A Blockchain-Enabled Quantum Encryption Scheme for Securing Consumer-Centric Digital Twin Healthcare Networks

Sunil Prajapat, Seong Oun Hwang, Pankaj Kumar, Mohammad Shabaz

***Abstract*—The integration of consumer-centric digital twin (CCDT) technology is set to transform healthcare systems, enabling blockchain-based solutions for enhanced medical services. By precisely simulating patients and medical processes, CCDT establish a link to the virtual healthcare environment, supporting improved diagnosis, real-time monitoring, and predictive analytics. Blockchain technology is critical in connecting the physical and virtual health care worlds, providing secure storage, efficient communication, reduced computational costs, and reliable hosting services. However, the security of patient data and its digital twin counterpart stored on the blockchain remains a potential vulnerability, as any alteration or unauthorized access to this information could pose significant risks. To address this challenge, we propose a blockchain-enabled quantum encryption protocol for CCDT healthcare networks to ensure secure communication. The proposed protocol leverages blockchain to authenticate patients without relying on third-party entities. At the same time, a secure quantum encryption mechanism ensures that CCDT do not need to authenticate repeatedly when interacting with multiple healthcare providers. A performance evaluation demonstrates the effectiveness of the proposed scheme compared to existing encryption methods. The results indicate that the suggested protocol is resilient against various security threats, showcasing its significant potential for enhancing communication security within CCDT healthcare networks.**

***Index Terms*—Consumer-Centric Digital twin (CCDT), Quantum Computing, Blockchain, Quantum-Sim, Quantum encryption.**

I. Introduction

One of the most important buzzwords in today's world is the CCDT, a transformative technology that has revolutionized numerous industries. In manufacturing, it is used for the design and testing of products. In aerospace and aviation, it helps to optimize fleet management and design. It has also brought about advances in renewable energy optimization, autonomous vehicle development, smart cities, retail businesses, entertainment, and gaming. However, one of its most significant applications is in healthcare care, primarily used to construct patient-specific models. A CCDT is a virtual representation of a physical object, process, or system continuously updated with data from its real-world counterpart. This enables the creation of dynamic, real-time simulations and optimizations of the physical entity [1]–[3]. A CCDT typically consists of three core components: a data interface or cloud service platform, which bridges the physical and virtual worlds for real-time data updates; the virtual model, which serves as the digital counterpart of the entity; and the physical entity, the real-world object. An illustration of this model specifically focused on healthcare services can be seen in Fig. 1.

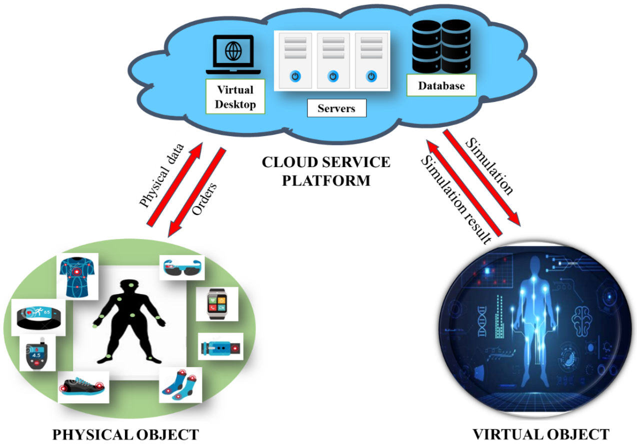


Fig. 1. The structure for CCDT healthcare services.

In this work, the focus is on the healthcare application of the CCDT. As depicted in Fig. 1, the physical object includes individuals and medical devices embedded with sensors. These sensors, linked to the patient's physical environment, form the physical entity. A virtual object serves as a digital clone, representing a virtual counterpart of the physical entity. The cloud service platform is pivotal in establishing the twinning environment and performing simulations on the virtual object. This model enables the collection of valuable patient information from the physical entity, such as physiological data (vital signs such as heart rate, blood pressure, and body temperature), biochemical data (hormonal profiles, reproductive history, and personal information such as sexual orientation), and lifestyle or behavioral data (activity levels, dietary habits, and sleep

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. RS-2024-00340882).

Sunil Prajapat is with the Department of Computer Engineering-AI & Big Data, Marwadi University, 360003 India. (e-mail: sunilprajapat645@gmail.com).

Seong Oun Hwang is with the Department of Computer Engineering, Gachon University Republic of Korea (e-mail: sohwang@gachon.ac.kr).

Pankaj Kumar is with the Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, India (e-mail: pkumar240183@gmail.com).

Mohammad Shabaz is with the Marwadi University Research Center, Department of Computer Engineering, Faculty of Engineering and Technology, Marwadi University, Rajkot, Gujarat, 360003, India (e-mail: bhatsab4@gmail.com).

Corresponding authors: Seong Oun Hwang, Pankaj Kumar

patterns) [4]–[6]. Moreover, the virtual object provides insights such as simulated physiological responses, drug interaction alerts, health status visualizations, comorbidity analysis, and precision medicine recommendations. Both data types are continuously transmitted to the cloud service platform, ensuring seamless integration and real-time updates for effective healthcare management.

Compared to other domains such as manufacturing or smart cities, the healthcare sector presents uniquely stringent security requirements. Patient data includes highly sensitive physiological, behavioral, and biochemical information, which is subject to strict privacy regulations. Unlike industrial systems, healthcare CCDTs must support real-time access across multiple providers while ensuring data integrity, confidentiality, and traceability. Moreover, the ethical implications of data misuse-ranging from misdiagnosis to discrimination-make healthcare a high-risk domain for CCDT deployment. These factors necessitate robust, decentralized, and quantum-resilient security mechanisms tailored specifically to healthcare environments.

Since this concept is relatively new, its application in healthcare has increased substantially. Over the past few years, increasing research in this area has led to a rise in the number of physical items integrated into CCDT systems. As a result, there has been a significant increase in data generation, which could potentially negatively impact network performance. This issue can be addressed by a platform that is capable of storing large amounts of data, has scalability, and can do direct management of network hardware [7]–[10]. The cloud service platform is a widely recognized platform that not only possesses these capabilities but also provides robust security measures. Although possessing the benefits of a secure platform, there are still possibilities that the security of the platform can be compromised due to hardware or software faults and human error [11]–[13]. Additionally, cloud service providers can resort to malicious behavior, such as altering or mishandling data, to uphold their reputation. This can lead to a breach in the data integrity of users. Consequently, these security breaches can lead to serious repercussions, particularly in the healthcare domain that deals with sensitive human information. To make sure that people can trust and rely on these systems, it is important to provide secure ways to check the integrity of data between the real and virtual worlds.

The construction of robust algorithms can be a potential solution for mitigating these security concerns. But due to increased research in the current digital era, even the strongest conventional cryptographic algorithms and protocols are facing major challenges. These protocols are complex due to their reliance on advanced mathematical principles, making them difficult to breach. However, today these protocols can be easily breached using quantum computing [14], which uses principles of quantum physics. Moreover, researchers have extensively explored conventional cryptography, highlighting the need for more secure protocols that can withstand the capabilities of quantum computing. So, to counter this, quantum cryptography has proven to be a promising solution. Quantum computing offers unparalleled security, as the protocols intrinsically withstand the computational power of quantum computers. Quantum Key Distribution (QKD) is one of the most widely used methods in this context. CCDT networks face more than just security issues; their dependence on centralized authorities also poses a significant challenge. Many security breaches, including Sybil attacks and impersonation attacks, could potentially undermine the interoperability of virtual environments. So, another concept known as blockchain can be very useful. Blockchain technology is a foundational element of Web 3.0 and is used to facilitate secure digital transactions and promote interoperability across diverse virtual ecosystems. Hence, in the CCDT environment, integrating blockchain with quantum cryptography can address most of the aforementioned security and interoperability challenges. Additionally, this integration offers significantly enhanced communication speeds within CCDT networks. The decentralized nature of blockchain also reduces latency and improves data verification processes. Combined, these advantages create a robust CCDT healthcare network, providing users with an immersive experience free from concerns about data integrity and security breaches.

