future internet

MDPI

Article

Securing the Internet of Things, Lightweight Mutual Authentication Based on Quantum Key Distribution

Muhammad Nawaz Khan [1], Inam Ullah [2,*], Sokjoon Lee [1] and Mohsin Shah [2,*]

[1] Department of Smart Security, Gachon University, Seongnam-si 13120, Republic of Korea; muhammadnawaz@gachon.ac.kr (M.N.K.); junny@gachon.ac.kr (S.L.)
[2] Department of Computer Engineering, Gachon University, Seongnam-si 13120, Republic of Korea
* Correspondence: inam@gachon.ac.kr (I.U.); symnshah@gachon.ac.kr (M.S.)

Abstract

The Internet of Things (IoT) and quantum computing revolutionized the era of conventional and classical computing into a new paradigm of Quantum-IoT where *qubits* and entanglement make IoT more interactive, powerful, and secure. They facilitate numerous tasks by increasing productivity and efficiency, paving the path for a smarter and more connected future. In this article, we propose a novel authentication scheme, "Securing the Internet of Things, Lightweight Mutual Authentication Based on Quantum Key Distribution (LMA-QIoT)". LMA-QIoT enables mutual authentication using various parameters including quantum key distribution, symmetric keys and timestamps, as well as additional quantum random numbers. All these parameters play a crucial role in thwarting man-in-the-middle, backtracking and nonce reuse attacks. The evaluation of LMA-QIoT demonstrates that quantum key distribution and quantum numbers enhance system performance by reducing CPU usage by 25% and memory requirements 30% compared to an IoT edge-based system and without a server, respectively. In the reconfiguration ratio, the efficiency metric grows exponentially and remains constant on the initial line in edge-server-based systems. In comparison, LMA-QIoT confirms a much reduced overall computational complexity by 16.64%, with the lowest computational cost of $O(n^2)$. At 1024 Bytes, the original data length and increased data length (normalized) sizes stay constant with $2logn(klogn)$. Comparing the total overhead, LMA-QIoT demonstrates a reduction of 33 ms, which corresponds to approximately 16.63% less than the baseline mechanisms.

Keywords: mutual authentication; quantum computing; authentication error; computational cost; computational complexity; quantum random numbers

Check for updates

Academic Editors: Jose I. Moreno Novella and Paolo Bellavista

Received: 4 March 2026
Revised: 31 March 2026
Accepted: 22 April 2026
Published: 24 April 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The Internet of Things (IoT), often referred to as the Internet of Everything, significantly enhances people's daily lives by providing seamless connectivity and enhanced customer services [1]. IoT provides convenience by reducing effort and saving precious time through the use of smart home appliances such as voice assistants and automatic dishwashing systems [2,3]. With smart locks, cameras and doorbells, it offers integrated home security, allowing only those with authorization to access the house. By delivering e-health services, the IoT has enhanced medical and healthcare services [4]. There are many medical devices based on IoT, which include fitness trackers and remote patient monitoring chips. These gadgets monitor and track all physical activity, such as sleep habits, heart rate, blood sugar levels and even the body's hormone levels [5]. There are a hundred wearable IoT

chip-based devices used to collect vital human body data and send it to medical servers for further processing. Telemedicine and remote patient monitoring are the main categories of medical IoT-based medication systems. Other applications are industrial IoT, smart cities, and IoT used in agriculture and smart farming [6]. Some critical applications are drug discovery, cryptographical ciphers and materials sciences. Quantum tools and techniques are now emerging in every field of computing for their accuracy and correctness. It can solve complex problems millions of times faster than traditional computing machines [7].

With the enormous applications of IoT, a huge volume of data is exchanged between different IoT infrastructures, as shown in Figure 1, which may create serious security threats to their potential users. The existing security models are based on complex classical primitives such as RSA and ECC [8,9]. However, quantum computers and quantum-assisted tools have completely replaced the classical primitives with a new idea of entanglement and *qubits*. With the emergence of these quantum-based models, the classical encryption primitives will no longer be used. Quantum computing is derived from the idea of quantum mechanics and its principles. It provides more processing power and faster operations, where normal system execution can face limitations [10,11]. Classical computers use bit operations, while quantum computers use *qubits* with the principle of uncertainty and the no-cloning theorem. The quantum-assisted tools have now emerged with IoT to offer promising and secure services for customers. The integration of both of these technologies can change everything and create a faster and safer world. IoT devices create a large amount of data, where quantum techniques can help make faster decisions [12].

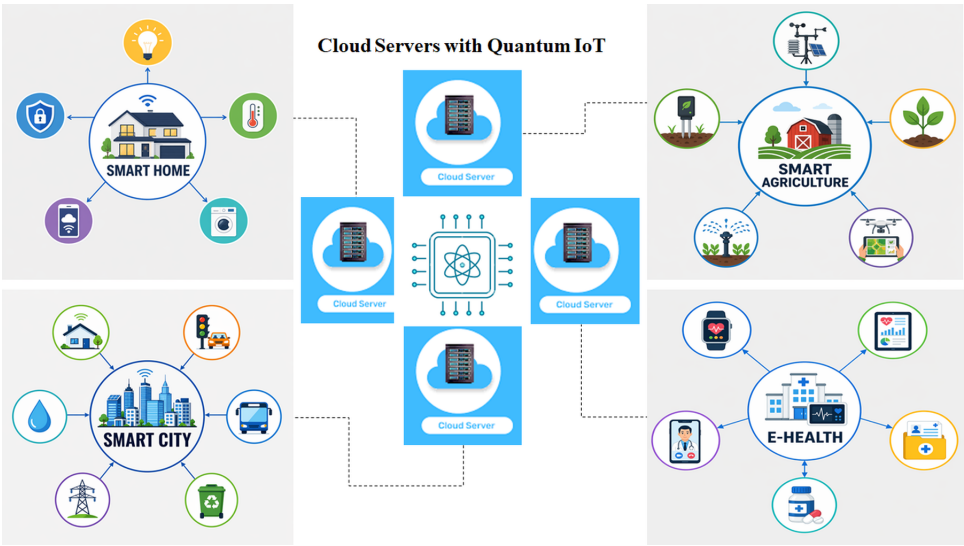


Figure 1. IoT infrastructure with cloud servers and quantum-based algorithms.

IoT devices are always connected to the public internet, and customer-critical data such as usernames, passwords, and PIN codes circulate from devices to servers. Compromising these IoT devices can cause the severe consequences of losing customer data and leaking critical information [13,14]. Computationally heavy security mechanisms are not supported by IoT devices due to their inherent restrictions in resources. The situation is more dangerous if quantum tools and applications are applied on the attacker's side to compromise these devices [15,16]. With these two issues of resource restriction and the use of quantum-assisted tools in IoT, there is a requirement for quantum-based authentication. This mechanism should be lightweight, scalable, and robust with quantum-based key management to protect IoT devices from any unauthorized access [17]. The proposed scheme should avoid complex authentication and follow automatic login steps. Each device must authenticate other devices with the assistance of edge devices and a cloud server with the

use of a quantum-based procedure [18,19]. The conventional key distribution based on RSA and ECC should be replaced with the quantum key distribution. The random numbers commonly used in these operations should be replaced by quantum random numbers with a huge permutation to ensure complete randomness and no clues.

Contributions

The main contributions in this work are as follows:

- A review of Quantum-IoT technologies for IoT devices that pose a threat to conventional security measures. Using conventional techniques for security presents both possibilities and problems in the context of quantum IoT devices. IoT systems that deploy post-quantum approaches significantly impact resources; hence, a new mechanism is needed.
- Implement a quantum key-based mutual authentication with a distributed approach to asymmetrically share symmetric keys for IoT devices. These devices then communicate with each other without using servers with the help of quantum keys and quantum numbers. Quantum IoT makes it easier and more efficient to provide ubiquitous services.
- Implement the model using specified parameters and verify the model using various metric values. Furthermore, attempt to check the suggested method in various settings and environments to confirm its efficacy. A set of criteria for different attacks on IoT with quantum-based keys is used to test the proposed mechanism.

The rest of the paper is arranged as follows: Section 2 presents related work with a title of Authentication Schemes in Quantum IoT, Section 3 introduces the proposed solution (Lightweight Mutual Authentication Based on Quantum Key Distribution), Section 4 is the Performance Evaluation, and in Section 5, LMA-QIoT is compared with SOTA schemes. Finally, this work concludes in Section 6 with some future directions.

2. Authentication Schemes in Quantum IoT

IoT security is achieved by the use of various mechanisms based on quantum algorithms and techniques. They are using different procedures to protect the system from well-known attacks. Some common surveys for quantum-secure authentication and key agreement protocols (KPAs) are beneficial for comprehending and implementing in IoT infrastructure [20–23]. To provide a base for critical analysis, the following are some of the schemes that are deployed and suggested to secure IoT infrastructures.

TFA-HQ [24], which has used two-factor authentication for the IoT-enabled healthcare ecosystem. It is based on the random oracle model and is useful in analyzing the protocol's functionality and security. The main steps are user anonymity and mutual authentication. These steps ensure resistance to biometric template alteration, stolen smart cards and privileged insider attacks. **Ring-LWE** [8] is a technique that assists the location and identity privacy. It is more efficient due to signature systems and also uses post-quantum hybrid code-based encryption techniques. The foundation is provided by a Simplified Log Domain Sum-Product Algorithm (SLDSPA) and Diagonal Structure QC-LDPC Codes mixed with loop optimization to ensure lightweight encryption. **LSS-IoT** [25] is based on Goldreich–Goldwasser–Halev (GGH) and quantum key distribution, which safeguard against quantum threats. It prevents eavesdropping and ensures secure authentication, and it is validated in the AVISPA tool for known and unknown attacks. **LAAC** [26] mainly handles the authentication of the e-health system, where integer factorization and discrete logarithm are used in securing the system. It systematically follows the lattice-based authentication and access control system for e-health systems enabled with IoT. LAAC is robust in homogeneous small-integer assumptions, and it is a verifiable security study.

PQCA [27] is a lattice-based cryptography-based authentication and access control mechanism. It uses private medical data at risk from impersonation, desynchronization and smart card theft attacks. It is a unique method of using the lattice-based key encapsulation method. **ACGA** [28] is another lattice cryptography-based group authentication mechanism that uses identity-based encryption (IBE) and a lattice-based aggregate signature algorithm. It reduces the storage overhead of the core network by doing away with the public key certificate management process and providing a formal security analysis of the proposed protocol with the tool ProVerif. **QRHA** [29] is a lightweight and two-party handover authentication procedure based on NTRU for mobile devices. BAN logic and the random oracle model are used for accuracy to ensure system security. It is recommended for lower communication overhead. **LMA-IoT** [30] is a public key encryption based on a mutual authentication protocol. It provides better security in terms of communication costs and efficiency. It is in a position with the RSA and ECC-based schemes regarding efficiency. **PiLike** [31] is an identity-based authenticated key exchange mechanism. It uses lattice hard assumptions that thwart any type of attack. It resists any quantum attacks to ensure lower communication overhead and less energy consumption. It stores the cryptographic key with minimum computing costs. **QSLT** [32] is a lightweight authentication and its main aim is to reduce the burden of eavesdropping. Sensitive IoT data is always encrypted using a one-time key. Any two devices negotiate the session key using an in-band key-selection technique. **LB-ID-2PAKA** [33] is an identity-based cryptography (IBC) that is used to eliminate the overhead associated with certificate maintenance. It assists in examining security strength using the random oracle to demonstrate its resilience to upcoming quantum attacks. It ensures resistance against known-key security (K-KS), unknown key-share (UK-S), and man-in-the-middle attacks.

