Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.037531
Article

BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the Internet of Medical Things

Sahar Badri[1], Sana Ullah Jan[2,*], Daniyal Alghazzawi[1], Sahar Aldhaheri[1] and Nikolaos Pitropakis[2]

[1]Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 80200, Saudi Arabia
[2]School of Computing, Edinburgh Napier University, Edinburgh, EH10 5DY, UK
*Corresponding Author: Sana Ullah Jan. Email: S.Jan@napier.ac.uk
Received: 07 November 2022; Accepted: 02 February 2023

Abstract: Rapid technological advancement has enabled modern healthcare systems to provide more sophisticated and real-time services on the Internet of Medical Things (IoMT). The existing cloud-based, centralized IoMT architectures are vulnerable to multiple security and privacy problems. The blockchain-enabled IoMT is an emerging paradigm that can ensure the security and trustworthiness of medical data sharing in the IoMT networks. This article presents a private and easily expandable blockchain-based framework for the IoMT. The proposed framework contains several participants, including private blockchain, hospital management systems, cloud service providers, doctors, and patients. Data security is ensured by incorporating an attribute-based encryption scheme. Furthermore, an IoT-friendly consensus algorithm is deployed to ensure fast block validation and high scalability in the IoMT network. The proposed framework can perform multiple healthcare-related services in a secure and trustworthy manner. The performance of blockchain read/write operations is evaluated in terms of transaction throughput and latency. Experimental outcomes indicate that the proposed scheme achieved an average throughput of 857 TPS and 151 TPS for read and write operations. The average latency is 61 ms and 16 ms for read and write operations, respectively.

Keywords: Blockchain; cybersecurity; IoT; IoMT; smart healthcare

1 Introduction

The Internet of Things (IoT) has revolutionized almost every aspect of human life. Among several IoT-based smart applications, healthcare has gained great attention from academia and industries worldwide [1,2]. The healthcare industry is progressing exponentially with rapid advancements in smart manufacturing, artificial intelligence (AI), fast communication protocols, and robust cybersecurity mechanisms. As a modern application, the Internet of Medical Things (IoMT) has set new trends in the healthcare sector, such as smart sensors, wearable devices, advanced diagnoses, and medical procedures [3,4]. These technologies are highly capable of improving the quality of healthcare with

economical and time-saving responses. Modern healthcare systems enable patients to monitor their health conditions via smart apps, providing remote consultations with doctors for diagnosis. Doctors can also prescribe medicines and offer medical interventions.

The IoMT is a great combination of medical equipment and apps capable of connecting to healthcare information technology systems via networking technologies. Connecting patients to their physicians and permitting the transfer of medical data through a secure network can minimize the pressure on healthcare systems. Most IoMT systems are usually built on centralized frameworks that provide fast information processing and data analysis facilities [5,6]. Despite having strong computational and management capabilities, the growth of IoMT networks has also increased security and privacy issues. With the rapid growth of IoMT networks, the security and privacy of valuable healthcare data have become a critical challenge [6]. Therefore, IoMT systems demand economical, lightweight, immutable, and robust security solutions. Single-point failure is one of the biggest disadvantages of centralized architectures, as it can expose the entire IoMT network to cyber criminals [7,8]. Therefore, centralized frameworks are not recommended for sensitive healthcare record services. Furthermore, the expansion of the IoMT network significantly increases the amount of sensing data, which may burden the centralized system and can further lead to the instability of the network.

These issues can be addressed using blockchain technology. A blockchain is a distributed ledger that facilitates the secure and immutable recording of transactions. It has several key characteristics, including immutability, anonymity, persistency, decentralization, and security [9,10]. It also enables the underlying communication frameworks to provide secure and trustworthy transactions with cryptographic primitives [11,12]. Blockchain is initially introduced for secure digital currency transactions. It is a decentralized and distributed ledger that stores data throughout its peer-to-peer network and addresses blocks using asymmetric cryptography. This ensures the accessibility of data at the block level for all parties concerned. Consequently, blockchain reduces the hazards associated with data centralization, including data tampering.

In the past few years, blockchain has gained much attention from academia and industry for healthcare applications. Blockchain technology offers secure and robust storage solutions to maintain valuable healthcare records. Although several blockchain-based frameworks have been proposed for healthcare applications, most do not provide access control mechanisms. Furthermore, the IoMT network contains hundreds of smart IoT devices that cannot process complex cryptographic algorithms because of their resource-constrained nature. To overcome these challenges, this paper presents a private blockchain-enabled framework for the IoMT. The main contributions of this paper are as follows.

- This work realizes the capabilities of emerging blockchain technologies for the next generation of healthcare applications.
- A decentralized, flexible, and private blockchain framework based on ciphertext policy attribute-based encryption is proposed for the IoMT that can perform several healthcare-related operations in a secure and trustworthy manner.
- To analyze the effectiveness of the suggested framework, extensive experiments are conducted, and performance is analyzed in terms of system throughput and latencies.

The remaining article is organized as follows. Section 2 presents some state-of-the-art research in the area of blockchain-based healthcare frameworks. Section 3 briefly discusses the mathematical model of the proposed architecture. Section 4 presents the operation of multiple medical services through the proposed framework. Section 5 presents simulations and a discussion of the results. Finally, a brief conclusion is presented in Section 6.

2 Literature Review

This section presents some latest studies related to blockchain technology for healthcare applications. Recent advancements in blockchain technologies have enabled modern healthcare systems to provide authenticity, security, privacy, and trustworthiness in data sharing at multiple levels. Wang et al. [13] presented a hybrid blockchain framework to enhance the accuracy of diagnosis and medical treatment. The authors constructed a consortium blockchain to link patients, doctors, and hospitals for comprehensive healthcare data sharing. Wong et al. [14] developed a blockchain-enabled system for clinical trial processes. The authors utilized real data from clinical trials and conducted extensive experimentation on web portal applications. The experimental findings proved the effectiveness of the proposed system for efficient management and security of clinical trial data. Vazirani et al. [15] introduced a secure and interoperable blockchain infrastructure to maintain medical history. The proposed system maintains the ownership of patients without compromising the security and privacy of sensitive healthcare data. Access to a patient's medical record is important in medicine prescription. Tanwar et al. [16] presented an access control privacy scheme with blockchain to enhance data accessibility among healthcare system participants. The authors implemented a Hyperledger-based framework for healthcare record sharing. Garg et al. [17] developed an advanced blockchain-based authentication protocol for the healthcare environment to address this issue. The proposed technique ensures secure key management between personal servers and medical devices. It facilitates authorized users to access medical data from the blockchain network in a secure manner. Experimental outcomes confirmed the higher performance of the suggested technique over several state-of-the-art studies.

