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.2025.3631827

Blockchain-Enabled Quantum Signature Scheme for Securing Consumer Electronics-Centric IoT Networks

Sunil Prajapat, *Member, IEEE*, Seong Oun Hwang, *Senior Member, IEEE*, M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*—The rapid proliferation of Consumer-Centric Internet of Things (CCIoT) devices has resulted in massive volumes of data being generated and transmitted across edge and cloud infrastructures. However, limited computational and memory resources, coupled with the vulnerabilities of open communication networks, expose CCIoT ecosystems to severe security threats. With the advent of quantum computing, traditional cryptographic schemes risk becoming obsolete, necessitating the integration of quantum cryptography into edge-assisted CCIoT protocols. In this paper, we propose a blockchain-enabled quantum-designated verifier signature protocol designed to ensure secure data transmission and storage within CCIoT networks. The protocol leverages a private blockchain, where peer nodes generate blocks from service-provider data, thereby enhancing confidentiality and integrity. Informal security verification and informal analysis confirm the robustness of the scheme against both classical and quantum adversaries. Extensive experiments, implemented in Python, evaluate the proposed quantum signature protocol theoretically and practically. The results demonstrate strong encryption performance, achieving a computational cost of 41.5 ms and communication overhead of 834 bits, outperforming recent benchmark schemes. The findings highlight the superior reliability, scalability, and efficiency of our approach, offering a viable quantum security solution for future CCIoT ecosystems.**

***Index Terms*—Consumer-Centric Internet of Things, Quantum Security, Digital Signature, Quantum Teleportation, Blockchain.**

I. Introduction

THE circumstances surrounding the coronavirus pandemic have accelerated the transformation of traditional infrastructures into digital ecosystems, leading to the rise of e-services across multiple domains. In parallel, the Internet of Things (IoT) market has witnessed significant expansion. The Consumer-Centric Internet of Things (CCIoT) represents the integration of IoT technologies with consumer-oriented applications, offering numerous advantages over conventional systems [1]. For example, CCIoT enables real-time monitoring, remote accessibility, cost-effective operations, and enhanced quality of services [2], [3]. The scientific and technological potential of CCIoT significantly improves daily life by offering convenience, personalization, and efficiency. Its consumer-driven approach reduces the need for direct human intervention, making services more accessible and time-saving. Furthermore, CCIoT supports the intelligent management of resources, devices, and services across different domains. The structural framework of CCIoT typically consists of sensors or smart devices, cloud servers, consumers, and service providers. A variety of devices and sensors deployed in consumer environments continuously collect real-time data for analysis and decision-making. This data is stored, processed, and analyzed on cloud platforms, enabling secure and seamless access for authorized stakeholders. Consequently, service providers can deliver timely and personalized solutions by leveraging consumers real-time data stored on the cloud [4]–[6].

However, the widespread availability and accessibility of consumer data over open networks has led to growing challenges concerning unauthorized access, information leakage, and data breaches. Any tampering or deletion of sensitive consumer information by a malicious actor can cause severe consequences. For instance, consider a scenario where smart energy consumption data is altered; incorrect decisions could result in financial losses or system failures. As such, data security and contextual privacy have become critical concerns in CCIoT environments [7], [8]. To ensure reliable operations and maintain trust, essential security requirements include non-repudiation, availability, confidentiality, authentication, and integrity. Cryptography-based algorithms, such as digital signatures, provide robust mechanisms to address these requirements and strengthen the security of CCIoT systems.

Yang et al. [9] provided an extensive survey on the security and privacy of multimedia data, highlighting the classification of data across various security parameters and application domains. Their study examined both conventional methods, such as watermarking and cryptography, and emerging approaches, including federated learning and blockchain, thereby offering a comprehensive perspective on multimedia protection in IoT environments. Similarly, Ma et al. [10] addressed the challenges of securing surveillance recordings, noting the latency and complexity of traditional schemes like steganography. To overcome these issues, they proposed a blockchain-

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), and also supported by Ongoing Research Funding program-Research Chairs (ORF-RC-2025-0700), King Saud University, Riyadh, Saudi Arabia.

Sunil Prajapat is with the Department of Computer Engineering, AI Security Research Center, Gachon University, Seongnam, South Korea. (e-mail: sunilprajapat645@gmail.com).

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

M. Shamim Hossain is with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 13273, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Corresponding Authors: Seong Oun Hwang and M. Shamim Hossain

based framework that employs virtualization and decentralized ledgers to guarantee immutability and integrity of surveillance data. Dwivedi et al. [11] further contributed by designing a privacy-preserving authentication system using Zero-Knowledge Proofs (ZKP), which ensures confidentiality in sensitive domains such as healthcare. Related efforts by Singh et al. [12] and Dhar et al. [13] combined blockchain with ZKP to provide robust storage, transmission, and authentication of IoT data.

Advancements in quantum cryptography have also been explored for enhancing data protection in cloud and communication systems. Sasikumar et al. [14] introduced a simulation model that integrates Quantum Key Distribution (QKD) with non-abelian encryption to secure cloud data through quantum key exchange over optical fibers, addressing concerns of privacy and authorization. Other studies [15] combined AES and quantum keys or directly applied QKD to strengthen cloud security and improve key generation efficiency. Zhao et al. [16] analyzed critical performance aspects of QKD systems, confirming their potential for large-scale applications. Quantum identity authentication has likewise gained traction, with Mihara [17] and Lee et al. [18] proposing entanglement-based authentication schemes involving trusted authorities and GHZ states to support multi-user authentication.

Quantum cryptography, which bridges quantum mechanics with classical encryption, ensures secure information exchange by leveraging the fundamental laws of physics rather than relying solely on computational hardness. Unlike traditional cryptographic approaches that depend on mathematically complex problems, quantum cryptographic techniques-most notably QKD derive their strength from the principles of quantum mechanics [19]–[21]. QKD enables secure key exchange by preventing adversaries from intercepting qubits undetected, eliminating the need for unlimited computational resources, and allowing communicating parties to identify any eavesdropping attempts. These properties make QKD a highly suitable choice for open and dynamic networks such as CCIoT.

The unconditional security of QKD arises from two foundational principles: the no-cloning theorem and the Heisenberg Uncertainty Principle [22]. The no-cloning theorem asserts that it is impossible to replicate or reproduce the exact quantum state of a qubit without prior knowledge of its measurement basis. Similarly, when measurement bases are chosen randomly, any interception attempt by an adversary inevitably alters the quantum state, making detection straightforward. Since quantum state measurement destroys the original state, any interference becomes evident, thereby alerting legitimate parties to the presence of an eavesdropper [23]. These protocols demonstrated superior efficiency and error handling compared to BB84. Building on this line of research, our work presents an innovative approach that integrates QKD with electron paramagnetic resonance (EPR) [24], leveraging the no-cloning theorem to generate highly secure quantum keys while ensuring computational and energy efficiency. The summary of the existing works is also given in Table I.