LZIA [34] is based on a unique identifier with a hashing mechanism to distribute device IDs in IoT. It uses a low-complexity registration mechanism for direct communication. It ensures the device key management between the embedded device and the authentication server. For authentication, it combines all intermediate values into a polynomial and substitutes Chebyshev polynomial operations for conventional cryptographic procedures. **AFADT** [35] is a quantum-resistant access authentication and data delivery procedure. It uses lattice-based homomorphic encryption technology and access authentication for a concurrent collection of NB-IoT devices. **QSUA** [36] is based on the NTRU cryptosystem for a cipher and gives an authentication that uses a Gateway Node. It ensures authentication with cloud computing, IoT, and legacy systems. The one-time password also makes the procedure more secure. **QAKA** [37] is a security scheme that ensures complete protection against traditional and cutting-edge quantum attacks. It utilizes quantum hashing with quantum passwords and quantum key distribution. It also uses Greenberger–Horne–Zeilinger states and quantum teleportation to transport data securely between IoT devices. **RLWE** [38] is based on the Ring Learning With Error (RLWE) issue on lattices for IoT devices. This resists any attack on quantum IoT attacks. They provide an effective session setup process for device mutual authentication. **SIoT-QC** [39] is a post-quantum digital signature algorithm (DSA) and key encapsulation mechanism (KEM). It uses a TLS-based, low-power IoT architecture. The parameters used in the evaluation are energy, latency and memory. It is used to increase the bandwidth demand of post-quantum primitives, rather than the cryptographic computation itself.

After explaining quantum-based security mechanisms, the main features are checked and each of them is marked accordingly in Table 1.

Table 1. Enhanced comparison of IoT authentication schemes.

Scheme	Primitive	Mutual Auth.	Computational Over.	Energy Enhan.	Security	Scalability	Post-Quantum C.
TFA-HQ	Hash + RO	Yes	Yes	No	Med	Med	No
Ring-LWE	Lattice	Yes	Yes	Yes	High	High	Yes
LSS-IoT	GGH + QKD	Yes	Yes	No	High	Low	Partial
LAAC	Classical	Yes	Yes	No	Med	Med	No
PQCA	Lattice	Yes	No	No	High	Med	Yes
ACGA	Agg. Sign	No	Yes	Yes	Med	High	No
QRHA	NTRU	Yes	Yes	No	High	Med	Yes
LMA-IoT	Hash	No	Yes	No	Med	High	No
PiLike	Lattice	Yes	No	No	High	Med	Yes
QSLT	Q-assisted	Yes	Yes	No	High	Low	Partial
LB-ID-2PAKA	Lattice	Yes	Yes	Yes	High	Med	Yes
LZIA	Hash	Yes	Yes	No	Med	High	No
AFADT	Hybrid	Yes	Yes	No	High	Med	Partial
QSUA	NTRU + OTP	Yes	Yes	Yes	High	Med	Yes
QAKA	Q-hash	Yes	Yes	No	Med	Low	Partial
RLWE	RLWE	Yes	No	No	High	Med	Yes
SIoT-QC	PQ-TLS	Yes	Yes	No	High	High	Yes

Motivation and Research Gaps

Although all of the above mechanisms are quantum-based, and they ensure authentication with respect to some dedicated attacks and scenarios. They provide significant advancements in authenticating in IoT but these mechanisms are vulnerable to quantum threats and the use of such mechanisms hinders real lightweight authentication. The use of quantum-based authentication faces many challenges such as high communication overhead, excessive energy consumption, channel noise with poor scalability and the need for specialized hardware. It is therefore the integration of lightweight authentication with QKD that is necessary to address these challenges. The main goal is to achieve an efficient, scalable, and energy-aware authentication mechanism in resource-constrained IoT while preserving quantum-level confidentiality. Some critical gaps in the current literature are as follows:

- Lacking a lightweight and privacy-preserved authentication mechanism based on QKD that meets the needs of resource-constrained IoT devices.
- Due to the highly dynamic infrastructure of large-scale IoT networks, it always suffers from scalable key distribution.
- Lack interoperability between classical and quantum architectures for quantum-assisted attacks and no auditing for vulnerabilities in the hybrid architecture.

Although many existing mechanisms employ QKD, QRNs, and lattice primitives in different ways, LMA-QIoT utilized a unified and interaction-aware procedure to specifically address the limitations of IoT environments. The following is the main rationale for establishing the proposed mechanism.

- It is a unified design of QKD-generated keys and QRN-assisted permutations in a lightweight mutual authentication for IoT.
- A novel lightweight sequencing mechanism for IoT to minimize authentication rounds, reduce device-side computation and maintain quantum-based security.
- A novel architecture using a hybrid classical–quantum infrastructure which addressed latency and energy limitations of IoT devices.

3. Lightweight Mutual Authentication Based on Quantum Key Distribution

There are many entities in IoT infrastructure and a large amount of data is generated when these IoT entities collaboratively provide services to customers. To secure all these

entities and to ensure the authentication of customers we have proposed a novel scheme of "Lightweight Mutual Authentication Based on Quantum Key Distribution (LMA-QIoT)". It provides an automatic, lightweight authentication of all entities in IoT systems with quantum keys and QRNs. LMA-QIoT makes the system more resistant to unauthorized attempts using quantum procedures to log into the IoT structures. The IoT devices do not need to be authentic each time; rather, they work in the background to complete the authentication in an automatic and invisible way. Frequent and repetitive authentication is avoided in LMA-QIoT to enhance performance. It also minimizes time-consuming tasks by using automated and mutual authentication. It ensures the authenticity of customers and only allows authentic and legitimate customers. LMA-QIoT adopts a novel technique that does not permit users to reveal credentials under any condition, which ensures anonymity. It also validates each device, including the server and gateway, to guarantee that all parties are verified before the sharing of data.

3.1. LMA-QIoT System Model

For implementing an IoT system with quantum techniques, let us consider a connected network N_{IoT} of devices DV_n, where $n = 1, 2, 3, \ldots, n+1$. There are a gateway GT_{IoT} and a cloud server C_{IoT}, which provide cloud IoT and quantum services for IoT systems. Each DVn is connected to the other DV_{n+1} and makes a connected N_{IoT} with many GT_{IoT} and C_{IoT}. Euclidean distance DS_{ij} is calculated between two or more DV_n along the x and y axis in any plane of area. Most connections between these DV_n are hybrid and make connections directly or indirectly. This heterogeneous network connectivity is restricted to dt_{ij} and DT_{ij}, where dt_{ij} is the distance between two DV_n and DT_{ij} is the whole N_{IoT}, which makes the connected network with less distance between DV_n. The symbols used in the LMA-QIoT system model are defined and presented in Table 2.

Table 2. Symbol table for LMA-QIoT.

Symbols	Meaning
QRN_n	Quantum random number
C_{IoT}	Cloud server
$qubits_n$	Quantum bit (logical parameter for quantum)
CS_{key}	Super key generated by cloud-server
DV_n	IoT-devices
ID_{DV}	Unique ID of each device
GT_{IoT}	IoT-gateway
ID_{GT}	Identity of IoT-gateway
K_n	Session key for each session
DT_{ij}	Distance between any two IoT devices
T_n	Time stamps
Cer_{GT}	Certificate of gateway
$PR_{C_{IoT}}$	Private key of cloud server
PU_{DV_n}	Public key of any device
PU_{CST}	Public key of customer/user
$PR_{C_{IoT}}$	Private key of cloud server
E_n	Encryption process
D_n	Decryption process
T_{ex}	Time of expiry

3.2. Lattice in LMA-QIoT

A lattice-based security system is more robust and quite resistant to any quantum attack, either in encryption or authentication. Quantum approaches that use lattices are more efficient and have quantum-resistant security for digital communications in IoT.

Rather than integer factorization such as in RSA, or finding discrete logarithms such as in ECC, a lattice-based system is a mechanism different from *qubit* logic.

Let us define some terms, such as the independent set linear vector V = v1, v2, . . . , vn, which covers the whole space with Euclidean vector space S_n. Based on this, the lattice can be defined as any lattice for which $\mathbf{L_n}$ is a discrete additive subgroup of S_n for each element and created by the linear combination of the basis of V = v1, v2, . . . , vn.

$$\mathbf{L_n}V = v_i \sum_{i=1}^{n+1} \xi_i v_i : v_i \in V \tag{1}$$

The lattice computational complexity can be found by first finding the minimum non-zero vector lattice length, $\mathbf{L_n}V$. It should satisfy the non-zero vector V_i.

$$V_i \in \mathbf{L_n}V : \forall v_i \in \lambda \mathbf{L_n}V \tag{2}$$

While the basis V = v1, v2, . . . , vn, is surely in $\mathbf{L_n}$, and it provides the smallest possible factor of the polynomial.

3.3. LWE Distribution over the Space

The Learning with Errors (LWE) problem finds a solution to linear equations. These equations change with smaller random errors but affect the whole system of linear equations. Most of the time, a secret vector **Vs** is given to determine the value of **Vs**. These are calculated from the interference of noise with random and casual vectors. We can define it as follows.

- **Secret Vector**: $\mathbf{Vs} \in \mathbb{Z}_{\beth_i}^{j}$ where i is any polynomial and j is any prime number.
- **Random Vectors**: $\mathbf{R}_v \in \mathbb{Z}_{\beth_i}^{j}$
- **Error Terms**: $\mathbf{E}_i$ derived from error distribution δ

For random samples of LWE, we can figure out these values using

$$(\mathbf{R}_v, \xi_i = \langle \mathbf{R}_v, \mathbf{Vs} \rangle + R_v \mod (j))$$

where $\langle \mathbf{R}_v, \mathbf{Vs} \rangle$ are the inner noise values of $\mathbf{R}_v$ and **Vs**, and E_i is the error in the LWE samples. The LWE distribution is calculated from the error term (E_i) while ξ_i is mentioned as QRN. With this assumption of ξ_i equivalent and works as a random number.

3.4. Working Procedure of LMA-QIoT

In a quantum-based IoT system, each DV_n connects to the other DV_{n+1} to share data in collaboration and provide different services. Connected devices in IoT collect basic information and timely transmit to C_{IoT}. The C_{IoT} is connected to a central management system, which ensures quantum tools and procedures. The following is the step-by-step procedure and phases.