Alqaralleh et al. [18] presented a hybrid image transmission approach for the IoMT using deep learning with a blockchain-based infrastructure. The suggested technique contains multiple processes, including data collection, hashing, secure transactions, and classification. First, researchers utilized elliptic curve cryptography and calculated its keys using the fruit fly optimization algorithm. After that, the hash values are encrypted using the neighborhood indexing sequence with burrow wheeler transform. In the final stage, a deep belief network is employed to diagnose the disease. Extensive experiments are conducted to identify the appropriate analysis of the supplied model's outcomes, and the results are analyzed from several perspectives. Recent advances in IoMT have made it possible for smart devices to produce and send voluminous Electronic Medical Records (EMRs). However, an EMR has several sensitive properties that some unauthorized users might access for malevolent reasons. Wang et al. [19] presented an access control technique compatible with a blockchain-based transaction system. Moreover, they designed a privacy-preserving framework for access control. Researchers assessed their methodology using EMRs of 100,000 patients in real time. The experimental outcomes demonstrate that the proposed framework protects patient privacy more effectively than conventional access control mechanisms in smart healthcare environments. Egala et al. [20] introduced a novel blockchain-enabled distributed data storage system for the IoMT. The authors addressed the multiple issues of cloud-centric healthcare systems, including high storage costs, high latency, and single-point failure. Jin et al. [21] proposed an integrated cross-cluster federated learning and blockchain-based system for IoMT. The authors conducted extensive experiments to analyze the feasibility and efficiency of the suggested scheme. The proposed framework efficiently addressed the issue of high latency in the IoMT network. In another recent study, Akkaoui [22] developed a smart contract-based authentication framework for healthcare devices using blockchain technology. The proposed scheme addresses several security issues in traditional healthcare systems due to their centralized architecture. Singh et al. [23] designed a patient-centric blockchain system for healthcare record management. The authors conducted extensive experiments using the Hyperledger caliper

benchmarking tool. The experimental outcomes confirm the effectiveness of the proposed architecture in terms of resource utilization, throughput, latency, etc.

In smart healthcare systems, security and privacy are the major issues in the IoMT paradigm. Blockchain can overcome a wide range of these issues in IoMT. Several research efforts have been made regarding blockchain deployments in healthcare applications. However, the aforementioned studies have a few limitations. First, most of the existing model's utilized open-source frameworks for blockchain deployments. Using third-party services can occasionally create severe privacy issues in healthcare-based applications. Secondly, the breadth of the existing studies on healthcare operations is limited. Most of the studies focus only on the efficient recording of healthcare data; the feasibility of blockchain for other necessary medical operations is not deeply considered. Third, the evaluation of the proposed architecture in the context of IoMT is not discussed. To overcome the aforementioned issues, this paper presents a private, flexible, and lightweight blockchain-based framework for IoMT.

3 Design of the Proposed Architecture

Integrating blockchain technology with IoMT enhances the security of the overall healthcare architecture. The blockchain contains all the key essential features for a secure IoMT network. This article proposed a blockchain-based scheme for security, privacy, and trustworthiness in the IoMT systems.

3.1 Main Participants

The proposed scheme contains five main participants: private blockchain, hospital management services, cloud service providers, doctors, and patients. These modules are shortly described in the following.

1. Private Blockchain: The proposed framework is based on a private network that only authorizes registered users to access the services. The distributed ledger is made up of a chain of cryptographically linked blocks. Each block contains a timestamp, hash value, hash value of the previous block, and Merkle roots. The authorized users can access and modify the ledger through smart contracts. These contracts consist of mathematical and logical function-based code that enables the users to access the blockchain without any third-party involvement. The consensus mechanism allows the new transaction to be added to the blockchain network. The proposed framework uses a proof of authentication (PoAh) consensus algorithm. The PoAh technique follows a conventional blockchain working mechanism with lightweight block verification [24]. Therefore, it is considered a lightweight and IoT-friendly consensus algorithm suitable for resource-constrained IoMT networks.
2. Hospital Management Service (HMS): The main function of HMS is to provide hospital-related services to patients. HMS generates the master and public keys for the healthcare management system and private keys for the users and patients.
3. Cloud Service Provider (CSP): CSP facilitates the storage of encrypted medical data by doctors, helps implement policy matching, and provides data storage services to users and patients. CSP also generates and publishes the decryption parameters to only access the stored data by authorized users.
4. Doctors: The medical practitioners diagnose the patients, suggest suitable treatments for the diagnosed diseases, and generate an encrypted electronic medical record for all the patients.

5. Users: Patients are the most important participants of the proposed framework. Users can register themself in a blockchain network through an authorization process, get doctor's appointments, lab facilities, information about prescribed medicines, and can get access to their medical history.

Table 1 shows notations and descriptions of all parameters used in this paper.

Table 1: Notations and description of utilized parameters

Notation	Description
$\boldsymbol{\delta}$	Master key
$\boldsymbol{\varphi}$	Public key
$\boldsymbol{\psi_u}$	Secret key
$\boldsymbol{\eta}$	Attacker
$\boldsymbol{T}$, $\boldsymbol{T^*}$	Access structure
$\boldsymbol{C}$, $\boldsymbol{C^*}$	User's list
$\boldsymbol{\chi}$	Message
$\boldsymbol{At}$	Attribute set
$\boldsymbol{\vartheta_{ui}}$	Intermediate parameter
$\boldsymbol{\xi_{pi}}$	Cipher text

3.2 Mathematical Model of the Proposed Security Scheme

Let's initiate a security challenge between an opponent ϕ and an attacker η. The security challenge is described in the following.

1. The opponent ϕ chooses the access structure T^* and the user's list C^*, and submits T^* and C^* to the attacker η.
2. The B generates the master key δ and public key φ, sends φ to ϕ, and keeps δ secrete by using an initialization algorithm.
3. Based on attribute sets At, ϕ continuously requests the private keys ψ_u from η. Meanwhile, B uses the key generation algorithm to return the private keys ψ_u.
4. A sends two messages, χ_1 and χ_2, to η, where $|\chi_1| == |\chi_2|$. η chooses a user set $u \in \{0, 1\}$ at random and uses the encryption technique to encrypt χ using T^* and C^*. ϕ is given the result ξ_p.
5. ϕ requests the private keys as in step 3.
6. ϕ estimates $u' \in \{0, 1\}$. If $u' == u$, ϕ wins the challenge, and can be described as:

$$Adv(\phi) = \left| pr[u' == u] - \frac{1}{2} \right|.$$

We can consider the suggested technique secure if all polynomial-time competitor has a trifling advantage in the given challenge. To put it another way, it can withstand plaintext attacks.

3.3 Mathematical Model of the Suggested Protocol

3.3.1 Overview

Some functions are defined to enable secure and traceable medical data exchange in IoMT.

