Journal of Computer Networks and Communications

WILEY

RESEARCH ARTICLE OPEN ACCESS

PQ-AuthN-IIoT: A Lightweight, LWE-Based Postquantum and Privacy-Preserving Mutual Authentication Scheme for Resource-Constrained Industrial IoT Systems

Tinashe Magara | Mampilo Phahlane

Department of Information Systems, College of Science, Engineering and Technology, University of South Africa, Pretoria 0003, South Africa

Correspondence: Tinashe Magara (tinashenosh@gmail.com)

Received: 4 November 2025 | **Revised:** 21 January 2026 | **Accepted:** 14 February 2026

Academic Editor: Debabrata Singh

Keywords: BAN logic | industrial IoT | LWE | mutual authentication | privacy preserving | quantum security | ROM analysis

ABSTRACT

The rapid expansion of the Industrial Internet of Things (IIoT) presents pressing challenges for secure, efficient, and privacy-preserving communication among users, sensors, and cloud infrastructures. Existing lightweight authentication schemes, primarily based on classical cryptographic assumptions, are increasingly vulnerable to the emerging threat of quantum computing. To address these challenges, we propose a lightweight, quantum-resilient, and privacy-preserving mutual authentication scheme tailored to the IIoT ecosystem. The proposed scheme integrates the learning with errors (LWE) assumption to achieve post-quantum secure authentication and identity protection, hash functions for message integrity, and ephemeral elliptic curve Diffie–Hellman (ECDH) to provide classical forward secrecy within a hybrid security model. A novel use of ephemeral pseudonyms further enhances unlinkability and resilience against traceability attacks. The security of the scheme is established through informal analysis, covering resistance to forgery, impersonation, replay, man-in-the-middle, and key compromise impersonation attacks, and through formal analysis in both the random oracle model (ROM) and BAN logic, proving mutual authentication and secrecy properties. Performance evaluation demonstrates that the scheme achieves low computational cost for resource-constrained sensors (≈ 4 ms) and practical communication overhead while maintaining comprehensive security features superior to existing solutions. These results highlight that the proposed scheme provides a robust, efficient, and deployable framework for postquantum secure authentication in IIoT ecosystems.

1 | Introduction

The Internet of Things (IoT) and its industrial counterpart, the Industrial Internet of Things (IIoT), have become central to the digital transformation of modern society [1]. These interconnected systems facilitate real-time data collection, analysis, and control across diverse sectors, including smart cities, healthcare, manufacturing, and critical infrastructure [2]. An IoT ecosystem is characterized by a wide array of devices, often equipped with sensors and actuators, that communicate over resource-constrained networks to automate tasks and inform decision-making [3]. However, the open and heterogeneous nature of these networks introduces significant security and privacy vulnerabilities, particularly concerning inter-device communication and user interaction [4].

A foundational requirement for securing IoT environments is mutual authentication [5], which ensures that each communicating entity can verify the legitimacy of its counterpart before exchanging sensitive information. Designing robust authentication schemes for IoT is inherently challenging due to the severe resource constraints of edge devices, such as limited memory,

processing power, and energy [6, 7]. In this context, therefore, effective authentication protocols must be lightweight, minimizing computational and communication overhead.

The rapid advancement of quantum computing poses a significant threat to classical cryptographic algorithms [8]. Algorithms such as Shor's and Grover's have demonstrated the potential to efficiently break traditional encryption and digital signature schemes [9]. This imminent threat necessitates the development of quantum-resilient cryptographic solutions to ensure long-term security in the postquantum era [10].

Simultaneously, privacy preservation is a critical concern in IoT-based mutual authentication [11]. Device communications often reveal identifiable information, such as unique IDs or behavioral patterns, which can be exploited for tracking, profiling, or impersonation [12]. An effective authentication scheme must therefore guarantee anonymity, unlinkability, and minimal metadata exposure [13, 14].

While numerous authentication schemes have been proposed, most fail to simultaneously satisfy the trifecta of lightweight design, quantum-resilience, and privacy preservation under the real-world constraints of IoT/IIoT deployments [15]. This study addresses this gap by proposing a novel, a lightweight, quantum-resilient, and privacy-preserving mutual authentication framework that is secure, efficient, and resilient to both classical and quantum attacks.

The proposed scheme adopts a hybrid security model. While the authentication, identity protection, and session binding mechanisms are fully postquantum secure under the learning with errors (LWE) assumption, the session key establishment phase employs ephemeral elliptic curve Diffie–Hellman (ECDH) to provide forward secrecy against classical adversaries. This design choice reflects a pragmatic trade-off between postquantum security and computational efficiency for resource-constrained IIoT devices.

The main contributions are as follows:

- We propose a novel lightweight mutual authentication scheme tailored for resource-constrained IoT/IIoT devices, which offers postquantum security by employing lattice-based cryptographic primitives. The scheme ensures robustness against both classical and quantum adversaries through the use of hard lattice assumptions.
- The proposed construction follows a lightweight reconciliation-based authentication structure, integrating error reconciliation techniques to significantly reduce computational and communication overhead.
- We establish a mutual authentication mechanism based on ephemeral session keys, random nonces, and secure identity binding. The scheme achieves resistance to impersonation, replay, and man-in-the-middle (MITM) attacks, while ensuring forward secrecy in dynamic session exchanges.
- The scheme supports essential privacy-preserving features, including device anonymity and session unlinkability, through the generation of dynamic pseudonyms and session-specific identifiers.
- We conduct a comprehensive security evaluation, including formal analysis and informal analysis of privacy and attack resilience. The scheme is proven secure against a broad class of classical and postquantum adversaries.
- We provide a detailed performance assessment and comparison with state-of-the-art authentication schemes. The evaluation includes functional capabilities, computational cost, and communication overhead, demonstrating that the proposed scheme achieves enhanced efficiency and stronger security guarantees than existing approaches.

1.1 | Article Structure

The remainder of this study is organized as follows. Section 2 reviews the related literature. Section 3 presents the proposed system architecture along with the adversary model. Section 4 introduces the quantum preliminaries required for the protocol design. Section 5 details the proposed lightweight, quantum-resilient mutual authentication scheme for IoT and IIoT resource-constrained devices. Section 6 provides a comprehensive security analysis of the scheme. Section 7 evaluates its performance and compares the results with existing approaches. Finally, Section 8 concludes the study and outlines directions for future research.

2 | Related Work

The IoT continues to evolve rapidly, introducing billions of interconnected devices across industrial, healthcare, and smart city domains [16]. However, the heterogeneous and resource-constrained nature of these devices presents serious security and privacy challenges [17]. Lightweight mutual authentication has emerged as a foundational requirement to secure IoT environments [18]. Additionally, the rise of quantum computing necessitates revisiting cryptographic assumptions, as traditional public key schemes such as RSA and ECC are vulnerable to quantum attacks [19].

This section reviews the progression of lightweight authentication schemes in the literature, with an emphasis on their cryptographic foundations, efficiency, privacy guarantees and resilience to classical and quantum attacks. The review is organized chronologically to illustrate the evolution of authentication mechanisms and to motivate the need for our proposed architecture, which addresses the combined requirements of quantum resilience, mutual authentication, and privacy preservation tailored for constrained IoT environments.

Earlier schemes such as those by [20, 21] proposed mutual lightweight authentication frameworks for IoT using symmetric cryptography and ECC. These works focused primarily on reducing communication and computation overhead to meet the constraints of low-powered devices. Notably [20], proposed a lightweight ECC-based scheme offering mutual authentication and anonymity, though it remained vulnerable to unlinkability and MITM attacks under certain conditions. Similarly [21], designed an ECC authentication model for smart devices, emphasizing biometric privacy. While efficient, these models rely on ECC, which is susceptible to Shor's algorithm in the quantum era.

As postquantum cryptography (PQC) gained traction, researchers explored lattice-based primitives like LWE and its module learning with rounding (MLWR) [22, 23, 24]. Introduced

a lattice-based key exchange scheme designed for lightweight edge devices. Their scheme demonstrated strong quantum resistance and formal security under standard lattice assumptions. However, high-dimensional lattices still imposed computational burdens.

Privacy preservation emerged as a parallel focus; as shown in [25], an identity-based anonymous authentication scheme was introduced, employing dynamic pseudonyms and unlinkable session tokens to conceal user identities and enhance conditional privacy. While effective against basic traceability threats, the scheme does not incorporate postquantum cryptographic primitives, thereby exposing it to quantum-capable adversaries. Additionally, similar to other certificateless aggregate signature (CLAS) frameworks, it remains vulnerable to signature forgery attacks, limiting its applicability in real-world VANET deployments. Similarly [26], proposed privacy-preserving mutual authentication for fog-based IoT using hash-based tokens. Though efficient, it lacked provable resilience to quantum-capable adversaries.

Recent works began to integrate PQC schemes with classical protocols [27]. In [28] proposed a lightweight and secure authentication scheme for IoT networks operating within a publish–subscribe fog computing architecture. The hybrid approach integrates the efficiency of the elliptic curve Diffie–Hellman ephemeral (ECDHE) key exchange with preshared keys (PSK), aiming to balance low computational overhead with enhanced security. While the scheme benefits from the established maturity of ECC and introduces perfect forward secrecy (PFS), it is limited by increased handshake latency arising from dual verification procedures, and it does not incorporate mechanisms to resist quantum era adversaries. In [29], the authors proposed a hash-based privacy-preserving authentication scheme leveraging forward-secure hash chains and ephemeral tokens to ensure lightweight privacy in vehicular networks. While the approach provided strong anonymity and low computational overhead, it faced significant scalability limitations in large-scale V2X deployments. Moreover, the lack of architectural optimization introduced operational inefficiencies when compared to more structured solutions like SCMS. Table 1 provides an overview of existing authentication schemes, highlighting their main characteristics and inherent limitations.