3.4.1. Initialization Phase

In this phase, the authentication process is initiated by each DV_n and creates a unique session key based on ID_{DV}. In hierarchical N_{IoT}, there are many GT_{IoT} and they need to connect to all the local IoT DV_n. All these GT_{IoT} are further connected to edge/cloud servers C_{IoT}. The C_{IoT} exercises the quantum procedure, which is already shown in Figure 1 in the Introduction part. Initially, DV_n starts communication and generates quantum states encoded as we have already discussed. These quantum states are broadcast GT_{IoT} using a quantum channel. If there are any eavesdropping attempts, they create detectable disturbances. In response, GT_{IoT} checks and verifies authenticity using different

parameters. It also sends the authenticated information to C_{IoT} based on ID_{DV}. The shared secret key K_{qkd} is derived on the basis of error correction and privacy amplification in the following way:

$$K_{qkd} = \mathcal{H}(ID_{DV}) \tag{3}$$

The GT_{IoT} also has a unique identity ID_{GT}. Each DV_n also connects to C_{IoT} for various tasks. The hash function $\mathcal{H}$ is calculated for each DV_n based on QRN_i. The $\mathcal{H}$ is calculated as follows:

$$\mathcal{H}[ID_{DV} \otimes K_{qkd}] + QRN_1 \tag{4}$$

This is the hashing value, which QRN_n plays a vital role in producing true random numbers. The DV_n will send this parameter with $\mathbf{R}_v$, ξ_i with timestamp T_{n1} in the form of a message from M_1 to GT_{IoT}.

$$DV_n \overset{M_1}{\rightarrow} GT_{\text{IoT}} : M_1 = \mathcal{H}[ID_{DV} \otimes K_{qkd}] + QRN_1 + \mathbf{R}_v + \xi_i + T_{n1} \tag{5}$$

Now, the GT_{IoT} calculates the $\mathcal{H}$ and verifies the messages from these hashes for checking the integrity. It also computes ξ_i' to check the message's authenticity and verification.

$$\xi_i' = \langle \mathbf{R}_v, \mathbf{Vs} \rangle \mod (j) \tag{6}$$

$$\xi_i - \xi_i' < \tau \tag{7}$$

The DV_1 is verified at GT_{IoT}, and now it forwards these messages to C_{IoT} and adds its own ID_{GT} with T_{n2}. The M_2 will send to C_{IoT}.

$$GT_{IoT} \overset{M_2}{\rightarrow} C_{IoT} :: M_2 = \mathcal{H}[ID_{DV} \otimes K_{qkd}] + QRN_1 + \mathbf{R}_v + \xi_i + T_{n1} || [ID_{GT} + T_{n2}] \tag{8}$$

All the above steps are true for DV_n that are already known for GT_{IoT}, but for the new DV_{n+1}, we need a challenge and response method. The DV_{n+1} initiates the authentication by sending its identity with the Hello message to GT_{IoT}.

$$Dv_n \overset{Hello+ID}{\rightarrow} GT_{IoT} : \quad Hello + ID \tag{9}$$

When GT_{IoT} receives the identity, it generates a random nonce N_{nonce} to ensure freshness for the current session.

$$GT_{IoT} \overset{N_{nonce}}{\rightarrow} DV_n : \quad N_{nonce} \tag{10}$$

The N_{nonce} is a cryptographically secure random number. The DV_{n+1} is calculated with its ID_{n+1}, received N_{nonce}

$$DV_n \overset{Hello+ID}{\rightarrow} GT_{IoT} : \quad H(ID_{n+1} \parallel N_{nonce}) \tag{11}$$

where H is a one-way hash function, while in some cases, a pre-shared secret key can also be concatenated with these messages, but the key is already shared between all entities. From this message, the GT_{IoT} calculates the hash values and verifies if the values match. All these equations and step-by-step procedures are shown in Algorithm 1.

Algorithm 1 Quantum-Enhanced LWE-Based IoT Authentication (Authentication P-I).

Input: IoT device DV_n, gateway GT_{IoT}, cloud server C_{IoT}
Output: Authenticated device and verified session
Initialization Phase
for each IoT device DV_n **do**
    Assign unique identity ID_{DV}
    Generate QKD-based key:
        $K_{qkd} = \mathcal{H}(ID_{DV})$
    Select secret vector $\mathbf{V}_s \in \mathbb{Z}_j^i$
Gateway has identity ID_{GT}
Cloud server defines modulus j, error distribution δ, threshold τ
LWE-Based Authentication Phase at DV_n
Generate random vector $\mathbf{R}_v \in \mathbb{Z}_j^i$
Sample error $\mathbf{E}_i \leftarrow \delta$
Compute LWE sample:
$\xi_i = \langle \mathbf{R}_v, \mathbf{V}_s \rangle + \mathbf{E}_i \bmod j$
Generate quantum random nonce QRN_1
Generate timestamp T_{n1}
Compute authentication hash:

$$\mathcal{H}_n = \mathcal{H}\Big((ID_{DV} \otimes K_{qkd}) \parallel QRN_1 \parallel T_{n1}\Big)$$

Construct message:
$M_1 = \{\mathcal{H}_n, QRN_1, \mathbf{R}_v, \xi_i, T_{n1}\}$
Send M_1 to GT_{IoT}
Verification Phase at GT_{IoT}
Check timestamp freshness of T_{n1}
Recompute:

$$K_{qkd} = \mathcal{H}(ID_{DV})$$

$$\hat{\mathcal{H}}_n = \mathcal{H}(ID_{DV} \otimes K_{qkd}) \parallel QRN_1 \parallel T_{n1}$$

if $\mathcal{H}_n = \hat{\mathcal{H}}_n$ **then**
    Compute LWE verification:
        $\xi_i' = \langle \mathbf{R}_v, \mathbf{V}_s \rangle \bmod j$
    if $|\xi_i - \xi_i'| < \tau$ **then**
        Device authentication successful
        Generate new timestamp T_{n2}
        Construct:
        $M_2 = M_1 \parallel (ID_{GT} \parallel T_{n2})$
        Forward M_2 to C_{IoT}
    else
        Reject device (LWE verification failed)
else
    Reject device (Hash mismatch)
Cloud-Level Final Verification
Validate ID_{GT} and timestamp T_{n2}
Confirm integrity of forwarded parameters
Register authenticated DV_n

3.4.2. Login Phase at C_{IoT}

The C_{IoT} receives these messages and checks the message's authenticity and integrity. The timestamps T_{n1} and T_{n2} calculate the time it takes for the message to be transmitted until it is received. If the time the message takes is more than the threshold, the daily time is calculated and either accepted or discarded. Depending on the calculation with the largest daily time, those messages are discarded. The integrity and correctness of the message are checked $\mathcal{H}$ and C_{IoT} the authenticity of the message is verified with GT_{IoT}. Here ξ'' is calculated.

$$\xi_i'' = \langle \mathbf{R}_v, \mathbf{Vs} \rangle \mod (j) \tag{12}$$

$$\xi_i' - \xi_i'' < \tau \tag{13}$$

All these important parameters verify C_{IoT} that the messages are not tampered with in any way in the transmission channel. After these verifications, C_{IoT} create a response with a message that contains the public certificate Cer_C embedded with a new timestamp T_{n3}. This is the digital identity of C_{IoT} and the timestamp verifies the generation time of these Cer_C. Both ensure the integrity and authenticity of C_{IoT} for any DV_n. This T_{n3} is used to keep the audit records of these messages in order while Cer_C verifies the C_{IoT} authenticity. We can write these messages for GT_{IoT} as follows:

$$C_{IoT} \rightarrow GT_{IoT}([Cer_C]||T_{n3}) \tag{14}$$

To verify the C_{IoT} authenticity, DV_n can verify it from these parameters in Cer_C.

$$Cer_C = E_n(PR_{C_{IoT}}[T_{n3}||ID_C||PU_{C_{IoT}}||T_{ex}]) \tag{15}$$

All these steps are explained in a systematic method in Algorithm 2. In the above equations, replay attacks at initial authentication are thwarted by applying multi-level timestamps $(T_{n1}, T_{n2}, T_{n3},)$. The man-in-the-middle is thwarted by applying LWE and hash function binding, while for avoiding impersonation, it uses certificates and QKD keys. LWE hardness is used in thwarting any quantum attack on the IoT.

Algorithm 2 Cloud-Level Verification and Response Generation (Authentication P-II).

Input: Forwarded message M_2 from GT_{IoT}
Output: Verified authentication response
C_{IoT} receives:
$M_2 = \{\mathcal{H}_n, QRN_1, \mathbf{R}_v, \xi_i, T_{n1}, ID_{GT}, T_{n2}\}$
Step 1: Timestamp Validation
Compute transmission delay using T_{n2}
if Delay $> \Delta T$ **then**
    Discard message (replay detected)
Step 2: Hash Integrity Verification
Recompute:

$$K_{qkd} = \mathcal{H}(ID_{DV})$$

$$\hat{\mathcal{H}}_n = \mathcal{H}\big((ID_{DV} \otimes K_{qkd}) \parallel QRN_1 \parallel T_{n1}\big)$$

if $\mathcal{H}_n \neq \hat{\mathcal{H}}_n$ **then**
    Reject message (integrity failure)

Step 3: LWE Authenticity Re-Verification
Compute:
$\xi_i'' = \langle \mathbf{R}_v, \mathbf{V}_s \rangle \bmod j$
if $|\xi_i - \xi_i''| \geq \tau$ **then**
    Reject message (LWE verification failed)
Step 4: Gateway Authentication
Verify legitimacy of ID_{GT} and timestamp T_{n2}
Step 5: Certificate Generation
Generate new timestamp T_{n3}
Construct cloud certificate:

$$Cer_C = E_n\big(PR_{C_{IoT}}[T_{n3} \parallel ID_C \parallel PU_{C_{IoT}} \parallel T_{ex}]\big)$$

Step 6: Response Transmission
Send:
$C_{IoT} \rightarrow GT_{IoT} : M_3 = (Cer_C \parallel T_{n3})$

3.4.3. Verification of C_{IoT}

The DV_n verifies the identities and legitimacy of C_{IoT} by decrypting the received message with PU_C.

$$C_{IoT} \rightarrow DV_n([Cer_C]||T_{n3}) \tag{16}$$

DV_n uses the PU_C to check and verify the server. In the following equation, the decryption of this message results in verifying the $T3$, ID_C, PU_S and T_{ex}.

$$D_n(PU_C, Cer_C) = D_n(PU_C, E_n(PR_C[T3||ID_C||PU_S||T_{ex}])) = [T3||ID_C||PU_S||T_{ex}] \tag{17}$$

All the attached devices DV_n use the same procedure to verify whether C_{IoT} is genuine and legitimate.

$$Cer_C = E_n(PR_C, [T_n||ID_1||PU_1||T_{ex}]) \tag{18}$$

A certificate is a digital document that proves the identity of C_IoT, GT_{IoT} and for all devices DV_n. It binds the identity with a public key and any entity can verify the authenticity of the other entity. For decryption, the system performs in the following ways in a generic format.

$$\begin{aligned} D_n(PU_C, Cer_{Cn+1}) &= D_n\Big(PU_C, E_n\big(PR_C[T3\|ID_{n+1}\|PU_{n+1}\|T_{ex}]\big)\Big) \\ &= [T3\|ID_{n+1}\|PU_{n+1}\|T_{ex}] \end{aligned} \tag{19}$$

By exchanging these messages among C_{IoT}, GT_{IoT}, and DV_n, a secure channel has been established between all three entities. The C_{IoT} knows about all the attached DV_n with proper identities, their functions, and the services that they are providing. It is a centralized C_{IoT} with authentication that only allows legitimate and authentic devices. The C_{IoT} is responsible for all trust development between these entities inside the IoT system. After establishing the initial trust between the main entities, C_{IoT} takes over the control of DV_n, and GT_{IoT}. Now, each entity in this connected system can communicate directly without the involvement of C_{IoT}. This process makes the QIoT lightweight and feasible for IoT scenarios. All these steps are depicted in Algorithm 3.