A. Motivation and Contributions

In the past few years, many encryption schemes [15]–[20] were proposed to secure data transmission in the CCDT network. These works primarily focus on the secure encryption of patient personal medical information during its transmission to healthcare professionals. However, the primary goal of the protocol we developed is to identify the most effective methods for transmitting sensitive patient information to physicians in a highly secure manner. The main contributions of this paper are:

- Firstly, we propose a blockchain-enabled quantum encryption scheme is presented for healthcare CCDT networks to validate the integrity of digital twin data. The protocol utilizes a consortium blockchain to enhance data integrity and security within the proposed network. Users can safely store medical data within the blockchain architecture, ensuring the integrity and confidentiality of patients' sensitive biological information and physicians' medical prescriptions from potential threats.
- Secondly, we demonstrate that the proposed protocols satisfy existential unforgeability based on quantum principles. Furthermore, informal analysis and experimental simulations show that our approach is both viable and efficient.
- Finally, we utilize the Quantum Sim (Qsim), AES256, SARGO, and KMB09 libraries and protocols for our programming tasks. A comprehensive evaluation of the proposed protocol's operational capabilities and security attributes is provided in comparison to existing protocols. The results indicate the superiority of the proposed work, characterized by minimal computational and communication overheads, and the experimental outcomes confirm the high suitability of the protocol.

B. Related Works

The concept of simulation using virtual clones was first introduced by Grieves and Vickers in 2002 [21], later formalized as a digital twin by NASA in 2010. Glaessgen et al. [22] defined the digital twin as an “integrated, multiscale, multiphysics, probabilistic simulation of an as-built system" designed to replicate the lifecycle of its real-world counterpart using advanced physical models and sensor updates. Alam and Saddik [23] extended this concept by proposing a reference architecture for CCDT within a cloud-based cyber-physical system, enabling simulations using real-time data from physical assets and relaying results back to the system.

Recent studies have focused on expanding the application of digital twin technology. Liu et al. [24] proposed a framework that integrates digital twins with cloud-based healthcare services, emphasizing care for elderly patients. Wang et al. [25] introduced a sustainable management architecture that combines digital twins with blockchain technology for Internet of Things (IoT) environments, facilitating secure data sharing and decentralized operations. Similarly, Huang et al. [26] utilized blockchain to maintain immutable records of item-specific digital twins. To enhance communication efficiency, Son et al. [27] developed a blockchain-enabled framework for the secure exchange and verification of digital twin data.

In parallel, quantum cryptography has emerged as a promising solution to address security challenges in modern digital ecosystems. The foundational BB84 protocol, introduced by Bennett et al. in 1984, revolutionized QKD by leveraging quantum phenomena to establish secure cryptographic keys between sender and receiver, effectively thwarting eavesdropping attempts [28]. The protocol’s strength lies in the principles of quantum mechanics, where any attempt at non-invasive measurement of quantum states introduces detectable disturbances. Despite advancements in QKD implementations [29], the simplicity and robustness of the BB84 protocol make it a cornerstone of quantum cryptography.

Several studies have extended QKD’s applicability to authentication systems in diverse contexts [30]–[32]. In addition, simulation environments for BB84 have been explored to validate performance metrics and improve protocol efficiency [33], [34]. However, existing research often overlooks the dual requirements of secure re-authentication mechanisms and access revocation in scenarios like healthcare, where digital twins play a critical role. This study addresses this gap by introducing a quantum encryption scheme that integrates blockchain technology within a digital twin network. The proposed framework enables secure patient re-authentication without requiring redundant validation steps, streamlining healthcare operations. Restricted data is securely stored on the blockchain and accessible only to authorized users, ensuring data integrity and mitigating unauthorized access. Moreover, the decentralized nature of blockchain ensures that any tampering with a single block impacts the entire chain, safeguarding the system from breaches. When patients transition to a new physician, their data is retrieved directly from the blockchain, eliminating the need for repeated authentication, thus enhancing efficiency and reducing computational overhead.

C. Structure of the Article

The remainder of this paper is structured as follows: Section II provides the foundational concepts of quantum theory, including superposition, measurement, the no-cloning theorem, quantum entanglement, and the inter-conversion rule (ICR), along with an overview of blockchain networks. Section III introduces the system model and outlines the framework of the proposed approach. Section IV elaborates on the proposed quantum encryption scheme, detailing its key generation, encryption, decryption mechanisms, and integration with blockchain technology. Section V conducts a security analysis, presenting both informal assessments and formal verification using the Scyther tool. Section VI evaluates the performance of the proposed scheme, analyzing computational and communication costs, along with security features. Finally, Section VIII concludes the paper and highlights potential directions for future research.

II. Preliminaries

The subsequent sections delineate the foundational concepts to be employed in the envisaged scheme.

A. Superposition

In quantum mechanics, superposition allows a quantum state or system to exist in multiple states simultaneously. A d-dimensional quantum system can be mathematically represented as:

$$|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle + \cdots + a_{n-1} |n-1\rangle \tag{1}$$

where $a_0, a_1, \ldots, a_{n-1}$ are complex numbers.

B. Measurement

Another essential concept in quantum mechanics involves a set of operators in a Hilbert space, denoted as $\mathcal{S}_m$, where m represents a potential measurement outcome, is measurement. The operators involved should satisfy the completeness relation as follows:

$$\sum_{m=0} \mathcal{S}_m^* \mathcal{S}_m = I \tag{2}$$

where I is the identity operator.

C. No-Cloning Theorem

The no-cloning theorem, first formulated by Wootters and Zurek in 1982, stands as a pivotal principle in quantum mechanics. This theorem posits the impossibility of replicating an exact copy of an arbitrary unknown quantum state. This characteristic holds profound significance for the security of quantum communication, notably in QKD protocols, as it prohibits the replication of qubits.

D. Quantum Entanglement

The phenomenon of quantum entanglement was first described by Einstein, who observed that two particles, regardless of their distance apart, become correlated in such a way that the state of one particle directly affects the state of another. In the quantum realm, this property enables the transfer of information between entangled particles, thereby facilitating communication in quantum networks.

E. Inter-Conversion Rule (ICR)

The conversion between binary bits and qubits in our proposed protocol is controlled by the following rule [35]:

$$\begin{aligned} |\rightarrow\rangle &\Longleftrightarrow 0 \\ |\uparrow\rangle &\Longleftrightarrow 1 \\ |\nearrow\rangle &\Longleftrightarrow 0 \\ |\nwarrow\rangle &\Longleftrightarrow 1. \end{aligned}$$

Using this ICR, the sender can decide which "polarized photon (linear or circular)" represents the binary values '0' or '1'. Figure 2 representation the photon polarization for proposed protocol.