A. Motivation and Research Contributions

Although conventional designated verifier signature schemes are relatively efficient, they are not inherently resistant to quantum attacks and may become obsolete with the advent of practical quantum computers. Quantum cryptography, on the other hand, offers resilience against such threats, thereby ensuring the long-term confidentiality, integrity, and reliability of CCIoT communications. Motivated by this need, we propose a quantum-designated verifier signature scheme tailored for CCIoTs. The main contributions of this research are summarized as follows:

- Secure Communication in CCIoT: We design a quantum-based designated verifier signature protocol to ensure authentication and message integrity between consumer-centric IoT device and edge getaway.
- Security Verification: Both informal analysis and is conducted to establish the robustness of the proposed scheme. The process for detecting forged signatures during verification is also described.
- Implementation and Performance Evaluation: The scheme is implemented using Quantum Sim, OMNeT++, and BB84 libraries. We benchmark the computational costs of our protocol against existing designated verifier signature methods, with results confirming the feasibility, efficiency, and security advantages of our approach for real-world CCIoT networks.

B. Paper Structure

The structure of the paper is as follows. Section II presents of the preliminaries, which contain the network model. Section III has the proposed works construction. Section IV has present security analysis. Section V presents the computational assessment of the proposed work. Section VI contains a discussion of the practical feasibility of the proposed scheme in the actual world, and the limitations of the proposed work.Finally, in Section VII concludes the paper.

II. Quantum Preliminary

The following sections outline the foundational concepts to be used in the proposed scheme

A. Quantum Teleportation

A process that allows the transfer of a quantum state from one location to another without physically moving the particle itself, using entanglement and classical communication.

- **Mathematical Formulation:** Suppose Alice wants to teleport an unknown qubit

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \quad (1)$$

Alice and Bob share a Bell state:

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The combined state is:

$$|\psi\rangle \otimes \left|\Phi^+\right\rangle_{AB}$$

TABLE I: Summary of Key References, Highlights, and Limitations

Reference	Highlights	Limitations
[1]	Introduced the concept of CCIoT integrating IoT technologies with consumer-focused applications.	Did not address security vulnerabilities and privacy threats arising from open network data exchange.
[3]	Emphasized benefits such as real-time monitoring, remote accessibility, and improved Quality of Service in CCIoT systems.	Lacked analysis of trust management and data integrity in multi-stakeholder environments.
[5]	Proposed cloud-based storage and processing models enabling personalized, real-time CCIoT services.	Did not fully explore secure data transmission and authentication frameworks for sensitive consumer data.
[7]	Highlighted critical security challenges such as unauthorized access, data leakage, and breaches in IoT ecosystems.	Limited focus on quantum-resistant or next-generation cryptographic mechanisms.
[9]	Conducted an extensive survey on security and privacy of multimedia data using watermarking, cryptography, federated learning, and blockchain.	The study was generalized, with insufficient emphasis on CCIoT-specific use cases.
[10]	Proposed a blockchain-based framework for securing surveillance recordings with immutability and decentralization.	The approach involved high latency and computational complexity due to blockchain overhead.
[12]	Developed privacy-preserving authentication schemes using ZKP combined with blockchain for healthcare and IoT systems.	ZKP-based models require significant computational resources, reducing feasibility for resource-constrained IoT devices.
[14]	Enhanced cloud security through QKD and quantum AES hybrid systems, improving key generation efficiency and eavesdropping resistance.	Practical implementation scalability and integration with IoT systems remain challenging.
[18]	Introduced entanglement-based quantum authentication using GHZ states for multi-user environments.	Early-stage theoretical work; lacks experimental validation and integration with large-scale IoT or CCIoT systems.
[20]	Discussed quantum cryptographic foundations QKD, no-cloning theorem, and Heisenberg uncertaintyfor unconditional security in dynamic networks.	Did not yet evaluate energy efficiency and system-level performance under real-world network conditions.

After Alice performs a Bell basis measurement, the state collapses into one of four possible outcomes. Alice sends two classical bits to Bob, who applies the appropriate Pauli operator (I, X, Z, XZ) to recover $|\psi\rangle$.

B. Entangled Particles

A pair or group of quantum particles whose states are interdependent, such that the measurement of one immediately determines the state of the others, regardless of distance.

- **Mathematical Formulation:** Bell state (maximally entangled):

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Measurement on one qubit instantly determines the other:

$$P(0_A, 0_B) = P(1_A, 1_B) = \frac{1}{2},$$
$$P(0_A, 1_B) = P(1_A, 0_B) = 0.$$

C. No-Cloning Theorem

A fundamental principle of quantum mechanics which states that it is impossible to create an identical copy of an unknown quantum state. This prevents adversaries from duplicating quantum signatures.

- **Mathematical Proof** Suppose a universal cloning machine U exists:

$$U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$$

For two arbitrary states $|\psi\rangle, |\psi\rangle$:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$$

This implies $\langle\psi|\phi\rangle = 0$ or 1 , which means only orthogonal states can be cloned. Hence, arbitrary quantum states cannot be copied.

D. Measurement Disturbance

In quantum mechanics, any measurement on a quantum system disturbs its original state. This ensures that unauthorized interception or eavesdropping is detectable.

- **Mathematical Relation:** Heisenberg Uncertainty

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

Any measurement introduces unavoidable disturbance. In cryptography:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

If attacker measures in the wrong basis, collapse occurs with probability $\neq 1$, leaving detectable traces.

E. Entanglement Correlations

The predictable relationships between the outcomes of measurements on entangled particles. These correlations form the basis of secure verification in quantum signature schemes.

F. Authenticity

A security property that ensures the message genuinely originates from the claimed sender and not from an impersonator.

G. Integrity

A property guaranteeing that the transmitted message has not been altered or tampered with during communication.

H. Non-Repudiation

A property ensuring that the sender cannot later deny having sent the message or signature, providing undeniable proof of origin.

I. System Model

We integrate quantum communication primitives with an IoT stack to secure sensing, signing, and verification. The entities are:

- **CCIoT Devices (D):** Resource-constrained nodes (sensors/actuators) that capture message $M = \{m_1, \ldots, m_n\}$ and interact with the environment. Devices forward data to the edge and cloud (see Fig. 1).
- **Edge Gateway (G):** A nearby compute node that aggregates device data, performs lightweight cryptography, and within our protocol acts as the signer. It holds one qubit from a tripartite entangled state.
- **Cloud Service (S):** Provides storage/analytics and acts as the designated verifier. It holds one qubit of the entangled triplet and validates quantum signatures and message integrity.
- **Registration Authority (RA):** A trusted third party that bootstraps the system: generates per-entity keys, prepares/distributes tripartite entanglement, and sets public parameters.
- **Quantum Key Distribution (QKD):** Used to derive symmetric keys for confidential channels between $\{D, G, S\}$. QKD ensures key secrecy and integrity.
- **Quantum Channel:** Satellite or fiber links transport qubits (for QKD and entanglement distribution), ensuring long-distance quantum connectivity with integrity checks.
- **Blockchain:** Tamper-evident storage for hashes of data and verification outcomes, enabling auditability without revealing plaintext.
- **Classical Primitives:** ASCON (AEAD) protects ciphertext integrity/confidentiality; Zero-Knowledge Proofs ($\mathcal{ZKP}$) authenticate endpoints ($D \leftrightarrow G$, $G \leftrightarrow S$) without revealing secrets.