3.4.4. Direct Communication of Different IoT Devices DV_n

All attached DV_n, before connecting to C_{IoT}, develop trust with GT_{IoT} and C_{IoT}. All the above equations are used for establishing a secure channel. After the third message from DV_n, the C_{IoT} responds by encrypting the same request and embedding the PU_2. These messages enabled them to communicate directly without the involvement of the C_{IoT}. The following is the message for the DV_n from the C_{IoT}:

$$C_{IoT} \rightarrow DV_n(E_n(PR_C[PU_C||T_3)) \tag{20}$$

The DV_1 and DV_2 gain information about each other, including identities, services, and other information. The PR_C is used to encrypt this important information with a high level of confidentiality. For decryption, DV_n use PU_C to decrypt these messages. The C_{IoT} creates a direct and secure link between the two DV_n by adding the encrypted request and the DV_n public key in the response. All this reduces the need for C_{IoT} to act as an intermediary by allowing DV_1 to communicate directly to DV_2. Therefore, communication between DV_n becomes more efficient as it avoids the extra steps and delays associated with sending messages through C_{IoT}. Avoiding extra steps and minimizing the delay involved in sending the message through C_{IoT}, the DV_1 sends messages straight to any other DV_2.

$$DV_1 \rightarrow DV_2(E_n(PU_2[ID_1||QRN_1) + Cer_1)) \tag{21}$$

This message consists of an individual QRN_1, $ID1$ and Cer_1. The ID_1 and the QRN_1 are encrypted using DV_2's PU_2. To verify their uniqueness, the QRN_n are encoded in every transaction. These steps are properly explained in Algorithm 4.

Algorithm 3 Verification Phase at C_{IoT} (Authentication P-III).

Input: Cer_C, PU_C, PR_C, $T3$, ID_C, PU_S, T_{ex}
Output: Verification of C_{IoT}
for each DV_n **do**
    Step 1: Decrypt the certificate
    $Decrypted_C \leftarrow D_n(PU_C, Cer_C)$
    Step 2: Check if the decrypted value matches expected values
    if $Decrypted_C = [T3 \parallel ID_C \parallel PU_S \parallel T_{ex}]$ **then**
        C_{IoT} is verified
    else
        C_{IoT} is not verified
for each other DV_n **do**
    Step 4: Decrypting certificates for other devices
    $Decrypted_{DV_n} \leftarrow D_n(PU_C, Cer_{C1})$
    if $Decrypted_{DV_n} = [T3 \parallel ID_1 \parallel PU_1 \parallel T_{ex}]$ **then**
        C_{IoT} is verified
    else
        C_{IoT} is not verified
    $Decrypted_{DV_n} \leftarrow D_n(PU_C, Cer_{C2})$
    if $Decrypted_{DV_n} = [T3 \parallel ID_2 \parallel PU_2 \parallel T_{ex}]$ **then**
        C_{IoT} is verified
    else
        C_{IoT} is not verified
for $n = 1$ to N **do**
    Step 5: Decrypt certificates for N number of devices
    $Decrypted_{DV_{n+1}} \leftarrow D_n(PU_C, Cer_{Cn+1})$
    if $Decrypted_{DV_{n+1}} = [T3 \parallel ID_{n+1} \parallel PU_{n+1} \parallel T_{ex}]$ **then**
        C_{IoT} is verified
    else
        C_{IoT} is not verified

Algorithm 4 Direct Communication of Different IoT Entities (Authentication P-IV).

Input: $DV_n, PU_2, PR_C, T_3, ID_1, QRN_1, Cer_1$
Output: Secure direct communication between IoT entities
for each DV_n request **do**
    C_{IoT} develops trust with messages
    if 3rd message received from DV_1 **then**
        C_{IoT} encrypts request with PR_C and embeds PU_2
        $C_{IoT} \rightarrow DV_n(E_n(PR_C[PU_C \parallel T_3]))$

        Enable Direct Communication:
        for each pair of DV_n **do**
            C_{IoT} creates direct link by adding encrypted request and PU_2
            $DV_1 \rightarrow DV_2(E_n(PU_2[ID_1 \parallel QRN_1]) + Cer_1)$
        end for
        DV_n decrypt messages using PU_C

3.4.5. Encryption and Decryption with Shared Keys Between Different Entities

After the exchange of these messages, trust is developed between the sender and the recipient. Using QRN_n it on sending and receiving sides ensures authenticity.

$$DV_2 \rightarrow DV_1(E_n(PU_1||QRN_1||QRN_2)) \tag{22}$$

The DV_1 also follows the same procedure to decrypted these messages from DV_2. To prevent replay attacks, the encrypted message contains QRN_n. This message uses DV_2's PU_2 to encrypt QRN_2. This confirms the message's legitimacy by showing that DV_1 is the legitimate sender. The trust between two parties DV_n is further verified in this step.

$$DV_1 \rightarrow DV_2(E_n(PU_2[QRN_2])) \tag{23}$$

All these equations and processes are further explained in Algorithm 5.

Algorithm 5 Encryption and Decryption with Shared Keys between Different Entities (Authentication P-V).

Input: QRN_n, PU_n, PR_1, *Messages*
Output: Secure communication between entities
Step 1: Exchange Messages
for each DV_1, DV_2 **do**
    Trust is developed between sender and recipient using QRN_n
    Encrypt messages with public key and QRN_n values
    $DV_2 \rightarrow DV_1(E_n(PU_1 \parallel QRN_1 \parallel QRN_2))$
Step 2: Decrypt Messages
for each received message **do**
    Decrypt using recipient's private key PR_1
    Verify QRN_n to ensure authenticity and prevent replay attacks
    $DV_1 \rightarrow DV_2(E_n(PU_2[QRN_2]))$
Step 3: Verify Trust
for each DV_n **do**
    Verify trust between sender and recipient using QRN_n

4. Performance Evaluation of LMA-QIoT

In this section, the LMA-QIoT has been evaluated using different parameters and metric values. The behavior is mapped on different graphs after assessments in changing the metric values of these parameters. The real implementation of quantum computing fundamentally relies on physical quantum properties such as *qubits*, superposition, and entanglement. These features cannot be implemented directly on a conventional CPU and memory setup. However, many quantum-based systems are implemented using hybrid classical-quantum architectures, while quantum techniques are only used for key generation or key exchange, classical processors typically handle protocol logic, key management, and authentication tasks. Table 3 shows the basic parameters for these experiments with their metric values and symbolic representations. All these parameters are implemented in the NS-2 [40] and Cupcarbon TwinIoT [41] simulators, which allowed the implementation of some symmetric and asymmetric cryptography concepts of public and private keys in IoT scenarios. Various parameters have been preset for the devices within the simulation.

Table 3. Evaluation parameters, symbols and metric values.

Parameter	Symbol	Metrics
Simulation Dynamics	A_xXA_x	250 × 250 m
Simulation Time	Tm	1000 s
Distance B/W Pair of DV_n	DT_{ij}	10–15 m
Data Rate at each DV_n	DR_{DV}	250 Kbps
Baud Rate at IoT N_{IoT}	BR_N	50–400 kBaud/s
No of DV_n	DV_n	100 (maximum)
Buffer at Transmitter + Receiver	B_{Memory}	256 Bytes
Distance of GT	DT_{GT}	50–120 m
Uplink Resource for DV-IoT	DV-IoT	Single-tone with 15 kHz, 5 RUs
Downlink Resource for DV-IoT	DV-IoT	1 PRB, 5 SFs
Power-Saving Strategy	PSM_n	PSM
T3324 Timer	Tm_{T2224}	30 s
T3412 Timer	Tm_{T2224}	1 h
No. of Devices	DV_n	50–200
Gateways	(GT_{IoT})	5–20
Cloud Server	(C_{IoT})	1
Communication Topology	Nt_{work}	Hierarchical
Traffic Pattern	T_p	Periodic data + event-driven alerts
Packet Size	Pk_n	32–128 bytes
Key Size (Symmetric/Asymmetric)	K_n	128-bit/2048-bit
Hash Function	$(\mathcal{H})$	SHA-256
Number of Simulation Repetitions	Sim_n	30 runs
Confidence Interval	$C_{interval}$	95%

4.1. CPU and Memory Requirements of LMA-QIoT

The system has been experimented with in three scenarios for memory and CPU requirements. The results prove that quantum-based systems lessen the burden on IoT DV_n, while pure connected IoT systems the DV_n feel extra overhead regarding memory and CPU requirements. Quantum IoT improved efficiency, improved system scalability and reduced energy consumption. The quantum-based servers minimize cryptographic complexity at the protocol level, but not system-wide cost. It uses a small cryptographic key size and also minimizes the number of authentication rounds. In the first case, when IoT devices are connected and make a connection N_{IoT}, each device consumes more memory and its clock cycles are busy for longer periods as shown in Figure 2. These devices experience additional overhead and increased resource consumption, nearly 75% of memory and 80% of CPU usage. In the second case, the edge server/cloud servers are placed at each edge of the IoT system. These servers provide more processing power for data acquisition and analysis, making the system uniform when placing these edge servers. The results obtained from this experiment mentioned the effective role of these servers and it is proven that establishing an edge server reduces the burden on these IoT DV_n. In this case, the memory consumption is 60%, while the CPU cycle utilization is 65%. By establishing the quantum technique in the same scenario as cloud servers, the system performs better on CPU cycles and memory requirements in both cases. It decreases memory use by up to 30% while utilizing 25% CPU. With quantum configuration, it optimizes resource consumption and enhances scalability. In a quantum-based context, it offloads heavy cryptos from IoT and hence impacting the system's overall performance. This indicates that end devices require reduced computational power and memory, rather than the quantum server itself.

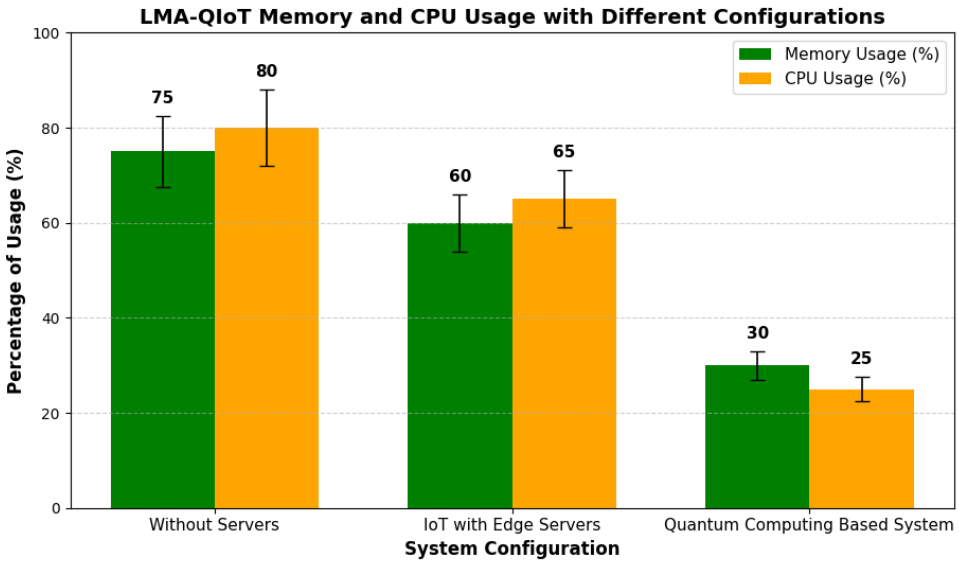


Figure 2. Memory and CPU usage in percentages with different configurations.