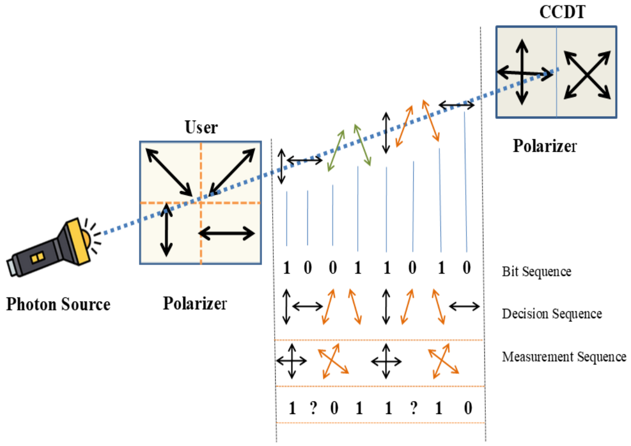


Fig. 2. The representation of photon polarization for proposed protocol.

F. Blockchain Network

Blockchain is a continuously growing list of data records, called blocks, which are linked and secured using cryptographic hashes. This technology functions as a decentralized, distributed ledger within a peer-to-peer network. Each block in the blockchain comprises two main components: the header and the body. The header contains crucial metadata, such as the block number, cryptographic hashes of the current and preceding blocks, a timestamp, and a nonce, among other elements. The body of the block holds the actual data transactions. The interconnectedness of blocks is ensured by including the hash of the previous block in the header of each new block, making the blockchain immutable and tamper-resistant. Any alteration in a block's data would necessitate changing the hash values of all subsequent blocks, thereby ensuring transparency and security. Transactions are only recorded on the blockchain after successful verification. Once validated through a consensus mechanism, new blocks are added to the chain. Blockchains can be categorized into three types: public, private, and consortium blockchains. The architecture of our proposed protocol is illustrated in Figure 3.

III. System Models

We define a quantum-secure communication framework involving three primary entities: Users $(\mathcal{U})$, their associated Consumer-Centric Digital Twins $(\mathcal{DT})$, and a decentralized Blockchain ledger $(\mathcal{B})$. The interaction between these entities is shown in Figure 4. The system operates over discrete time steps $t \in \mathbb{N}$ and supports secure quantum communication and verifiable storage.

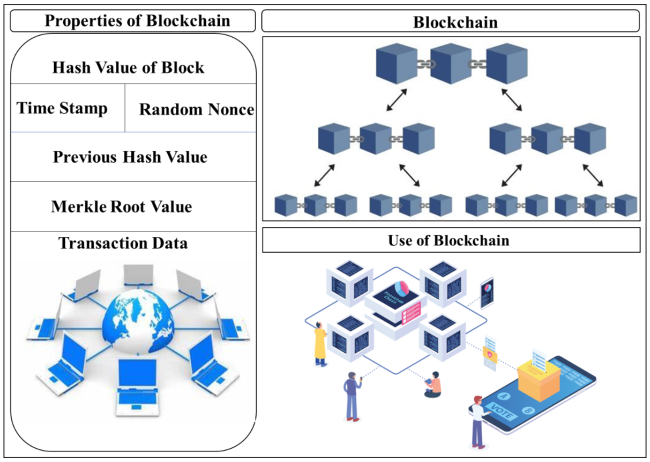


Fig. 3. Blockchain architecture.

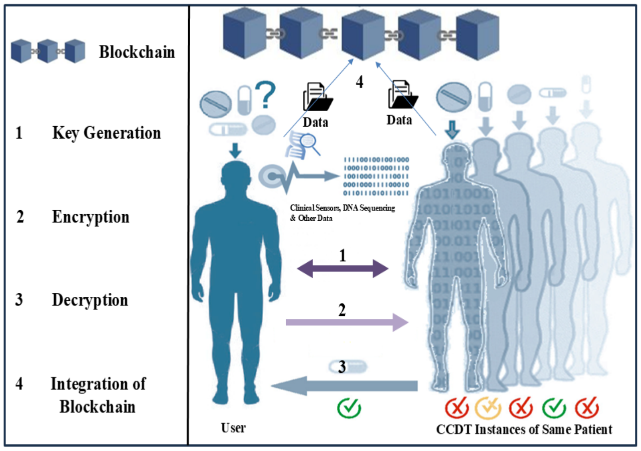

Blockchain
1 Key Generation
2 Encryption
3 Decryption
4 Integration of Blockchain
Data
4
Data
Clinical Sensors, DNA Sequencing & Other Data
1
2
3
User
CCDT Instances of Same Patient

Fig. 4. System model.

A. Entity Definitions

- User $(\mathcal{U}_i)$: Each user $i \in \mathbb{Z}^+$ is a physical participant who generates and owns sensitive quantum data $|\psi_i\rangle \in \mathbb{C}^2$, to be securely transmitted and verified. The user is responsible for key generation and partial decryption in the protocol.
- Digital Twin $(\mathcal{DT}_i)$: A virtual representation of $\mathcal{U}_i$, associated 1:1. It acts as a remote agent that applies transformations, encrypts data, and facilitates return of the original quantum state. The digital twin performs quantum operations $\mathcal{R}_A$ and inverse transformations as needed.
- Blockchain $(\mathcal{B})$: A decentralized, append-only ledger that stores quantum metadata (r_i, a_i, b_i, t_i), verification logs, and audit trails. The blockchain maintains integrity using a PBFT-based consensus algorithm and smart contracts.

B. System Communication and Interactions

Let $\mathcal{K}_{\mathcal{U}} = (\mathcal{P}_S, e_S)$ denote the public-private key pair of the user $\mathcal{U}$. The communication sequence can be defined via a series of labeled transitions:

$\mathcal{U} \xrightarrow{\text{KeyGen}} (\mathcal{P}_S, e_S)$ (User generates key set)

$\mathcal{U} \xrightarrow{|\psi\rangle} \mathcal{DT}$ (Quantum state transmitted)

$\mathcal{DT} \xrightarrow{r_A} \left|\psi^1\right\rangle = r_A \left|\psi\right\rangle$ (Encryption with unitary set)

$\mathcal{DT} \xrightarrow{\left|\psi^1\right\rangle} \mathcal{U}$ (Send encrypted state)

$\mathcal{U} \xrightarrow{r_T} \left|\psi^2\right\rangle = r_T \left|\psi^1\right\rangle$

$\mathcal{U} \xrightarrow{\left|\psi^2\right\rangle} \mathcal{DT}$

$\mathcal{DT} \xrightarrow{r_A^*} \left|\psi^3\right\rangle = r_A^* r_T \left|\psi^1\right\rangle$

$\mathcal{DT} \xrightarrow{\left|\psi^3\right\rangle} \mathcal{U}$

$\mathcal{U} \xrightarrow{r_T^*} \left|\psi\right\rangle = r_T^* \left|\psi^3\right\rangle$ (Original state retrieved)

All interactions are logged and verified via $\mathcal{B}$

C. Operational Responsibilities

The proposed system comprises three core entities: the User ($\mathcal{U}$), the Digital Twin ($\mathcal{DT}$), and the Blockchain ($\mathcal{B}$). Each entity has distinct operational responsibilities, as detailed below:

1) **User ($\mathcal{U}$)**
   - Initiates the protocol by generating a quantum key pair: a public key $\mathcal{P}_S$ and a private key e_S using a set of unitary transformations.
   - Sends the quantum state $|\psi\rangle$ to the CCDT for processing.
   - Performs decryption operations using transformation r_T and retrieves the original state through r_T^*.
   - Participates in data verification and audits using the blockchain to ensure data integrity and authenticity.
2) **CCDT ($\mathcal{DT}$)**
   - Acts as a virtual proxy of the physical user, simulating, storing, and operating on quantum states.
   - Encrypts the received quantum state using a randomly composed unitary operation r_A derived from the public key set.
   - Applies inverse transformations and returns processed qubits during decryption.
   - Logs all state interactions and cryptographic operations on the blockchain for traceability and accountability.
3) **Blockchain ($\mathcal{B}$)**
   - Functions as a secure, decentralized ledger that records metadata and quantum transaction trails.
   - Verifies user identities and digital signatures through smart contracts.
   - Facilitates consensus and finalizes block addition using Practical Byzantine Fault Tolerance (PBFT).
   - Maintains the integrity and immutability of the communication process by storing $\left|\psi^1\right\rangle$, key metadata, and operational records.