1. *IDGen* (*passwrd*) $\rightarrow$ *addr* $\hbar$: This function facilitates the users to generate an account address *addrID* through blockchain-enabled service.
2. *Setup*(μ) $\rightarrow$ (φ, δ): This function aids in obtaining the φ and δ of the system by providing the security parameter μ.
3. *KeyGen*(δ, At_{ui}, *addr* $\hbar_{ui}$) $\rightarrow$ ($\vartheta_{ui}, \psi_{ui}$): This function accepts inputs such as δ, the attributes set At_{ui}, and the user identity *addr* $\hbar_{ui}$ and produces a private key ψ_{ui} as well as an intermediate parameter ϑ_{ui} for user u_i.
4. *Encrypt* ($\varphi, \Delta_i, \chi_i, C$) $\rightarrow$ ξ_{pi}: This function accepts the φ, Δ_i, M_i, C, as inputs and returns a ciphertext ξ_{pi} associated with Δ_i.
5. *Delegate*($\varphi, At_{ui}, \vartheta_{ui}, \xi_{pi}$) $\rightarrow$ (ε_{ui}, ξ_i'): This function receives the inputs φ, At_{ui}, ϑ_{ui}, and ξ_{pi}, and returns ε_{ui} and $\xi T'$.
6. *Decrypt*($\xi_{pi}^{,}, \varepsilon_{ui}, \psi_{ui}$) $\rightarrow$ χ_i: This function takes the inputs ε_{ui}, $\xi T'$and ψ_{ui}, and returns the plaintext χ_i'.
7. *Trace*($\varphi, At_{ui}, \vartheta_{ui}$) $\rightarrow$ (*addr* $\hbar_{ui}/\perp$): This function accepts the inputs φ, At_{ui}, and ψ_{ui}, and returns the user's address *addr* $\hbar_{ui}$ or $\perp$.
8. *Re* $-$ *Encrypt*($\varphi, \Delta_i, \chi_i, C'$) $\rightarrow$ ξ_i': This function receives the φ, Δ_i, χ_i, C'' as inputs, and returns a ciphertext ξ_i' associated with Δ_i.
9. *Tran_save*(ψ, *addr* $\hbar$, *content*, *timeStamp* $-$ *amp*): This function facilitates the users to store their valuable data in the blockchain network. It accepts a private key ψ for data signing, the transaction address of the sender *addr* $\hbar$, the real information to be stored, and the *timeStamp*.

The detailed operation is depicted in Fig. 1 and the process is elaborated in the following.

1. The users that want to register them in the blockchain generate the account address as *addr* $\hbar_{ui}$.
2. The HMS generates the master keys δ and public keys φ by using the security parameter μ.
3. The HMS transmits its attribute set At_{ui} and *addr* $\hbar_{ui}$ to the HMS to generate ($\vartheta_{ui}, \psi_{ui}$) by using the function *KeyGen*().
4. The doctor creates a matching access policy Δ_i based on the requirements of the patients for medical data protection, then uses *Encrypt*() to build the ciphertext ξ_{pi}, which is subsequently sent to the cloud service provider.
5. The user enquires about medical information by sending ϑ_{ui} and the attributes set to CSP.
6. CSP uses *Delegate*() to match policies. On success, it delivers the parameters for decryption and the ciphertext. After that, the ciphertext can be decoded using *Decrypt*().
7. The HMS can track the decoding process by using the intermediate parameters retrieved through CSP.
8. If the user is anomalous and involved in data leaks, then its address *addr* $\hbar$ will be put on the cancellation list and forwarded to the doctor. The doctor encrypts the data again using *ReEncrypt*().

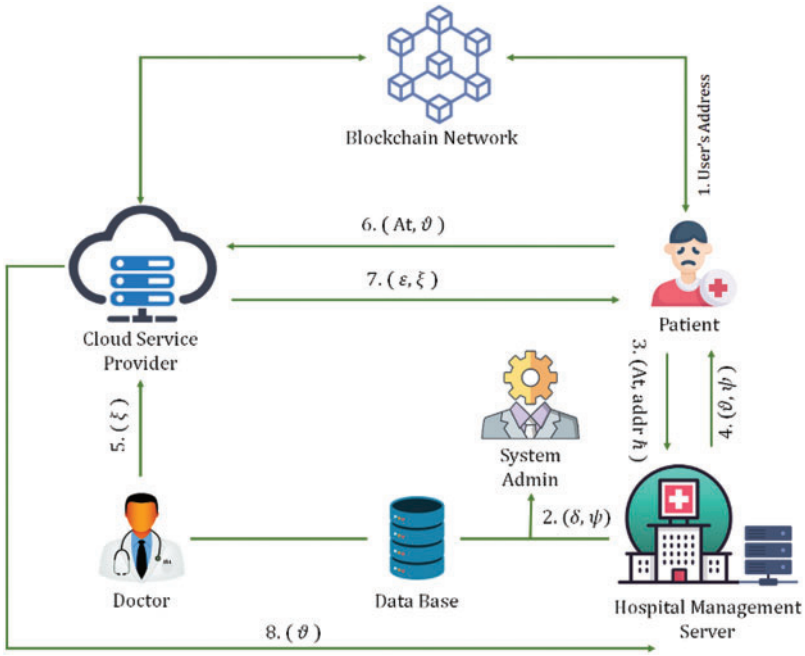

Figure 1: Flow of the proposed security protocol

3.3.2 *Description of Protocol*

The system protocol contains several stages that are described in the following.

a) System Setup: The setup (μ) function is used to generate φ *and* δ. First, two groups (G, GT) are selected on the order P. Then the function e: $G \times G \rightarrow GT$ is defined, based on two generators g and ω. Define $U = \{addr\ \hbar_{ui} | 1 \leq i \leq n\}$ as the group users and define $attr = \{a_j | 1 \leq i \leq m\}$ as the global characteristic set. After that, the query list ω with the ϕ is generated with a random parameter and a *addr* $\hbar$. Finally, selecting H: $\{0, 1\} \rightarrow G$, a hash function, and selecting q_1 and q_2 randomly, where $q_1, q_2 \in Z_\Delta$. After completion, the $\varphi$and δ are returned.