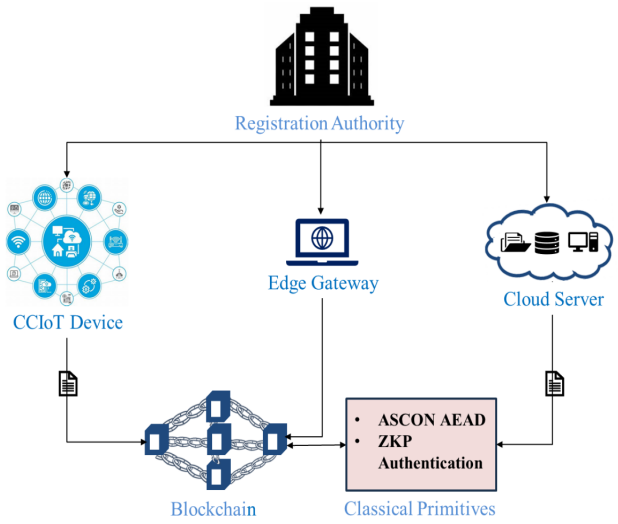

Fig. 1: CCIoT-Quantum System Model.

1) Operational Framework:

- **Sensing:** D acquires measurements M (sensor readings, device states).
- **Keying via QKD:** Pairwise QKD sessions derive symmetric keys among (D, G, S); qubits are transported via Sat/Fiber links.
- **Authenticated Channels:** $\mathcal{ZKP}$ is used to mutually authenticate D, G, S; ASCON provides AEAD on classical payloads.
- **Uplink:** D sends ASCON-encrypted data to G/S over authenticated channels.
- **Quantum Signature:** G (signer) uses its entangled qubit and RA parameters to produce a quantum signature $|S\rangle$ bound to M.
- **Verification:** S (cloud) applies unitary checks, measures, and compares one-way quantum images $|f(x)|$ to validate $|S\rangle$ and recover M'.
- **Ledgering:** S records $\mathrm{Hash}(M)$ and verification status on the blockchain. Periodic updates maintain integrity of the data stream.

III. Proposed Scheme

We consider three entangled particles shared among the IoT stack and four logical roles: 1) Owner: D (device),2) Signer: G (edge), 3) Verifier: S (cloud), and 4)TTP: RA. The protocol has three stages: A.) Initialization, B.) Signature Generation, and C.) Verification.

A. Initialization Phase

1) **Key Setup:** RA generates per-entity secrets: $K_D = \{d_1, \ldots, d_n\}$, $K_G = \{g_1, \ldots, g_n\}$, $K_S = \{s_1, \ldots, s_n\}$, and derived pairs $K_{DG} = \{d_i g_i\}_{i=1}^n$, $K_{DS} = \{d_i s_i\}_{i=1}^n$. Keys are delivered to (D, G, S) via QKD-secured channels.
2) **Entanglement and State Preparation:** RA prepares tripartite entanglement and a basis state $|\gamma_T\rangle = |\alpha_{d_i, s_i}\rangle$ chosen from: $|\gamma_{0,0}\rangle = |0\rangle$, $|\gamma_{1,0}\rangle = |1\rangle$, $|\gamma_{0,1}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|\gamma_{1,1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. RA also sets $\gamma_G = \gamma_S = \gamma_{s_i \oplus r_i}$ for fresh randomness r_i and sends (γ_T, γ_G) to G and γ_S to S.
3) **Message Binding.** Let $M = \{m_1, \ldots, m_n\}$ be the device data. RA (or D) computes $x_i = m_i \oplus d_i \oplus s_i, x = \{x_1, \ldots, x_n\}$, and publishes $|f(x)\rangle$ where $f : |u\rangle \mapsto |x\rangle$ is a quantum one-way function. The three entangled particles are distributed to D, G, and S respectively. D privately sends M to S over an ASCON+QKD channel.

Algorithm 1 Initialization Phase

Input: $M = \{m_i\}$
Output: Keys and entangled states.

1: RA generates K_D, K_G, K_S and K_{DG}, K_{DS}; delivers via QKD.
2: RA prepares $|\gamma_T\rangle$ and tripartite entanglement; sends (γ_T, γ_G) to G, γ_S to S.
3: Compute $x_i = m_i \oplus d_i \oplus s_i$; publish $|f(x)\rangle$.
4: Distribute entangled qubits to D, G, S; $D \to S$: send M using ASCON over authenticated channel with $\mathcal{ZKP}$.

B. Signature Generation Phase

1) **Signer Activation:** S authorizes G to sign on D's behalf. G samples $R_r = \{r_i\} \subset \{0,1\}$ () and publishes

$$K_{\text{pub}} = R_r \oplus K_{DS} \oplus K_S.$$

2) **Signature State:** G derives the initial signature

$$|S\rangle = N^{(1)}(|\gamma_T\rangle),$$
$$N^{(1)} = \bigotimes_{i=1}^{n} E_i^{(1)} F_i^{(1)},$$

where $E_i^{(1)} = E(d_i \oplus r_i)$ and $F_i^{(1)} = F(s_i \oplus r_i)$ with

$$E(1) = |0\rangle\langle 1| - |1\rangle\langle 0|,$$
$$E(0) = |0\rangle\langle 0| + |1\rangle\langle 1|,$$
$$F(1) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|,$$
$$F(0) = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

3) **Key Exchange:** S chooses $R_S = \{p_i\}$. Then $|K_G\rangle = \sigma_{r_i}|\gamma_S\rangle = \sigma_{r_i}|\gamma_{s_i \oplus r_i}\rangle$, $|K_S\rangle = \sigma_{p_i}|\gamma_G\rangle$. G sends $|K_G\rangle$ to S, and S sends $|K_S\rangle$ to G (quantum channel).
4) **Shared Secret:**

$$|K_{GS}\rangle = \sigma_{r_i}\sigma_{p_i}|\gamma_S\rangle,$$
$$|K_{SG}\rangle = \sigma_{p_i}\sigma_{r_i}|\gamma_G\rangle,$$
$$K = |K_{GS}\rangle = |K_{SG}\rangle.$$

5) **Bell Outcomes for Teleportation:** D performs a Bell measurement on $(M, 1)$, records Ω_D, and sends $E_{K_{DG}}(\Omega_D)$ to G and $E_{K_{DS}}(\Omega_D)$ to S. G decrypts, measures its particle to obtain Ω_G, and forwards $E_K(\Omega_D, \Omega_G)$ to S.