IV. Proposed Scheme

The protocol comprises three phases: A) Key Generation, B) Encryption, and C) Decryption.

A. Key Generation

The suggested protocol aims to guarantee the secure transmission of a qubit from User to DT. Consequently,we want to prevent a prospective Eve attacker from obtaining the qubit. Identify the qubit in state (3) as the qubit designated for transmission

$$\psi = a\,|0\rangle + b\,|1\rangle \tag{3}$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

Encrypting the qubit in state (3) signifies an action that prevents an adversary from ascertaining the probability amplitudes a and b, regardless of the quantity of measurements conducted. The suggested protocol employs a collection of $m + 1$ unitary transformations, $r = \{r_0, r_1, ..., r_m\}$. All transformations in the r set adhere to the standard structure of a quantum gate for a single qubit system, namely the one outlined in (4).

$$r_j = \begin{bmatrix} a & b \\ -e^{j\phi}b^* & e^{j\phi}a^* \end{bmatrix}, 0 \le j \le m \tag{4}$$

Where $a, b \in \mathbb{C}$ and $\phi \in \mathbb{R}$ $|a|^2 + |b|^2 = 1$.

Assume that for the security analysis of the scheme, the numbers a, b and ϕ can be expressed using t bits. Key generation occurs as follows:

1) $\mathcal{U}$ generates random numbers a, b and t , then builds the matrix (4):

$$r_0 = \begin{bmatrix} a & b \\ -e^{j\phi}b^* & e^{j\phi}a^* \end{bmatrix}$$

2) $\mathcal{U}$ produces m random numbers, each expressed using t bits. We observe these values as $\mathcal{P}_1$, $\mathcal{P}_2$,...,$\mathcal{P}_m$.
3) $\mathcal{U}$ computes the transformations $r_j = r_0^{\mathcal{P}_j}$, for $1 \le j \le m$.
4) $\mathcal{U}$'s public key, represented as $\mathcal{P}_S$, comprises the set of transformations $\{r_0, r_1, ..., r_m\}$, whereas her private key, designated as e_S, corresponds to the transformation r_0.

B. Encryption

Encryption is performed in the following manner:

1) $\mathcal{DT}$ randomly generates a set of a integers within the range of 1 to m. We define this set as $A = a_1, a_2, ..., a_m$, where $1 \le a_j \le m$.
2) We represent the composition of the transformations $r_{a_1}, r_{a_2}, ..., r_{a_m}$, as r_A. In other terms, $r_A = \prod_{j=1}^{m} r_{a_j}$. $\mathcal{DT}$ applies the transformation r_A to a qubit in state (3). The qubit's new state is now $\left|\psi^1\right\rangle = r_A\,|\psi\rangle$. $\mathcal{DT}$ transmits the qubit in the state $\left|\psi^1\right\rangle$ to $\mathcal{U}$ via an insecure channel.

C. Decryption

Following are $\mathcal{U}$'s steps for decryption:

1) We denote by r_T the composition of the transformations from the set r. In other terms, $T = \prod_{j=0}^{m} r_j$. $\mathcal{U}$ applies the transformation r_T to a qubit in the state $\left|\psi^1\right\rangle$. The qubit state is now $\left|\psi^2\right\rangle = r_T \left|\psi^1\right\rangle$. $\mathcal{U}$ transmits to $\mathcal{DT}$ the qubit in the state $\left|\psi^2\right\rangle$.
2) $\mathcal{DT}$ computes the inverse of r_A based on the set A. We designate the conjugate transpose of r as r^*. Therefore, $r_A = \prod_{j=1}^{m} r^*_{a_j}$. $\mathcal{DT}$ applies the transformation r^*_A to the qubit in the state $\left|\psi^2\right\rangle$, resulting in the new state $\left|\psi^3\right\rangle = r^*_A \left|\psi^2\right\rangle = r^*_A r_T \left|\psi^1\right\rangle = r^*_A r_T r_A \left|\psi\right\rangle = I r_T \left|\psi\right\rangle = r_T \left|\psi\right\rangle$. $\mathcal{DT}$ transmits the qubit in the state $\left|\psi^3\right\rangle$ to $\mathcal{U}$.
3) $\mathcal{U}$ applies the transformation r^*_T to the qubit she got from $\mathcal{DT}$, which is in the state $\left|\psi^3\right\rangle$. Consequently, the new state of the qubit is $r^*_T \left|\psi^3\right\rangle = r^*_T r_T \left|\psi\right\rangle = I \left|\psi\right\rangle = \left|\psi\right\rangle$. $\mathcal{U}$ retrieves the original qubit from $\mathcal{DT}$.

D. Integration of Blockchain

This section describes the process of block formation, validation through smart contracts, and consensus establishment via a voting mechanism.

- *Block Formation:* Any user node within the blockchain network can initiate a transaction, which is authenticated using the user's private key. Nodes with mining capabilities are responsible for collecting these transactions and generating a new block. A miner node organizes the received transactions and uses a random oracle to structure them into a fresh block. Each transaction includes essential details, such as the sender's identity and encryption key e_S, represented as $\left|\psi^1\right\rangle$. The resulting block is expressed as $Block_j = r, a, b, t, r_A$. Once the block is formed, it is disseminated across the blockchain network for further processing.
- *Block Verification:* After a miner node has effectively generated a block, it is broadcast to the decentralized network for validation. Before verifying the accuracy of $\left|\psi^1\right\rangle$, the network nodes initially authenticate the sender's identity. Upon successful verification, the block advances to the consensus step for incorporation into the blockchain.
- *Block Addition:* In order to obtain consensus regarding block inclusion, the blockchain network that has been proposed implements a voting-based consensus mechanism. The system employs the "Practical Byzantine Fault Tolerance (PBFT)" protocol, a well-established consensus algorithm noted for its strong fault tolerance capabilities. This protocol maintains the integrity of block addition through a systematic voting process that engages network participants. The steps involved in the consensus process are detailed in Algorithm 1, encompassing the validation of smart contracts and the finalization of block acceptance.

