Blockchain-enabled Secure Privacy-preserving System for Public Health-center Data

Md. Shohidul Islam, Mohamed Ariff Bin Ameedeen, Husnul Ajra, Zahian Binti Ismail*
Faculty of Computing, Universiti Malaysia Pahang, Kuantan, Malaysia

***Abstract*—Health center data implicates a large scale of individual health records and is immensely concealment sensory. In the virtual era of large-size data, the increasingly different health informatization causes it important that health data needs to be stored precisely and securely. However, daily health data transactions carry the risk of privacy leaks that make sharing difficult. Moreover, the recently permitted blockchain applications suffer from deficient performance and lack of privacy. This study presents a privacy-preserving and secure sharing and storage system for public health centers based on the blockchain method to dispose of these issues. This system utilizes a hash-256-based access controller and transaction signature with the consensus policy and provides security to share and store health data in the blockchain. In this approach, blockchain guarantees scalability, privacy, integrity, and availability for data retention. Also, this paper measures the performance of transactions with supporting confidentiality-preserving and shows the average transaction time and acceptable latency when accessing health data.**

***Keywords*—Blockchain; data; health; public; secure transaction**

I. Introduction

Blockchain is currently inclining extensive importance and remarkable investment policy of shareholders across an exhaustive range of different initiatives [1]: sharing economy, digital currency, energy trades, financial security, copyright defense, and e-government. Blockchain, as a security defense technology, is evolving into a critical enabling approach for various organizations to create and deploy different decentralized applications and perform many digital sharing [2]. In order to make high-grade services to users, transactions in such applications must be high-speed, less latency, safe, and robust. In this regard, the integration of several emerging technologies in the health industry makes the processing of health information growingly knowledge [3], which defines the health record as the most creative and shareable resource. Nowadays, the medical records generated in the global health sector are growing explosively.

As the level of health information in health centers is increasing day by day, information systems are becoming increasingly complex, and the importance of information security and privacy [4] is increasing incredibly. Nowadays, the traditional paper-based health records of health sectors and their data management systems face serious risks to the privacy and integrity of storing patients' health information. Furthermore, as most health centers are sequestered from each other, long-term storage, sharing, and maintenance of health information are not facilitative to better treatment and counseling. As a result, there is potential for wastage of medical equipment and key data in the healthcare sector. Furthermore, there has been some work on the security of data transactions in the health industry. This sector has some common work and authentication process issues that ignore health resource-controlled transactions and performance. Due to some conceptual issues, such as a lack of trusted transactions, data security, integrity, scalability, etc. The application development based on many technologies in the health sector for digital transactions is fairly slow. For these reasons, it is challenging to find a standard approach to preserve and manage humane and rational services on a large scale.

Fortunately, the recent rise of blockchain technology could open up new horizons for the secure data repository in the healthcare sector [5]. The blockchain approach can provide a trustworthy solution to health management as a rich database with features of decentralization, integrity, security, privacy, and transparency. The emergence of blockchain-based data management in the health sector has motivated the advancement of a rich data platform instead of traditional health record systems that revolutionizes the processing of health information privacy and integrity in health centers. The foremost intent of this paper is to design a secrecy-conserving and secure data storage system for health centers using blockchain [6]. Blockchain-based healthcare platform adds a timestamp to guarantee data immutability during data transactions, and user nodes access data through approved blockchains. Specifically, PoW consensus can accomplish entire decentralization in this design. All transaction records are imitated to all nodes over the blockchain [7] network.

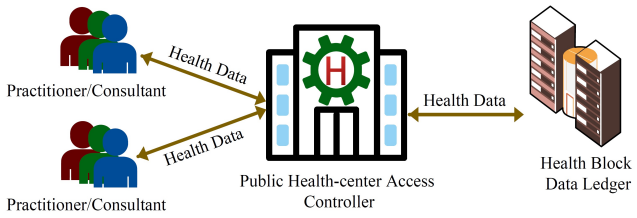

Fig. 1. General functions of public health center.

In Fig. 1, an operative scenario of the public health center exhibits how to conduct secure data transactions in the blockchain-enabled health center system. Authorized health practitioners and consultants can access public health centers and provide necessary health advice using health data. This system will ensure security, scalability, privacy, and integrity while storing and making health records accessible through blockchain technology [8]. Blockchain executes computational tasks and data mining through smart contracts on the chain

*Corresponding Authors.

using the consensus algorithm. All instructions, block size, and block confirmation precisely restrains the space resources available and time for the smart contract. Each node collects public health records and performs data transactions sequentially. The verifiable data is stored in the chain of systems that support privacy-preserving, including high performance. In this way, health records can be stored on the blockchain by a medical practitioner or user, improving the interoperability issues of current health record systems. With this blockchain-based framework, health records can be protected from malicious misuse and tampering. Hence, the applicability of health data and various use cases, blockchain can produce tamper-proof records while maintaining data privacy.