While existing schemes provide important contributions, several persistent gaps remain:

- Most lightweight authentication schemes rely on ECC or symmetric primitives that are not secure against quantum adversaries.
- Privacy-preserving schemes often overlook forward secrecy or are not resistant to traceability under active attacks.
- Postquantum schemes, particularly lattice-based ones, often impose computational costs unsustainable for ultra-constrained devices.
- No current scheme achieves an integrated solution that is simultaneously lightweight, quantum resilient, privacy preserving, mutually authenticating, and optimized for the cloud IoT architecture.

Most conventional schemes fail to meet the combined demands of quantum resistance, low computation overhead, strong mutual authentication, and privacy preservation, all while being feasible for resource-limited IoT systems. As quantum computing advances and IoT continues to proliferate across industrial and critical infrastructures, there is a pressing need for new techniques that bridge these gaps.

Therefore, an ideal scheme must be lightweight, resist classical and quantum attacks, provide mutual authentication, ensure anonymity and unlinkability, and be explicitly designed for IoT edge cloud architectures. None of the existing works collectively satisfy these criteria.

To address these limitations, we propose a novel, lightweight, quantum-resilient, and privacy-preserving mutual authentication scheme tailored for IoT environments. The proposed architecture integrates lattice-based postquantum primitives with hash-based authentication, lightweight cryptographic operations, and dynamic pseudonym mechanisms to provide secure, efficient, and privacy-aware authentication across device gateway cloud infrastructures.

3 | Proposed System and Adversary Model

Figure 1 shows the proposed system model. The proposed architecture shows the IIoT ecosystem, which comprises three entities: The industrial IoT user ($\mathcal{U}_i$), the trusted cloud server ($\mathcal{CS}$), and industrial IoT sensors ($\mathcal{S}_i$).

- The industrial IoT user ($\mathcal{U}_i$): IIOT Users use mobile devices to access industrial systems. After authentication, users can access IoT sensor data and receive analytic outputs from the CS.
- Trusted cloud server ($\mathcal{CS}$): The cloud server is a trusted entity with sufficient computing and storage capacity. To enable mutual authentication, industrial IoT users and sensors must first register with the cloud server. After mutual authentication, the cloud server stores data from Industrial IoT sensors and employs AI to provide users with analysis and decision-making.
- Industrial IoT sensors ($\mathcal{S}_i$): Smart industries rely on resource-constrained IIoT sensors. These sensors collect real-time information on industrial indicators such as moisture content, temperature, pH, and so on.
- Gateway: The gateway serves as a communication channel by facilitating the exchange of data between all three entities.

3.1 | Adversary Model

We assume that the adversary ($\mathcal{A}$) possesses advanced capabilities, including both classical and quantum attack vectors. Specifically, the adversary is capable of the following:

- Insider attacks: ($\mathcal{A}$) can act as a legitimate, certified participant in the network, such as an IoT sensor, gateway, or cloud server that has been compromised.
- Control of communication channels: ($\mathcal{A}$) can fully control public communication channels. This includes the ability to:
  - Eavesdrop on messages exchanged between participants.
  - Intercept, modify, delete, inject, or replay scheme messages.

TABLE 1 | Summary of existing schemes.

Author	Approach	Key features	Limitations
[20]	ECC-based mutual authentication	• Session key agreement • Anonymity	• ECC is not quantum safe • Replay attacks
[21]	Biometric + ECC	• Lightweight • Biometric privacy	• Quantum vulnerable • Limited scalability
[24]	Lattice-based	• Quantum safe	• High computational cost on constrained devices
[25]	Identity-based	• Privacy preserving	• No postquantum resistance
[26]	Client-server model + symmetric encryption	• Lightweight mutual authentication • Symmetric session key establishment	• Classical only primitives (no postquantum resistance) • Centralized architecture
[28]	Fog computing + MQTT protocol + ECDHE PSK	• Lightweight mutual authentication • Perfect forward secrecy (PFS) • Certificate-free security	• Classical security only (no postquantum resistance) • Limited privacy preservation (no anonymity/unlinkability) • Assumes secure preshared key distribution
[29]	Certificate-based vehicular PKI (VPKI)	• Authenticated vehicle communication • Certificate revocation mechanism • Architectural aimplification	• Classical cryptography (vulnerable to quantum attacks) • High infrastructure complexity (pre-enhancement) • Privacy is still partially dependent on revocation mechanisms

- Launch MITM attacks between any two parties (e.g., device ⟷ gateway, gateway ⟷ server).

- Limited physical access: ($\mathcal{A}$) may capture IoT devices or gateways physically but cannot extract secure credentials protected by tamper-resistant hardware.
- Privacy attacks: ($\mathcal{A}$) may attempt to trace or identify IoT devices by analyzing communication metadata or linking sessions. These attacks are mitigated using:
  - Ephemeral pseudonyms.
  - Session unlinkability techniques.
  - Privacy-preserving authentication.
- Resource-based attacks**:** ($\mathcal{A}$) can attempt to exhaust the resources of constrained IoT devices by:
  - Triggering repeated authentication requests.
  - Launching DoS or DDoS attacks.
  - However, lightweight cryptographic operations and rate-limiting countermeasures reduce the impact of such attempts.
  - Quantum computational power: ($\mathcal{A}$) may have access to quantum computing capabilities.
- Despite the assumptions of the adversary capabilities, the ($\mathcal{A}$) cannot perform the following:
  - Derive private keys, nonces, or session tokens from public parameters.
  - Break the postquantum cryptographic primitives used.
  - Compute pre-images or collisions for secure hash functions within practical time.

3.2 | Design Goals

The primary objective of this work is to design and establish a mutual authentication scheme suitable to the resource-constrained nature of IoT environments, while also providing resistance against potential quantum attacks. The proposed architecture is based on five basic design concepts and is intended to meet the critical security and efficiency requirements of IoT devices. It offers secure mutual authentication, protects user privacy, and is viable for devices with limited computational and energy resources. The system architecture is created with the following major goals:

- Quantum resilience: To develop a cryptographic framework that is secure against adversaries equipped with quantum computational capabilities, thereby ensuring long-term robustness and viability in the postquantum era.
- Lightweight: To construct a scheme suitable for deployment on resource-constrained IoT devices by minimizing computational, memory, and energy overhead, enabling seamless integration with low-power embedded systems such as microcontrollers and smart industrial sensors.
- Mutual authentication: To ensure secure, bidirectional authentication between communicating entities, thereby preventing impersonation and unauthorized access.

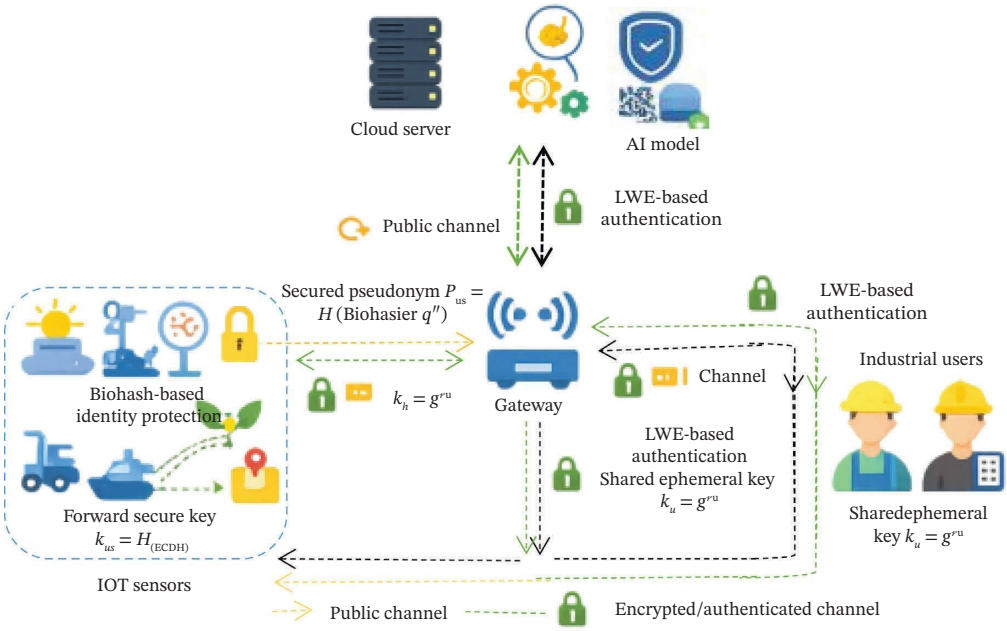

FIGURE 1 | Proposed system architecture.

- Privacy preservation: To protect the identity and communication patterns by preventing traceability and ensuring unlinkability across authentication sessions.
- Low computational overhead: To design an efficient scheme that minimizes processing and communication costs, facilitating real-time authentication in practical IoT deployments without compromising security.
- In this work, a scheme is considered lightweight if it satisfies the following criteria: (i) computational cost suitable for microcontroller-class devices; (ii) limited memory footprint; and (iii) low communication overhead compatible with low-bandwidth industrial networks.