4.2. Reconfiguration Time in LMA-QIoT

For reconfiguration, LMA-QIoT is tested in two scenarios, one with only edge servers and the second with quantum techniques with cloud servers. In IoT, DV_n reconfiguration is needed due to the dynamic environment. The edge-server-based system is reconfigured under a classical algorithm with a uniform authentication rate. In an edge-based system, it works sequentially or with limited parallel processing capabilities. Using sequential configurations, the number of reconfigurations remains the same, with no score on the efficiency matrix, while quantum-based systems, where *qubit* logic is used with parallelism, can perform a huge volume of tasks concurrently and accelerate the reconfiguration process. *qubit* logic is based on superposition and entanglement, and all systems built on it lower the temporal complexity of reconfiguration operations. The quantum entanglement system performs better in the efficiency matrix after the fifth reconfiguration has started, as shown in Figure 3. At the ninth reconfiguration authentication state, the system responds with a maximum efficiency matrix.

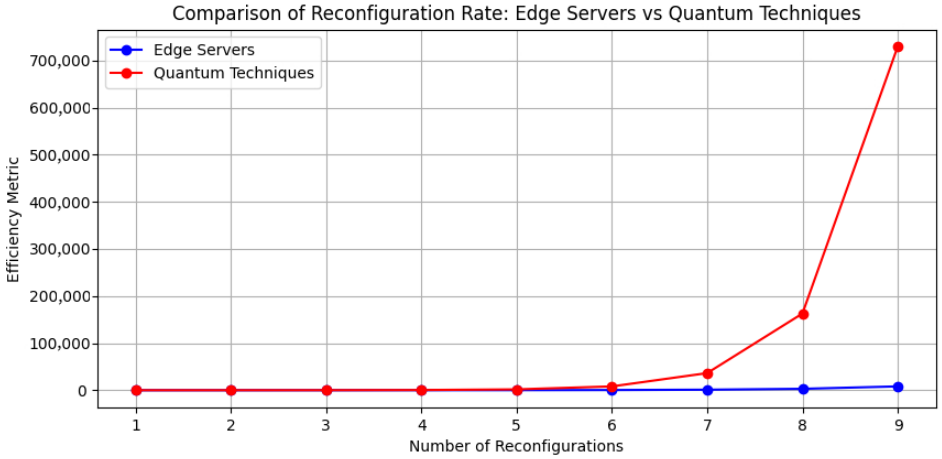


Figure 3. Reconfiguration of LMA-QIoT in edge server compared with quantum-based system.

4.3. Authentication Error in LMA-QIoT

The authentication error rate is determined in both cases for edge-server-based and for quantum-assisted IoT. The results are mapped in Figure 4, in which both cases are visible with behavior in simultaneous authentications. First, the authentication error rises when

reconfiguration starts, decreases to a lower level and then stabilizes. The high rate of the quantum-based models is due to the complexity of quantum operations and their related quantum random numbers. With an increasing number of experiments on a trial basis, the values stabilize and the error mitigation is quite low. In the case of an edge-server-based model, there is an increasing error in the authentication with a higher authentication missing ratio. The edge-based model uses classical algorithms that work systematically. The increased error rate results from network latency and software malfunctions which may account for a more uniform error rate.

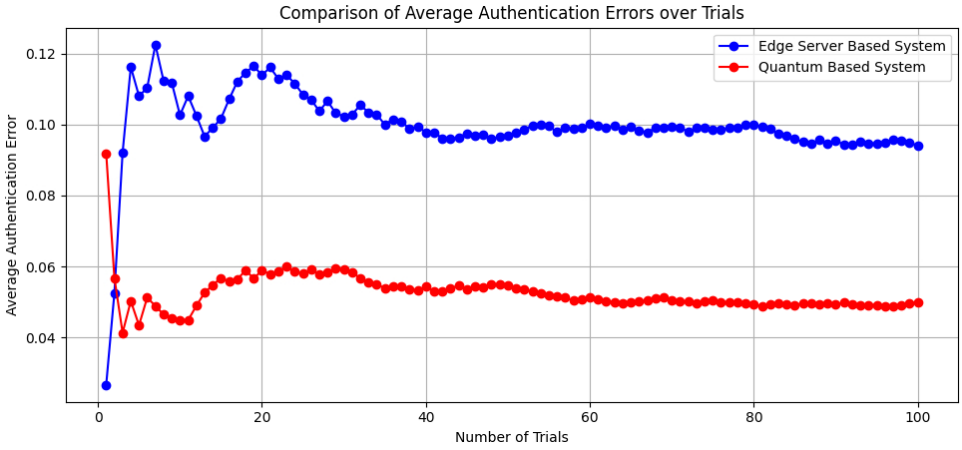


Figure 4. Authentication error LMA-QIoT in edge server compared with quantum-based system.

4.4. Execution Time Comparison in Message Sizes

For testing the system for this parameter, it is experimented with using different data sizes in both cases. The system's behavior is mapped for edge-server and quantum-assisted models in Figure 5. It is shown that a quantum-assisted model performs faster execution times than an edge-server-based model. It is due to superposition and entanglement which make it possible for the processing of data packets to be faster on a more practical basis. The error margins are also shown in the same figure, which depicts the reliability and consistency of the system.

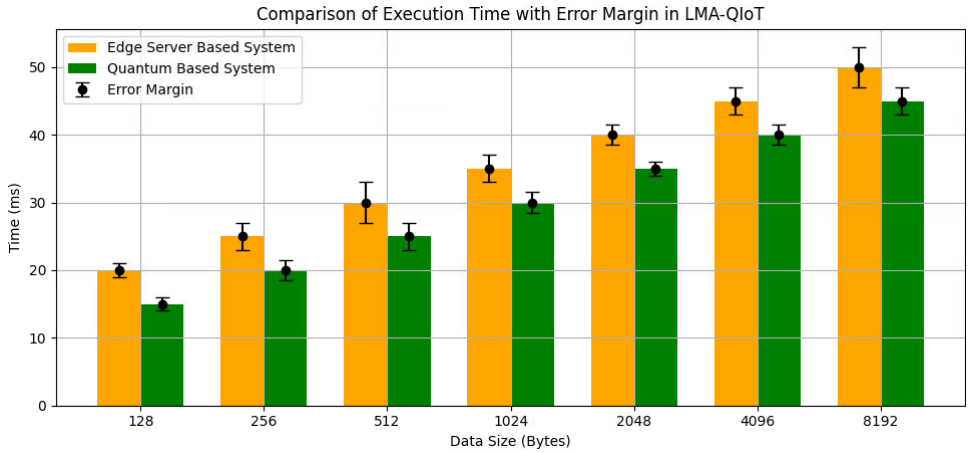


Figure 5. Execution times in message sizes for edge server compared with quantum-based system.

4.5. Formal Verification of LMA-QIoT Using AVISPA

AVISPA is used for formal verification of security protocols to check the validity and verification of different processes. It is a widely used tool to check the level of security against known and unknown attacks [42,43]. The language used in AVISPA is a high-level protocol specification language (HLPSL) in which any procedure can be defined as

a role for participating activities. The basic parameters are provided to these roles and define the communication rules with other channels. There are four back ends for input, which are the on-the-fly model checker (OFMC), a tree automaton based on automatic approximations for the examination of security protocols, a constraint-logic-based attack searcher (CL–AtSe), and a SAT-based model checker. In LMA-QIoT, we have verified authentication and some man-in-the-middle and replay attacks. Although AVISPA lacks formal verification facilities for quantum processes, QKD is thought to be sufficiently secure. Furthermore, these are modeled as a pre-shared secret for any protocol that is checked on AVISPA. The *public key* and *symmetric key* are two types of keys and const defines constants in roles. The text is used as fresh nonces and the function is used as an irreversible one-way hash function. After analysis, it just marks a protocol as being in a safe or unsafe state. We have designed and checked the LMA-QIoT for mutual authentication. The attacks used were replay, man-in-the-middle and session key using the Dolev–Yao intruder model. The design goal of our mechanism is to get and validate the required properties. AVISPA checks each message based on defined roles and marks it as safe. All these values are summarized in Table 4. For the session key, it was also tested with the ROR (Real-Or-Random) model [44,45]. The process clarifies the legitimacy of the session key, either to distinguish it or not. For an attacker A_T with an advantage, $adg_{\mathcal{AT}}$ is mathematically described as given in Equation (24).

$$adg_{\mathcal{AT}} = \left| Pr[\mathcal{AT} \text{ wins}] - \frac{1}{2} \right| \tag{24}$$

Here, in LMA-QIoT, the session keys are derived from the QKD and QRN with traditional hash functions. The hashing values and QRN secure sessions and thwart any attack for session compromise. We can derive it via $adg_{\mathcal{AT}} \approx 0$, which ensures strong resistance to any session key attack. For QBER and key rate analysis, we can use the relation as [46,47] as the ratio of the number of erroneous bits to the total transmitted bits in a unit of time. In BB84, this value is used, $QBER < 11\%$, while in our case of LMA-QIoT, this value is $QBER \approx 2\% - 5\%$. The secret key rate is $R(S) = S_{Rate} \cdot [1 - 2Bi(QBER)]$; with S_{Rate} being the sifted rate of the key and Bi is the binary entropy function.

Table 4. AVISPA verification results of the proposed authentication scheme.

Security Property	Attack Model	AVISPA Result
Mutual Authentication	Dolev–Yao	SAFE
Replay Attack Resistance	Dolev–Yao	SAFE
Man-in-the-Middle Attack	Dolev–Yao	SAFE
Session Key Secrecy	Dolev–Yao	SAFE

5. Comparative Analysis of LMA-QIoT with Other Schemes

The performance of LMA-QIoT is compared for different parameters with other state-of-the-art schemes. For comparison, we have selected **MAKe** [9], **LMA** [48] and **EHCBA** [49], due to their same mutual authentication but in a different manner. MAKe is quantum-based mutual authentication in IoT, LMA is a classical method of mutual authentication with lightweight procedures and EHCBA is blockchain-based mutual authentication in IoT. In LMA, we have used classical cryptographic primitives to optimize low computational overhead with efficient communication. LMA-QIoT extends this baseline by incorporating quantum-assisted entropy enhancement for improved key randomness. On the basis of this process, quantum-assisted key establishment ensures more secure and efficient authentication, which thwarts MIM and replay attacks. The scenarios have been tested for different parameters like communication cost/overhead and computational complexities.

5.1. Time Cost and Overhead

We derived these parameters for the overhead calculation and checked them against other metric values. Let us assume different metric values of Mul_xP, which is the matrix multiplication of modulus P. In the same way, the Vec_xP is the vector multiplication of modulus P, and Add_xP is the vector addition modulus P, and $\mathcal{H}P$ is the hash function [50]. We calculate the total cost, time, or overhead from these parameters and mention these values in Table 5. Each scheme starts with initialization, handshaking and authentication. Some phases remain the same for all, while others change with the change in technique. The total cost/overhead is also mapped for each scheme in Figure 6. The total computational cost of LMA-QIoT is marginally higher than that of LMA, ranging from 25.491 ms to 23.112 ms, which is indicative of the additional overhead introduced by quantum-assisted operations but is quite minimal compared to both MAKe and EHCBA. Taking the average of these three schemes (MAKe, EGCBA, LMA) and calculating the difference, LMA-QIoT decreases the computational overhead by 16.632%. The statistical analysis for this experiment has been tested at different time values and is mentioned in Table 6.