The key contributions of this study can be synopsized as follows:

- This paper provides a health center data repository and sharing system based on blockchain technology.
- This paper equips a system workflow to develop the proposed system and provides sequence diagram.
- This paper designs an evaluation measurement setting and demonstrates the performance of the proposed system.

The leftover of this study is as follows. In Section II, this study introduces the related work. Section III discusses the entire proposed model with design. In Section IV, this paper confers the results and discussion of the experimental appraisal of the proposed model. Lastly, Section V concludes the presented work with the conclusion of this paper.

II. Existing Related Work

This segment briefly discusses the current studies related to the present work. This paper here surveys existing blockchain-based safe data storage and secure record-sharing issues. Typically, in healthcare resources, traditional systems suffer from some complications when storing and exchanging data to securely integrate interconnected networks. A lot of scholars have suggested various approaches to health record information sharing where in some cases, access control, secure storage, confidentiality, scalability, and integrity of information have not been considered or are deficient.

Through its decentralized standards in the healthcare sector, blockchain can accurately formulate medical functionality to monitor primary clinical data of human life, share secure patient data, and protect data storage [9]. Yang and Li [10] suggested a blockchain-based EHR construction. This construction controls the misusage and tampering of Electronic Health Records by pursuing entire circumstances in the blockchain network. Bowman et al. [11] demonstrated an approach called Private Data Object (PDO) that facilitates reciprocally unreliable groups to conduct intelligent contracts on personal information employing Intel SGX. PDO uses the interpreter enclave, and it executes an intelligent agreement composed in the structure. Cheng et al. [12] presented a system named Ekiden that incorporates secrecy-preserving contracts into a blockchain-enabled Trusted Execution Environment (TEE) as a common framework. By exploiting a Proof-of-Publication protocol, Ekiden can sustain blockchain designs, including indecisive consensus that depends on authorized timers. In this case, such a system may add certain runtime overhead, induce security concerns and indicate an outsized attack surface.

Kushch et al. [13] introduced a particular data structure as a blockchain tree for reserving health records in the blockchain. The blockchain tree is designed by one or additional patient identity records and a sub-chain. As the primary blocks of the sub-chain, this sub-chain holds more critical facts and blocks. Tanzila Saba et al. [14] proposed a protected and energy-efficient Internet of Medical Things (IoMT) framework for e-healthcare over a wireless body area network in clinics. Through this, necessary actions can be taken by tracing the health of remote patients and required monitoring of the data. Moreover, sensitive health records are likely to be disclosed due to biased energy-efficient data transfer and limited sensor capabilities. Ashutosh Sharma et al. [15] described a blockchain-based IoMT scheme with smart contracts for e-healthcare management, which is based on the preset code short script that will enrich agreement execution and eliminate intermediaries for delivering trust, security, and certification among its stakeholders.

D'Arienzo et al. [16] and Yu et al. [17] discoursed the benchmarking scheme named BLOCKBENCH for assessing the execution of private blockchain on behalf of required information processing workloads. This technique works on energy-efficient persistent data security and fault-tolerant storage systems. Zhang et al. [18] introduced a scheme named OpTrak that concentrated extensively on employing blockchain to deal with the U.S. opioid concern. The intent of this system was to permit direct control of records in an access control method for the prescription database to prevent overprescription. Fan et al. [19] offered a secure radio frequency identification (RFID) system based on a lightweight cloud authentication framework for IoT-based ecosystems. The system is constructed to perform at less computational power. Liu et al. [20] introduced a cloud-based scheme called CloudDTH constructed on digital twin medical care prescriptions. The scheme is developed to encourage the convergence and interaction of the digital twin in the medical sector based on various clinical procedures.

According to the aforementioned context, research in this sector has some general and authentication process problems which ignore resource-controlled transactions and the performance of health tasks. This paper offers possible solutions to maintain secure transactions and healthy data integrity. The proposed architecture can deliver optimal transaction times and low latency for different user nodes.

III. Materials and Methods

This section presents a proposed determination based on blockchain technology to overcome the current complexity of storing sensitive records of public health centers, especially guaranteeing a safe healthcare process. It illustrates the coordination process of healthcare activities, sequence diagrams, and block-generated flow results.

A. Public Health Center Modeling using Blockchain

In this portion, this paper mainly presents a framework to enhance system performance for health centers to support the privacy, integrity, verifiability, and security of authorized health records, and it also introduces the workflow of the scheme.

Fig. 2 depicts a secure storage architecture for the health center using blockchain. The functions and methods used in a health center data security storage scheme based on blockchain and access control are expressed here. Constructing such a new blockchain-based secure data cloud architecture for any health center can meet the goals of executing high-performance, privacy, and integrity authorization frameworks. The security and scalability of health information in this model can produce satisfaction and rightfulness of data services among any clinic's stakeholders. This system will build stakeholders' confidence in the need to use blockchain-based secure and professional services in this sector. The key design concept and functions of this platform are based on the health data user or consultant, health center controller, and secure data repository.