3.3 | Design Rationale for Hybrid Key Establishment

Our proposed system does not currently implement fully postquantum key encapsulation mechanisms (KEMs), such as those based on Kyber or NTRU. This design choice was necessitated by the severe resource constraints characteristic of ultra-constrained IIoT sensors, where the comparatively higher communication overhead, memory footprint, and implementation complexity of these postquantum algorithms remain prohibitive. Instead, ephemeral ECDH was selected as the core key exchange mechanism. This option provides a rigorously optimized and lightweight primitive, delivering practical forward secrecy and maintaining full compatibility with established industrial cryptographic deployments. Consequently, the present architecture adopts a hybrid strategy. This approach guarantees immediate operational deployability within existing ecosystems while establishing a clear, seamless migration path for the future integration of postquantum KEMs, once their performance and efficiency characteristics align with the demands of the most constrained IIoT environments.

4 | Quantum Preliminaries

In this section, we describe the concepts and mathematical foundations that are used in the development of the proposed lightweight, quantum-resilient, and privacy-preserving mutual authentication, including the adversary model and notations.

4.1 | LWE: Cryptosystem

The LWE problem was first introduced by Oded Regev in 2005 and has been seen as the cornerstone of modern cryptography, especially in the context of securing data against future quantum computers [30]. The concrete of the LWE is based on the challenge of solving equations that have been deliberately "noised" or distorted. Let a secret vector $\mathfrak{z} \in \mathbb{Z}_q^n$ and a set of linear equations be defined as: $\mathbf{A}_i \cdot \mathfrak{z} + e_i = \mathbf{B}_i \bmod q$ where

- $\mathbf{A}_i$ is a known matrix with entries in $\mathbb{Z}_q$,
- e_i is a small error vector sampled from a noise Gaussian distribution,
- $\mathbf{B}_i$ is the resulting vector.

The objective is to find $\mathfrak{z}$ given $(\mathbf{A}_i, \mathbf{B}_i)$. The presence of the error vector e_i makes this problem computationally hard, forming the basis of the LWE cryptosystem.

4.2 | One-Way Hash Function

Consider a hash function $\hbar : \{0,1\}^* \longrightarrow \{0,1\}^n$ that accepts an arbitrary-length binary string $x \in \{0,1\}^*$ as input and outputs an n-bit hash value $y \in \{0,1\}^n \therefore y = \hbar\{x\}$.

Let $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Hash}}(t)$ denote the advantage of an adversary $\mathcal{A}$ in finding a collision in the hash output. We define, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Hash}}(t) = \underbrace{\Pr}_{x, x' \overleftarrow{\circ} \mathcal{A}}[x \neq x' \bigwedge \hbar(x) = \hbar(x')]$ where $(x, x' \overleftarrow{\circ} \mathcal{A})$ denotes that the pair is generated at random by adversary $\mathcal{A}$. We say that $\mathcal{A}$ is a (ε, t) adversary against the

collision resistance of $\hbar(\cdot)$ if, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Hash}}(t) \leq \varepsilon$ and the running time of $\mathcal{A}$ does not exceed t.

4.3 | Ephemeral ECDH

The ephemeral ECDH cryptographic protocol uses the algebraic structure of elliptic curves over finite fields to enable secure key exchange across an insecure channel.

Let $F_\mathfrak{p}$ denote a finite field of prime order $\mathfrak{p}$. Define an elliptic curve E over $F_\mathfrak{p}$ by the Weierstrass equation: $E(F_\mathfrak{p}): \; y^2 \equiv x^3 + ax + b (\mathrm{mod}) \mathfrak{p} \; : \; a, b \in F_\mathfrak{p} | 4a^3 + 27b^2 \neq 0 \bmod \mathfrak{p}$

Let $G \in E(F_\mathfrak{p})$ be a publicly agreed upon base point generator of prime order n such that

- $[G] = \{O, G, 2G, \; \ldots, (n \; - \; 1)G\}$,
- The curve order satisfies $|E(F_\mathfrak{p})| = \hbar n$, where $\hbar \in \mathbb{Z}^+$ is the co factor.

4.4 | Bio-Hashing

Bio-hashing is a biometric feature protection strategy that generates a non-invertible binary representation by combining a biometric sample (e.g., a facial image, fingerprint) with user-specific pseudorandom vectors. Then, the bio-hashing functions are defined as follows: $\mathrm{Y}_\mathfrak{i} = (\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3 \ldots \mathfrak{y}_n) \in \mathbb{R}^n$.

- Pseudorandom vector generation: Given a secret hash key $\mathcal{YK}$, generate m pseudorandom vectors—$\mathfrak{r}_\mathfrak{i} \in \mathbb{R}^m, \mathfrak{i} = 1, 2, 3, \; \ldots, n | \mathfrak{r}_1, \quad \mathfrak{r}_2, \quad \mathfrak{r}_3, \; \ldots, \mathfrak{r}_n$ are linearly independent
- Orthonormalization: Applying Gram–Schmidt orthonormalization to $\{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \; \ldots, \mathfrak{r}_n\}$, we obtain $\mathfrak{a}_\mathfrak{i} \in \mathbb{R}^m, \langle \mathfrak{a}_\mathfrak{i}, \quad \mathfrak{a}_j \rangle = \begin{cases} 1, \mathfrak{i} = j \\ 0, \mathfrak{i} \neq j \end{cases}$
- Projection and thresholding: $\forall$ orthonormal vector $\mathfrak{a}_\mathfrak{i}$, we compute the scalar projection of $\mathfrak{y}$ onto $\mathfrak{a}_\mathfrak{i}$: $\mathfrak{b}_\mathfrak{i} = \langle \mathfrak{y}, \mathfrak{a}_\mathfrak{i} \rangle$ and we binarize using a fixed threshold $\psi \in \mathbb{R}: \mathfrak{c}_\mathfrak{i} = \begin{cases} 1, \mathfrak{a}_\mathfrak{i} \leq \psi \\ 0, \mathfrak{a}_\mathfrak{i} > \psi \end{cases}$
- Biohash code: Therefore the final Biohash is given as the binary vector as follows: $\mathrm{Biohash}_{\mathcal{YK}}(\mathfrak{y}) = (\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3, \; \ldots \mathfrak{c}_n) \in \{0, 1\}^n$

4.5 | Notations and Symbols

Table 2 summarizes the notation and definitions used in this study.

5 | Proposed Mutual Authentication Scheme

In this section, we introduce a lightweight, quantum-resilient, and privacy-preserving mutual authentication. The scheme integrates LWE for quantum resistance, hash functions for integrity, ephemeral ECDH for forward secrecy, and bio-hashing to ensure robustness against classical and quantum adversaries.

5.1 | The System Setup Phase

The trusted cloud server ($\mathcal{CS}$) initializes system parameters:

- Let security parameter be λ
- Chooses modulus q, dimension n and error distribution χ
- Generates public matrix $\mathbf{A} \in \mathbb{Z}_q^{\mathrm{nxn}}$
- Selects a master secret $\mathfrak{s} \in \mathbb{Z}_q^n$ and publishes: $\mathfrak{p}\mathfrak{k} = (\mathbf{A}, \mathbf{A} \cdot \mathfrak{s} + e \bmod q), \mathfrak{s}\mathfrak{k} = \mathfrak{s}$ where $e \longrightarrow \chi^n$ and public parameters: $\Delta = \{q, n, \mathbf{A}, H(\cdot), \hbar(\cdot), G, \mathrm{Biohash}(\cdot)\}$

Where H, $\hbar$ are secure hash functions, G is an elliptic curve base point and Biohash(·) is the biometric protection primitive. Each entity $E \in \{\mathcal{U}_\mathfrak{i}, \mathcal{S}_\mathfrak{i}, \mathcal{CS}\}$ generates an ephemeral random vector $x_\mathrm{E} \in \mathbb{Z}_q^n$ for each session and computes the corresponding ephemeral public value as $B_E = x_E^* \cdot A (\bmod q)$.

The timestamps T_1, T_2, T_3 and T_4 are considered valid only if they are received within a predefined acceptance window ΔT. To account for network latency and processing delays inherent in resource-constrained IIoT environments, ΔT is conservatively set to approximately 2–5 s. This tolerance ensures that minor clock drift among participating entities does not affect the correctness or security of the protocol, as only messages received within the allowed time window are processed. Any timestamp that falls outside ΔT leads to the immediate and safe termination of the session, without altering the system state, thereby preserving protocol integrity and security guarantees. In networks with significant clock drift, lightweight time resynchronization protocols (e.g., NTP-lite or gateway-assisted resynchronization) can be employed without modifying the authentication protocol.

5.2 | Industrial IoT User (U_i) Registration Phase

- $\mathcal{U}_\mathfrak{i}$ submits identity $ID_{\mathcal{U}_\mathfrak{i}}$, and biometric sample $\mathfrak{y}$.
- $\mathcal{CS}$ computes biohash: $BH_{\mathcal{U}_\mathfrak{i}} = \mathrm{Biohash}_{\pi_K}(\mathfrak{y})$ where π_K is a secret projection key.
- $\mathcal{CS}$ generates private credential: $\mathfrak{s}\mathfrak{k}_{\mathcal{U}_\mathfrak{i}} = (\mathfrak{r}_{\mathcal{U}_\mathfrak{i}} + H(ID_{\mathcal{U}_\mathfrak{i}}) \cdot \mathfrak{s}) \bmod q$ with random $\mathfrak{r}_{\mathcal{U}_\mathfrak{i}} \in \mathbb{Z}_q^n$.