Algorithm 2 Signature Generation

Input: $|\gamma_T\rangle$, keys, randomness
Output: $|S\rangle$

G: sample R_r, compute and publish $K_{\text{pub}} = R_r \oplus K_{DS} \oplus K_S$.
G: compute $|S\rangle = N^{(1)}(|\gamma_T\rangle)$.
S: sample R_S; exchange $|K_G\rangle$, $|K_S\rangle$ with G over quantum channel.
Both derive K from $\sigma_{r_i}\sigma_{p_i}$ commutation.
D: send $E_{K_{DG}}(\Omega_D)$ to G and $E_{K_{DS}}(\Omega_D)$ to S; $G \to S$: send $E_K(\Omega_D, \Omega_G)$.

C. Verification Phase

1) **Unitary Check.** S computes $|S_V\rangle = N^{(2)}(|S'\rangle)$, $N^{(2)} = \bigotimes_{i=1}^{n} E_i^{(2)} F_i^{(2)}$, with $E_i^{(2)} = E(d_i \oplus r_i \oplus u_i)$ and $F_i^{(2)} = F(s_i \oplus r_i \oplus v_i)$ for public modifiers u_i, v_i derived from K_{pub}.
2) **One-Way Image Match.** S measures $|S_V\rangle$ to obtain $x = \{x_i\}$, computes $x_i' = m_i \oplus y_i$ where $y_i = d_i \oplus s_i$, forms $|f(x')\rangle$, and verifies $|f(x)\rangle \stackrel{?}{=} |f(x')\rangle$ and update blockchain.
3) **Teleportation Completion.** Using (Ω_D, Ω_G), S applies the correction on its qubit to reconstruct M'. If $M' = M$, the signature is *Valid*; otherwise *Invalid*.

Algorithm 3 Verification

Input: $|S\rangle$, Ω_D, Ω_G
Output: Valid $\in \{0, 1\}$

$|S_V\rangle = N^{(2)}(|S'\rangle)$ using K_{pub}.
Measure $|S_V\rangle \to x$; compute x' and verify $|f(x)\rangle = |f(x')\rangle$.
Update blockchain.
Apply correction with (Ω_D, Ω_G) to recover M'.
if $M' = M$ **then**
    return Valid $= 1$;
    write Hash(M) & status to blockchain.
else
    return Valid $= 0$.
end if

D. Correctness

RA publishes the one-way quantum image $|f(x)\rangle$, where $x_i = m_i \oplus d_i \oplus s_i$. At verification, the cloud recomputes $x_i' = m_i \oplus y_i$, with $y_i = d_i \oplus s_i$. Substituting y_i: $x_i' = m_i \oplus (d_i \oplus s_i)$. Using associativity/commutativity of XOR $x_i' = (m_i \oplus d_i) \oplus s_i$. Comparing with initialization $x_i = (m_i \oplus d_i) \oplus s_i$. Hence, for every i: $x_i = x_i'$. Because f is applied bitwise: $|f(x)\rangle = |f(x')\rangle$. Thus, the verifier's measurement outcomes match the signer's published image. Using Bell outcomes (Ω_D, Ω_G), the verifier applies the correction operator:

$$U(\Omega_D, \Omega_G)|\psi\rangle \to |M'\rangle.$$

Since the basis states are consistent and no discrepancy exists in x vs. x', we have:

$$|M'\rangle = |M\rangle.$$

The verification holds if and only if

$$|f(x)\rangle = |f(x')\rangle \quad \text{and} \quad M' = M$$

which always occurs under honest execution of $\uparrow\downarrow$ protocol.

IV. Security Analysis

A. Threat Model and Assumptions

- *Adversary:* We consider a quantum polynomial-time (QPT) adversary $\mathcal{A}$ with the ability to eavesdrop, inject, delay, and reorder messages on both classical and quantum channels between D, G, S. $\mathcal{A}$ may corrupt up to one of $\{D, G, S\}$ (insider attack) but not the RA. Side-channel and implementation attacks are discussed separately.
- *Trust and Channels:* RA is trusted for key generation and state preparation. Classical channels are protected with AEAD (ASCON) and mutual authentication via zero-knowledge proofs ($\mathcal{ZKP}$). Pairwise keys are established by QKD with standard decoy-state checks; if the QBER exceeds a threshold τ, the session is aborted. Quantum

links (satellite/fiber) may be monitored by $\mathcal{A}$, but disturbance is detectable.

- *Security Goals:*
  - *Confidentiality* of M in transit and at rest.
  - *Authenticity & integrity* of signed data.
  - *Unforgeability* of signatures against existential forgery under adaptive chosen-message attacks (EUF-CMA-like notion adapted to quantum setting).
  - *Designated-verifier* property: only S can validate; verifiability is non-transferable to third parties.
  - *Forward secrecy* of classical session keys and *KCI resistance*.
  - *Auditability* (tamper-evidence) via blockchain logs.

B. Building-Block Guarantees

- **QKD:** Information-theoretic secrecy of pairwise keys; eavesdropping is detected by elevated QBER ($> \tau$).
- **AEAD/ASCON:** IND-CPA + INT-CTXT security for classical payloads (ciphertext confidentiality and integrity).
- **$\mathcal{ZKP}$:** Soundness (prevents impersonation), zero-knowledge (no secret leakage), and HVZK/zero-knowledge under composition.
- **Quantum One-Way Map f:** Hard to invert (preimage resistance) for QPT adversaries; only image states $|f(x)\rangle$ are public.
- **No-cloning & monogamy of entanglement:** Prevents copying of unknown states and precludes sharing of perfect correlations with more than the intended parties.

C. Message Confidentiality

Theorem 1. *The M remains confidential against any eavesdropper and any single corrupted party.*

Proof. The M is transmitted as ASCON-AEAD ciphertext using fresh QKD keys between $D \to S$ (or $D \to G \to S$). AEAD assures confidentiality and ciphertext integrity; QKD keys give information-theoretic secrecy. The Bell outcomes (Ω_D, Ω_G) are separately encrypted under QKD-derived keys and do not leak M without both outcomes plus the entangled correction at S. Thus, neither an eavesdropper nor a single insider (only D, only G, or only S) can recover M without the required combination. □

D. Authenticity, Integrity, and Designated Verification

Theorem 2. *An adversary cannot transform a valid signature state $|S\rangle$ on M into a different valid signature on $M^\star \neq M$, nor alter $|S\rangle$ without detection by S.*

Proof. The signature state is $|S\rangle = N^{(1)}(|\gamma_T\rangle)$, with $N^{(1)}$ parametrized by (d_i, s_i, r_i). Any tampering on $|S\rangle$ induces a detectable disturbance upon S's check $N^{(2)}$ and measurement, altering $x = \{x_i\}$ and causing a mismatch $|f(x)\rangle \neq |f(x')\rangle$. Because $x_i = m_i \oplus d_i \oplus s_i$ is bound to M, and f is one-way, producing a matching $|f(x')\rangle$ for $M^\star \neq M$ would require either inverting f or predicting the hidden mask $d_i \oplus s_i$, both infeasible for QPT $\mathcal{A}$. □

Theorem 3. *Only S can validate a signature; verification is non-transferable.*

Proof. Verification needs: (i) K_{pub} derived from (R_r, K_{DS}, K_S); (ii) the encrypted Ω_D and Ω_G; and (iii) S's entangled qubit and correction. A third party lacks the entangled share and outcomes, hence cannot reproduce the verification transformation or demonstrate validity to others. □

E. Unforgeability

We adopt an EUF-CMA-style notion: $\mathcal{A}$ with oracle access to signing interactions (choosing messages M_j and observing valid transcripts/signature states) must not output a fresh valid signature on a new message $M^\dagger \notin \{M_j\}$ with non-negligible probability.