Algorithm 1 Consensus Mechanism in Blockchain

```
Input: Suppose a leader $Leader_{CS_m}$ picks a block, $Block_j = \{r, a, b, t, r_A\}$ where $j = 1, 2, 3..., n_t\}$
Output: Status of block commitment (YES/NO)
Set a $Target\ Number = 2*(M-1)/3+1$
$N_i \leftarrow$ (empty)
Distribute $Block_j$ to replica nodes in cloud servers network
for every replica node $RN_j$ do
    Set $Vote_{Consensus_j} = NO$
    Calculate $Block_{Hash} = Hash(Block_j)$
    if ($Block_{Hash} = Curr_{Block_h}$) then
        if ($|\psi^1\rangle$) then
            Calculate Merkle tree root ($MTR'_{Tx_i}$) utilizing the $n_i$ transactions contained within the block payload
            if ($MTR'_{Tx_i} = MTR_{Tx_i}$) then
                Set $Vote_{Consensus_j} = YES$
            end if
        end if
    end if
    Add $Vote_{Consensus_j}$ to $N_i$
end for
Set $Vote_{Count} \leftarrow 0$
for each vote ($Vote_{Consensus_j}$) reply to $N_i$ do
    if ($Vote_{Consensus_j}$ is YES) then
        $Vote_{Count} = Vote_{Count} + 1$
    end if
end for
if ($Vote_{Count} \geq Target\ Number$) then
    Add $Block_j$ into the blockchain
    Share the status of block commitment as "YES" with the entire blockchain network
end if
```

E. Correctness

The correctness of the proposed quantum encryption and decryption protocol lies in the ability of the receiver to reconstruct the original quantum state $|\psi\rangle$ after performing a sequence of defined unitary operations and their inverses. We begin by assuming that the user $\mathcal{U}$ intends to securely transmit a single-qubit state to its CCDT $\mathcal{DT}$. Let the original quantum state be:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad \text{where } a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

The encryption and decryption steps are composed of a series of unitary transformations as follows:

- **Encryption by $\mathcal{DT}$:** A set of indices $A = \{a_1, a_2, \ldots, a_m\}$ is selected randomly. Based on the public key $\mathcal{P}_S = \{r_0, r_1, \ldots, r_m\}$, the CCDT computes the composite transformation $r_A = \prod_{j=1}^{m} r_{a_j}$ and applies it to the state $|\psi\rangle$:
$$\left|\psi^1\right\rangle = r_A\,|\psi\rangle\,.$$
- **Transformation by $\mathcal{U}$:** The user computes $r_T = \prod_{j=0}^{m} r_j$ using her private and public keys, and applies it to the encrypted state:
$$\left|\psi^2\right\rangle = r_T\left|\psi^1\right\rangle = r_T r_A\,|\psi\rangle\,.$$
- **Decryption by $\mathcal{DT}$:** The CCDT computes the Hermitian conjugate (inverse) of r_A, denoted r^*_A, and applies it:
$$\left|\psi^3\right\rangle = r^*_A\left|\psi^2\right\rangle = r^*_A r_T r_A\,|\psi\rangle\,.$$

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2025.3634583

- **Final recovery by $\mathcal{U}$:** The user applies the Hermitian conjugate of r_T, denoted r_T^*:
$$|\psi'\rangle = r_T^* \left|\psi^3\right\rangle = r_T^* r_A^* r_T r_A \left|\psi\right\rangle .$$

To retrieve the original state $|\psi\rangle$, the following condition must be satisfied:
$$r_T^* r_A^* r_T r_A = I,$$
where I is the identity matrix. Since each r_j is defined as a unitary transformation (i.e., $r_j^* = r_j^{-1}$), both r_T and r_A are products of unitary matrices and thus also unitary. As a result, their respective inverses exist and:
$$(r_T r_A)^* = r_A^* r_T^* \quad \text{and} \quad (r_T r_A)^*(r_T r_A) = I.$$
Therefore, we obtain:
$$|\psi'\rangle = r_T^* r_A^* r_T r_A \left|\psi\right\rangle = I \left|\psi\right\rangle = \left|\psi\right\rangle .$$

V. Security Analysis

In this section, we present an informal and formal security analysis of our scheme to validate its secure and robust nature against a variety of attacks.

A. Informal Security Analysis

This section discusses the informal security analysis of the proposed protocol. The protocol is secure against various attacks, which are discussed below:

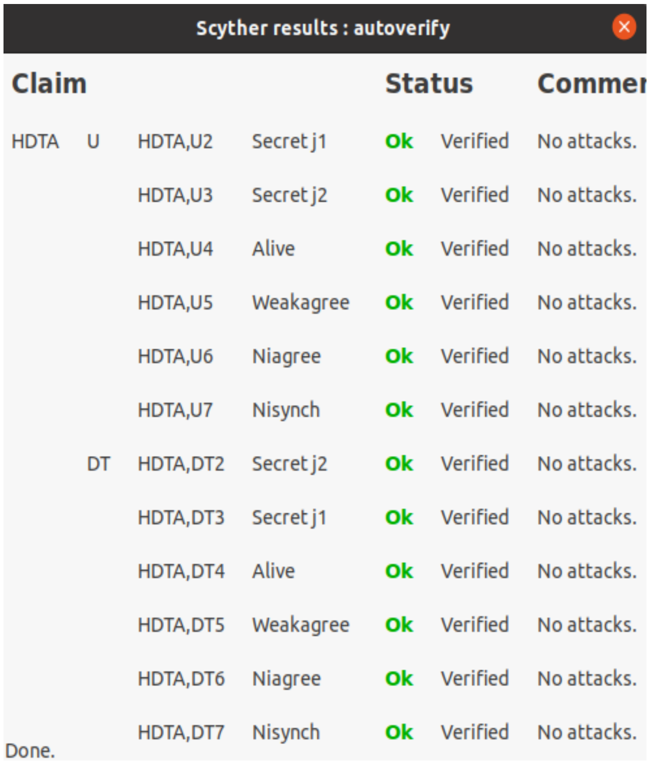
- **Eavesdropping Attack:** This attack takes place when an adversary attempts to gain unauthorized access to sensitive data by intercepting the communication between devices. In this protocol, the QKD ensures that any attempt to measure or intercept quantum states introduces detectable errors. As a result, whenever an eavesdropper attempts to intercept the communication, the variations in quantum state statistics facilitate the detection of such eavesdropping efforts. Consequently, this renders the protocol impervious to eavesdropping attacks.
- **Side-Channel Attack:** Side-channel assaults compromise a system by exploiting indirect information, such as power consumption, electromagnetic emissions, or timing variations. Secure hardware components, including devices with differential power analysis (DPA) countermeasures and physically unclonable functions (PUFs), are incorporated into the proposed scheme to protect against such vulnerabilities. To guarantee that potential data leakage points are identified and addressed, comprehensive assessments of power, electromagnetic, and timing channels are conducted. This layered approach aids in the mitigation of risks associated with electromagnetic radiation or power consumption, thereby fortifying the protocol against side-channel exploits.
- **Replay Attack:** Replay attacks involve retransmitting previously captured messages to deceive the system. In the proposed scheme, qubits γ used during encryption and decryption processes are embedded with random numbers, ephemeral credentials, and verification requirements. Each session employs unique random numbers, ensuring the freshness of messages. Consequently, even if an adversary retransmits old messages, the protocol detects and neutralizes the threat, maintaining communication integrity.
- **Sybil Attack:** An adversary uses a Sybil attack to compromise a network by assuming several false identities. The proposed technique addresses this by utilizing quantum transformations specifically associated with each user. These transformations effectively prevent identity deception and fraudulent entities from infiltrating or dominating the network by insuring that public keys are verifiable and unique.
- **Quantum State Obfuscation:** The quantum message $|\psi\rangle$ is encrypted using randomly chosen unitary transformations r_A and r_T, known only to the legitimate entities. These transformations are dynamically selected and composed of Clifford gates, which resist efficient reverse engineering even under quantum adversaries.
- **Key Confidentiality via Blockchain Anchoring:** Although the public key set $\mathcal{P}_S$ is recorded on the blockchain $\mathcal{B}$, the private indices A and the full composition of r_T are not. This separation of public and private randomness thwarts quantum attackers from reconstructing the encryption operators necessary for reverse-engineering the state.
- **No Reusability of Quantum States:** Quantum no-cloning theorem inherently prevents adversaries from duplicating $|\psi\rangle$ during transmission. Even in the event of interception, any measurement or disturbance to the state will collapse it, which can be detected via quantum error checking (e.g., fidelity checks or trace distance monitoring).
- **Logged Interactions via Blockchain $\mathcal{B}$:** All classical exchanges and index references used to determine r_A and r_T are logged on the blockchain in hashed or encoded forms, which adds transparency without leaking quantum state or transformation information.