5.3 | The Industrial IoT Sensors (S_i) Registration Phase

- Sensor $\mathcal{S}_\mathfrak{i}$ provides $ID_{\mathcal{S}_\mathfrak{i}}$
- $\mathcal{CS}$ generates key pair: $\mathfrak{s}\mathfrak{k}_{\mathcal{S}_\mathfrak{i}} = (\mathfrak{r}_{\mathcal{S}_\mathfrak{i}} + H(ID_{\mathcal{S}_\mathfrak{i}}) \cdot \mathfrak{s}) \bmod \mathfrak{p} \; \mathfrak{p}\mathfrak{k}_{\mathcal{S}_\mathfrak{i}} = \mathfrak{r}_{\mathcal{S}_\mathfrak{i}}^* \cdot \mathbf{A}$

5.4 | Cloud Server Registration

$\mathcal{CS}$ holds the global master key $\mathfrak{s}$ and public database of $(ID_\mathrm{E}, \mathfrak{p}\mathfrak{k}_\mathrm{E})$ for all registered entities $E \in \{\mathcal{U}_\mathfrak{i}, \mathcal{S}_\mathfrak{i}\}$.

5.5 | Mutual Authentication Scheme

Authentication occurs between $\mathcal{U}_\mathfrak{i} \longleftrightarrow \mathcal{CS} \longleftrightarrow \mathcal{S}_\mathfrak{i}$ via the gateway.

Each session employs ephemeral pseudonyms and postquantum challenge response.

Step I: Login request: $\mathcal{U}_\mathfrak{i} \longrightarrow \mathcal{CS}$

- $\mathcal{U}_\mathfrak{i}$ generates ephemeral pseudonym: $\mathrm{PID}_{\mathcal{U}_\mathfrak{i}} = \hbar(ID_{\mathcal{U}_\mathfrak{i}} || \mathrm{nonce} || T_1)$

TABLE 2 | Notations.

Symbol	Description
$\mathcal{U}_i$	Industrial IoT $\mathcal{U}_i$, who accesses IoT data and analytics through mobile/edge devices
$\mathcal{S}_i$	Industrial IoT Sensor $\mathcal{S}_i$, a resource-constrained sensor node collecting industrial data
$\mathcal{CS}$	Trusted cloud server responsible for system setup, parameter generation, credential issuance registration, authentication, and data analytics
$ID_{\mathcal{U}_i}$, $ID_{\mathcal{S}_i}$	Permanent identity of user $\mathcal{U}_i$. and sensor $\mathcal{S}_i$, respectively
$\mathrm{PID}_{\mathcal{U}_i}$	Ephemeral pseudonym of user $\mathcal{U}_i$, generated per session to preserve privacy
$\mathrm{PID}_{\mathcal{S}_i}$	Ephemeral pseudonym of sensor $\mathcal{S}_i$, generated per session to ensure unlinkability
$\mathfrak{s}$	Master secret key held by the $\mathcal{CS}$
$\mathfrak{sk}_{\mathcal{W}}$	Secret key of entity $\mathcal{W} \in \{\mathcal{U}_i, \mathcal{S}_i\}$ generated from the master secret and entity identity
$\mathfrak{pk}_{\mathcal{W}}$	Public key of entity $\mathcal{W}$
$\mathbf{A}$	Public matrix in $\mathbb{Z}_q^{nxn}$ used for LWE-based cryptographic construction
q	Large modulus defining the finite field $\mathbb{Z}_q$
n	Dimension parameter in the LWE problem (security parameter)
χ	Error distribution (discrete Gaussian) used in LWE hardness assumption
$r_{\mathcal{W}}$	Random vector associated with entity E used in key generation
$\|\|$	Concatenation operation
$\sigma_{\mathcal{U}_i}$	Authentication signature-like response generated by $\mathcal{U}_i$ during login
$\sigma_{\mathcal{S}_i}$	Authentication response generated by $\mathcal{S}_i$ during $\mathcal{CS}$ challenge verification
$\sigma_{\mathcal{CS}}$	Authentication token generated by $\mathcal{CS}$ to confirm mutual authentication
$\delta_{\mathcal{CS}}$	Challenge value computed by $\mathcal{CS}$ for verifying sensor response
T_1, T_2, T_3, T_4	Timestamps used to ensure freshness and prevent replay attacks
$H(\cdot)$	One-way hash function used for pseudonym generation and message authentication codes
$\hbar(\cdot)$	Collision-resistant hash function used in session key derivation
Biohash(·)	Bio-hashing function used to protect biometric features of $\mathcal{U}_i$
G	Base point generator of elliptic curve used in ECDH key exchange
x_i	Ephemeral private scalar chosen by entity i for ECDH key computation
P_i	Ephemeral public point computed as $P_i = x_i \cdot G$
K	Session key derived after mutual authentication using LWE, pseudonyms, and ECDH contribution
Δ	Public parameters: $\{q, n, \mathbf{A}, H, \hbar, G,$ Biohash$\}$

- Computes authentication tag: $\sigma_{\mathcal{U}_i} = (\mathfrak{sk}_{\mathcal{U}_i} + \mathrm{H}(\mathrm{PID}_{\mathcal{U}_i} \| \mathrm{T}_1) \cdot r_{\mathcal{U}_i}) \mod q$
- Sends $M_1 = \{\mathrm{PID}_{\mathcal{U}_i}, \sigma_{\mathcal{U}_i}, T_1\}$

Step II: Challenge: $\mathcal{CS} \longrightarrow \mathcal{S}_i$

- $\mathcal{CS}$ verifies $\mathcal{U}_i$ by checking the LWE relation: $\sigma_{\mathcal{U}_i} \cdot \mathrm{A} \stackrel{?}{=} \mathfrak{pk}_{\mathcal{U}_i} + H(\mathrm{PID}_{\mathcal{U}_i} \| T_1) \cdot (A \cdot \mathfrak{s})$, if fails fails or T_1 stale $\longrightarrow$ abort
- If valid, $\mathcal{CS}$ generates challenge for $\mathcal{S}_i$: $\sigma_{\mathcal{CS}} = H(ID_{\mathcal{S}_i} \| T_2)$
- Sends $M_2 = \{\sigma_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{U}_i}, T_2\}$ to the gateway for delivery to $\mathcal{S}_i$

Step III: Response: $\mathcal{S}_i \longrightarrow \mathcal{CS}$

- $\mathcal{S}_i$ computes response: $\sigma_{\mathcal{S}_i} = (\mathfrak{sk}_{\mathcal{S}_i} + \sigma_{\mathcal{CS}} \cdot r_{\mathcal{S}_i}) \mod q$
- Sends $M_3 = \{\sigma_{\mathcal{S}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_3\}$
- $\mathcal{CS}$ verifies using the same LWE-based relation

Step IV: Mutual confirmation: $\mathcal{CS} \longrightarrow \mathcal{U}_i$

- On successful verification of $\mathcal{S}_i$, $\mathcal{CS}$ authenticates back to $\mathcal{U}_i$ with: $\sigma_{\mathcal{CS}} = (\mathfrak{s} + H(\mathrm{PID}_{\mathcal{U}_i} \| \mathrm{PID}_{\mathcal{S}_i} \| \mathrm{T}_4) \cdot r_{\mathcal{CS}}) \mod q$
- Sends $M_4 = \{\sigma_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{S}_i}, T_4\}$

- $\mathcal{U}_i$ verifies the $\mathcal{CS}$ equation, achieving mutual authentication

5.6 | Session Key Establishment

After successful mutual authentication, both $\mathcal{U}_i$ and $\mathcal{S}_i$ derive a fresh session key with $\mathcal{CS}$ mediation.

- Ephemeral ECDH contribution: Each party selects random scalars x_i and computes: $P_i = x_i \cdot G$
- Exchange: The tuples $(P_{\mathcal{U}}, P_S)$ are exchanged via $\mathcal{CS}$
- Shared session key: $K = H(\mathrm{P}_{\mathcal{U}} \cdot x_S \| \mathrm{PID}_{\mathcal{U}_i} \| \mathrm{PID}_{S_i} \| T_1 \| T_4)$

This ensures the following:

- Forward secrecy (due to ECDH)
- Quantum resistance (via LWE hardness assumption)
- Privacy preservation (through pseudonyms and bio-hashing)

6 | Security Analysis

6.1 | Informal Analysis

6.1.1 | Resistance to Forgery Attack

During authentication, $\mathcal{U}_i$ computes $\sigma_{\mathcal{U}_i} = (\mathfrak{sk}_{\mathcal{U}_i} + H(\mathrm{PID}_{\mathcal{U}_i} \| T_1) \cdot r_{\mathcal{U}_i}) \bmod q$. $\mathcal{CS}$ verifies $\sigma_{\mathcal{U}_i} \cdot A \stackrel{?}{=} \mathfrak{pk}_{\mathcal{U}_i} + H(\mathrm{PID}_{\mathcal{U}_i} \| T_1) \cdot (A \cdot \mathfrak{s})$. Forgery requires $\mathcal{A}$ to generate a valid $\sigma_{\mathcal{U}_i}$ without knowing $\mathfrak{sk}_{\mathcal{U}_i}$ which is equivalent to solving the LWE problem.

