2019**, *90*, 307–316. [CrossRef]
31. Wang, S.; Zhang, D.; Zhang, Y. Blockchain-based personal health records sharing scheme with data integrity verifiable. *IEEE Access* **2019**, *7*, 102887–102901. [CrossRef]
32. Guo, R.; Shi, H.; Zheng, D.; Jing, C.; Zhuang, C.; Wang, Z. Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. *IEEE Access* **2019**, *7*, 88012–88025. [CrossRef]
33. Parameswari, C.D.; Mandadi, V. Healthcare data protection based on blockchain using solidity. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 577–580. [CrossRef]
34. Choi, B.; Sohn, J.Y.; Yoon, S.W.; Moon, J. Secure clustered distributed storage against eavesdropping. *IEEE Trans. Inf. Theory* **2019**, *65*, 7646–7668. [CrossRef]
35. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* **2018**, *42*, 152. [CrossRef] [PubMed]