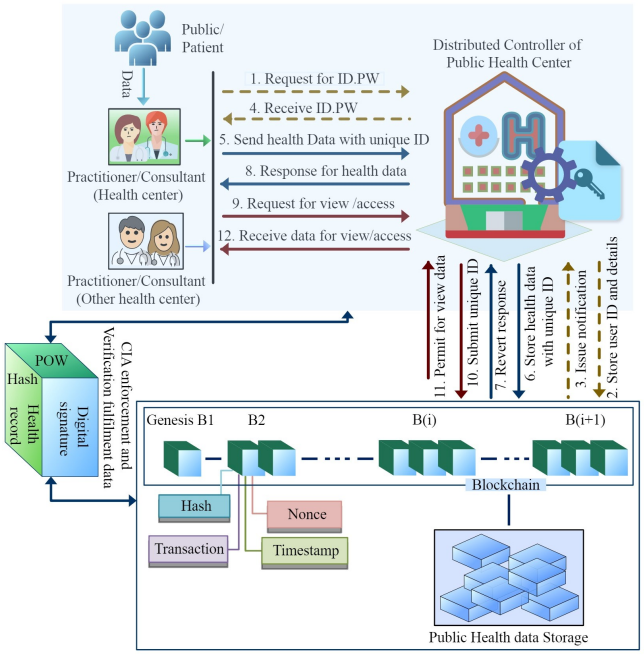

Fig. 2. Blockchain-based public health center model.

The functionality of the data user or consultant of the blockchain-based health center model is operated by the health center controller. The respective users or consultants perform the health care functions existing on this platform as data privacy-keepers. In this scheme, only relevant users or consultants can individually access health data and create or update health data smart contracts on the blockchain. Health data users or consultants collect all health information from patients or individuals under treatment and record it in the blockchain by generating public keys. Consultants can generate a set of private keys for each patient or individual's unique health record.

In this scheme, the health center controller initially allows respective health data users or consultants to generate their own unique identity to register. Then for registration at a health center, the controller issues a unique digital ID with a password individually to users or consultants through this framework. In this case, the Bcrypt algorithm is used to create the digital identity of users or consultants. All this information is stored in data storage. Then, registered authorized health information users or consultants can access the blockchain network using their unique digital keys. In this case, verification and authentication processes must be followed to access the blockchain network. This framework can create a unique data identity for each patient or individual's unique health record. In a blockchain-based secure framework, accessing data from the database, such as adding, viewing, or sharing data, must communicate with the blockchain to ensure system confidentiality, security, and availability.

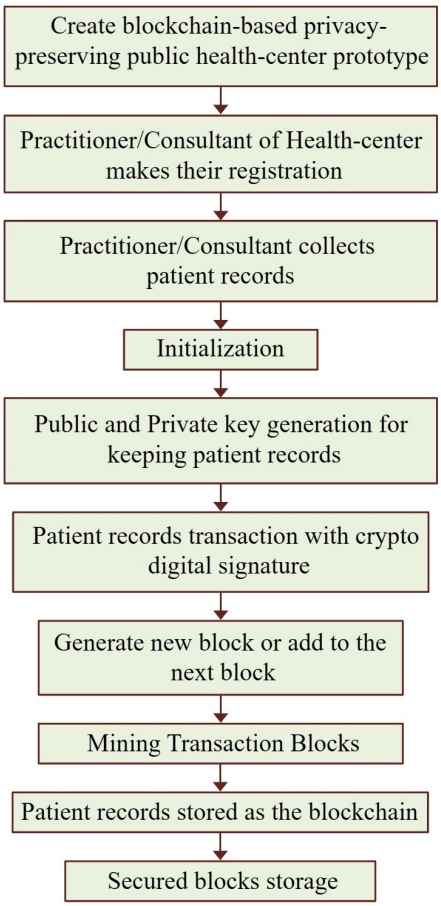

Fig. 3. Workflow for blockchain-based public health center system.

The blockchain network ensures the preservation, accuracy, and security of health records in the storage system through trusted and authorized user or consultant nodes. In this platform, health data is uploaded to the blockchain for immutable storage based on transaction signatures. Entire data is cross-referenced by generating the SHA-256 hash to securely store health data under integrity and confidentiality. PoW consensus policy is executed to conduct the full decentralization of health data in this blockchain network. Sequencing of each SHA256 hash inspects and verifies any tampering of transaction data by hash, nonce, timestamp, and encoding value. Transaction block history is effectively verified by miners. Otherwise, the data chain will logically be declared invalid if any kind of interruption is encountered.