6.1.2 | Resistance Against Impersonation Attack

To impersonate $\mathcal{S}_i$, $\mathcal{A}$ must produce a valid σ_{S_i} that satisfies $\mathcal{CS}$'s LWE-based check. Since $\mathrm{PID}_{S_i} = H(ID_{S_i} \| \mathrm{nonce} \| T_2)$ and σ_{S_i} depends on the hidden $\mathfrak{sk}_{S_i}$, impersonation is infeasible.

6.1.3 | Resistance Against User Identity Guessing Attacks

User identities ID_{S_i} are never transmitted. Instead, ephemeral pseudonyms $\mathrm{PID}_{\mathcal{U}_i} = H(ID_{\mathcal{U}_i} \| \mathrm{nonce} \| T_1)$ mask the real identity. Guessing $ID_{\mathcal{U}_i}$ requires inverting H, assumed collision resistant.

6.1.4 | Privileged Insider Attack

An insider at $\mathcal{CS}$ may view pseudonyms and tokens, but cannot recover master secret $\mathfrak{s}$. Since fresh pseudonyms and bio-hashing outputs are session specific, insiders cannot link multiple sessions or reconstruct $ID_{\mathcal{U}_i}$.

6.1.5 | Resistance to User Masquerade Attack

If $\mathcal{A}$ attempts to masquerade as $\mathcal{U}_i$ using stolen $\mathrm{PID}_{\mathcal{U}_i}$, they must still compute $\sigma_{\mathcal{U}_i}$. Without $\mathfrak{sk}_{\mathcal{U}_i}$, verification fails, preventing masquerade.

6.1.6 | Anonymity

Each session uses fresh pseudonyms ($\mathrm{PID}_{\mathcal{U}_i} \mathrm{PID}_{S_i}$). Even with multiple transcripts, $\mathcal{A}$ cannot correlate sessions, ensuring anonymity.

6.1.7 | Masquerading and Tampering Attacks

Tampering with transmitted tuples $(\mathrm{PID}_E, \sigma_E)$ invalidates the hash bound value Δ_E. $\mathcal{CS}$ rejects altered messages, preventing tampering.

6.1.8 | Resistance to Replay Attack

Messages contain timestamps (T_1, T_2, T_3, T_4). $\mathcal{CS}$ discards outdated tokens, and replayed values cannot pass freshness checks.

6.1.9 | Resistance to Traceability Attack

Since pseudonyms are rerandomized every session and unlinkable to ID_E, adversary $\mathcal{A}$ cannot track devices across sessions.

6.1.10 | Resistance to Stolen Verifier Attack

$\mathcal{CS}$ stores only public credentials. No verifier equivalent to a password hash exists, so compromising $\mathcal{CS}$ does not allow impersonation.

6.1.11 | Resistance to Unknown Key Share (UKS) Attack

The session key: $H(\mathrm{P}_{\mathcal{U}} \cdot x_S \| \mathrm{PID}_{\mathcal{U}_i} \| \mathrm{PID}_{S_i} \| T_1 \| T_4)$ is explicitly bound to both pseudonyms. Adversaries cannot convince $\mathcal{U}_i$ and $\mathcal{S}_i$ they share a key with different partners.

6.1.12 | Resistance to MITM Attack

MITM attacks require modifying messages M_1, M_2, M_3 and M_4. Since σ_E values are tied to Δ_E and $\mathfrak{sk}_E$, tampering causes verification to fail unless $\mathcal{A}$ solves LWE.

6.1.13 | Perfect Forward and Backward Secrecy

The session key derives from ephemeral randomness. Even if $\mathfrak{sk}_E$ or one session key is exposed, past and future keys remain secure.

6.1.14 | Resistance Against Known Session Specific Temporary Information Attacks

If temporary values are exposed, the adversary cannot reconstruct $\mathfrak{sk}_E$ or other sessions' keys. Thus leakage is session limited.

6.1.15 | Mutual Authentication

$\mathcal{CS}$ authenticates $\mathcal{U}_i$ ($\sigma_{\mathcal{U}_i}$), $\mathcal{CS}$ authenticates $\mathcal{S}_i$ (σ_{S_i}), $\mathcal{U}_i$ authenticates $\mathcal{CS}$ (σ_{CS}). All three must succeed, guaranteeing bidirectional trust.

6.1.16 | Resistance to Known Key Attack

Session keys K differ each run due to fresh $(\mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{S_i}, T_1, \ldots, T_4)$. Knowledge of one session key gives no advantage in future sessions.

6.1.17 | Resistance to Key Compromise Impersonation (KCI) Attack

Even if $\mathfrak{sk}_{\mathcal{U}_i}$ is compromised, $\mathcal{A}$ cannot impersonate $\mathcal{CS}$ or $\mathcal{S}_i$, since their tokens require distinct secrets. Verification equations ensure isolation of roles.

6.2 | Formal Analysis

In this section, we prove the robustness of our proposed scheme against known attacks through the random oracle model (ROM) and the "Burrows–Abadi–Needham" (BAN) logic.

6.2.1 | ROM Analysis

We demonstrate that the secrecy of the authentication tokens and the integrity of the identity binding rely exclusively on the hardness of the LWE problem, thereby guaranteeing post-quantum security. The forward secrecy of the derived session key is further contingent upon the hardness of the ECDH problem, which ensures classical PFS. To attain postquantum forward secrecy, a lattice-based KEM would be required in place of ECDH; the exploration of this enhancement is deferred to future work.

6.2.1.1 | Setup: Oracles and adversary model

a. Security parameters and assumptions

Public: $q, n,$ $\mathbf{A}$, $P = \mathfrak{z}^* \cdot \mathbf{A}$. Hash $\mathbf{H}$ modeled as random oracle. Hardness assumptions: LWE (postquantum) and classical ECDH.

b. Adversary $\mathcal{A}$ capabilities $\mathcal{A}$ is a probabilistic polynomial time that controls public channels and can query oracles:

- **Register** (E, ID_E, ...) for honest entities,
- **Send** (session, party,msg) to interactively run scheme instances,
- **Corrupt** (E) to obtain long-term secrets of E (subject to model),
- **Reveal** (session) to obtain session key of completed session, Random oracle queries $H(\cdot)$.
- **Test** (session) returns either the real session key of a fresh session or a uniformly random string (ROR game).

c. Goal

- Bound $\mathrm{ADV}_{\mathcal{A}}^{\mathrm{ROR}}$ the ability to distinguish real versus random session key and $\mathrm{ADV}_{\mathcal{A}}^{\mathrm{Forge}}$ the ability to forge a valid authentication token that passes.

6.2.1.2 | Unforgeability of Authentication Tokens (Forgery Game ⟶ LWE Reduction).

Forgery: $\mathcal{A}$ wins if it produces a fresh tuple $(\mathrm{PID}^*, P^*, B^*, T^*, \sigma^*)$ such that the verification equation holds: $\sigma^* \cdot A \equiv P^* + h^* P + \Delta^* B^* \pmod q$, with $h^* = H(ID^* \| P^*)$, $\Delta^* = H(P^* \| B^* \| \mathrm{PID}^* \| T^*)$ and the tuple was not honestly issued.

Theorem 1. *If $\mathcal{A}$ forges with non-negligible advantage ϵ, then there exists $\mathcal{B}$ that breaks LWE with non-negligible advantage $\approx \epsilon$.*

6.2.1.3 | Reduction

i. B receives an LWE instance $A, u = A\mathfrak{z}^* * + e \bmod q)$. Set $P = u$. Use A, P as system parameters.

ii. **B** simulates honest parties (registration, Send) for $\mathcal{A}$. For each honest E, choose r_E and set $P_E = r_E^* \mathbf{A}$. Program H to yield consistent h_E.

iii. To answer signing/token queries (requests to produce σ_E), **B** uses programmable random oracle H: pick x_E and set Δ_E so that a uniformly chosen σ_E satisfies the verification equation. (This is standard in ROM reductions for signature-like constructs.)

iv. When $\mathcal{A}$ outputs a fresh forgery $(P^*, \mathbf{B}^*, \Delta^*, \sigma^*)$, **B** has: $(\sigma^* - \Delta^* x^* - r^*)^* \mathbf{A} \equiv h^* P \pmod q$. If **B** can produce two forgeries with same P^* but different Δ (by rewinding/programming H2), it obtains two linear relations allowing elimination of r^* and extraction of a non-negligible relation on P that yields information on $\mathfrak{z}^*$ (standard lattice signature reduction technique). This contradicts LWE hardness.

v. Hence forging implies solving LWE with advantage $\approx \epsilon$ (modulo simulation abort probability ⟶ negligible loss). Therefore, we conclude that $\mathrm{ADV}_{\mathcal{A}}^{\mathrm{Forge}} \leq \mathrm{ADV}_{\mathrm{LWE}} + \mathrm{negl}(\lambda)$.

6.2.1.4 | Session Key Secrecy (ROM Game).