Theorem 4. *Under the no-cloning principle, monogamy of entanglement, the one-wayness of f, and the secrecy of (d_i, s_i) from QKD, the scheme is existentially unforgeable for a designated verifier.*

Proof. Suppose $\mathcal{A}$ forges a valid signature on $M^\dagger$. By correctness, verification enforces $|f(x)\rangle = |f(x')\rangle$ with $x_i = m_i \oplus d_i \oplus s_i$ and $x'_i = m_i^\dagger \oplus (d_i \oplus s_i)$. Hence $m_i^\dagger = m_i$ for all i, contradicting $M^\dagger \neq M$, unless $\mathcal{A}$ finds $(d_i \oplus s_i)$ or inverts f. Learning $(d_i \oplus s_i)$ requires breaking QKD or extracting from measured entangled states without disturbance (ruled out by monogamy/no-cloning and QKD parameter checks). Thus the success probability is negligible. □

F. Intercept-Resend Attacks

Any measurement by $\mathcal{A}$ on qubits (QKD or signature states) introduces disturbance. Elevated QBER aborts key establishment; tampering with $|S\rangle$ alters x and fails $|f(x)\rangle$ check.

G. Man-in-the-Middle Attacks

Classical MITM is blocked by $\mathcal{ZKP}$ mutual authentication and ASCON integrity. Quantum MITM on QKD is detected by parameter estimation (decoys/QBER). MITM on entangled states disrupts verification at S.

H. Replay Attacks

Nonces and session randomness (R_r, R_S) plus fresh QKD keys bind sessions. Replaying (Ω_D, Ω_G) or old $|S\rangle$ fails because K_{pub} and session keys change per run; blockchain logs detect duplicates.

I. Impersonation Attacks

Without passing $\mathcal{ZKP}$, $\mathcal{A}$ cannot be accepted as D, G, or S. Even if $\mathcal{A}$ reuses recorded transcripts, freshness checks and changed keys prevent acceptance.

J. Key-Compromise Impersonation

Compromise of K_G (or K_D) alone does not allow $\mathcal{A}$ to impersonate other parties because verification depends on Ss secret share, fresh QKD keys, and entanglement-based corrections. Session keys are derived afresh via QKD, providing forward secrecy.

K. Insider Attacks.

Malicious G: Cannot forge on arbitrary $M^\star$ without D/S-bound masks in x_i and the correction data at S. *Malicious D:* Cannot cause S to accept altered $M^\star$ due to f-binding and G's transformation. *Malicious S:* As designated verifier, S could always accept/reject; however, blockchain-anchored logs and cross-checkable Ω transcripts provide accountability.

L. Collusion Attacks

Two-party collusion (e.g., $D + G$ without S) lacks S's entangled share and cannot validate externally; $G + S$ cannot fabricate a valid transcript for a *different* $M^\star$ due to the f-binding with d_i unknown to S alone.

M. Entanglement-Swapping

Injecting forged entanglement breaks the monogamy structure and is detected by verification or by RAs state tests (e.g., random basis checks when distributing states). Any swap changes correlations and fails the f-equality test.

N. Denial-of-Service Attacks

Dropping or delaying qubits/messages can cause aborts but not undetected forgeries or data leaks. Liveness can be improved by timeouts and resynchronization; security is unaffected.

O. Forward Secrecy and Post-Compromise Security

Because session keys are established via QKD per run and never reused, compromise of long-term classical secrets later does not reveal past session keys (forward secrecy). Similarly, leakage of one phases randomness (R_r, R_S) does not enable decryption or forging in other sessions.

P. Privacy and Minimal Leakage

Only $|f(x)\rangle$ is public; by one-wayness, it leaks no usable information about x or M. Ω_D, Ω_G are encrypted under QKD keys. Blockchain records store only hashes and statuses, preventing plaintext exposure while enabling audit.

Q. Security Parameterization and Abort Conditions

Let n be the bit-length of M and keys; let τ be the QBER abort threshold. The probability of undetected eavesdropping on QKD decreases exponentially in the number of decoy rounds; the probability of a successful forgery is bounded by $\neg(n)$ assuming one-wayness of f and soundness of $\mathcal{ZKP}$. The protocol *must* abort when (i) QBER $> \tau$, (ii) $\mathcal{ZKP}$ fails, or (iii) ASCON verification fails.

R. Malicious IoT Devices

A malicious device cannot forge arbitrary signatures or alter data undetected because:

- Each message is bound to device-specific randomness and RA-distributed masks (d_i, s_i) that cannot be derived by a single party.
- Even if the device injects falsified data, verification at the cloud fails since $f(x)$ will mismatch the expected one-way image.

S. Scyther Tool

A formal security evaluation can be performed using various automated verification frameworks, including Scyther, ProVerif, CryptoVerif, AVISPA, and TAMARIN. In this work, we employed the Scyther tool to analyze the security properties of the proposed protocol. Scyther is specifically designed to validate whether a protocol upholds its claimed security guarantees by rigorously checking compliance with predefined security features. The tool requires the protocol to be described in the Security Protocol Description Language (SPDL), which allows researchers to define roles, communication flows, and security goals. During analysis, Scyther generates assertions for each role and automatically verifies their correctness. If any assertion is violated, the tool produces a graphical representation of the corresponding attack trace, thereby aiding in the identification and resolution of vulnerabilities. For our study, the proposed scheme was modeled in SPDL, and Scyther successfully verified all targeted security properties. All security assertions passed without error, and the tool?s automated verification reported the outcome as "ok," confirming the robustness of the protocol. The results are presented in Fig. 2, which illustrates the Scyther output for the proposed scheme.