B. Formal Security Verification using Scyther Tool

Formal security analysis can be conducted using a variety of tools, such as “Scyther,” “ProVerif,” “CryptoVerif,” “AVISPA,” and “TAMARIN.” This study utilizes the Scyther tool to assess the security attributes of the proposed protocol. Scyther is explicitly engineered to evaluate and validate the security claims of protocols by assessing their adherence to established security features. The Scyther tool necessitates the protocol to be articulated in the “Security Protocol Description Language (SPDL)” as input. This language facilitates the specification of roles, message flows, and security attributes for the protocol. Scyther produces security assertions for each role and verifies their accuracy. Should any assertion fail, the tool offers a visual depiction of the attack scenario, facilitating the identification and remediation of vulnerabilities. The proposed protocol was executed via SPDL in our analysis. The Scyther tool validated the security attributes of the scheme, and the findings corroborated its resilience, with all security assertions successfully passing. The tool’s automated verification designated

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2025.3634583

the outcome as "ok," signifying that the protocol meets its targeted security assurances. Figure 5 illustrates the output of the Scyther tool using the proposed methodology.



Claim				Status		Commen
HDTA	U	HDTA,U2	Secret j1	Ok	Verified	No attacks.
		HDTA,U3	Secret j2	Ok	Verified	No attacks.
		HDTA,U4	Alive	Ok	Verified	No attacks.
		HDTA,U5	Weakagree	Ok	Verified	No attacks.
		HDTA,U6	Niagree	Ok	Verified	No attacks.
		HDTA,U7	Nisynch	Ok	Verified	No attacks.
	DT	HDTA,DT2	Secret j2	Ok	Verified	No attacks.
		HDTA,DT3	Secret j1	Ok	Verified	No attacks.
		HDTA,DT4	Alive	Ok	Verified	No attacks.
		HDTA,DT5	Weakagree	Ok	Verified	No attacks.
		HDTA,DT6	Niagree	Ok	Verified	No attacks.
		HDTA,DT7	Nisynch	Ok	Verified	No attacks.

Done.

Fig. 5. The Scyther tool result.

VI. Performance Analysis

This section provides a comprehensive evaluation of the protocol's performance. The quantum communication protocol BB84, its modified version "SARGO KMB0", and the cryptosystems "AES256" and one-time pad are fundamentally compatible with Quantum-Sim (QSim). Additionally, QSim enables designers to develop new DTHA protocols. This simulation tool is utilized to capture the behavior of $\mathcal{DT}$ and the attacks perpetrated by adversaries against it. It comprises quantum communication layered simulators, an established user-simulator known as "MOSAIK", and two new simulators: $\mathcal{DT}$-sim and Attacker-sim. Through "MOSAIK", users can monitor occurrences in real time via the configurable web-based interface offered by QSim. An OMNET++ simulator is employed to integrate conventional communication layers in DTHA through power flow-based methodologies. The interface was modified, and a benchmark configuration was implemented, employing a radial low-voltage DTHA to connect 40 hospitals in a local area for testing the planned work. The proposed protocol implements an encrypted communication channel to authenticate DTHA entities using BB84 QKD. We evaluated the efficacy of the proposed work by simulating it with QSim on a "Windows 11 PC featuring an Intel Core i7 CPU operating at 3.20 GHz and 16 GB of RAM". The efficiency of communication is assessed by measuring the rate of qubit exchange and validation per second, under the assumption of a zero probability of attack. The present study achieves an average communication efficiency of 49%. Utilizing the BB84 protocol, which theoretically exhibits a communication efficiency of 51%, our proposed methodology presents encouraging outcomes. Significantly, when the number of exchanged qubits exceeds 41, our results demonstrate considerable stabilization in the validated qubits. Moreover, our assessment of the Man-in-the-Middle (MITM) attack frequency, with an assault probability of 40%, indicates a noticeable link. A direct correlation exists between the rise in the MITM detection rate and the augmentation of qubits exchanged per second. Additionally, the specific elements of the proposed effort concerning computational expense and communication are detailed below:

A. Computational cost

We consider the time required to execute various cryptographic operations in order to assess the computational cost of the proposed protocol. The operations encompass ECC point multiplication (T_m), one-way hash (T_H), MAC (T_{mac}), HMAC (T_{Hmac}), biometric hash function (T_b), decryption function (T_d), and encryption function (T_e). The corresponding durations for these operations are 7.529 ms, 0.0003 ms, 8.1 ms, 8.1 ms, 0.01 ms, 0.1303 ms, and 0.1303 ms [16]. The proposed method entails the calculation of T_{Hmac} during the login and authentication procedures. A decryption operation is performed to verify the authenticity of the received user, incurring a computational cost of T_d. During the user data authentication and verification step, the computational cost is equivalent to the execution time of T_{Hmac}. Consequently, the total computing cost of the proposed method is $2T_{Hmac} + T_d + T_e$. The computational cost of the existing approach is compared to alternative schemes in Table I. Consequently, our methodology yields reduced computing expenses, as illustrated in Figure 6.

TABLE I
Computational Costs

S. No.	Protocol	Computational cost (in ms)
1	Pakniat *et al.* [15]	88.947
2	Xu *et al.* [16]	114.7665
3	Yang *et al.* [17]	83.6909
4	Liu *et al.* [18]	38.4008
5	Fan *et al* [19]	75.2653
6	Tu *et al.* [20]	59.9517
7	Our	27.8046

B. Communication cost

We examine the total communication costs of the proposed protocol in comparison to other existing schemes [15]–[19], and [20]. The protocol delineates the subsequent bit sizes: 160 bits for $\mathcal{DT}$ and $\mathcal{U}$ identification, 128 bits for the random nonce, 32 bits for the timestamp, 320 bits for the ECC point, 160 bits for the hash function output, and 256 bits for symmetric encryption and decryption. Furthermore, we assess the costs linked to each protocol for the login and authentication processes. The methodology outlined in reference [15] comprises a message totaling 1152 bits. The cost of each message in the protocol outlined in [16]–[19] and

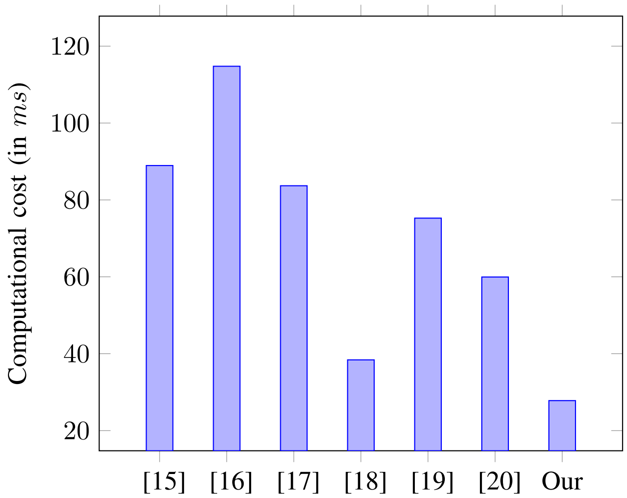


Fig. 6. Variation in computational costs. (in ms)

[20] is as follows: 1312 bits, 1452 bits, 1672 bits, 1052 bits, and 1782 bits, respectively. In the encryption and decryption phases, our scheme entails broadcasting messages that require a cumulative cost of 972 bits. Table II demonstrates that the cost of our technique is markedly inferior to that of [15]–[19], and [20]. Consequently, our methodology demonstrates enhanced efficiency, as illustrated in Figure 7.