The process of transmitting and receiving records is mentioned in public health center model. Users or consultants need to provide valid Identity (ID) and Password (PW) to access

the scheme of the health center. Through authentication, they can request the controller of the health center to access the blockchain storage. In this case, they can send encrypted health data to storage for accumulating purposes. If necessary, they can receive data from blockchain storage. When encrypted health data is stored in the block, a unique data identity (DID) will be generated for each patient or person under treatment. The controller supports storing or retrieving patient data in the database through DID. The workflow of the proposed system based on the blockchain technique is presented in Fig. 3. Each process and operation of building the approved blockchain-based health center model is manipulated. Based on this workflow, various functional interactions and functions of the user or consultant are programmed with the blockchain.

B. Coordination Process

As indicated by the proposed model, the distributed controller of the public health centers allows medical practitioners or consultants to access health data on the blockchain. It comprises practitioners or consultants as the user, distributed controller as the registration process and access task, and a blockchain ledger. Here the blockchain governs the highly distributed ledger to store various information about the health of the public or patients and to conduct timely transactions, to which only authorized participants to have access or permission. Participating network nodes are engaged in inputting, storing, viewing, and verifying different health data. The sequence diagram of the proposed model for user activities is illustrated in Fig. 4. This sequence diagram is designed to show the sequence of activities of the proposed model. The performing operations of this framework are briefly introduced as follows.

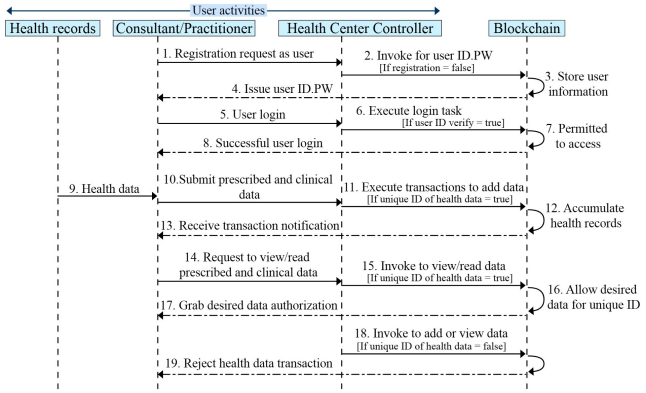

Fig. 4. Sequence diagram of user activities for blockchain-based public health center.

Step1: In this case, each medical practitioner or consultant sends a request for registration to the public health center controller with all their information. The health center controller receives all the information and verifies whether the doctors or consultants have already registered in the system. After verification, it takes the registration decision and invokes storing all user information in the blockchain. After storing the information of the doctors or consultants, the blockchain user login credentials and issues them a unique identity with a password through the distributed controller for login. Consultants can successfully login into the system at any time through verification and get data access.

Step2: After login, each medical practitioners or consultant collects information from the public or patients and submits the prescribed and clinical data to the health center controller. The health center controller calls for creating unique identities of individual health information in the context of public or patient health information received from consultants. Blockchain produces and accumulates unique identities with hash-based values of individual health records. Only those consultants or doctors who have been permitted access rights to this blockchain platform can add or transact patient medical records. After publishing the health record in the blockchain, participants receive the confirmation notification of the data transaction.

Step3: Each medical doctor or consultant can interact with the blockchain through the health center controller to at look public health records. If each medical doctor or consultant wishes to view and read the prior health data from the blockchain, first, they need to login into the system using their unique identity with a password through the distributed controller. In this case, they must have unique identities of individual health information of their prescribed people or patient. Then, they use the unique identities of patients to request access to the public health center's controller to view prior prescribing and clinical data. The health center controller receives their requests and verifies whether the unique identities of patients are already generated in the system. After verification, it allows to visit and read the pre-prescribed health information of the unique identity of those people from the blockchain. Finally, medical doctors or consultants get the opportunity and authorization to view and read the prior prescribed health information. The medical doctor can monitor the current health data along with the previous health information of the prescribed patient to make new prescriptions and add them to the data block of the system. But in this case, the blockchain system will reject the transaction to view the health data if it is found to be incorrect/false while verifying the unique identity of the patients collected by the doctors or consultants.

The various activities that take place between different actors for health data processing within the proposed platform, authorize combining blockchain technology with public health data. The sequence diagram norms of blockchain transaction process are depicted in Fig. 5. The sequence diagram of blockchain transaction process consists of medical practitioners or consultants, security enforcement and blockchain process. Medical doctors or consultants collect public or patient health records and interact with the blockchain to complete the transaction. Separate public key and private key pairs are generated by employing key generation algorithms to able health data processing within the proposed platform. This system randomly generates these keys.