Given the session key derivation as follows:

$$\begin{aligned} \mathbb{k}_{\mathrm{LWE}} &= x_{\mathcal{U}_i}^* \mathrm{A} x_{S_i}, K_{EC} = u \cdot P_S^{EC} = v \cdot P_{\mathcal{U}}^{EC}, \\ K &= H\left(\mathbb{k}_{\mathrm{LWE}} \| \mathrm{Compress}(K_{EC}) \| \mathrm{PID}_{\mathcal{U}_i} \| \mathrm{PID}_{S_i} \| T_1 \| T_4\right). \end{aligned} \tag{1}$$

Game-based proof:

i. Hybrid H: Replace H with true ROM. Any distinguishing advantage against the real key versus random implies either distinguishing the ROM or learning the preimage input to H.

ii. Case analysis: To win test, $\mathcal{A}$ must either (a) recover $\mathbb{k}_{\mathrm{LWE}}$, or (b) recover K_{EC}, or (c) break the ROM H.

iii.

a. Recovering $\mathbb{k}_{\mathrm{LWE}}$: Given $B_{\mathcal{U}} = x_{\mathcal{U}}^* A$ and $B_S = x_S^* \mathrm{A}$, recovering $\mathbb{k}_{\mathrm{LWE}} = x_{\mathcal{U}}^* A x_S$ reduces to solving a short vector inner product extraction problem of the LWE hardness. A successful distinguisher yields an LWE solver.

b. Recovering K_{EC}: This reduces to solving ECDH (classical). In a postquantum conservative model, replace ECDH with a PQ KEM; otherwise, it guarantees classical PFS.

c. ROM break: Distinguishing without recovering (a) or (b) implies distinguishing ROM outputs (modeled negligible).

iv. Combine bounds: $\mathrm{ADV}_{\mathcal{A}}^{\mathrm{ROM}} \leq \mathrm{ADV}_{\mathrm{LWE}} + \mathrm{ADV}_{\mathrm{ECDH}} + \mathrm{ADV}_{\mathrm{ROM}} + \mathrm{negl}(\lambda)$

PFS Corollary. Because $x_{\mathcal{U}}$, x_S, u, v are ephemeral and erased, compromise of long-term keys $\mathfrak{z}\mathbb{k}_E$ does not enable recovery of past $\mathbb{k}_{\mathrm{LWE}}$ or K_{EC} (reduction to LWE/ECDH is still required).

6.2.1.5 | Replay, MITM, KCI, and Other Attacks (Reduction Summary)

- Replay: Freshness enforced by timestamps T_j and session bound Δ_E depends on T_j. Replayed messages fail freshness checks.
- MITM/tampering: Any modification changes B_E or fields in Δ_E; forging a matching σ_E is a forgery (reduction to LWE).

- KCI and known key: Session binding to PIDs and ephemeral randomness prevents an adversary from leveraging a compromised $\mathfrak{sk}_E$ to impersonate other entities without additional forgeries (again LWE).
- Insider and stolen verifier: $\mathcal{CS}$ stores public P_E and pseudonyms; there is no password-style verifier that an adversary can use to impersonate without breaking LWE or inverting ROM.

6.2.2 | BAN Logic Analysis

We present a concise BAN logic derivation proving mutual belief in a fresh session key K after $M_1 - M_4$. The notations used are as follows:

- **P** believes **X** written $\mathbf{P}| \equiv \mathbf{X}$.
- **P** sees **X** written $\mathbf{P} \lhd \mathbf{X}$.
- **P** said **X** written $\mathbf{P} \lhd \mathbf{X}$.
- #(**X**) means **X** is fresh.
- $\{\mathbf{X}\}_{\boldsymbol{K}}$ means **X** protected (signed/encrypted) with key **K**.
- $\mathbf{P}|\Longrightarrow\mathbf{X}$ means **P** controls/jurisdiction over **X**.

6.2.2.1 | Idealized Messages (BAN Logic)

1. $M_1: \ \mathcal{U}_i \longrightarrow \mathcal{CS}: \ \mathrm{PID}_{\mathcal{U}_i}, \{\mathbf{B}_{\mathcal{U}_i}, P_{\mathcal{U}_i}, T_1\}_{\mathfrak{sk}_{\mathcal{U}_i}}$, the token $\sigma_{\mathcal{U}_i}$ attests that $\mathcal{U}_i$ said $\mathbf{B}_{\mathcal{U}_i}, P_{\mathcal{U}_i}, T_1$.
2. $M_2: \ \mathcal{CS} \longrightarrow \mathcal{S}_i: \ \sigma_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{U}_i}, T_2$
3. $M_3: \ \mathcal{S}_i \longrightarrow \mathcal{CS}: \ \mathrm{PID}_{\mathcal{S}_i}, \{\mathbf{B}_{\mathcal{S}_i}, P_{\mathcal{S}_i}, T_1\}_{\mathfrak{sk}_{\mathcal{S}_i}}$
4. $M_4: \ \mathcal{CS} \longrightarrow \mathcal{U}_i: \ \mathrm{PID}_{\mathcal{S}_i}, \{\mathbf{B}_{\mathcal{CS}}, P_{\mathcal{CS}}, \ \ \mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_4\}_{\mathfrak{sk}_{\mathcal{CS}}}$

6.2.2.2 | BAN Assumptions

A1. $\mathcal{CS}|\equiv(\mathfrak{sk}_{\mathcal{U}_i}$ is $\mathcal{U}_i$'s secret).

A2. $\mathcal{CS}|\equiv$ ($\mathfrak{sk}_{\mathcal{S}_i}$ is $\mathcal{S}_i$'s secret).

A3. $\mathcal{CS}|\equiv(\mathfrak{sk}_{\mathcal{CS}}$ is $\mathcal{CS}$'s secret).

A4. $\mathcal{CS}|\equiv \#(T_1)$ and likewise parties believe their timestamps are fresh.

A5. $\mathcal{CS} \mid \Longrightarrow (\mathrm{PID}_{\mathcal{U}_i} \longmapsto ID_{\mathcal{U}_i})$—$\mathcal{CS}$ has jurisdiction on pseudonym binding from registration.

A6. Parties trust the verification relation and the ROM properties that bind Δ to the fields (modeled as part of message meaning).

Goal (G): After M_4, obtain mutual beliefs:

- $\mathcal{U}_i(|\equiv\mathcal{U}_i \overset{K}{\longleftrightarrow} \mathcal{S}_i)$—$\mathcal{U}_i$ believes it shares key K with $\mathcal{S}_i$
- $\mathcal{CS}|\equiv(\mathcal{U}_i \overset{K}{\longleftrightarrow} \mathcal{S}_i)$.
- Symmetrically for $\mathcal{S}_i$.

6.2.2.3 | BAN Derivation

Step 1—$\mathcal{CS}$ processes M_1.

- $\mathcal{CS} \lhd \{\mathbf{B}_{\mathcal{U}_i}, P_{\mathcal{U}_i}, T_1\}_{\mathfrak{sk}_{\mathcal{U}_i}}$ ($\mathcal{CS}$ sees the signed token).
- By the message–meaning rule: from A1 ($\mathcal{CS}$ believes only $\mathcal{U}_i$ knows $\mathfrak{sk}_{\mathcal{U}_i}$) and seeing $\{\cdot\}\mathfrak{sk}_{\mathcal{U}_i}$, $\mathcal{CS}$ derives: $\mathcal{CS} \mid \equiv \mathcal{U}_i \lhd (\mathbf{B}_{\mathcal{U}_i}, P_{\mathcal{U}_i}, T_1)$.
- By freshness: $\mathcal{CS}|\equiv\#(T_1)$.
- By the nonce-verification rule: $\mathcal{CS}|\equiv\mathcal{U}_i|\equiv(\mathbf{B}_{\mathcal{U}_i}, P_{\mathcal{U}_i}, T_1)$.
- $\mathcal{CS}$ believes $\mathcal{U}_i$ currently believes those fields: $\mathcal{U}_i$ recently said them.

Step 2—$\mathcal{CS}$ verifies and challenges $\mathcal{S}_i$ (M_2).

- $\mathcal{CS}$ constructs $\delta_{\mathcal{CS}}$ and sends M_2. No BAN inference is needed here other than $\mathcal{CS}$'s belief that it initiated a fresh challenge to $\mathcal{S}_i$.

Step 3—$\mathcal{CS}$ processes M_3

- $\mathcal{CS} \lhd \{\mathbf{B}_{\mathcal{S}_i}, P_{\mathcal{S}_i}, T_2\}_{\mathfrak{sk}_{\mathcal{S}_i}}$. With A2 and message–meaning: $|\equiv\mathcal{S}_i \lhd (\mathbf{B}_{\mathcal{S}_i}, P_{\mathcal{S}_i}, T_2)$.
- With freshness $\mathcal{CS}|\equiv\#(T_2)$, nonce-verification gives $\mathcal{CS}|\equiv\mathcal{S}_i|\equiv(\boldsymbol{B}_{\mathcal{S}_i}, P_{\mathcal{S}_i}, T_2)$.

Step 4—$\mathcal{CS}$ concludes both parties are genuine and computes session seed

From steps 1 and 3, $\mathcal{CS}$ believes $\mathcal{U}_i$ and $\mathcal{S}_i$ have produced the session inputs and that both are fresh. $\mathcal{CS}$ now believes (by jurisdiction of registration and binding to PID, A5) that both parties are legitimate participants in this session.