V. Performance Analysis

This section presents a comparative evaluation of our proposed scheme in terms of its security features, computational cost, and communication cost against existing protocols. The findings highlight that our approach incorporates a wider range of security attributes and demonstrates improved efficiency. The quantum communication protocol BB84 and its extended versions, such as "SARGO KMB09", are inherently supported by the simulation framework Q-Sim (Quantum-Simulation). Moreover, Q-Sim natively supports two widely adopted cryptosystems-AES-256 and the one-time pad-while also providing a flexible environment for designing and assessing new signature protocols. The tool simulates IoT devices and models the potential effects of adversarial attacks. It integrates a quantum communication layer simulator with the existing IoT simulator "MOSAIK" and introduces two additional simulators, namely $\mathcal{RA}$-sim and Attacker-sim. Q-Sim further allows real-time observation and interaction through a MOSAIK-based web customization interface. For experimentation, we used an "OMNET++" based IoT simulator, which enabled communication between conventional layers via power flow. To benchmark the performance, modifications were applied to the interface, and a configuration was set up to connect 46 IoT devices in a local area network through a radial low-voltage satellite system. This configuration was used to measure the practical effectiveness of the proposed scheme. Ultimately, the protocol ensures a secure authentication process for signature entities using BB84 QKD. The implementation was carried out on Q-Sim, running on a Windows 11 system with an Intel Core i7 processor (3.20 GHz) and 16 GB RAM. The achieved outcomes are summarized as follows. The communication efficiency was calculated as the ratio of exchanged and validated qubits per second, under the

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.2025.3631827

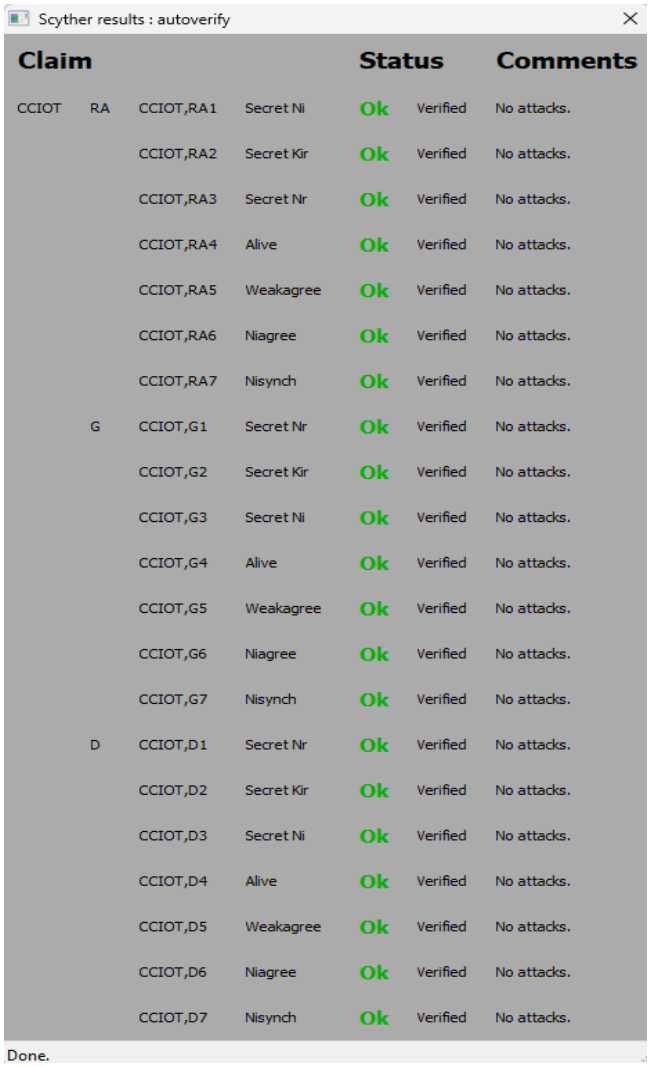

Fig. 2: The outcome of Scyther tool.

assumption of zero attack probability. The proposed scheme achieved an average communication efficiency of 48%, close to the theoretical efficiency of 50% for BB84. Furthermore, when the number of exchanged qubits exceeded 42, the number of validated qubits stabilized and remained nearly constant. We further assessed the protocol under a MITM attack scenario with 40% probability. The results show that the MITM detection rate increases as the number of qubits exchanged per second rises. In addition to this, we provide a detailed breakdown of the computational and communication overhead, as discussed below.

A. Computational Cost

The computational requirements of the proposed scheme are compared with state-of-the-art approaches during the signature generation and verification phases. To ensure fairness, we considered IoT devices with varying computing power and adopted security parameters equivalent to a 1024-bit RSA level. Specifically, bilinear pairing operations were implemented over a supersingular elliptic curve $E(F_q) : y^2 = x^3 + x \pmod p$, where p is a 160-bit prime and q is a 512-bit prime. For pairing-free curves, the elliptic curve equation takes the form $y^2 = x^3 + ax + b \pmod p$, with the same security parameters. Since operations such as addition, modular multiplication, and hashing introduce negligible overhead compared to heavy operations (modular exponentiation, point multiplication, modular inversion, and pairings), they are excluded from the cost analysis. Based on implementation benchmarks, the execution times for various cryptographic operations are as follows: Bilinear pairing (t_p): 16.65 ms, Exponentiation on G (t_e): 9.32 ms, Point multiplication (t_m): 5.49 ms, Modular inverse (t_i): 1.93 ms, Message Authentication Code (t_{mac}): 8.6 ms, Encryption function (t_E): 3.8 ms, Decryption function (t_D): 21.1 ms and cryptography hash function (t_h): 8.3ms. In our scheme, signature generation incurs a cost of $2t_h + t_E$, while verification requires one decryption operation t_D. Thus, the total computational overhead is: Total Cost= $2t_h + t_E + t_D \approx 41.5$ms. Table II provides a comprehensive breakdown of the computational overhead associated with the various protocols. Fig. 3 illustrates the computing overhead associated with the signature and verification phases. Both the signature phase and the verification phase of our scheme exhibit better operational efficiency.

TABLE II: Variation in computational cost.

Scheme	Signing cost	Verify cost	Total cost
Dong *et al.* [25]	$6t_m + t_i$	$4t_m$	56.83 ms
Chen *et al.* [26]	$3t_e + 2t_m + t_i$	$t_p + t_e + t_m$	72.33 ms
Liu *et al.* [27]	$6t_m + 2t_i$	$4T_m$	58.76 ms
Tan *et al.* [28]	$4t_e + 5t_m + 2t_i$	$t_p + t_e + t_m$	100.05 ms
Li *et al.* [29]	$2t_p + 8t_m + t_i$	$2t_p + t_e + t_i$	127.26 ms
Liu *et al.* [30]	$5t_m + t_i$	$3t_m$	45.85 ms
Ours	$2t_h + t_E$	t_D	41.5 ms

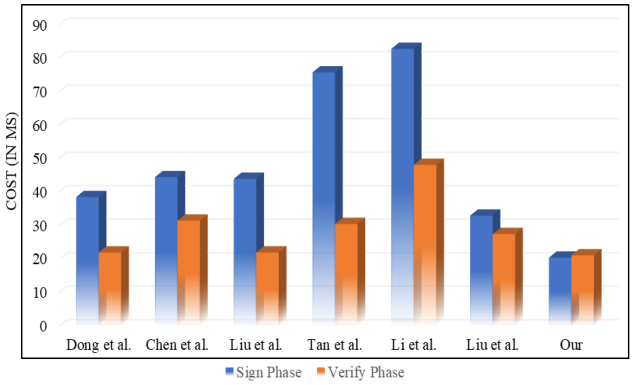

Fig. 3: Comparison based on computational costs (In ms).