$$v = \{q_1, q_2\} \tag{1}$$

$$\varphi = \{g, \omega, h = \omega^{q_2}, h = g^{q_2}, y = e\,(g, \omega)^{q_1}, H\,()\} \tag{2}$$

b) Key Generation: When a patient u_i interact with the hospital, the HMS selects the At_{ui} and *addr* $\hbar_{ui}$ as inputs. HMS chooses the random parameter $\tau \in Z_\Delta$ according to the *addr* $\hbar_{ui}$, and then computes $\hbar_{ui}^{(1)} = g^{\frac{q_1 + \tau}{q_2} + q_2 \tau}$, $\hbar_{ui}^{(2)} = \left\{g^{\tau H(aj)}\right\}_{aj \in L_{ui}}$, $\hbar_{ui}^{(3)} = g^{addr\,\hbar uiq_2 \tau}$ and $\hbar_{ui}^{(4)} = \mathrm{h}^{\tau}$. For the moment, it writes the parameters *addr* $\hbar_{ui}$, and τ into W. Then, it transmits $\psi_{ui} = (v_{ui}^{(3)}, \hbar_{ui}^{(4)})$ and $\vartheta_{ui} = (\tau, \hbar_{ui}^{(1)}, \hbar_{ui}^{(2)})$ to user u_i via a secure channel.

c) Data Encryption: The doctor generates medical data after interaction with the patient. Let χ_i represent the medical data generated by the doctor for patient u_i. C represents the cancellation user list, where $C = addr\ \hbar_j | 1 \leq j \leq n, |C| = r, rn$, and S represent the authorized user list. The

doctor encrypts χ_i through the φ and the system's access policy Δ_i by performing the following procedures. Create T_i based on the Δ_i.

1. Choose $\gamma \in Z_\Delta$, and computes ξ (1) $\Delta = \chi_i y^\gamma = \chi_i e(g,\omega)^{a\gamma}$ and $\xi_\Delta^{(2)} = h^\gamma$.
2. Let γ represent the root node's value for the tree T_i. Allocate the root nodes and unallocated all its sub-nodes.
3. For all leaf nodes $a_j \in T$, the system computes $\xi_{a_{j,k}}^{(3)} = \omega^{\gamma_k H(aj)^{-1}}$.
4. Select a random entity for each participant belonging to the cancellation list. Since $|C| = r$, the system selects r numbers that represent $\{t_j \in Z_\Delta\}_{1\le j\le r}$ and satisfy $\gamma = \sum_{j=1}^{r} t_j$.

Then, the ciphertext is defined as

$$\xi_{\Delta i} = \left(\xi_\Delta^{(1)}, \xi_\Delta^{(2)}, \left\{\xi_{a_{j,k}}^{(3)}\right\}_{a_j \in T_i}, \left\{\xi_{u_j}^{(4)}\right\}_{u_j \in C}, \left\{\xi_{u_j}^{(5)}\right\}_{u_j \in C}\right) \tag{3}$$

d) Decryption Delegation: When a patient sends a request to access healthcare services, he/she will send L_{ui} and ϑ_{ui} to the CSP. The CSP provides the decryption parameters and cipher text to the user through the decryption delegation function. The CSP chooses the minimum set L' that fulfill the T_i. For each attribute $a_j \in At'$, it calculates.

$$\vartheta_{ui} = \frac{e(\hbar_{ui}^{(i)}, \xi_\Delta^{(2)})}{\prod_{a_j \in At, i=index} e(\hbar_i^{(2)}, \xi_{aji}^{(3)})^{l_i(0)}} \tag{4}$$

Each attribute in the policy corresponds to a sub-secret sharing value, parameter γ can be computed according to $\sum_{i=0}^{t-1} \gamma_i l_i(0)$. In other words, it can obtain ε_{ui} by computing $e(\hbar_i^{(2)}, \xi_{aji}^{(3)})^{l_i(0)}$. For the moment, the CSP integrates the $\xi_{\Delta i}$ with r τ to generate the new ciphertext

$$\xi T_i' = \{\tau, \xi_{\Delta i}\} \tag{5}$$

and sends ε_{ui} and $\xi T_i'$ to the user.

e) Decryption: The user executes the decryption process after receiving $(\varepsilon_{ui}, \xi T_i')$. If *addr* $\hbar_{ui} \in C$, the algorithm is terminated. The plaintext can be obtained if *addr* $\hbar_{ui} \in S$. For each $a_j \in At'$, the system calculates

$$\varepsilon' = \prod\nolimits_{j=1, addr\ \hbar_{uj} \in C}^{r} \left[\frac{e(\hbar_{uj}^{(3)}, \xi_{uj}^{(4)})}{e(\xi_{uj}^{(5)}, \hbar_{uj}^{(4)})}\right]^{\frac{1}{addr\ \hbar_{ui} - addr\ \hbar_j}} \tag{6}$$

The decryption key ε can be computed using ε_{ui} and ε'. The ciphertext can be decrypted as:

$$\varepsilon = \frac{\varepsilon_{ui}}{\varepsilon'} \tag{7}$$

$$\chi_i' = \{\tau || \xi_\Delta^{\frac{1}{\xi}}\} = \{\tau | | \chi_i\} \tag{8}$$

After receiving $(\varepsilon_{ui}, \xi T_i')$, The only user *ui* who satisfies *addr* $\hbar_{ui} \in S$ can access the decryption key.

f) Anomalous User Tracking: The HMS validates ϑ_{ui} by determining whether the relevant user's address *addr* $\hbar$ can be found in list W. It employs τ to analyze the decoding behavior and to give referential elements for tracing down the users who illegally disseminated decryption keys.

As a result, an invalid ϑ_{ui} indicates that this user is not required to be tracked. There are two parts to the tracking process: verify and query.

Verify_phase. The HMS accepts the input parameters that include the attributes set of users At_{ui}, φ and ϑ_{ui} to verify the validity of ϑ_{ui}, and then calculates C_{s1} and C_{s2}. It can be described as:

$$C_{s1} = e\left(\hbar, h\right), C_{s2} = y \cdot e\left(\hbar^{(1)}, h^2, \omega^{H\left(a_i\right)_{a_i \epsilon L_{ui}}^{-1}}\right) \tag{9}$$

If $C_{s1} = C_{s2}$, then it indicates the successful process of verification and nominates the user as an authorized user.

Query_phase: The ϑ_{ui} is considered valid after the completion of a successful verification process. It can obtain the user's *addr* $\hbar$ from the list W through τ and then generate the *addr* $\hbar$ corresponding to τ. Otherwise, output $\perp$.

g) Data Re-encryption: As the cancellation list C was modified, only the items of $\left\{\xi_{uj}^4\right\}_{uj \in C}$ and $\left\{\xi_{uj}^5\right\}_{uj \in C'}$ are required to be updated according to the new C' in $\xi_{\Delta i}$. After adding an anomalous user address *addr* $\hbar_e$ to the cancellation list, it should add $\xi_e^{(4)} = h^{te}$ and $\xi_e^{(5)} = h_1^{addr\ \hbar_e te}$ to $\left\{\xi_{uj}^4\right\}_{uj \in C'}$ and $\left\{\xi_{uj}^5\right\}_{uj \in C'}$, respectively. The newly generated ciphertext $\xi T''_{\Delta i}$ is described as

$$\xi''_{\Delta i} = \left(\xi_{\Delta}^{(1)}, \xi_{\Delta}^{(2)}, \left\{\xi_{aj,k}^{(3)}\right\}_{a_j \in T_i}, \left\{\xi_{uj}^4\right\}_{uj \in C'}, \left\{\xi_{uj}^5\right\}_{uj \in C}\right) \tag{10}$$

3.4 Consensus Algorithm

A lightweight consensus algorithm (PoAh) is incorporated into the blockchain to verify and add new transactions to the blockchain. This algorithm adheres to conventional communications, with updates occurring only during block validation [25]. The network's precipitants, acting independently, create the initial transactions with the data and then combine them into a block. The public and private keys generated in the aforementioned steps are used here. Before the node broadcast, the source node signs the block with its private key ψ and makes its public key φ available to everyone. For block validation, there must be authorized nodes in the network. These nodes are put into service with just enough trust to qualify as authorized nodes, whereas all other nodes have no trust. After a block has been completely authenticated, the authorized nodes will receive a trust value.