TABLE II
COMMUNICATION COSTS

S. No.	Protocol	Communication cost (in bits)
1	Pakniat *et al.* [15]	1152
2	Xu *et al.* [16]	1312
3	Yang *et al.* [17]	1452
4	Liu *et al.* [18]	1672
5	Fan *et al.* [19]	1052
6	Tu *et al.* [20]	1782
7	Our	972

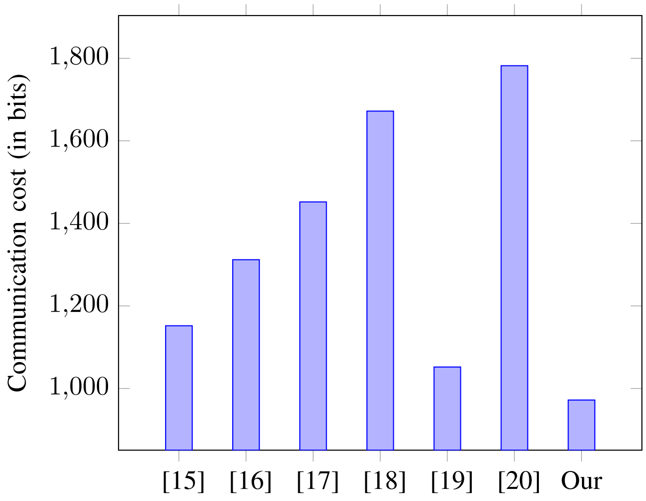


Fig. 7. Variation in communication cost (in bits)

C. Security Features

An evaluation of ten security and functionality attributes is conducted in this subsection to assess the devised protocol. In the table III, it is clear that the devised protocol is significantly more secure than other existing schemes, such as [15]–[19]] and [20].

TABLE III
SECURITY FEATURES

Features	[15]	[16]	[17]	[18]	[19]	[20]	Proposed
SF_1	×	×	×	×	×	×	✓
SF_2	✓	✓	✓	✓	✓	✓	✓
SF_3	✓	✓	✓	✓	✓	✓	✓
SF_4	✓	×	✓	✓	✓	✓	✓
SF_5	−	✓	−	−	−	−	✓
SF_6	✓	−	−	−	−	✓	✓
SF_7	✓	✓	✓	✓	✓	✓	✓
SF_8	×	×	×	×	×	×	✓
SF_9	×	×	×	✓	×	×	✓
SF_{10}	✓	✓	✓	✓	×	✓	✓

SF_1: Quantum Security, SF_2: Replay attack, SF_3: Impersonation attack, SF_4: MITM attack, SF_5: Eavesdropping attack, SF_6: Unconditional Security, SF_7: Mutual authentication, SF_8: Low computational cost, SF_9: Low communication cost, SF_{10}: Blockchain, ✓: Secure, ×: Insecure, −: Not considered.

VII. RESULT AND DISCUSSION

The outcomes of the operational competence analysis of the proposed blockchain-enabled quantum encryption scheme are outlined here. The evaluation of computational and communication costs (Figures 6 and 7) reveals that the devised protocol consistently outperforms existing schemes such as [15]–[19], and [20]. Specifically, the computational cost of our scheme is reduced to 27.80 ms, compared to values ranging from 38.40 ms to 114.76 ms in competing protocols, representing an improvement of 27%-76%. Similarly, the communication overhead of our protocol is limited to 972 bits, which is significantly lower than the 1052-1782 bits incurred by the baselines. These results indicate that the proposed scheme achieves both reduced latency and improved scalability in CCDT environments. From a security perspective (Table III), the scheme achieves a broader coverage of security features, including resilience against replay, impersonation, eavesdropping, MITM, and Sybil attacks, while also ensuring unconditional security. Notably, features such as quantum security and low communication cost, often neglected in prior works, are inherently supported by our framework. This confirms the enhanced operational robustness of the proposed protocol.

A critical observation is that while the simulation results using QSim demonstrate near-optimal communication efficiency (49% against the theoretical 51% of BB84), the assumptions of noiseless qubit transmission and perfect consensus latency may not hold in real-world healthcare environments. In practice, blockchain consensus mechanisms introduce delays, and quantum channels suffer from decoherence and error rates. Therefore, future extensions must incorporate error correction and analyze latency overheads for hospital-scale deployments. It is also important to note that the proposed mechanism is founded on classical hard problems such as the Elliptic Curve Discrete Logarithm Problem (ECDLP) and Elliptic Curve

Computational Diffie-Hellman (ECCDH). While effective in the near term, these assumptions face challenges from large-scale quantum computers. In this context, post-quantum cryptographic (PQC) approaches such as lattice-based and isogeny-based cryptography are gaining traction. Our framework can be adapted into a hybrid model, wherein PQC primitives coexist with quantum encryption to ensure long-term security. Furthermore, the scalability analysis indicates that while the scheme performs efficiently in simulations with up to 40 hospitals, large-scale CCDT networks with thousands of patients will impose additional storage and consensus overhead on the blockchain. Evaluating throughput, ledger growth, and hybrid deployment strategies with hospital IT systems is a promising avenue for real-world feasibility.

VIII. Conclusion

This paper introduces a novel encryption scheme utilizing quantum cryptography and blockchain technology, tailored for CCDT networks. The proposed framework harnesses blockchain, quantum principles, and encryption to eliminate the need for centralized authorities. By incorporating quantum entanglement and QKD alongside blockchain technology, the system ensures data integrity and security. The scheme employs entangled qubits and encryption methods to facilitate secure communication between users and their CCDT environments ($\mathcal{DT}$). Integrating blockchain enhances transparency, security, user autonomy, and interoperability within the CCDT network. The protocol effectively mitigates security challenges such as replay attacks, side-channel attacks, Sybil attacks, and eavesdropping. Furthermore, the scheme exhibits resilience against advanced security threats, including privacy breaches, man-in-the-middle attacks, entanglement measurement attacks, and anti-quantum attacks. A comprehensive performance analysis underscores the viability of the proposed approach, highlighting its competitive computational and communication overheads and superior security features compared to existing systems. The findings affirm that our method is both theoretically robust and practically implementable, potentially within a predefined teleportation framework.

In future, this work can be extended by implementing the proposed quantum-blockchain encryption framework in real-world CCDT network environments to evaluate its scalability and interoperability with existing digital twin infrastructures. Further studies may focus on optimizing quantum resource consumption, minimizing qubit decoherence, and improving fault-tolerance through quantum error correction techniques. Integration with post-quantum cryptographic algorithms can also strengthen hybrid security models, ensuring robustness against evolving cyber-quantum threats. Moreover, exploring AI-driven adaptive security mechanisms, cross-domain standardization, and deployment in large-scale industrial IoT and healthcare CCDT ecosystems will enhance practical adoption and global applicability of the proposed scheme.