When compared to other protocols, our scheme consistently shows lower execution times. For example, the scheme in [25] takes about 56.83 ms (26.97% slower), [26] about 72.33 ms (42.62% slower), [27] about 58.65 ms (29.011% slower), [28] about 100.05 ms (58.52% slower) and [29] about 127.26 ms (76.38% slower). Even the most efficient recent scheme, [30], incurs 45.85 ms (9.48% slower). Overall, both the signing and verification phases in our scheme achieve superior computational efficiency (see in Fig. 4).

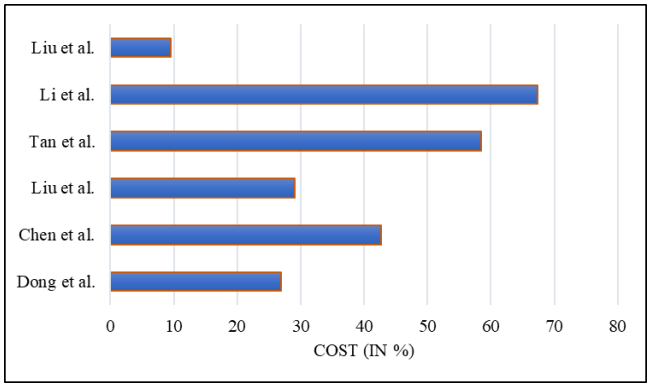

Fig. 4: Comparison based on computational costs (In %).

B. Communication Cost

Next, we analyze the communication overhead by considering the signature length. The group and finite field sizes were selected to achieve 128-bit security in bilinear pairings and ECC. The bit lengths of different parameters are: Elements in Z_q^*: 160 bits, Elements in G: 320 bits, Elements in G_1: 1024 bits. Using these parameters, the communication cost of our protocol is 834 bits. When compared with other schemes, our method demonstrates significantly lower overhead than high-cost protocols such as [26] (1184 bits), [28] (2208 bits), and [29] (1184 bits). However, it is slightly higher than lightweight schemes such as [25], [27], and [30] (all 882 bits). This shows (see in Table III and Fig 5) that our scheme strikes a balance between low communication cost and high security guarantees.

TABLE III: Comparison of Communication cost (In bits).

Scheme	Communication cost (bits)
Dong *et al.* [25]	882
Chen *et al.* [26]	1184
Liu *et al.* [27]	882
Tan *et al.* [28]	2208
Li *et al.* [29]	1184
Liu *et al.* [30]	882
Ours	834

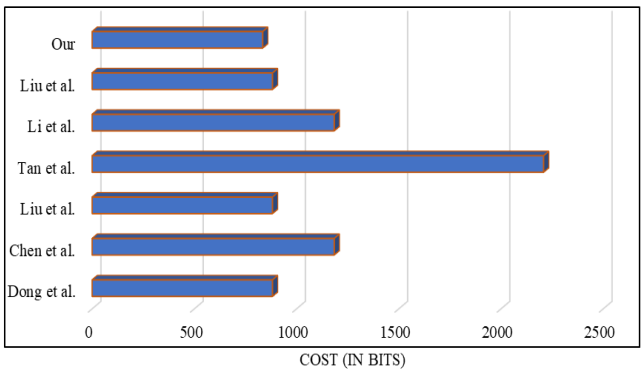

Fig. 5: Comparison based on communication costs (In bits).

C. Security Features

The security and functionality aspects of the proposed method are juxtaposed with previous state-of-the-art solutions in Table IV. In this context, ✓denotes secure, × indicates unsafe, and − represents not regarded. Our scheme evidently offers enhanced security assurances and superior functionality compared to prior solutions.

TABLE IV: Security Features

Features	[25]	[26]	[27]	[28]	[29]	[30]	Our
SF_1	×	×	×	×	×	×	✓
SF_2	✓	✓	✓	✓	✓	✓	✓
SF_3	✓	✓	✓	✓	×	✓	✓
SF_4	✓	×	✓	✓	✓	×	✓
SF_5	✓	−	−	✓	−	✓	✓
SF_6	✓	×	−	−	−	×	✓
SF_7	✓	✓	✓	✓	-	✓	✓
SF_8	×	×	×	×	×	×	✓
SF_9	×	×	×	×	×	×	✓

"F_1: Quantum Security, F_2: Intercept resending attack, F_3: Message and Signature Security, F_4: Forgery attack, F_5: Security against impersonation, F_6: Hiding Source, F_7: Disavowal Impossibility, F_8: Low computational cost, F_9: Low communication cost."

VI. Result and Discussion

The proposed blockchain-enabled quantum signature scheme demonstrates several significant advantages for securing consumer-centric IoT ecosystems. By combining quantum cryptographic primitives with blockchain, the scheme achieves confidentiality, authenticity, integrity, and non-repudiation even against powerful quantum adversaries. Performance evaluations show reduced computational overhead (41.5 ms) and minimized communication cost (834 bits), outperforming many existing benchmark protocols. This efficiency makes the scheme particularly suitable for resource-constrained IoT environments where lightweight security is essential. Moreover, the integration of quantum teleportation and entangled particles ensures robustness against eavesdropping and forgery attempts, while the blockchain layer provides tamper-proof auditability. The proposed quantum-secured CCIoT scheme holds strong potential for extension into high-security domains such as financial services and government infrastructure. These sectors demand rigorous compliance with regulatory standards like PCI-DSS, ISO/IEC 27001, and NIST guidelines. The framework?s modular design allows for seamless integration with legacy systems while preserving quantum-resilient security. In financial environments, it can secure transaction channels, ATM networks, and fraud detection systems. For government applications, it supports secure inter-agency communication, critical infrastructure monitoring, and defense-grade IoT deployments. Such properties make the protocol valuable in application domains like smart healthcare IoT systems, supply-chain monitoring, and secure consumer electronics networks, where trustworthy and low-latency data transmission is critical.

Despite these promising results, several limitations remain for real-world implementation. First, the reliance on quantum communication infrastructure, such as stable quantum channels and entanglement distribution networks, presents challenges since large-scale deployment is still in its infancy. Second, the integration cost and hardware requirements (e.g., quantum random number generators, entangled photon

sources, and quantum repeaters) may hinder adoption in cost-sensitive IoT markets. Third, while the proposed scheme performs efficiently in simulations, scalability under massive IoT deployments with millions of devices still requires experimental validation to assess latency, error rates, and synchronization overhead. Addressing these limitations will be crucial to transitioning from controlled testbeds to widespread practical adoption.

