electronics

MDPI

Article

A Lightweight Mutual Authentication Mechanism for Applications Utilizing Low-Power IoT Devices

Nai-Wei Lo, Jheng-Jia Huang and Ta-Chih Yang *

Department of Information Management, National Taiwan University of Science and Technology, Taipei City 106335, Taiwan; nwlo@cs.ntust.edu.tw (N.-W.L.); jhengjia.huang@mail.ntust.edu.tw (J.-J.H.)
* Correspondence: tcyang@livemail.tw

Abstract

Nowadays, Low-Power Internet of Things (LP-IoT) devices are widely utilized due to their affordability and low energy consumption. However, LP-IoT devices face significant security challenges, including data breaches, unauthorized access, and malicious attacks, due to their constrained hardware resources. These challenges are particularly critical in applications that involve the transmission of sensitive data. To enhance the security of LP-IoT devices, we propose a lightweight mutual authentication mechanism designed explicitly for LP-IoT devices. This mechanism utilizes simplified cryptographic operations to strike a balance between security requirements and resource constraints, thereby ensuring secure and reliable data transmission, as well as mutual authentication, between devices and servers. In addition, we demonstrate the potential of this mechanism in protecting data integrity and device security through a scenario in a financial technology application. Our proposed mechanism adapts to the characteristics of low-power devices while enhancing their security and practicality across different application environments, offering a secure and lightweight solution to the security challenges of LP-IoT devices.

Keywords: low-power internet of things; mutual authentication; lightweight authentication

check for updates

Academic Editor: Myung-Sup Kim

Received: 15 August 2025
Revised: 15 October 2025
Accepted: 22 October 2025
Published: 26 October 2025

Citation: Lo, N.-W.; Huang, J.-J.; Yang, T.-C. A Lightweight Mutual Authentication Mechanism for Applications Utilizing Low-Power IoT Devices. *Electronics* **2025**, *14*, 4178. https://doi.org/10.3390/electronics14214178

Copyright: © 2025 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 (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, Internet of Things (IoT) devices have gained widespread adoption across various industries due to their capability to connect numerous devices, enabling intelligent automation, remote monitoring, and efficient data management. IoT technologies are utilized in different fields, including healthcare, smart cities, agriculture, transportation, and industrial automation, significantly transforming traditional processes.

Within IoT technologies, low-power IoT (LP-IoT) technology plays a pivotal role in our daily life, due to its advantages of being low cost, requiring minimal energy consumption, and demonstrating suitability for long-term deployments in resource-constrained environments. LP-IoT devices can operate for extended periods using batteries or energy harvesting mechanisms, making them ideal for remote monitoring and scenarios where frequent maintenance is inconvenient. They collect and transmit data via sensors and wireless connections, enabling real-time decision-making and improving efficiency in various applications. For example, LP-IoT devices can be employed to detect and monitor wildfires, providing early warnings and critical real-time data to mitigate environmental damage and protect lives. In agriculture, LP-IoT helps monitor soil moisture, crop conditions, and weather parameters, thereby optimizing resource usage and improving yield efficiency. In

urban contexts, LP-IoT sensors facilitate the management of parking spaces, reducing congestion and enhancing mobility. In insurance companies, LP-IoT assists in assessing driving risks through "Pay as You Drive" (PAYD) and "Pay How You Drive" (PHYD) plans [1–3]. To balance profitability with the insured's risk, insurance companies install LP-IoT devices on policyholders' cars, enabling the tracking of driving patterns and sending data back to the insurance company.

Despite these advantages, LP-IoT devices face significant security challenges, including data breaches, unauthorized access, and malicious attacks, primarily due to their constrained computational power, memory capacity, and energy resources [4–12]. Existing security solutions, such as encryption and authentication mechanisms, often rely on computational ability and energy, and this is a limitation due to the characteristics of LP-IoT devices.

In particular, the use of LP-IoT in FinTech scenarios highlights the urgency of lightweight security solutions. Financial data and transaction records are highly attractive targets for adversaries, and if an LP-IoT device is impersonated or compromised, attackers may inject fraudulent data or disrupt decision-making, leading to severe financial and operational risks. Conventional cryptographic protocols, such as RSA or ECC, impose excessive computational and energy burdens on these devices. Therefore, it is essential to design a mutual authentication mechanism that ensures security while remaining feasible for disposable or resource-constrained LP-IoT deployments.