The blockchain process includes hashing and signing algorithms to enforce robust security on health data. When a medical practitioner or consultant shares a patient's health records with another, no assets are actually being sent to anyone. In this case, instead of sending data, the customer has to announce new data allocation by reallocating an amount of data to the blockchain. To reassign data, each data transaction

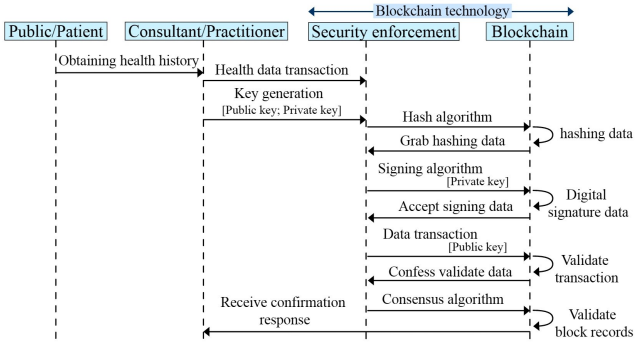

Fig. 5. Sequence diagram of blockchain transaction process.

must be signed by the sender's private key and verifiable using the sender's public key. Hash-256 function is used for data processing operations in this network. It retrieves health data by making a unique hash value while accessing health records through URLs in the web system.

Fig. 6. Consequence of block generated flow.

In addition, it allows user nodes to process health data within the platform to sign their transactions with private keys, and it can assure the integrity of stored data through verification to make secure share between the participants. As a PoW consensus algorithm, nodes select miners for the next block generation of the system and ensure continuity by synchronizing data. Due to the presence of this consensus procedure, the blockchain network achieves block record verification and reliability and establishes trust during data distribution. The consequence of block generated flow for data transactions on the blockchain after the mining process in this system are shown in Fig. 6. In this case, implementing RSA and SHA-256 in the system ensures the health data confidentiality of the blockchain storage and protects the published records. It also delivers timely data to the blockchain repository and ensures maximum availability.

In the proposed model, it shows the process of generating the cryptographic hash SHA-256 associated with the data structure of the blockchain, which is an explicit means of enforcing data integrity. Blockchain's data structure forms a hierarchical set of blocks for secure access where the current block accumulates values such as hash, block transaction, timestamp, nonce, blockchain address, and so on. The blockchain's header holds the block number, and then the previous block's hash value provides the reliability of the transaction data chain. In this case, the block body can incorporate one or more transactions of health data.

Algorithm 1 Generate transaction key-pair

if health data user start transaction **then**
  procedure set(transactionKeyGenerate)
  $RNG \leftarrow$ generate random(cryptographic value)
  $K_{pr} \leftarrow$ generate(RSA(1024, RNG))
  $K_{pb} \leftarrow K_{pr} \cdot K_{pb}(i)$
  decode in PEM, ascii (K_{pr}, K_{pb})
  get K_{pr}, K_{pb}
else
  do nothing
end if
end procedure

The asymmetric cryptographic algorithm RSA PKCS is operated for digital signatures and transactional matters from a provable security perspective with the aim of establishing trust between users and cloud servers. Also, digital signature verifiability is checked using the Elliptic Curve Digital Signature Algorithm (ECDSA) from both the user side and server side for data security. Failing this verification on tampering and altered data values will automatically discard the adversary message. Due to two-party verifiability, the selected transaction is unable to forge signatures on the data and will not be authenticated as a legitimate user. The process facts of the generated transaction signatures relative to the user nodes are shown in the sequence diagram of the blockchain transaction process mentioned.

Algorithm 2 Digital signature generation for health data trnsaction

procedure signature(transaction)
if health data user U_h requests transaction T over BC **then**
  $T \leftarrow$ makes T exclude sender's K_{pr}
  $K_{pr} \leftarrow$ create RSA.key(sender's K_{pr})
  $T_{signer} \leftarrow$ create crypto-sign.new(K_{pr})
  $H \leftarrow$ compute hash.encode(standard value)
  return $T_{signer}.sign(H).decode(ascii)$
else
  not creating signature for T
end if
end procedure

When health practitioners and consultants desire to initiate public health data transactions in this platform, a key pair as a public key (K_{pb}) and a private key (K_{pr}) is generated, which is illustrated in Algorithm 1. Accordingly, the RSA technique is

utilized for public health data encryption or data decryption, and the PEM method is mapped with ASCII to decode the transactions. The process of digital signature generation during health data transactions is shown in Algorithm 2, which will ensure confidentiality while accessing data on the network.