Once the authorized node receives the block, it is analyzed to determine its validity by obtaining the originating node's public key φ. Due to the asymmetric cryptography characteristic, the signature can only be verified using the public key. Furthermore, because of the discrete log problem properties, it is impossible to determine the value of while other values are known. In the second evaluation phase, the authorized node checks the MAC value once the signature has been verified. After verification, the reliable nodes will send out the block and the PoAh identity to the rest of the network. After that, the PoAh data in the block is sought by specific network nodes so that they may be appended to the chain. At last, nodes compute a hash of the block and store it to create a link to the following block; the previous hash value is also stored in the current block. Algorithm 1 details the steps involved in the PoAh process.

Algorithm 1: All the participants follow the hash algorithm

Input	All the participants have public and private keys
Output	Validated blocks

(Continued)

Algorithm 1: Continued

```
Participants combine the transactions to generate a block
Sign the blocks with own private keys
Broadcast the blocks after signing
Authorized participants verify the signature using a public key
If (Authentication Successful)
    Add the block to the chain
 else
    Discard block
Go to step 1 for a new block
```

4 Medical Services in the Proposed Architecture

This proposed architecture can perform several healthcare-related operations, including patient appointments, medical checkups, diagnostic services, and treatments. Furthermore, all these healthcare services are interconnected with each other. An overview of the blockchain-enabled healthcare system is presented in Fig. 2. This section briefly describes each module.

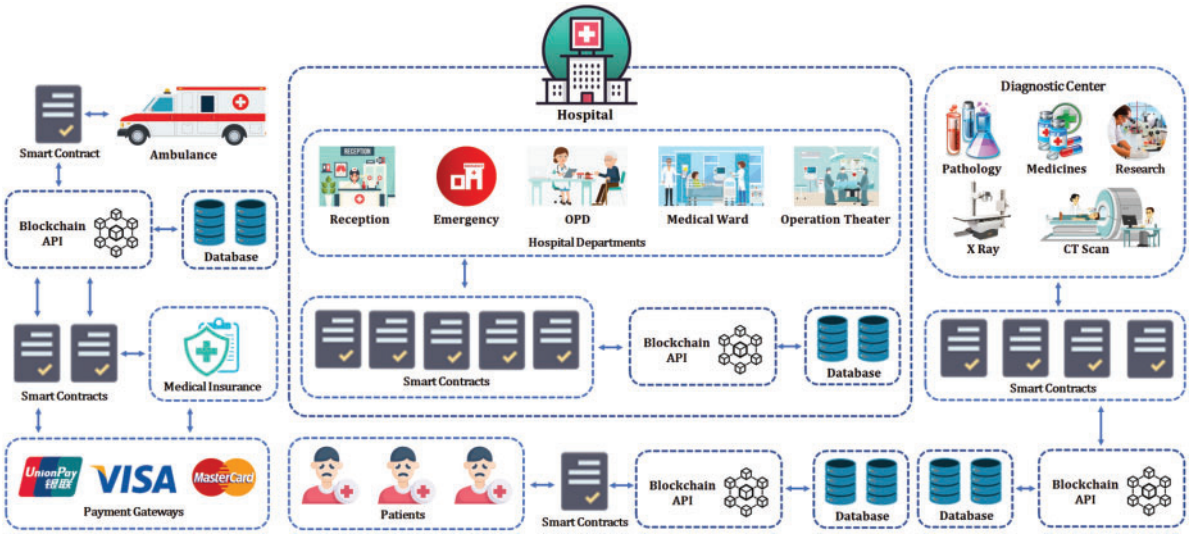

Figure 2: Overview of blockchain-enable services in IoMT

4.1 Patient Appointment

If a patient wants to make an appointment with a doctor, they would first submit a transaction proposal with their details such as name, gender, ID number, and age. The Blockchain API will execute this transaction and provide the user with a list of medical specialists. After selecting a medical specialist, the API forwards this request to the relevant doctor. If the doctor confirms their availability, the API informs the patient about the available date and time. After final confirmation from the patient, the blockchain submits a transaction proposal and executes a consensus algorithm. If the consensus is successful, a new block is generated and added to the blockchain. After a successful operation, the blockchain generates an appointment receipt and sends it back to the patient. The

receipt is encrypted, and a patient can extract the information using their private key. The flow of the appointment process is summarized in Algorithm 2.

Algorithm 2 : Appointment Process

```
begin
    patient submit a transaction proposal along with details
    API provides a list of medical specialists
    selection of desired medical specialist
    a request for an appointment forward to the doctor
    if (Dr_availabilty = = true)
        API inform about available date and time
    else
       inform patients about the unavailability
     final confirmation from the patient
     API executes PoAh
     if (PoAh = = successful)
         generate appointment receipt
     else
        return error ()
 end
```

4.2 Medical Checkup

For a medical checkup, the patient is required to visit the hospital on a specific date and time. First, a receptionist verifies the appointment details from the blockchain API. This is followed by payment confirmation details from the patient's bank account or insurance balance. Once everything is confirmed, the API will update the database, and the patient will move toward the OPD, where a medical specialist will perform the necessary checkup. The doctor can also acquire the patient's medical history from the blockchain API. Based on the checkup, the doctor can prescribe medicine or suggest some laboratory tests for further diagnosis. Once a checkup is completed, the doctor will update the record by submitting a transaction proposal to the blockchain API. After the successful execution of the consensus algorithm, the blockchain updates the record and issues an acknowledgment receipt that can only be accessed by the doctor, patient, or another authorized party. The flow of the medical checkup process is summarized in Algorithm 3.