Table 5. Comparing the computational overhead of LMA-QIoT with MAKe, LMA, and EHCBA.

Parameter	MAKe	EHCBA	LMA	LMA-QIoT
Initialization	Mul_xP_i	Mul_xP_i	Mul_xP_i	Mul_xP_i
Handshaking	$2Mul_xP_i$+$2Vec_xP_i$	$7Mul_xP_i$+ $\mathcal{H}P$	$2Mul_xP_i$+$3Vec_xP_i$	$3Mul_xP_i$+ $7\mathcal{H}P_i$
Authentication	$3Mul_xP_I$+$5Add_xP_i$+ $3H_xR$	$2Mul_xP_i$+Vec_xP_i+ $5\mathcal{H}P_i$	$3Mul_xP_i$+$3Vec_xP_i$+ $5\mathcal{H}P_i$	$2Mul_xP_i$+ $3\mathcal{H}P_i$
Total Cost	$7Mul_xP_i$+Vec_xP_i+ $9Add_xP_i$	$4Mul_xP_i$+Vec_xP_i+ $9\mathcal{H}P_i$	$8Mul_xP_i$+$7Vec_xP_i$+ Add_xP_i	$5Mul_xP_i$+ $9\mathcal{H}P_i$
Overhead (ms)	37.912	29.321	23.112	25.491

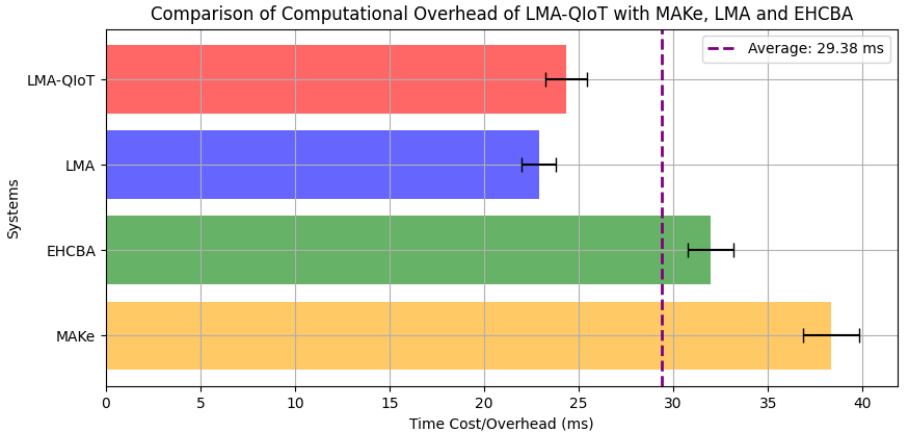


Figure 6. Overhead cost of LMA-QIoT compared with MAKe, LMA, and EHCBA.

Table 6. Statistical analysis of time cost/overhead of LMA-QIoT with MAKe, LMA, and EHCBA.

Scheme	Mul_xP	Vec_xP	Add_xP	$\mathcal{H}P$	Total Overhead (ms)
MAKe	12	18	10	8	48
LMA	10	15	8	7	40
EHCBA	14	20	12	9	55
LMA-QIoT	9	13	7	6	33
Average	12	17.7	10	8	47.7
Reduction (%)	−25%	−26.5%	−30%	−25%	16.632%

5.2. Computational Complexity

Computational complexity is another important parameter for comparing the system performance over time. LMA-QIoT is evaluated using MAKe, LMA, and EHCBA to assess its behavior in various settings. All the results for these models are shown in Table 7.

MAKe has experienced a high computational cost of $O(nlogn)$, but at the same time, it shows a low-complexity overhead with O(n). LMA remains in both parameters, with medium-complexity overhead and medium computational cost. The third scheme, EHCBA, has a low computational cost of $O(n)$, and simultaneously, a high-complexity overhead of $O(nlogn)$. The proposed LMA-QIoT has a low-complexity $O(n)$ overhead and maintains a very high computational cost of $O(n^2)$. All these values have been mapped on a graph and are shown in Figure 7.

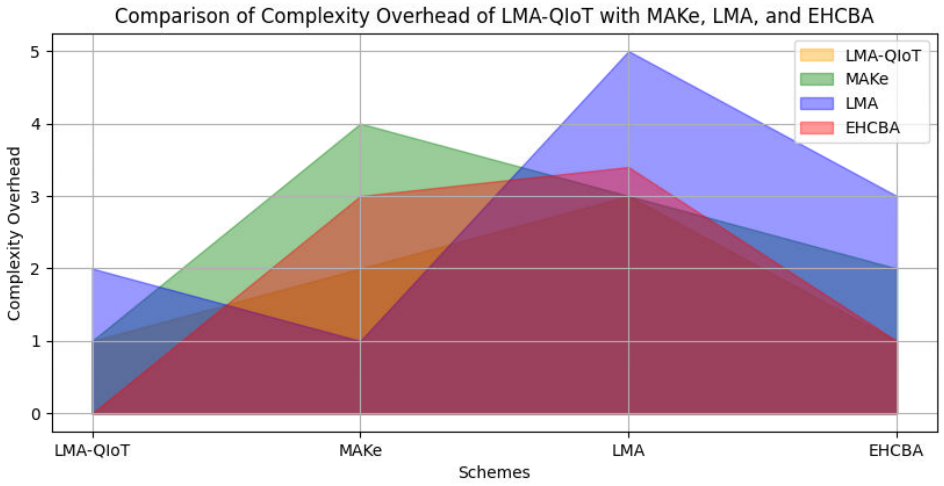


Figure 7. Complexity overhead of LMA-QIoT compared with MAKe, LMA, and EHCBA.

Table 7. Comparison of LMA-QIoT with MAKe, LMA, and EHCBA in complexity and computational cost (corrected).

Scheme	Complexity Overhead	Computational Cost
MAKe	$O(n)$ (Medium)	$O(n \log n)$ (High)
LMA	$O(\log n)$ (Low)	$O(\log n)$ (Low)
EHCBA	$O(n \log n)$ (High)	$O(n)$ (Medium)
LMA-QIoT	$O(n)$ (Medium)	$O(n^2)$ (Very High)

5.3. Storage Complexity

LMA-QIoT is tested with another important parameter of storage complexity. The whole procedure from initialization and authentication, needs to find these values for storage complexities of all four schemes. Frequent reconfiguration for authentication creates waiting loops and experiences daily latency. We have already determined and initiated some factors for the fixed packet size and the values of the hash function $\mathcal{H}P_i$ is $2log(n)$. Some other factors affecting storage are communication costs, which are $2log(n)(2nlog(n) + 11)$. These values of communication cost are calculated with storage complexity for each case in Table 8. These values show the tendency and variability of these schemes, providing a clear comparison of communication cost and storage complexities as shown in Figure 8. The overall comparison of the LMA-QIoT with MAKe, LMA, and EHCBA for different parameters are added in Table 9. For statistical analysis, we have mapped all these values in Table 10, which clearly indicates the improvement caused by using LMA-QIoT.

Table 8. Storage complexity of LMA-QIoT with MAKe, LMA, and EHCBA.

Scheme Name	Storage	Length of Data
Make	512/1024 Bytes	$2\,log\,n(k\,log\,n)+2$
LMA	512/1024 Bytes	$n(2\,k\,log\,n)+(n\,-\,1)$
EHCBA	1024	$3\,log\,n(2\,k\,log\,n)+1$
LMA-QIoT	1024	$2\,log\,n\,(k\,log\,n)$

Table 9. Comparing LMA-QIoT with MAKe, LMA, and EHCBA using different parameters.

Parameters	MAKe	EHCBA	LMA	LMA-QIoT
Authentication	Blockchain, decentralized	Centralized, cloud server	Edge server, centralized	Centralized, distributed
Data Integrity	Yes	No	Yes	Yes
Pseudo-Random Number	PRNs	Nonces	Nonces	QRNs
Resistance against MIM	Strong	Moderate	Strong	Very strong
Key Freshness	No	No	Yes	Yes
Non-Repudiation	Yes	No	No	Yes
Efficiency Level	Low efficiency	Moderate efficiency	Low efficiency	High efficiency
Keys	Symmetric and asymmetric	ECC and digital signature	Symmetric and asymmetric	Symmetric and asymmetric
Data Freshness	No	No	Yes	Yes

Table 10. Statistical analysis of LMA-QIoT for storage complexity compared to MAKe, LMA, and EHCBA.

Scheme	Total Score	Average Score	Improvement (%)
MAKe	8	0.89	-
EHCBA	6	0.67	-
LMA	10	1.11	-
Average (MAKe, EHCBA, LMA)	8	0.89	-
LMA-QIoT	13	1.44	61.8%

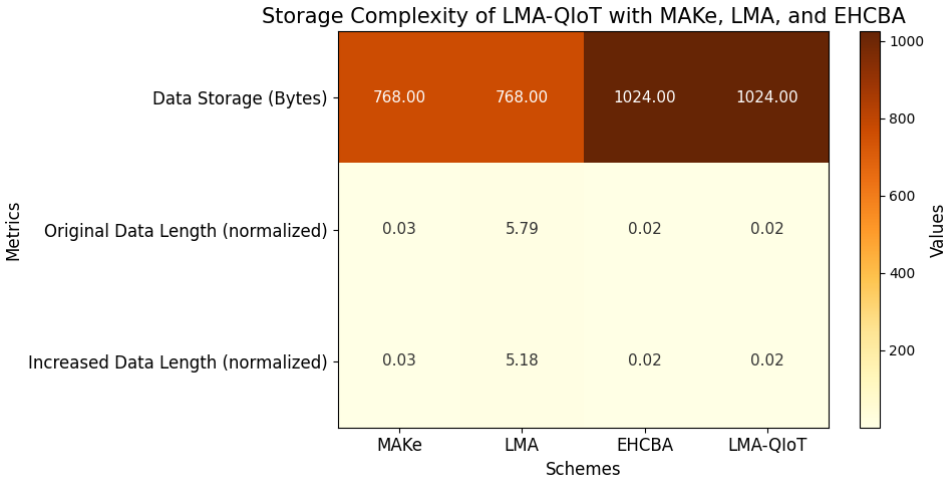


Figure 8. Storage complexity of LMA-QIoT compared with MAKe, LMA, and EHCBA.

5.4. Packet Loss Rate

The packet loss is directly related to processing delay and traffic congestion. On the basis of the previous parameters, we have experimented with the same scenario for packet loss rate in LMA-QIoT with three other baseline mechanisms. On the basis of computational overheads and time cost with buffer sizes, each scheme is tested. The behavior of each scheme is mapped in Figure 9. In these experiments, the EHCBA and MAKe exhibit a higher delay because they need more buffer. At some level, when the current buffer is full,

packet loss is initiated. The LMA exhibits the lowest delay, as its structure is traditional without the QKD and QRN. This shows the lower packet loss due to minimal queuing at edge devices and servers. LMA-QIoT exhibits a slightly higher delay than LMA but lower than MAKe and EHCBA. The increase in delay is due to many quantum-related operations, such as QKD initialization costs and permuting the QRN. These operations are applied only on initialization, and after developing the trust levels, the DV_n start communicating directly without the involvement of C_{IoT} and QKD. There is also a small delay due to hashing operations in the initial phase.