Algorithm 3 Creating and Adding a new block for hash-based health data transactions

procedure createNewBlock(health data)
Initialize health transaction (empty set)
set in $block \leftarrow (block_n, healthtransaction, nonce, timestamp, prehash)$;
if $block_n \leftarrow len(chain) + 1$ **then**
  append the $block$ for a new health transaction in $chain$;
  re-set regarding the running $transaction$;
  add health $block$s to $chain$;
end if
if $block_s \leftarrow$ json.$block$.encode(standard value) as a file **then**
  $hash256 \leftarrow$ hash.new(SHA256)
  update $hash256.block_s$
  return encoded $hash256$ in hexadecimal
else
  do nothing;
end if
end procedure

Algorithm 4 Append node to health blockchain network

procedure registration request(node)
if health data user request for a node **then**
  create a registration node
end if
Initialize parameters: ($healthtransaction$, $chain$, $nodes$, $genesis_{block}$)
urlNodeparse $\leftarrow$ parse.urlNode
if sets urlNodeparse.$Netloc$ and urlNodeparse.$path$. **then**
  add urlNodeparse.$Netloc$ and urlNodeparse.$path$ to $nodes$;
  append a new node to $nodes$;
else
  not make to append;
end if
end procedure

The process of creating and adding a new block for hash-based health data transactions is exhibited in Algorithm 3. Here, block data transaction contains blockn, health transaction data, nonce, timestamp, and hash value which are important to ensure the integrity and immutability of public health records. In the blockchain-based public health center network, the process of adding the new node is introduced in Algorithm 4. This framework allows new nodes to be added to ensure transactions in a distributed or decentralized network. The procedure of accumulating and accessing public health-center data over the blockchain is ascertained in Algorithm 5. In this case, the digital signature process in the transactional health data is employed and verified by defining the PKCS1 standard based on the RSA technique. The Proof of Work method is performed to accomplish the valid proof conditions of mining requirements, and the health transaction records are validated to share or access from one network node to another network node. The consensus Proof of Work process in the blockchain-based public health center system network will automatically adjust the number of new participating nodes and maintain the scalability of the network by speeding up the data transaction process. Finally, this model publishes the transactional data blocks of public health centers on the healthcare blockchain ledger.

Algorithm 5 Accumulating and accessing public health-center data over blockchain

procedure accumulating and publishing
Initialize transaction parameters for health data
generate health transaction block
verify digital transaction signature
$K_{pb} \leftarrow$ RSA.sender's K_{pb}
signverifier $\leftarrow$ PKCS1.new(K_{pb})
$hash$ = SHA.new(health $transaction$.encode($utf8$))
verify($hash$, hex transaction Signature)
perform proof-of-work method
accomplish mining valid proof conditions
synchronise blockchain's nodes
check the health transaction blockchain is valid
transmit health data to transaction chain array
if verify transaction signature **then**
  transaction or share from one node to another node
  access health data
end if
end procedure

IV. Results and Discussions

In this segment, this paper evaluates the performance of the presented secure storage management system with respect to user nodes for health centers using blockchain. The performance evaluation of this framework supports achieving the safety goals of the scheme. Experimental arrangement and qualitative analysis of this framework have been carried out to achieve data privacy and security objectives. It has been set a procedure evaluation environment to assemble the system demonstration and investigation using an Intel(R) Pentium(R) N5000 laptop (CPU -1.10GHz), x64-based processor, Windows 10, 4 GB RAM, 64-bit operating system. In the evaluation method, data access user or consultant node and blockchain node are embedded to investigate the underlying operations of the health scheme. To design the proposed model, it has been employed Python 3.9.0 (64-bit), Flask 1.1.1, and DevTools, including the web server gateway interface.

In order to evaluate and exhibit the health center's performance, multiple user or consultant nodes communicate with the blockchain server in this architecture. In this case, the average transaction time in milliseconds (ms) and latency in ms are evaluated for several data transactions on the blockchain by user nodes. In this case, the performance of each node is recorded by performing different data transmissions of this proposed system. In this scheme, it has been set nodes 1 to 5 to execute transactions. User nodes mine all transmitted blocks containing 1, 5, 10, and 15 transactions (T1, T5, T10, and T15) and propagate them to the blockchain-based public health center system. The specific results of the average transaction

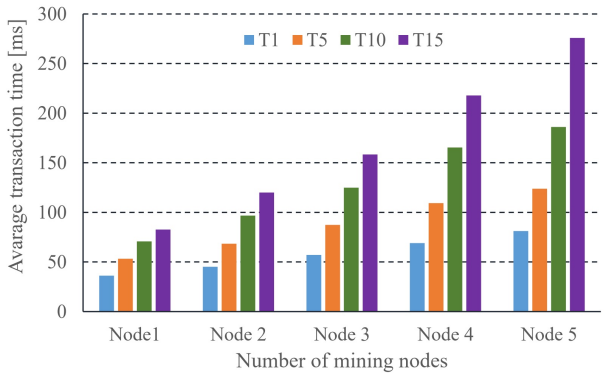

Fig. 7. Average transaction time for different user nodes.

time for different user nodes are shown in Fig. 7. As this test demonstration, by user or consultant node1, the health center scheme reaches 36.31 ms for T1 and 82.7 ms for T15. Again accordingly, by user node 5, the health center scheme reaches 81.11 ms for T1 and gradually reaches a maximum of 275.76 ms for T15. The corresponding average transaction time across network nodes is expected in this system for different block transactions.