References

[1] H. Yan, X. Xu, M. Bilal, X. Xia, W. Dou, and H. Wang, “Customer centric service caching for intelligent cyber–physical transportation systems with cloud–edge computing leveraging digital twins,” *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1787–1797, 2023.

[2] D. Kumari, P. Kumar, and S. Prajapat, “A blockchain assisted public auditing scheme for cloud-based digital twin healthcare services,” *Cluster Computing*, vol. 27, no. 3, pp. 2593–2609, 2024.

[3] H. Liu, T. Lu, Y. Yang, Y. Guo, Q. Wu, X. Xu, and H. Zeng, “Blockchain-based optimization of operation and trading among multiple microgrids considering market fairness,” *International Journal of Electrical Power & Energy Systems*, vol. 166, p. 110523, 2025.

[4] Y. Jiao, Z. Zhang, Z. Li, Z. Li, X. Li, and J. Liu, “A robust coverless image-synthesized video steganography based on asymmetric structure,” *Journal of Visual Communication and Image Representation*, vol. 104, p. 104303, 2024.

[5] J. Zhu, J. Jin, C. Chen, L. Wu, M. Lu, and A. Ouyang, “A new-type zeroing neural network model and its application in dynamic cryptography,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2024.

[6] G. Xu, X. Fan, S. Xu, Y. Cao, X.-B. Chen, T. Shang, and S. Yu, “Anonymity-enhanced sequential multi-signer ring signature for secure medical data sharing in iomt,” *IEEE Transactions on Information Forensics and Security*, 2025.

[7] M. Shabaz, M. Z. U. Rahman, M. Alsaadi, M. Raparthi, R. R. Maaliw, I. Keshta, M. Soni, J. C. Patni, and H. Byeon, “Leveraging consumer technology for healthcare systems using blockchain based bio-sensor devices,” *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 1521–1529, 2024.

[8] M. Zhang, E. Wei, R. Berry, and J. Huang, “Age-dependent differential privacy,” *IEEE Transactions on Information Theory*, vol. 70, no. 2, pp. 1300–1319, 2023.

[9] S. Sai, A. Rastogi, and V. Chamola, “Digital twins for consumer electronics,” *IEEE Consumer Electronics Magazine*, vol. 13, no. 6, pp. 11–16, 2023.

[10] J. Jin, M. Wu, A. Ouyang, K. Li, and C. Chen, “A novel dynamic hill cipher and its applications on medical iot,” *IEEE Internet of Things Journal*, 2025.

[11] S. P. Mohanty and F. Pescador, “Introduction consumer technologies for smart healthcare,” *IEEE Transactions on Consumer Electronics*, vol. 67, no. 1, 2021.

[12] S. Datta and S. Namasudra, “Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing,” *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4026–4036, 2024.

[13] J. Li, J. Li, C. Wang, F. J. Verbeek, T. Schultz, and H. Liu, “Outlier detection using iterative adaptive mini-minimum spanning tree generation with applications on medical data,” *Frontiers in Physiology*, vol. 14, p. 1233341, 2023.

[14] S. Prajapat, D. Gautam, P. Kumar, A. K. Das, and M. S. Hossain, “Designing lattice-based sequential aggregate signature scheme for securing consumer electronics-centric iomt,” *IEEE Transactions on Consumer Electronics*, 2025.

[15] N. Pakniat, D. Shiraly, and Z. Eslami, “Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial iot,” *Journal of Information Security and Applications*, vol. 53, p. 102525, 2020.

[16] L. Xu, J. Li, X. Chen, W. Li, S. Tang, and H.-T. Wu, “Tc-pedcks: Towards time controlled public key encryption with delegatable conjunctive keyword search for internet of things,” *Journal of Network and Computer Applications*, vol. 128, pp. 11–20, 2019.

[17] X. Yang, G. Chen, M. Wang, T. Li, and C. Wang, “Multi-keyword certificateless searchable public key authenticated encryption scheme based on blockchain,” *IEEE Access*, vol. 8, pp. 158 765–158 777, 2020.

[18] W. Liu, F. Wang, X. Jin, K. Chen, and Z. Shen, “Leveled multi-hop multi-identity fully homomorphic encryption,” *Security and Communication Networks*, vol. 2022, no. 1, p. 1023439, 2022.

[19] H. Fan, R. Huang, and F. Luo, “Efficient multi-identity full homomorphic encryption scheme on lattice,” *Applied Sciences*, vol. 13, no. 10, p. 6343, 2023.

[20] G. Tu, W. Liu, T. Zhou, X. Yang, and F. Zhang, “Concise and efficient multi-identity fully homomorphic encryption scheme,” *IEEE Access*, 2024.

[21] M. Grieves and J. Vickers, “Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems,” *Transdisciplinary perspectives on complex systems: New findings and approaches*, pp. 85–113, 2017.

[22] E. Glaessgen and D. Stargel, “The digital twin paradigm for future nasa and us air force vehicles,” in *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th*

AIAA/ASME/AHS adaptive structures conference 14th AIAA, 2012, p. 1818.

[23] K. M. Alam and A. El Saddik, “C2ps: A digital twin architecture reference model for the cloud-based cyber-physical systems,” *IEEE access*, vol. 5, pp. 2050–2062, 2017.

[24] Y. Liu, L. Zhang, Y. Yang, L. Zhou, L. Ren, F. Wang, R. Liu, Z. Pang, and M. J. Deen, “A novel cloud-based framework for the elderly healthcare services using digital twin,” *IEEE access*, vol. 7, pp. 49 088–49 101, 2019.

[25] C. Wang, Z. Cai, and Y. Li, “Sustainable blockchain-based digital twin management architecture for iot devices,” *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6535–6548, 2022.

[26] S. Huang, G. Wang, Y. Yan, and X. Fang, “Blockchain-based data management for digital twin of product,” *Journal of Manufacturing Systems*, vol. 54, pp. 361–371, 2020.

[27] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, “On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain,” *IEEE Access*, vol. 10, pp. 75 365–75 375, 2022.

[28] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[29] M. Kalra and R. C. Poonia, “Design a new protocol and compare with bb84 protocol for quantum key distribution,” in *Soft Computing for Problem Solving: SocProS 2017, Volume 2*. Springer, 2019, pp. 969–978.

[30] T. Mihara, “Quantum identification schemes with entanglements,” *Physical review A*, vol. 65, no. 5, p. 052326, 2002.

[31] L. Bi, M. Miao, and X. Di, “A dynamic-routing algorithm based on a virtual quantum key distribution network,” *Applied Sciences*, vol. 13, no. 15, p. 8690, 2023.

[32] Y.-G. Yang, B.-X. Liu, G.-B. Xu, Y.-H. Zhou, and W.-M. Shi, “Practical quantum anonymous private information retrieval based on quantum key distribution,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4034–4045, 2023.

[33] Z. Guitouni, S. Maize, M. Zrigui, and M. Machhout, “Security analysis of the bb84 protocol in iot networks,” *International Journal*, vol. 13, no. 4, 2024.

[34] M. Mehic, P. Fazio, M. Voznak, and E. Chromy, “Toward designing a quantum key distribution network simulation model,” *Advances in Electrical and Electronic Engineering*, vol. 14, no. 4, pp. 413–420, 2016.

[35] S. Prajapat, P. Kumar, and S. Kumar, “A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks,” *Cluster Computing*, pp. 1–17, 2024.