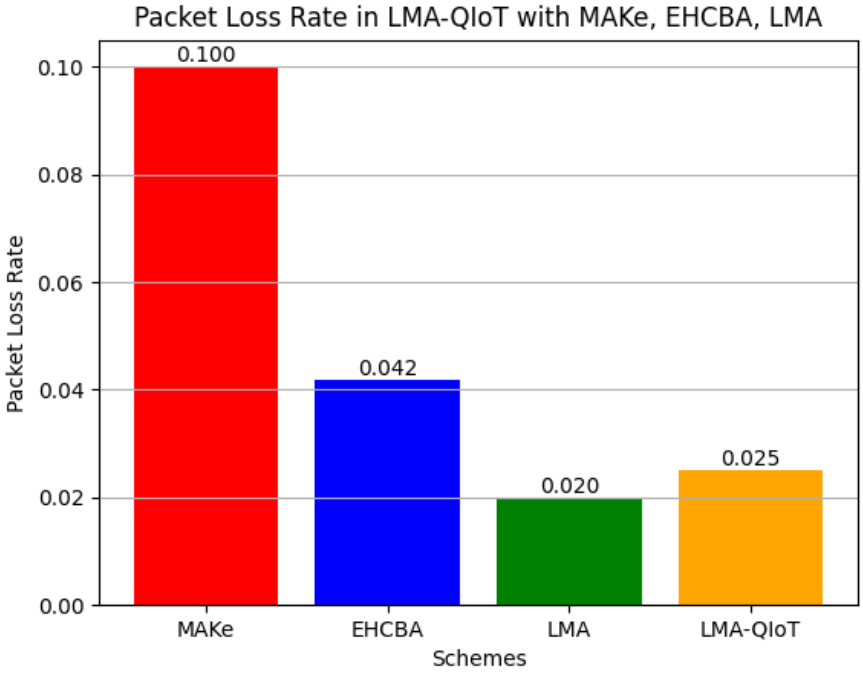


Figure 9. Packet loss rate in LMA-QIoT compared with MAKe, LMA, and EHCBA.

5.5. Scalability

To check the scalability in LMS-QIoT with other baseline schemes, we have used the packet loss with an increasing number of devices. As the number of DV_n increases, there is more traffic generated, and it increases the queue length. In the same experimental setup, MAKe exhibits higher packet loss with an increasing number of DV_n, which indicates the lower scalability. EHCBA also confirms a higher packet loss than LMA and LMA-QIoT but a lower packet loss than MAKe. This shows the moderate scalability and stability with MAKe. The LMA shows better scalability in all these schemes with the lowest packet loss. LMA-QIoT performs better than both MAKe and EHCBA while being lower in scalability than LMA. All these results are mapped in Figure 10. From these experiments, it is clear that with increasing the size of the network, the contention and queuing delays also increase, which leads to higher packet loss. The attacker's success rate in MAKe is 10%, with a higher delay of 37.9 ms and 6.5 in EHCBA, with 29.3 ms of delays. LMA confirms 2% and LMA-QIoT exhibits around 2.8% in the same scenario.

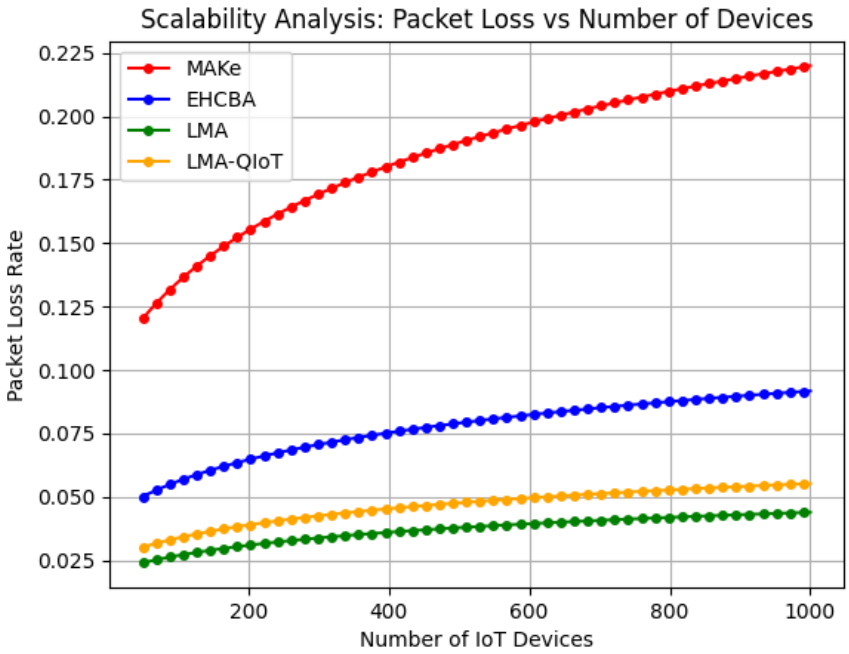


Figure 10. Scalability analysis in LMA-QIoT compared with MAKe, LMA, and EHCBA.

5.6. Attacker Success Rate

Based on packet loss and delay in response with AVISPA results, the attack success rate is calculated using statistical parameters. In an increasing number of DV_n, the computational overhead is rising with increasing latency. Ultimately, these parameters create congestion and synchronization gaps that provide provisions for the temporal attacking window. This increases the probability of successful replay and MIM attacks. The performance of the LMA-QIoT with MAKe, EHCBA, and LMA is mentioned in Table 11. In which MAKe and EHCBA confirm higher processing delays and packet loss, which provides a basis for higher probabilities of attack success. The traditional LMA exhibits lower delay with minimal queuing and fewer chances for an attacker to get into the system, reducing the attack success rate, while in LMA-QIoT, due to additional hashes and quantum-assisted keys, there is a slight increase in computational overhead. LMA is a traditional mechanism, while LMA-QIoT uses more permuted and secure QKD, which does not significantly impact the system's performance in terms of success rate for attacks.

Table 11. Attack success rate based on packet loss and delay.

Scheme	Delay (ms)	Packet Loss Rate	Attack Success Rate (%)
MAKe	37.912	0.100	10.0
EHCBA	29.321	0.065	6.5
LMA	23.112	0.020	2.0
LMA-QIoT	25.491	0.028	2.8

5.7. Key Entropy and QKD Error Rate (QBER)

For creating near-true randomness in the key generation process, we have used the Shannon entropy model. This provides complete randomness and uncertainty in key generation, is recommended in many systems and can be expressed for key K_n.

$$HF(K_n) = -\sum_i prob_i \log_2 prob_i \tag{25}$$

The $prob_i$ is the probability of occurrence of the i-th iteration. We have applied and obtained different values of HK as shown in Table 12. As the entropy of a secure system needs to be maximum, such as $HF(K_n) \approx n$. This shows the complete randomness and uniform distribution of the keys, which enhances the robustness of LMA-QIoT for man-in-the-middle and replay attacks.

Table 12. Shannon entropy analysis of QRN-inspired key generation (10 runs).

Run	$p(1)$	$p(0)$	Entropy $H(K)$
1	0.52	0.48	0.998
2	0.49	0.51	0.999
3	0.55	0.45	0.993
4	0.50	0.50	1.000
5	0.53	0.47	0.997
6	0.47	0.53	0.997
7	0.51	0.49	0.999
8	0.54	0.46	0.994
9	0.48	0.52	0.998
10	0.50	0.50	1.000

5.8. Limitations in LMA-QIoT

LMA-QIoT is implemented and evaluated in a specific scenario for dedicated attacks with a limited scope. There are many technical and functional issues in real-world implementations of LMA-QIoT. QKD is completely based on a quantum channel with quantum states. These channels are optical fibers or wireless connections tied to the physical properties of the same channels. In eavesdropping attacks, an intruder creates some disturbances to increase error rates. Other constraints are environmental noise and hardware limitations, which reduce the key generation rate and increase the quantum bit error rates. The QRN generator also relies on quantum physical processes such as photon arrival time or phase noise. For these factors, some thresholds are defined in dedicated models such as BB84. In LMA-QIoT, QKD and QRN are used only during the initial secure key establishment phase between DV_n, GT_{IoT} and C_{IoT}. After establishing a channel, all communications rely on lightweight symmetric cryptography, which avoids dependence on the QKD and QRN. The current design of LMA-QIoT reduces the physical limitations of noise and error rates.

6. Conclusions and Future Work

The integration of everyday objects, seamless communication and processing power is made feasible by quantum IoT. Quantum-assisted algorithms enable IoT to gather, share and act upon real-time data considerably more quickly and easily than they could previously. Our lives may be revolutionized by this paradigm shift, including how we participate in our homes and how companies enhance operations and provide services. It paves the way for a smarter and more connected future by making many things easier, more productive and more efficient. However, frequent use of these devices and super-connectivity makes these objects susceptible to post-quantum attacks. The classical and conventional authentication measures are not feasible in quantum-based IoT systems. To address the security challenges of authentication in Quantum-IoT, we presented a new scheme, "Securing the Internet of Things, Lightweight Mutual Authentication Based on Quantum Key Distribution (LMA-QIoT)". The proposed LMA-QIoT secures each entity of the IoT by presenting mutual authentication and server-based distributed authentication techniques. The evaluation shows that quantum techniques improve system performance by reducing memory requirements by 30% and CPU use by 25%. The efficiency metric value in the reconfiguration ratio rises considerably, whereas in edge-server-based systems,

it remains constant. Meanwhile, authentication errors have been significantly reduced in quantum-based systems compared with server-based solutions. When comparing LMA-QIoT with alternative methods, it demonstrates a significant 16.632% reduction in total computational complexity, with the lowest computational cost.

In the future, we are working to check it by adding it to machine learning techniques for the detection and prevention of quantum attacks. It needs to be customized for low latency for IoT devices to enable adaptive threat intelligence and provide resistance against quantum threats. We have tested the current model for man-in-the-middle and spoofing attacks, but need to check it on other quantum attacks with diverse datasets. The *qubit* and entanglement of bit positions are still in the early stages of development. Almost all previous techniques are tested primarily with simulation, not in a real IoT system, which limits generalizability against real-world quantum-capable attacks.

Author Contributions: Conceptualization, M.N.K.; methodology, M.N.K.; software, M.N.K.; validation, M.N.K.; formal analysis, S.L.; investigation, S.L.; writing—original draft preparation, M.S.; writing—review and editing, M.S.; supervision, I.U.; formal analysis, I.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data used in this study have been properly cited within the manuscript. No hidden or undisclosed data is involved.

Acknowledgments: This work was partly supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (RS-2023-00241376, Development of Security Monitoring Technology-Based Network Behavior Against Encrypted Cyber Threats in Maritime Environment, 50%) and (RS-2024-00396797, Development of Core Technology for Intelligent O-RAN Security Platform, 50%).