Moreover, practical studies report that LP-IoT deployments are frequently exposed to credential reuse, replay, and man-in-the-middle attacks in real-world settings, including finance-adjacent applications. These observations underscore the need for a lightweight yet robust mutual authentication mechanism to protect data integrity and device legitimacy under resource constraints [13,14].

In this study, we propose a lightweight mutual authentication mechanism specifically tailored for LP-IoT devices. The main contributions of this work are as follows: (1) we design a mechanism that balances strong security with lightweight operations; (2) we formalize the adversarial model and evaluate the scheme against practical attack vectors; and (3) we provide comparative performance analysis to demonstrate suitability for real-world deployment.

The paper is organized as follows: Section 2 reviews related works, highlighting the limitations of existing security mechanisms for LP-IoT devices. Section 3 introduces the proposed lightweight mutual authentication mechanism, detailing its design and implementation. Section 4 presents security and functional analyses, demonstrating the mechanism's capability to defend against common attack scenarios while maintaining efficiency. Finally, Section 5 concludes the study and outlines potential future research directions.

2. Related Work

Several authentication mechanisms have been proposed to enhance security for low-power IoT (LP-IoT) devices while balancing computational efficiency and energy consumption. In this section, we review key existing works and highlight their strengths and weaknesses.

Zhao et al. [15] conducted a comprehensive survey of IoT authentication mechanisms, highlighting the vulnerabilities associated with lightweight, low-power devices. They proposed using Chebyshev chaotic encryption as an alternative to elliptic curve cryptography (ECC), offering strong security with reduced computational cost. However, the mechanism still relies on iterative computations and modular arithmetic, which may be challenging for ultra-low-power IoT devices. Additionally, the security of the mechanism depends

heavily on initial parameter secrecy, and the lack of standardized protocols reduces its broad applicability.

Thakare et al. [16] introduced an authentication mechanism based on elliptic curve cryptography (ECC), hash functions, and XOR operations to optimize computational and storage overhead. While their mechanism was formally verified to defend against replay attacks, man-in-the-middle attacks, and insider threats, its reliance on ECC still imposes significant computational demands. The mechanism also has relatively high communication overhead (1408 bits), which may be a concern for bandwidth-constrained IoT networks.

Peivandizadeh et al. [17] designed a secure authentication and key agreement protocol specifically for low-power and Lossy Networks (LLNs). Their approach improved security by addressing vulnerabilities in the RPL routing protocol. The use of ECC-based cryptographic mechanisms, however, still presents challenges for ultra-low-power IoT devices, and the mechanism is tailored for RPL-based networks, limiting its applicability to broader IoT scenarios.

Zhou et al. [18] proposed a cloud-assisted authentication mechanism utilizing ECC, hash functions, and XOR operations. While their hierarchical four-party authentication model effectively distributes computational tasks, reducing device-side load, it heavily depends on cloud infrastructure. This reliance may not be suitable for all LP-IoT applications, particularly in environments with limited or intermittent network connectivity.

Das et al. [19] focused on smart healthcare IoT authentication, introducing a session key update mechanism for enhanced security. Their lightweight authentication and key agreement protocol used XOR and hash functions, ensuring resilience against common attacks while maintaining low computational and storage overhead. However, the reliance on IoT gateways for authentication could be a limiting factor in decentralized IoT environments, and the scalability of this mechanism has not been thoroughly evaluated.

From these works, we observe some challenges in the LP-IoT environment as follows:

1. Reliance on computationally intensive cryptographic operations (such as ECC), which may not be feasible for LP-IoT devices.
2. High communication overhead, making it unsuitable for bandwidth-constrained networks.
3. Limited scalability in dynamic IoT environments, where frequent device additions and removals can introduce security and performance concerns.
4. Some mechanisms, despite being lightweight, still requiring iterative computations or modular arithmetic, making them impractical for ultra-low-power IoT devices.

Therefore, there is a need for an authentication mechanism that minimizes power con-sumption while maintaining security and scalability for LP-IoT applications. In recent years, many lightweight authentication mechanisms have been proposed to enhance IoT device security. Zhao et al. [15] proposed a Chebyshev chaotic map-based scheme, while Thakare et al. [16] combined ECC, hash, and XOR operations for lightweight mutual authentication. Peivandizadeh et al. [17] further explored ECC-based approaches, whereas Zhou et al. [18] leveraged cloud computing resources to offload ECC computations. Das et al. [19] utilized lightweight hash and XOR operations to reduce computational overhead.