Algorithm 3: Medical Checkup

```
begin
    patient visit to the hospital
    receptionist verifies the appointment details
    verification of payment
    if (appointment and payment details = = true)
       API updates databased
       the patient moves toward OPD
    else
       return error ( ).
     doctor performs checkup
     access medical history from the database (if required)
```

(Continued)

Algorithm 3: Continued

```
        prescribe medicines or laboratory tests
        submit transaction proposal for record update
        if (PoAh = = successful)
            generate acknowledgment receipt
        else
            return error ( )
    end
```

4.3 Diagnostic Services

The patient must visit the diagnostic center if the doctor recommends laboratory tests such as blood, urine, X-rays, CT scans, etc. First, the diagnostic center will acquire details of the recommended tests from the blockchain API by using the patient's ID. Subsequently, the additional payment details for the specific test will be confirmed. Once the payment has been confirmed, the patient moves toward the laboratory. The laboratory staff will collect the required samples for the test. The time of each test result can vary according to the requirements. After completion of the process, the laboratory staff will update the blockchain API with the diagnosis results. All these results are in the form of encrypted reports. Only relevant doctors and patients can access these reports' contents using their private keys. The flow of the medical checkup process is summarized in Algorithm 4.

Algorithm 4: Diagnostic Services

```
begin
      patient visit to the diagnostic center
      lab staff verifies the test details through the patient's ID
      the payment process for the required test
      if (test and payment details = = true)
         the patient moves toward the lab
         lab staff collect the relevant sample
       processing started on the sample
      else
          return error ( ).
       lab staff submit transaction proposal after processing
       if (PoAh = = successful)
          blockchain API updates the database with results
          doctor and patient receive a notification about test results
       else
          return error ( )
  end
```

4.4 Medical Treatment

The doctor will decide on the medical treatment based on the diagnosis reports. This treatment can take several forms, according to a patient's health condition. First, a doctor can prescribe the medicine for a limited duration. In this case, the doctor will update the blockchain with their recommendation. Next, the patient must visit a pharmacy to collect the medicines. The pharmacy will have a detailed record of each medicine, including the type, company, manufacturer, expiry date, and prices. After a

successful payment process, the pharmacy will issue the medicines and update the blockchain record that will be accessible to both the doctor and the patient. In the second case, the doctor can suggest admitting the patient to the medical ward for continuous care and treatment. The ward administration will allocate a specific room and bed to the patient and update the database. The record of daily checkups, medicine, and healthcare procedures will be continuously updated on the blockchain for the doctor's access. In the third case, the doctor may suggest minor or major surgery for the patient. First, the patient will be allocated a specific surgery date. All the pre-surgical and post-surgical procedures will be updated in the blockchain database. After surgery, the patient's health status and prescribed medicines will be updated in the blockchain for future diagnosis and treatment. The flow of the medical treatment process is summarized in Algorithm 5.

Algorithm 5: Medical Treatment

```
begin
    doctor reviews the diagnosis reports
    treatment decision based on reports
    doctor's decisions can be (medicine, admission, or surgery)
    if (decision = medicine prescription)
        doctor update record with his/her recommendations
        patient visits the pharmacy to collect medicines
        pharmacy verifies the payment
        issue the prescribed medicines to the patient
        update blockchain records for doctor and patient
    if (decision = admit patient)
        doctor updates the record with a health care plan
        ward administration allocates the specific ward and bed
        maintain the daily record of checkups and medicines
        update the blockchain for doctor's information
    if (decision = surgery)
        the doctor decides the specific date of surgery
        decide the pre and post-surgical procedures
        update blockchain record
        conduct surgery and update the patient's health status after surgery
        prescribe medicine and future checkups
        update blockchain records to maintain medical history
end
```

5 Experiments and Performance Analysis

All the experiments are conducted using a Dell Inspiron Compact Desktop computer system with Intel® Core™ i7-11700 processor, 16 GB RAM, and Windows 10 operating system. The proposed blockchain framework is constructed in Python, JavaScript, and HTML languages by using open-source libraries. The performance of the proposed architecture is analyzed in terms of transaction throughput and latency.

Throughput and latency have always been useful performance indicators for assessing blockchain-based systems. Transaction throughput indicates the number of successful transactions per second from the first transaction deployment time. Latency indicates the difference between each transaction's

completion time and deployment time. In our experiments, the average transaction throughput and latencies are computed for all operations with varying transactions. In the first phase of experiments, we analyze the blockchain's read/write performance for the patient appointment process. The transactions are divided into five groups that contain 100, 250, 500, 750, and 1000 transactions. A comparative analysis of transaction throughput and latencies for the appointment process is presented in Fig. 3. In data reading, the throughput is almost linearly increased with the number of transactions. The maximum throughput was recorded as 96 TPS and 924 TPS for the smallest and largest groups of transactions. For middle groups, the throughputs were recorded as 232 TPS, 474 TPS, and 698 TPS, respectively. The read performance indicates that the latency is recorded between the interval of 19 ms to 45 ms. Results indicate that the overall latency is increased with the increase in the number of transactions. The data writing process decreases throughput compared to the reading process. The maximum throughput is recorded as 155 TPS for the largest group of transactions. The latency for the writing process is recorded between 3 ms to 13 ms. Experimental outcomes indicate that the proposed blockchain scheme achieved higher throughput for reading operation than for write operation. The suggested scheme indicates the lower latency for both read and writing operations suitable for resource-constrained IoMT networks.

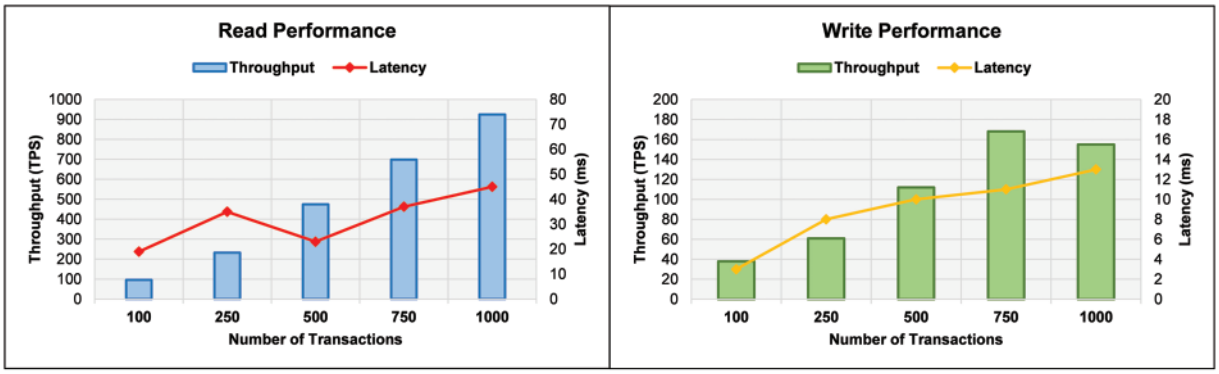

Figure 3: Blockchain read/write performance for the patient appointment process

In the second phase of experiments, we analyze the blockchain's read/write performance for the medical checkup process. Again, the transactions are divided into the same groups. A comparative analysis of transaction throughput and latencies for the medical checkup process is presented in Fig. 4. Data reading increases throughput with the number of transactions. The maximum throughput was recorded as 79 TPS and 910 TPS for the smallest and largest groups of transactions. For middle groups, the throughputs were recorded as 198 TPS, 395 TPS, and 710 TPS, respectively. The read performance indicates that the latency is recorded between the interval of 28 ms to 74 ms. Results indicate that the overall latency is increased with the increase in the number of transactions. The data writing process decreases throughput compared to the reading process. The maximum throughput is recorded as 132 TPS for the largest group of transactions. The latency for the writing process is recorded between 5 ms to 17 ms. Experimental outcomes indicate that the proposed blockchain scheme achieved higher throughput for reading operation than for write operation. The suggested scheme achieved a lower throughput and higher latency for the medical checkup process compared to the patient appointment process.