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

References

1. Loeys, S.; Boute, R.N.; Antonio, K. The Use of IoT Sensor Data to Dynamically Assess Maintenance Risk in Service Contracts. *Eur. J. Oper. Res.* **2025**, *324*, 454–465. [CrossRef]
2. Rosca, C.-M.; Stancu, A. Integration of AI in Self-Powered IoT Sensor Systems. *Appl. Sci.* **2025**, *15*, 7008. [CrossRef]
3. Park, K.; Kim, M.; Park, Y. Security Evaluation of Provably Secure ECC-Based Anonymous Authentication and Key Agreement Scheme for IoT. *Sensors* **2025**, *25*, 237. [CrossRef]
4. Khan, M.N.; Lee, S.; Shah, M. Adaptive Scheduling in Cognitive IoT Sensors for Optimizing Network Performance Using Reinforcement Learning. *Appl. Sci.* **2025**, *15*, 5573. [CrossRef]
5. Ullah, I.; Adhikari, D.; Su, X.; Palmieri, F.; Wu, C.; Choi, C. Integration of Data Science with the Intelligent IoT (IIoT): Current Challenges and Future Perspectives. *Digit. Commun. Netw.* **2025**, *11*, 280–298.
6. Dritsas, E.; Trigka, M. A Survey on the Applications of Cloud Computing in the Industrial Internet of Things. *Big Data Cogn. Comput.* **2025**, *9*, 44. [CrossRef]
7. Hwang, S.O.; Waseem, H.M.; Munir, N. Billiard Quantum Chaos: A Pioneering Image Encryption Scheme in the Post-Quantum Era. *IEEE Access* **2024**, *12*, 85150–85164. [CrossRef]
8. Kumari, S.; Singh, M.; Singh, R.; Tewari, H. A Post-Quantum Lattice-Based Lightweight Authentication and Code-Based Hybrid Encryption Scheme for IoT Devices. *Comput. Netw.* **2022**, *217*, 109327. [CrossRef]
9. Shekhawat, H.; Gupta, D.S. Quantum-Safe Lattice-Based Mutual Authentication and Key-Exchange Scheme for the Smart Grid. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e5017. [CrossRef]
10. Prajapat, S.; Thakur, G.; Kumar, P.; Kumar, G.; Sharma, K.P. Blockchain-Enabled Quantum Encryption Scheme for Securing Next-Generation IoT Networks. *IEEE Commun. Stand. Mag.* **2025**, *10*, 65–71. [CrossRef]
11. Han, K.; Lee, W.-K.; Karmakar, A.; Yi, M.-K.; Hwang, S.O. QuripfeNet: Quantum-Resistant IPFE-Based Neural Network. *IEEE Trans. Emerg. Top. Comput.* **2024**, *13*, 640–653.
12. Laktionov, I.; Diachenko, G.; Moroz, D.; Getman, I. A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography. *IoT* **2025**, *6*, 61. [CrossRef]

13. Waseem, H.M.; Munir, N.; Hwang, S.O. Advancing IoT-Driven Transportation Security: A Comprehensive Review of Privacy-Preserving Identity-Based Encryption With Quantum Enhancements. *IEEE Open J. Intell. Transp. Syst.* **2026**, *7*, 268–284.
14. Sebestyen, H.; Popescu, D.E.; Zmaranda, R.D. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. *Computers* **2025**, *14*, 61. [CrossRef]
15. Hafeez, M.A.; Lee, W.-K.; Karmakar, A.; Hwang, S.O. Efficient TMVP-Based Polynomial Convolution on GPU for Post-Quantum Cryptography Targeting IoT Applications. *IEEE Internet Things J.* **2024**, *11*, 23428–23443. [CrossRef]
16. Lee, W.-K.; Hwang, S.O. High Throughput Implementation of Post-Quantum Key Encapsulation and Decapsulation on GPU for Internet of Things Applications. *IEEE Trans. Serv. Comput.* **2021**, *15*, 3275–3288. [CrossRef]
17. Al Rawajbeh, M.; Maria Soosai, A.J.; Ramasamy, L.K.; Khan, F. Trustworthy Adaptive AI for Real-Time Intrusion Detection in Industrial IoT Security. *IoT* **2025**, *6*, 53.
18. Khan, S.; Lee, W.-K.; Karmakar, A.; Mera, J.M.B.; Majeed, A.; Hwang, S.O. Area–Time Efficient Implementation of NIST Lightweight Hash Functions Targeting IoT Applications. *IEEE Internet Things J.* **2022**, *10*, 8083–8095. [CrossRef]
19. Santhiya Devi, R.; Balaguru, R.J.B.; Amirtharajan, R.; Praveenkumar, P. A Novel Quantum Encryption and Authentication Framework Integrated with IoT. In *Security, Privacy and Trust in the IoT Environment*; Springer: Berlin, Germany, 2019; pp. 123–150.
20. Babu, P.R.; Kumar, S.A.P.; Reddy, A.G.; Das, A.K. Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. *Comput. Sci. Rev.* **2024**, *54*, 100676.
21. Gharavi, H.; Granjal, J.; Monteiro, E. Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1748–1774.
22. Cherbal, S.; Zier, A.; Hebal, S.; Louail, L.; Annane, B. Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *J. Supercomput.* **2024**, *80*, 3738–3816. [CrossRef]
23. Imran, M.; Altamimi, A.B.; Khan, W.; Hussain, S.; Alsaffar, M. Quantum cryptography for future networks security: A systematic review. *IEEE Access* **2024**, *12*, 180048–180078. [CrossRef]
24. Al-Saggaf, A.A.; Sheltami, T.; Alkhzaimi, H.; Ahmed, G. Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing. *Arab. J. Sci. Eng.* **2023**, *48*, 2347–2357. [CrossRef]
25. Benrebbouh, C.; Mansouri, H.; Cherbal, S.; Pathan, A.-S.K. A Lightweight Security Scheme to Defend against Quantum Attack in IoT-Based Energy Internet. *Int. J. Sens. Netw.* **2023**, *43*, 13–26. [CrossRef]
26. Gupta, D.S.; Islam, S.K.H.; Obaidat, M.S.; Karati, A.; Sadoun, B. LAAC: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments. *IEEE Syst. J.* **2020**, *15*, 3620–3627.
27. Adeli, M.; Bagheri, N.; Maimani, H.R.; Kumari, S.; Rodrigues, J.J.P.C. A Post-Quantum Compliant Authentication Scheme for IoT Healthcare Systems. *IEEE Internet Things J.* **2023**, *11*, 6111–6118. [CrossRef]
28. Xu, P.; Wu, H.; Tao, X.; Wang, C.; Chen, D.; Nan, G. Anti-Quantum Certificateless Group Authentication for Massive Accessing IoT Devices. *IEEE Internet Things J.* **2024**, *11*, 16561–16577.
29. Zhang, S.; Du, X.; Liu, X. A Novel and Quantum-Resistant Handover Authentication Protocol in IoT Environment. *Wirel. Netw.* **2023**, *29*, 2873–2890. [CrossRef]
30. Li, N.; Liu, D.; Nepal, S. Lightweight Mutual Authentication for IoT and Its Applications. *IEEE Trans. Sustain. Comput.* **2017**, *2*, 359–370. [CrossRef]
31. Gupta, D.S. PiLike: Post-Quantum Identity-Based Lightweight Authenticated Key Exchange Protocol for IIoT Environments. *IEEE Syst. J.* **2023**, *18*, 15–23.
32. Liu, G.; Han, J.; Zhou, Y.; Liu, T.; Chen, J. QSLT: A Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 4809210.
33. Gupta, D.S.; Ray, S.; Singh, T.; Kumari, M. Post-Quantum Lightweight Identity-Based Two-Party Authenticated Key Exchange Protocol for Internet of Vehicles. *Comput. Commun.* **2022**, *181*, 69–79.
34. Wang, Z.; Huang, J.; Miao, K.; Lv, X.; Chen, Y.; Su, B.; Liu, L.; Han, M. Lightweight Zero-Knowledge Authentication Scheme for IoT Embedded Devices. *Comput. Netw.* **2023**, *236*, 110021. [CrossRef]
35. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H. Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT Systems. *IEEE Internet Things J.* **2019**, *6*, 9794–9805.
36. Roy, K.S.; Kalita, H.K. A Quantum Safe User Authentication Protocol for the Internet of Things. *Int. J. Next-Gener. Comput.* **2019**, *10*, 178–193
37. Chawla, D.; Mehra, P.S. QAKA: A Novel Quantum Authentication and Key Agreement Protocol Using Quantum Entanglement for Secure Communication among IoT Devices. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4957. [CrossRef]
38. Mishra, D.; Singh, M.; Rewal, P.; Pursharthi, K.; Kumar, N.; Barnawi, A.; Rathore, R.S. Quantum-Safe Secure and Authorized Communication Protocol for Internet of Drones. *IEEE Trans. Veh. Technol.* **2023**, *72*, 16499–16507. [CrossRef]
39. Schoffel, M.; Lauer, F.; Rheinlander, C.C.; Wehn, N. Secure IoT in the Era of Quantum Computers: Where Are the Bottlenecks? *Sensors* **2022**, *22*, 2484. [CrossRef]

40. Rehmani, M.H.; Saleem, Y. Network Simulator NS-2. In *Encyclopedia of Information Science and Technology*, 3rd ed.; IGI Global: Hershey, PA, USA, 2015; pp. 6249–6258.
41. Mehdi, K.; Lounis, M.; Bounceur, A.; Kechadi, T. Cupcarbon: A Multi-Agent and Discrete Event Wireless Sensor Network Design and Simulation Tool. In Proceedings of the Seventh International Conference on Simulation Tools and Techniques, Lisbon, Portugal, 17–19 March 2014.
42. Oheimb, D.V. The high-lvel protocol specification language developed in the EU project AVISPA. In Proceedings of the APPSEM 2005, Frauenchiemsee, Germany, 12–15 September 2005; pp. 1–17.
43. Ram, A.; Dutta, M.P.; Chakraborty, S.K. An Authentication Mechanism to Prevent Various Security Threats in Software-Defined Networking Using AVISPA. *J. Sci. Ind. Res.* **2024**, *83*, 977–988.
44. Banerjee, S.; Odelu, V.; Das, A.K.; Srinivas, J.; Kumar, N.; Chattopadhyay, S.; Choo, K.-K.R. A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment. *IEEE Internet Things J.* **2019**, *6*, 8739–8752. [CrossRef]
45. Lopez Becerra, J.M.; Iovino, V.; Ostrev, D.; Skrobot, M. On the Relation between SIM and IND-RoR Security Models for PAKEs. In *Proceedings of the International Conference on Security and Cryptography*; SciTePress: Setubal, Portugal, 2017.
46. Sihare, S.R. Qubit and Bit-Based Quantum Hybrid Secret Key Generation. *Eur. Phys. J. D* **2022**, *76*, 222. [CrossRef]
47. Fiorini, F.; Pagano, M.; Garroppo, R.G. QBER Statistics to Determine Eavesdropper Position in Fiber-Based Quantum Key Distribution. In *IEEE INFOCOM 2025-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6.
48. Khan, M.N.; Rahman, H.U.; Hussain, T.; Yang, B.; Qaisar, S.M. Enabling Trust in Automotive IoT: Lightweight Mutual Authentication Scheme for Electronic Connected Devices in Internet of Things. *IEEE Trans. Consum. Electron.* **2024**, *70*, 5065–5078. [CrossRef]
49. Khashan, O.A.; Khafajah, N.M. Efficient Hybrid Centralized and Blockchain-Based Authentication Architecture for Heterogeneous IoT Systems. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 726–739. [CrossRef]
50. Huang, H.; Zheng, J.; Chen, Z.; Zhao, S.; Wu, H.; Yu, B.; Liu, Z. Review of Modular Multiplication Algorithms over Prime Fields for Public-Key Cryptosystems. *Cryptography* **2025**, *9*, 46. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.