Formally: $\mathcal{CS}|\equiv(\mathcal{CS}|\equiv\mathcal{U}_i|\equiv\mathrm{session}_{\mathrm{inputs}}) \ \wedge \ (\mathcal{CS}|\equiv\mathcal{S}_i|\equiv\mathrm{session}_{\mathrm{inputs}})$

Step 5—$\mathcal{CS}$ issues M_4 (authentication to $\mathcal{U}_i$)

- $\mathcal{CS}$ sends $\{\mathbf{B}_{\mathcal{CS}}, P_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_4\}_{\mathfrak{sk}_{\mathcal{CS}}}$.
- On receipt, $\mathcal{U}_i \lhd \{...\}_{\mathfrak{sk}_{\mathcal{CS}}}$. By message meaning and A3 ($\mathcal{U}_i$ trusts only $\mathcal{CS}$ knows $\mathfrak{sk}_{\mathcal{CS}}$):

$$\mathcal{U}_i|\equiv\mathcal{CS}| \lhd (B_{\mathcal{CS}}, P_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_4). \tag{2}$$

- By freshness $\mathcal{U}_i|\equiv \#(T_4)$ (assumed) and nonce-verification:

$$\mathcal{U}_i|\equiv\mathcal{CS}| \equiv (\mathbf{B}_{\mathcal{CS}}, P_{\mathcal{CS}}, \mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_4). \tag{3}$$

Thus $\mathcal{U}_i$ believes $\mathcal{CS}$ currently believes that these values (hence the session) are valid.

Step 6—Deriving shared key belief

- $\mathcal{CS}$ has computed a session key K from the authenticated inputs and believes it is fresh and shared with the participants ($\mathcal{CS}$ knows the derivation includes $\mathrm{PID}_{\mathcal{U}_i}, \mathrm{PID}_{\mathcal{S}_i}, T_1, T_4$ and ephemeral contributions).
- From Steps 4 and 5 and jurisdiction ($\mathcal{CS}$ controls session key construction and binding), we apply the Jurisdiction rule: Since $\mathcal{CS}|\equiv(\mathcal{U}_i|\equiv\mathrm{session}_{\mathrm{inputs}})$ and $\mathcal{U}_i|\equiv(\mathcal{CS}|\equiv\mathrm{session}_{\mathrm{inputs}})$ and $\mathcal{CS}$ says K is the session key for $\mathcal{U}_i$ and $\mathcal{S}_i$, both parties

TABLE 3 | Cryptographic operations and execution time (ms).

Operation	Execution time (ms)
Modular multiplication ($\mathbb{Z}_q$)	1.200
LWE multiplication	3.800
ECC scalar multiplication	2.200
Hash function	1.225
Modular multiplication ($\mathbb{Z}_q$)	1.200
Bio-hashing (projection + binarization)	1.915

TABLE 4 | Total computational costs.

Entity	Operations	Total cost (ms)	Notes
($\mathcal{U}_i$)	1 LWE + 2 H + 1 BIO + 1 ECC	≈ 10.365	Dominated by ECC scalar multiplication
($\mathcal{S}_i$)	1 LWE + 1 H	≈ 5.025	Very lightweight, suitable for constrained devices
($\mathcal{CS}$)	2 LWE + 3 H + 1 ECC	≈ 15.545	Easily supported by cloud hardware

TABLE 5 | Communication overhead.

Scheme	No. of messages	Total cost (ms)
Shuai et al. [31]	2	4.740
Tanveer and Aldossari [32]	3	6.530
Rangwani et al. [33]	6	2.920
Dabra et al. [34]	4	2.618
Ours	4	2528

come to believe they share a fresh key: $\mathcal{U}_i(| \equiv \mathcal{U}_i \overset{K}{\longleftrightarrow} \mathcal{S}_i), \mathcal{CS}| \equiv (\mathcal{U}_i \overset{K}{\longleftrightarrow} \mathcal{S}_i)$

7 | Performance Evaluation

This section evaluates the efficiency and practicality of the proposed lightweight, quantum-resilient and privacy-preserving mutual authentication scheme in terms of computational costs, communication overhead, and energy consumption. Comparative analyses with existing schemes are also presented.

7.1 | Scalability and Cloud Server Load

The cloud server processes authentication requests independently and statelessly per session. Each authentication involves a small number of LWE multiplications and hash evaluations, which are trivially parallelizable. Given modern cloud hardware, the server can handle thousands of concurrent authentication sessions with negligible latency. Unlike sensor nodes, the cloud server is not resource constrained, and thus the computational burden of LWE verification does not affect system scalability.

7.2 | Computational Costs

We analyze the computational complexity of the scheme by counting the number of cryptographic operations performed by each entity ($\mathcal{U}_i$, $\mathcal{S}_i$ and $\mathcal{CS}$). Operations include modular multiplications, hash evaluations, LWE-based multiplications, and elliptic curve scalar multiplications. The execution times of these operations on a typical ARM Cortex M4 device are shown in Table 3.

Table 4 summarizes the total computational costs of the proposed scheme, presenting the cumulative execution times of the cryptographic operations performed by each participating entity.

7.3 | Communication Costs

We compute the communication overhead based on the number and size of messages exchanged during the mutual authentication process. Table 5 summarizes the communication costs of the proposed scheme and compares them with the existing schemes.

7.4 | Energy Consumption

The energy consumption of IIoT devices is estimated by mapping the execution time of cryptographic operations to energy values, assuming standard hardware specifications for constrained IoT nodes. $E = \sum_i (T_i \times P_{CPU})$, where T_i is the execution time of operation i and P_{CPU} is the average power consumption of the IoT device processor.

7.5 | Comparative Security Features

We compare the security guarantees of the proposed scheme against [31–34], focusing on resistance to the attacks that have been highlighted in the current literature such as resistance to impersonation, replay, insider, and quantum attacks, as well as support for anonymity, unlinkability, and forward secrecy. Table 6 presents a comparative analysis of the security features of the proposed scheme against existing approaches.

7.6 | Reproducibility

All cryptographic parameters used in the evaluation (LWE dimensions, modulus sizes, elliptic curve parameters, and hash functions) are explicitly specified in Section 4. The

TABLE 6 | Comparative analysis of security features.

Security feature	[31]	[32]	[33]	[34]	Ours
Resistance to quantum attacks	✗	✗	✗	✓	✓
Mutual authentication	✓	✓	✓	✓	✓
Resistance to forgery attack	✓	✓	✓	✓	✓
Resistance against impersonation attack	✓	✓	✓	✓	✓
Resistance against user identity guessing attacks	✓	✓	✓	✓	✓
Privileged insider attack	✗	✗	✓	✗	✓
Resistance to user masquerade attack	✓	✓	✓	✓	✓
Anonymity	✓	✓	✗	✓	✓
Masquerading and tampering attacks	✗	✓	✓	✓	✓
Resistance to replay attack	✓	✓	✗	✗	✓
Resistance to traceability attack	✓	✗	✗	✓	✓
Resistance to stolen verifier attack	✓	✗	✓	✓	✓
Resistance to unknown key share (UKS) attack	✗	✗	✓	✓	✓
Resistance to man-in-the-middle (MITM) attack	✓	✓	✓	✓	✓
Perfect forward and backward secrecy	✗	✓	✓	✓	✓
Resistance against known session specific temporary information attacks	✓	✓	✓	✓	✓
Resistance to known key attack	✓	✗	✓	✓	✓

implementation was conducted using standard cryptographic libraries on ARM Cortex-M4 emulation.

8 | Conclusion and Future Work

This study introduced a lightweight, quantum-resilient, and privacy-preserving mutual authentication scheme for the IIoT. The scheme integrates the LWE assumption for postquantum security, hash functions for integrity, ephemeral ECDH for forward secrecy, and bio-hashing for user privacy. A rigorous security analysis, both informal and formal (ROM and BAN logic), demonstrates that the scheme achieves mutual authentication, anonymity, unlinkability, resistance to classical and quantum attacks, and forward/backward secrecy. Performance evaluation shows that the scheme maintains low computational cost for constrained sensors (≈ 4 ms) and acceptable communication overhead (≈ 2.2 KB per session, depending on parameterization), making it suitable for real-world IIoT environments.

The proposed scheme is particularly well suited for industrial settings where heterogeneous devices, constrained sensors, and cloud-based analytics must coexist securely. By offloading heavier operations to users and the cloud, the design ensures that sensors perform only lightweight computations. While the communication cost is higher than some classical ECC-based schemes, this tradeoff is justified by postquantum resilience. Furthermore, with practical optimizations, such as coefficient packing, hybrid KEM integration, and selective message compression, the scheme can be deployed in IIoT ecosystems with limited bandwidth and strict energy constraints.

Several directions remain open for future exploration:

- Implementation and benchmarking: A full implementation on widely used IoT hardware (e.g., ARM Cortex-M4, RISC-V embedded devices) would provide concrete runtime and energy benchmarks beyond the analytical estimates provided here.
- Protocol optimization: Techniques such as message aggregation, ciphertext compression, and hybrid LWE–KEM integration could further reduce communication overhead while maintaining security guarantees.
- Quantum random oracle nodel (QROM): While our analysis considered PPT adversaries in the ROM, extending proofs to QPT adversaries in the QROM remains a critical step for strong postquantum assurance.
- Scalability and dynamic membership: Real-world IIoT deployments often involve dynamic sensor registration, revocation, and mobility across gateways. Incorporating efficient rekeying and revocation mechanisms tailored for dynamic large-scale networks is an important next step.
- Cross-domain applications: Beyond industrial environments, the scheme could be adapted to vehicular networks, satellite IoT, and disaster response communications, where postquantum secure and privacy-preserving authentication is equally critical.