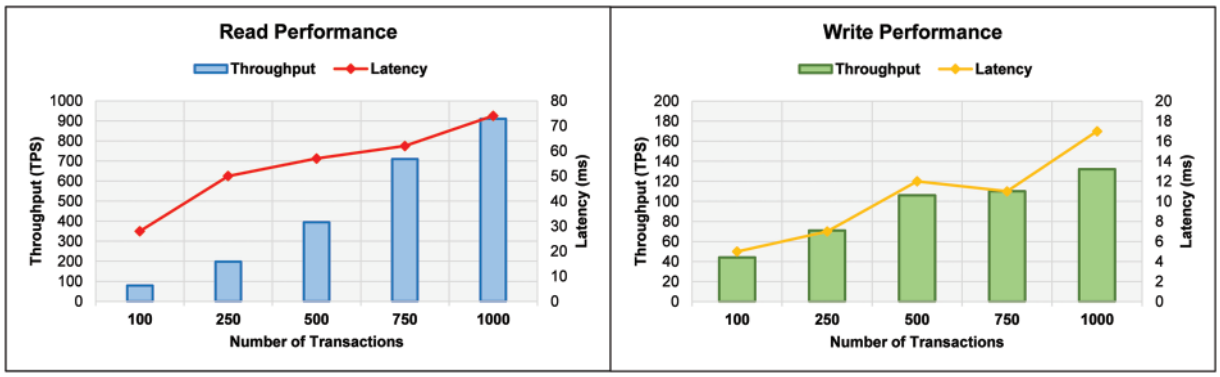

Figure 4: Blockchain read/write performance for medical checkup process

In the third phase of experiments, the blockchain's read/write performance is analyzed for diagnostic services. The same groups of transactions are also maintained here. A comparative analysis of transaction throughput and latencies for diagnostic services is presented in Fig. 5. The results indicate that the diagnostic service is the heaviest operation as compared to other operations. In data reading, the throughput is increased with the number of transactions. The maximum throughput was recorded as 83 TPS and 723 TPS for the smallest and largest groups of transactions. For middle groups, the throughputs were recorded as 201 TPS, 474 TPS, and 705 TPS, respectively. The read performance indicates that the latency is recorded between the interval of 14 ms to 69 ms. Results indicate that the overall latency is increased with the increase in the number of transactions. The data writing process decreases throughput compared to the reading process. The maximum throughput is 167 TPS for the largest group of transactions. The latency for the writing process is recorded between 5 ms to 18 ms.

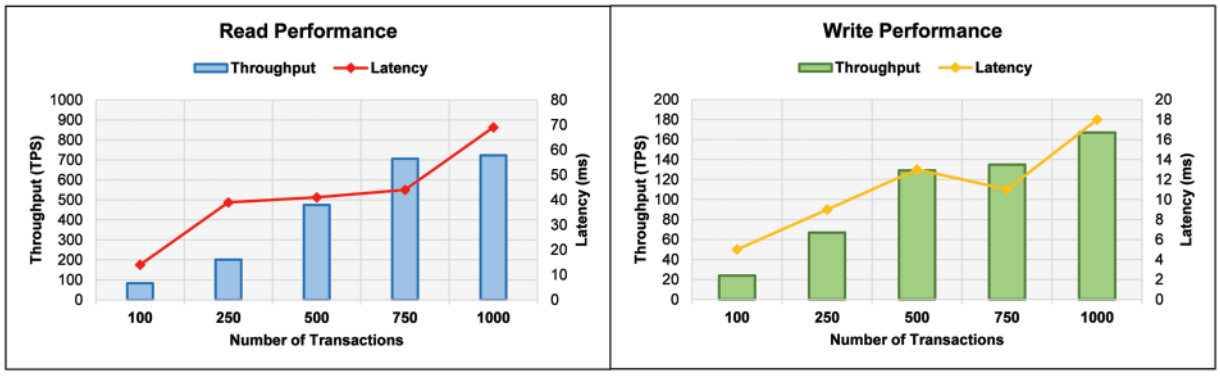

Figure 5: Blockchain read/write performance for diagnostic service process

In the final phase of experiments, the blockchain's read/write performance is analyzed for medical treatment services. The same groups of transactions are also maintained here. A comparative analysis of transaction throughput and latencies for diagnostic services is presented in Fig. 6. The throughput is increased with the number of transactions in data reading. The maximum throughput was recorded as 63 TPS and 872 TPS for the smallest and largest groups of transactions. For middle groups, the throughputs were recorded as 231 TPS, 467 TPS, and 622 TPS, respectively. The read performance indicates that the latency is recorded between the interval of 16 ms to 56 ms. Results indicate that the overall latency is increased with the increase in the number of transactions. In the data writing process,

throughput is decreased as compared to the reading process. The maximum throughput is 149 TPS for the largest group of transactions. The latency for the writing process is recorded between 2 ms to 16 ms. Experimental outcomes indicate that the proposed blockchain scheme achieved higher throughput for reading operation than for write operation.