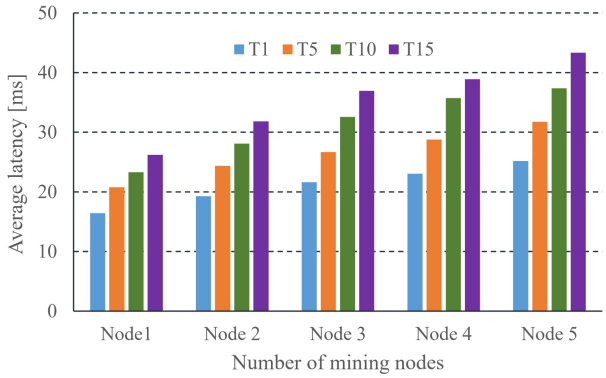

Fig. 8. Latency for different number of user nodes.

Next, it has been measured various transaction-based latencies across the setup nodes in this scheme. For this scheme, the precise consequences of latency for the different numbers of user nodes are shown in Fig. 8. As the work demonstration, it measures the latency of 16.42 ms through the user or consultant node1 for T1 to transmit and receive data block to the blockchain server. It also measures a latency of 26.21 ms for T15 using node 1. Moreover, for a capacity of user node5, the system observes a latency of 25.18 ms for T1 and a maximum latency of 43.35 ms for T15.

Finally, the overall performance induced by this scheme is analyzed by comparing the latency of several nodes. In this case, it sends and receives a data block for 10 transactions to each node in the blockchain server. It measures system latency under different nodes as a benchmark performance. The observation analysis of Latency per client node for publishing transactions between the native blockchain [21] and the proposed work is shown in Fig. 9. According to the exposition of this analysis, the latency of the proposed system compared to the native blockchain is 23.7 ms for node 1. Accordingly, the latency of the proposed system is found to be 48.7 ms compared to the native blockchain for node 8. It can be observed that the proposed system exhibits the most promising consequences in terms of latency than the native blockchain. Therefore, it exposes relatively good scalability in health center data transactions.

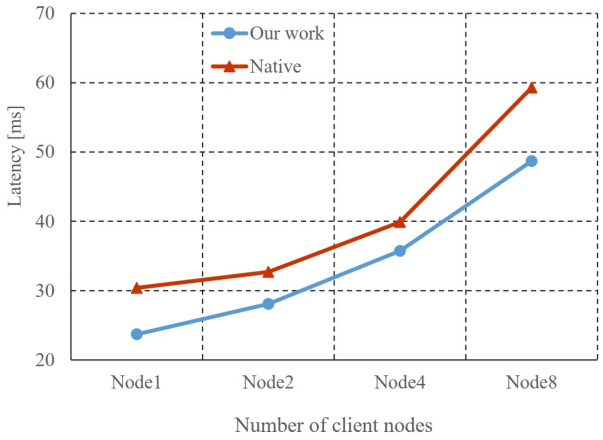

Fig. 9. Comparative analysis of latency per client node for publishing transaction.

This paper exhibits the functionalities comparison of the presented scheme with some other existing works on blockchain-based data storage in Table 1. For this comparison, by using available (✓) and not available (×), This paper includes some different technical functionalities such as availability (A), Confidentiality (C), Integrity (I), server-side verifiability (SSV), and user-side verifiability (USV). However, most relevant schemes lack many other significant technical features that are not committed to securely storing health data. The comparison consequences exhibit that the mentioned structure accomplishes better than the recent systems and hence can afford an optimistic determination for enhancing existing health data storage applications.

TABLE I. FUNCTIONALITIES COMPARISON

Ref.	A	C	I	SSV	USV
[22]	×	✓	✓	×	×
[23]	✓	✓	✓	×	×
[24]	✓	×	✓	×	×
[25]	×	×	✓	×	×
[26]	×	×	✓	×	×
[27]	×	✓	✓	×	×
Our work	✓	✓	✓	✓	✓

V. CONCLUSION

Encouraged by the demand for health center digitalization, this paper designed a secure storage system for data management by deploying a privacy-preserving and performance-enhanced blockchain. In this study, a trusted access control strategy based on blockchain is designed to control user access to confirm secure and efficient health record sharing. The proposed system specifies functional units and follows a systematic process for blockchain-enabled decentralized data

repository and record sharing. This scheme may allow consultants or users to store data more securely than conventional schemes, particularly by ensuring confidentiality, availability, scalability, and integrity. Then, this work has exhibited the performance evaluation of the system by measuring the publishing transaction time cost and its latency on the blockchain employing different user nodes. Compared to traditional schemes, the presented framework can be a reliable and promising determinant in the health center industry towards efficient and secure management of health records. It may consume a significant amount of energy during data transactions and storage in the system, which is enough to raise environmental concerns and can be considered a system limitation. In future work, this work will extend and study this scheme toward auditing the metadata of the cloud storage.