VII. Conclusion

In conclusion, the proposed blockchain-enabled quantum-designated verifier signature protocol provides a robust and efficient solution for securing data transmission and storage in CCIoT networks. By combining private blockchain technology with quantum cryptographic mechanisms, the framework ensures confidentiality, integrity, and authenticity even in the presence of classical and quantum adversaries. The integration of quantum key distribution, zero-knowledge proofs, and lightweight signature schemes further strengthens key management and communication security. Experimental evaluations and informal security analyses confirm that the protocol achieves low computational and communication overhead while maintaining scalability and energy efficiency. Overall, this work demonstrates that leveraging quantum cryptography in conjunction with blockchain offers a practical, high-performance approach to safeguarding future CCIoT ecosystems, addressing the critical security challenges posed by the rapid proliferation of connected devices.

In the future work will focus on enhancing scalability to support large-scale IoT deployments with millions of devices. Improving quantum resource efficiency, including optimized entanglement distribution and faster key generation, will be an essential step. Hybrid integration of post-quantum cryptography with quantum primitives can provide transitional compatibility with classical systems. Real-world deployment over satellite-based QKD and optical-fiber infrastructures will be explored to validate performance. Developing lightweight and cost-effective quantum hardware for resource-constrained IoT devices will further strengthen practical adoption. Incorporating AI-driven intrusion detection can help achieve adaptive and intelligent defense mechanisms. Blockchain scalability may be addressed using advanced consensus algorithms, sharding, or layer-2 solutions. Seamless interoperability with 6G-enabled IoT systems will be targeted to meet low-latency global communication requirements. Enhanced quantum error correction methods will be integrated to mitigate noise and loss in quantum channels. Formal verification under quantum composability frameworks will improve the scheme?s theoretical rigor. Application-driven customization, particularly for smart healthcare, financial IoT, and defense data management, will be prioritized. Experimental testbeds combining IoT, blockchain, and quantum communication simulators will be extended toward real-world prototypes. Collaborative frameworks involving academia and industry will accelerate technology transfer. Privacy-preserving computation models, such as secure multi-party quantum computation, may also be integrated. Ultimately, the goal is to transition this protocol from simulation to robust real-world deployment in diverse domains.

References

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] Y. Chen, X. Liang, H. Zhou, X. Yang, L. Wu, and G. Lv, "Gendn: A geospatially-enhanced ndn framework for location-related pub/sub services in ntn-enabled iot," *IEEE Internet of Things Journal*, 2024.

[7] S. Muralidharan, B. Yoo, and H. Ko, "Decentralized me-centric framework-a futuristic architecture for consumer iot," *IEEE Consumer Electronics Magazine*, vol. 12, no. 3, pp. 39–50, 2022.

[8] K. Lin, J. Luo, L. Hu, M. S. Hossain, and A. Ghoneim, "Localization based on social big data analysis in the vehicular networks," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1932–1940, 2016.

[9] W. Yang, S. Wang, J. HuHu, and N. M. Karie, "Multimedia security and privacy protection in the internet of things: research developments and challenges," *International Journal of Multimedia Intelligence and Security*, vol. 4, no. 1, pp. 20–46, 2022.

[10] Z. Ma, L. Zhu, F. R. Yu, and J. James, "Protection of surveillance recordings via blockchain-assisted multimedia security," *International Journal of Sensor Networks*, vol. 37, no. 2, pp. 69–80, 2021.

[11] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba, and O. Said, "Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 10, pp. 4639–4649, 2022.

[12] R. Singh, A. D. Dwivedi, G. Srivastava, P. Chatterjee, and J. C.-W. Lin, "A privacy-preserving internet of things smart healthcare financial system," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18 452–18 460, 2023.

[13] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, p. e4621, 2023.

[14] S. Sasikumar, K. Sundar, C. Jayakumar, M. S. Obaidat, T. Stephan, and K.-F. Hsiao, "Modeling and simulation of a novel secure quantum key distribution (sqkd) for ensuring data security in cloud environment," *Simulation Modelling Practice and Theory*, vol. 121, p. 102651, 2022.

[15] S. Fatima and S. Ahmad, "Quantum key distribution approach for secure authentication of cloud servers," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 11, no. 3, pp. 19–32, 2021.

[16] B. Zhao, X. Zha, Z. Chen, R. Shi, D. Wang, T. Peng, and L. Yan, "Performance analysis of quantum key distribution technology for power business," *Applied Sciences*, vol. 10, no. 8, p. 2906, 2020.

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

[18] H. Lee, J. Lim, and H. Yang, "Quantum direct communication with authentication," *Physical Review A-Atomic, Molecular, and Optical Physics*, vol. 73, no. 4, p. 042305, 2006.

[19] S. Prajapat, P. Kumar, D. Kumar, A. K. Das, M. S. Hossain, and J. J. Rodrigues, "Quantum secure authentication scheme for internet of medical things using blockchain," *IEEE Internet of Things Journal*, 2024.

[20] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[21] S. Prajapat, P. Kumar, A. K. Das, and G. Muhammad, "Generative ai-enabled quantum encryption algorithm for securing iot-based healthcare application using blockchain," *IEEE Internet of Things Journal*, 2025.

[22] G. M. D'Ariano, "On the heisenberg principle, namely on the information-disturbance trade-off in a quantum measurement," *Fortschritte der Physik: Progress of Physics*, vol. 51, no. 4-5, pp. 318–330, 2003.

[23] X. Xin, Z. Wang, Q. Yang, and F. Li, "Quantum designated verifier signature based on bell states." *Quantum Information Processing*, vol. 19, no. 3, 2020.

[24] J. A. Weil and J. R. Bolton, *Electron paramagnetic resonance: elementary theory and practical applications*. John Wiley & Sons, 2007.

[25] G. Dong, F. Gao, W. Shi, and P. Gong, "An efficient certificateless blind signature scheme without bilinear pairing," *Anais da Academia Brasileira de Ciências*, vol. 86, pp. 1003–1011, 2014.

[26] H. Chen, L. Zhang, J. Xie, and C. Wang, "New efficient certificateless blind signature scheme," in *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016, pp. 349–353.

[27] S. Liu, Y. Zhu, and R. Wang, "Pairing-free certificateless blind signature scheme for smart grid," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10 145–10 156, 2022.

[28] P. Tan, Z. Qin, W. Wan, S. Zhang, J. Zhang, and J. Xia, "An improved certificateless partial blind signature scheme based on homomorphic encryption," in *International Conference on Artificial Intelligence and Security*. Springer, 2022, pp. 207–221.

[29] X. Li, M. Wang, and F. Li, "A certificateless-based blind signature scheme with message recovery," in *International Conference on Machine Learning for Cyber Security*. Springer, 2022, pp. 382–389.

[30] S. Liu, Z. Wan, Y. Yuan, Q. Dong, B. Yang, and F. Hao, "An efficient certificateless blind signature scheme with conditional revocation for mobile crowd sensing within smart city," *IEEE Internet of Things Journal*, 2024.