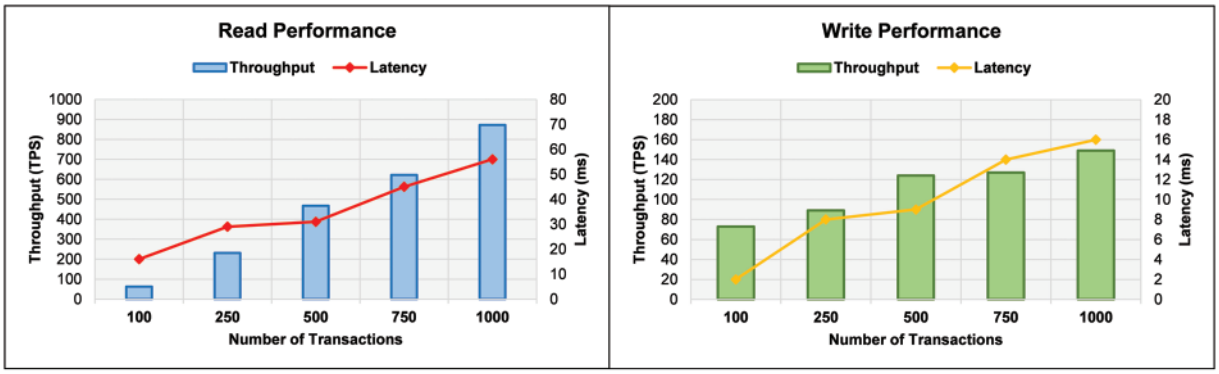

Figure 6: Blockchain read/write performance for the medical treatment process

Experimental outcomes indicated that the overall performance of the proposed blockchain architecture is good. Furthermore, the suggested scheme attained a high throughput and lower latency for all the discussed healthcare services, making it the best suitable for large-scale deployment in the IoMT networks. To further analyze the effectiveness of the proposed scheme, a brief comparison with the state-of-the-art is presented in Table 2.

Table 2: Performance comparison with the state-of-the-art

Reference	Architecture	Encryption algorithm	Access control mechanism	EHR sharing system	Performance evaluation
Wang et al. [13]	√	✗	√	√	✗
Wong et al. [14]	√	√	✗	✗	√
Vazirani et al. [15]	√	✗	√	√	✗
Tanwar et al. [16]	√	✗	√	√	√
Garg et al. [17]	√	√	√	✗	√
Alqaralleh et al. [18]	√	√	✗	✗	√
Wang et al. [19]	√	√	√	✗	√
Egala et al. [20]	√	√	✗	√	√
Jin et al. [21]	√	✗	√	✗	√
Akkaoui [22]	√	√	✗	✗	√

(Continued)

Table 2: Continued

Reference	Architecture	Encryption algorithm	Access control mechanism	EHR sharing system	Performance evaluation
Singh et al. [23]	√	✗	✗	√	√
Proposed scheme	√	√	√	√	√

6 Conclusion

This paper presented a blockchain-based framework for secure and trustworthy services on the IoMT. The proposed framework is based on a private blockchain network that ensures the security and decentralization of IoMT using attribute-based cryptography and PoAH consensus algorithm. As a result, several healthcare operations, including patient appointments, medical checkups, diagnostic services, and treatments, can be performed securely and trusted. The proposed architecture is evaluated for all healthcare services throughput and latency. The experimental results proved the optimum performance of the proposed architecture. For future endeavors, the performance of the suggested scheme can be further enhanced by incorporating the hardware accelerators in the existing network.

Funding Statement: The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under grant no. (RG-91-611-42).

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] S. Latif, M. Driss, W. Boulila, Z. E. Huma, S. S. Jamal *et al.,* "Deep learning for the industrial internet of things (IIoT): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions," *Sensors*, vol. 21, no. 22, pp. 1–45, 2021.

[2] J. A. Alzubi, O. A. Alzubi, A. Singh and M. Ramachandran, "Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 1080–1087, 2022.

[3] M. Alraja, "Frontline healthcare providers' behavioural intention to internet of things (IoT)-enabled healthcare applications: A gender-based, cross-generational study," *Technological Forecasting and Social Change*, vol. 174, pp. 1–15, 2021.

[4] F. Tujman, M. H. Nawaz and U. D. Ulusar, "Intelligence in the internet of medical things era: A systematic review of current and future trends," *Computer Communications*, vol. 150, no. 1, pp. 644–660, 2020.

[5] G. Manogaran, N. Chilamkurti and C. H. Hsu, "Emerging trends, issues, and challenges in internet of medical things and wireless networks," *Personal and Ubiquitous Computing*, vol. 22, no. 5, pp. 879–882, 2018.

[6] J. A. Alzubi, "Blockchain-based lamport merkle digital signature: Authentication tool in IoT healthcare," *Computer Communications*, vol. 170, no. 1, pp. 200–208, 2021.

[7] J. Srivastava, S. Routray, S. Ahmad and M. M. Waris, "Internet of medical things (IoMT)-based smart healthcare system: Trends and progress," *Computational Intelligence and Neuroscience*, vol. 2022, no. 4, pp. 1–17, 2022.

[8] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop *et al.,* "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, pp. 1–15, 2022.

[9] S. Zhao, S. Li and Y. Yao, "Blockchain enabled industrial internet of things technology," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1442–1453, 2019.

[10] S. Latif, Z. Idrees, Z. E. Huma and J. Ahmad, "Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, pp. 1–37, 2021.

[11] A. Bhattacharjya, K. Kozdroj, G. Bazydlo and R. Wisniewsk, "Trusted and secure blockchain-based architecture for internet-of-medical-things," *Electronics*, vol. 11, no. 16, pp. 1–19, 2022.

[12] S. Latif, Z. Idrees, J. Ahmad, L. Zheng and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things," *Journal of Industrial Information Integration*, vol. 21, no. 1, pp. 100190, 2021.

[13] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan *et al.,* "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, 2018.

[14] D. R. Wong, S. Bhattacharya and A. J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain," *Nature Communications*, vol. 10, no. 1, pp. 1–8, 2019.

[15] A. A. Vazirani, O. Donoghue, D. Brindley and E. Meinert, "Blockchain vehicles for efficient medical record management," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–5, 2020.

[16] S. Tanwar, K. Parekh and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, no. 10, pp. 102407, 2020.

[17] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues *et al.,* "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[18] B. A. Y. Alqaralleh, T. Vaiyapuri, V. Subbiah Parvathy, D. Gupta, A. Khanna *et al.,* "Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment," *Personal and Ubiquitous Computing*, pp. 1–11, 2021.

[19] S. Wang, G. Wu, Z. Ning and Jun Li, "Blockchain enabled privacy preserving access control for data publishing and sharing in the internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8091–8104, 2021.

[20] B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021.

[21] H. Jin, X. Dai, J. Xiao, B. Li, H. Li *et al.,* "cross-cluster federated learning and blockchain for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15776–15784, 2021.

[22] R. Akkaoui, "Blockchain for the management of internet of things devices in the medical industry," *IEEE Transactions on Engineering Management*, pp. 1–12, 2021.

[23] A. K. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi *et al.,* "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5779–5789, 2020.

[24] S. Maitra, V. P. Yanambaka, A. Abdelgawad, D. Puthal and K. Yelamarthi, "Proof-of-authentication consensus algorithm: Blockchain-based IoT implementation," in *IEEE 6th World Forum on Internet of Things (WF-IoT)*, New Orleans, LA, USA, pp. 1–2, 2020.

[25] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, 2018.