ACKNOWLEDGMENT

This work was supported by the University Malaysia Pahang (UMP), Malaysia under the research grant scheme with reference RDU210310.

REFERENCES

[1] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," IEEE Access, vol. 7, pp. 99573–99588, 2019.

[2] S. Kim, "Two-phase cooperative bargaining game approach for shard-based blockchain consensus scheme," IEEE Access, vol. 7, pp. 127772–127780, 2019.

[3] R. Srivastava and D. Prashar, "A Secure Block-chain Enabled Approach for E-Heath-care System," In 2021 International Conference on Computing Sciences (ICCS) IEEE, pp. 194–201, 2021.

[4] M. Hema Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Real time two hop neighbour strategic secure routing with attribute specific blockchain encryption scheme for improved security in wireless sensor networks," Int. J. Comput. Networks Appl., vol. 8, no. 4, pp. 300–310, 2021.

[5] M.S. Islam, M.A.B. Ameedeen, M.A. Rahman, H. Ajra, and Z.B. Ismail, "Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard," Computers, MDPI, vol. 12(2), pp.46, 2023.

[6] K. M. S. Khan and S. S. Nisha, "BTDEC: Blockchain-Based Trible Data Elliptic Curve Cryptosystem with Fine-Grained Access Control for Personal Data," Int. J. Comput. Networks Appl., vol. 9, no. 2, pp. 214–228, 2022.

[7] A. Johari and R. Alsaqour, "Blockchain-Based Model for Smart Home Network Security," Int. J. Comput. Networks Appl., vol. 9, no. 4, pp. 497–509, 2022.

[8] M.A. Rahman, M.S. Abuludin, L.X. Yuan, M.S. Islam and A.T. Asyhari, "EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0," IEEE Transactions on Industrial Informatics, vol. 18(3), pp.1930-1938, 2021.

[9] A. Khatoon, "A blockchain-based smart contract system for healthcare management," Electron., vol. 9, no. 1, 2020.

[10] G. Yang and C. Li, "A design of blockchain-based architecture for the security of electronic health record (EHR) systems," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2018-December, pp. 261–265, 2018.

[11] M. Bowman, A. Miele, M. Steiner, and B. Vavala, "Private Data Objects: an Overview," arXiv preprint arXiv:1807.05686, 2018.

[12] R. Cheng et al., "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," Proc. - 4th IEEE Eur. Symp. Secur. Privacy, EURO S P 2019, pp. 185–200, 2019.

[13] S. Kushch, S. Ranise, and G. Sciarretta, "Blockchain Tree for eHealth," 2019 IEEE Glob. Conf. Internet Things, GCIoT 2019, IEEE, pp. 1-5, 2019.

[14] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," J. Infect. Public Health, vol. 13, no. 10, pp. 1567–1575, 2020.

[15] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B. G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare," Electron., vol. 9, no. 10, pp. 1–14, 2020.

[16] M. P. D'Arienzo, A. N. Dudin, S. A. Dudin, and R. Manzo, "Analysis of a retrial queue with group service of impatient customers," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 6, pp. 2591–2599, 2020.

[17] X. Yu, Y. an Tan, Z. Sun, J. Liu, C. Liang, and Q. Zhang, "A fault-tolerant and energy-efficient continuous data protection system," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 8, pp. 2945–2954, 2019.

[18] P. Zhang et al., "OpTrak: Tracking Opioid Prescriptions via Distributed Ledger Technology," Int. J. Inf. Syst. Soc. Chang., vol. 10, no. 2, pp. 45–61, 2019.

[19] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A Lightweight Authentication Scheme for Cloud-Based RFID Healthcare Systems," IEEE Netw., vol. 33, no. 2, pp. 44–49, 2019.

[20] Y. Liu et al., "A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin," IEEE Access, vol. 7, pp. 49088–49101, 2019.

[21] M. Brandenburger, C. Cachin, R. Kapitza, and A. Sorniotti, "Trusted computing meets blockchain: Rollback attacks and a solution for hyperledger fabric," In 2019 38th Symposium on Reliable Distributed Systems (SRDS), IEEE, pp. 324-32409, 2019.

[22] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," IEEE Access, vol. 6, pp. 53698–53708, 2018.

[23] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," Journal of medical systems, vol. 42, no. 8, pp. 152, 2018.

[24] A. R. Lee, M. G. Kim, and I. K. Kim, "SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR," Proc. - 2019 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2019, pp. 1087–1090, 2019.

[25] C. D. Parameswari and V. Mandadi, "Healthcare data protection based on blockchain using solidity", Fourth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), IEEE, pp. 577-580, 2020.

[26] N. Al Asad, MT. Elahi, A. Al Hasan and MA. Yousuf, "Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing," in 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT) 2020 Nov 28, IEEE, Dhaka, Bangladesh, pp. 35–40, 2020.

[27] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems," 2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc., 2018.