In conclusion, this work lays the foundation for a practical, postquantum-secure and privacy-aware authentication framework for IIoT, while opening several promising avenues for further research and deployment.

Author Contributions

Tinashe Magara: conceptualization, design, experimentation, formal analysis, investigation, software, methodology, validation, visualization, writing–original draft, and writing–review and editing. Mampilo Phahlane: supervision, methodology, validation, and writing–review and editing.

Funding

No funding was received for this manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. I. P. Okokpujie and Tartibu, "Study of the Economic Viability of Internet of Things (IoTs) in Additive and Advanced Manufacturing: A Comprehensive Review," *Progress in Additive Manufacturing* 10, no. 5 (2025): 3175–3194, https://doi.org/10.1007/s40964-024-00822-7.

2. N. Alsadi, W. Hilal, A. McCafferty-Leroux, S. Gadsden, and J. Yawney, "Smart Systems: A Review of Theory, Applications, and Recent Advances," *Internet of Things* 33 (2025): 101667, https://doi.org/10.1016/j.iot.2025.101667.

3. O. Vermesan, et al., "Internet of Robotic Things–Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms," *In Cognitive Hyperconnected Digital Transformation* (Europe, Belgium, 2022), 97–155.

4. M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A Survey on Privacy and Security of Internet of Things," *Computer Science Review* 38 (2020): 100312, https://doi.org/10.1016/j.cosrev.2020.100312.

5. M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual Authentication in IoT Systems Using Physical Unclonable Functions," *IEEE Internet of Things Journal* 4, no. 5 (2017): 1327–1340, https://doi.org/10.1109/jiot.2017.2703088.

6. A. Roy, J. Kokila, N. Ramasubramanian, and B. S. Begum, "Device-Specific Security Challenges and Solution in IoT Edge Computing: A Review: A. Roy et al," *Journal of Supercomputing* 79, no. 18 (2023): 20790–20825, https://doi.org/10.1007/s11227-023-05450-6.

7. A. N. Alsheavi, A. Hawbani, W. Othman, et al., "Iot Authentication Protocols: Challenges, and Comparative Analysis," *ACM Computing Surveys* 57, no. 5 (2025): 1–43, https://doi.org/10.1145/3703444.

8. P. Fernando, "Post-Quantum Cryptography: Current Developments, Challenges, and Future Directions," *Path of Science* 11, no. 6 (2025): 4001–4012, https://doi.org/10.22178/pos.119-4.

9. Mehra and P. S. Chawla, "QSMAH: A Novel Quantum-Based Secure Cryptosystem Using Mutual Authentication for Healthcare in the Internet of Things," *Internet of Things* 24 (2023): 100949, https://doi.org/10.1016/j.iot.2023.100949.

10. J. H. Park and M. Kim, "Quantum-Resilient Security for 6G Networks: A Comprehensive Survey on Challenges, Solutions, and Research Opportunities," *Journal of Supercomputing* 81, no. 9 (2025): 1086, https://doi.org/10.1007/s11227-025-07544-9.

11. J. O. Odeh, X. Yang, O. W. Samuel, S. Dhelim, and C. I. Nwakanma, "Systematic Investigation of Privacy Preservation Techniques for Industrial IoT-Enabled Critical Edge Network Infrastructure," *Cluster Computing* 28, no. 6 (2025): 407, https://doi.org/10.1007/s10586-025-05114-5.

12. J. Carlton and Malik, "Safeguarding Personal Identifiable Information (PII) After Smartphone Pairing With a Connected Vehicle," *Journal of Sensor and Actuator Networks* 13, no. 5 (2024): 63, https://doi.org/10.3390/jsan13050063.

13. E. Lanus, C. J. Colbourn, and G. J. Ahn, "Guaranteeing Anonymity in Attribute-Based Authorization," *Journal of Information Security and Applications* 87 (2024): 103895, https://doi.org/10.1016/j.jisa.2024.103895.

14. Y. Wen, M. Wan, J. Zhao, Z. Gong, and Y. Deng, "RSH-BU: Revocable Secret Handshakes With Backward Unlinkability From VLR Group Signatures," *Computer Standards and Interfaces* 93 (2025): 103966, https://doi.org/10.1016/j.csi.2024.103966.

15. F. Yi, L. Zhang, L. Xu, S. Yang, Y. Lu, and D. Zhao, "WSNEAP: An Efficient Authentication Protocol for IIoT-Oriented Wireless Sensor Networks," *Sensors* 22, no. 19 (2022): 7413, https://doi.org/10.3390/s22197413.

16. G. K. Walia, M. Kumar, and S. S. Gill, "AI-Empowered Fog/Edge Resource Management for IoT Applications: A Comprehensive Review, Research Challenges, and Future Perspectives," *IEEE Communications Surveys and Tutorials* 26, no. 1 (2023): 619–669, https://doi.org/10.1109/comst.2023.3338015.

17. M. Kumhar and J. Bhatia, "Software-Defined Networks-Enabled Fog Computing for Lot-Based Healthcare: Security, Challenges and Opportunities," *Security and Privacy* 6, no. 5 (2023): e291, https://doi.org/10.1002/spy2.291.

18. M. N. Kha, H. Ur Rahman, T. Hussain, B. Yang, and S. Mian Qaisar, "Enabling Trust in Automotive IoT: Lightweight Mutual Authentication Scheme for Electronic Connected Devices in Internet of Things," *IEEE Transactions on Consumer Electronics* 70, no. 3 (2024): 5065–5078, https://doi.org/10.1109/tce.2024.3410300.

19. R. Al-Dabbagh, M. Alkhatib, and T. Albalawi, "Efficient Post-Quantum Cryptography Algorithms for Auto-Enrollment in Public Key Infrastructure," *Electronics* 14, no. 10 (2025): 1980, https://doi.org/10.3390/electronics14101980.

20. S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT," *IEEE Systems Journal* 16, no. 3 (2021): 4938–4949, https://doi.org/10.1109/jsyst.2021.3127438.

21. D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A Lightweight Remote User Authentication Scheme for IoT Communication Using Elliptic Curve Cryptography," *Journal of Supercomputing* 77, no. 2 (2021): 1114–1151, https://doi.org/10.1007/s11227-020-03318-7.

22. A. E. Budroni and Mårtensson, "Further Improvements of the Estimation of Key Enumeration With Applications to Solving LWE," *Cryptography and Communications* 16, no. 5 (2024): 1163–1182, https://doi.org/10.1007/s12095-024-00722-1.

23. A. A. Pandit and Mishra, "Efficient Implementation of Post Quantum MLWR-Based PKE Scheme Using NTT," *Computers and Electrical Engineering* 118 (2024): 109358, https://doi.org/10.1016/j.compeleceng.2024.109358.

24. D. S. Gupta and P. BiswasG, "A Novel and Efficient Lattice-Based Authenticated Key Exchange Protocol in C-K Model," *International Journal of Communication Systems* 31, no. 3 (2018): e3473, https://doi.org/10.1002/dac.3473.

25. F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A Security-Enhanced Certificateless Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems* 24, no. 10 (2023): 10456–10466, https://doi.org/10.1109/tits.2023.3275077.

26. M. A. Jan, et al., "Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in industrial-CPS," *IEEE Transactions on Industrial Informatics* 17 (2020).

27. E. Fathalla and Azab, "Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations," *IEEE Access* 12 (2024): 175969–175987, https://doi.org/10.1109/access.2024.3485602.

28. S. Amanlou, M. K. Hasan, and K. A. A. Bakar, "Lightweight and Secure Authentication Scheme for IoT Network Based on Publish–Subscribe Fog Computing Model," *Computer Networks* 199 (2021): 108465, https://doi.org/10.1016/j.comnet.2021.108465.

29. M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, L. T. D. Ferraz, and M. V. M. Silva, "Privacy-Preserving Certificate Linkage/Revocation in Vanets Without Linkage Authorities," *IEEE*

Transactions on Intelligent Transportation Systems 22, no. 6 (2020): 3326–3336, https://doi.org/10.1109/tits.2020.2981907.

30. Regev and Oded, "On Lattices, Learning With Errors, Random Linear Codes, and Cryptography," *Journal of the ACM* 56, no. 6 (2009): 1–40, https://doi.org/10.1145/1568318.1568324.

31. M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and Privacy-Preserving Authentication Scheme for Wireless Body Area Networks," *Journal of Information Security and Applications* 52 (2020): 102499, https://doi.org/10.1016/j.jisa.2020.102499.

32. M. Tanveer and S. A. Aldossari, "RAM-MEN: Robust Authentication Mechanism for IoT-Enabled Edge Networks," *Alexandria Engineering Journal* 112 (2025): 436–447, https://doi.org/10.1016/j.aej.2024.10.116.

33. Rangwani and H. Om, "Four-Factor Mutual Authentication Scheme for Health-Care Based on Wireless Body Area Network," *Journal of Supercomputing* 78, no. 4 (2022): 5744–5778, https://doi.org/10.1007/s11227-021-04099-3.

34. V. Dabra, A. Bala, and S. Kumari, "LBA-PAKE: Lattice-Based Anonymous Password Authenticated Key Exchange for Mobile Devices," *IEEE Systems Journal* 15, no. 4 (2020): 5067–5077, https://doi.org/10.1109/jsyst.2020.3023808.