In addition, the Anti-Poisoning Attack Decentralized Privacy-Enhanced Federated Learning (APDPFL) scheme [20] has been proposed to address poisoning threats in federated learning systems. Although this direction focuses on data-level protection rather than device-level authentication, it reflects the breadth of IoT security research and complements our study by showing advances in parallel domains.

3. Proposed Mechanism

In this section, we introduce our proposed mechanism, detailing its system components and workflow. This mechanism is specifically designed to address the unique security requirements of LP-IoT devices, ensuring secure communication and data integrity without excessive resource consumption.

3.1. System Introduction

The proposed mechanism is based on LP-IoT devices, assuming they are equipped with storage and 4G/5G network connection capabilities. A Data Collection Server is placed to collect all the data that LP-IoT transfers back. Users can use this data in the Data Collection Server for further applications.

Due to the hardware limitations of LP-IoT devices, it is not possible to execute complex encryption mechanisms and perform frequent authentication. Our proposed mechanism enables the LP-IoT device to operate a secure authentication mechanism with the Data Collection Server, ensuring data security both in storage and during transit. In this system design, we focus on the device and data security between LP-IoT devices and the Data Collection Server.

3.2. The Lightweight Mutual Authentication Mechanism

In this study, we demonstrate our proposed mechanism in a general scenario with a simple application model. Our research focuses on the authentication process between an LP-IoT device and a Data Collection Server. The LP-IoT data collection model is shown in Figure 1.

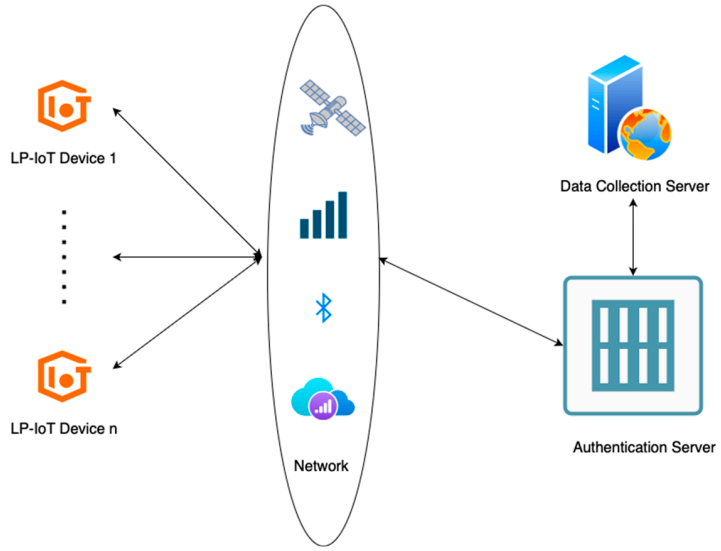


Figure 1. The LP-IoT data collection model.

The hardware devices or servers involved in the proposed authentication mechanism are depicted in Table 1.

Table 1. Hardware notations used in the proposed authentication mechanism.

Device/Server	Description
LP_i	The LP_i is the i^{th} device used in the default deployment environment.
DCS	The Data CollectionServer, which is responsible for collecting and storing the data transferred from LP_i.
AS	The Authentication Server is responsible for registering the LP-IoT device and sending the generated secret key.

The notations used are shown in Table 2 as follows.

Table 2. Symbol notations used in the proposed authentication mechanism.

Symbol	Description
$LPID_i$	The i^{th} LP-IoT device ID
ISC_i	The sec ret number of the i^{th} LP-IoT device
p_i, q_i	Two distinct large prime numbers
t_j	A timestamp, where $j \in \{1, 2 \ldots, n\}$
ΔT	A predefined, reasonable length of time for the party that receives a message with a timestamp to ensure the freshness of the received message.
TD_i	The transferred data from the LP-IoT device i
$h(\,)$	Hash function
$\oplus$	XOR operation

3.2.1. Registration Phase

AS Figure 2 shows, when the users initiate these kinds of IoT-based data collection applications, they will assign a unique LP-IoT device ID $\boldsymbol{LPID_i}$ and a corresponding secret number $\boldsymbol{ISC_i}$ to each LP-IoT device. A user can then register its LP-IoT device with these values at the AS. The AS will generate $\boldsymbol{p_i}$ and $\boldsymbol{q_i}$ and calculate the following operations:

$$A = h\left(LPID_i \bigoplus ISC_i \bigoplus p_i \bigoplus q_i\right) \tag{1}$$

$$B = A \bigoplus h\left(ISC_i \bigoplus LPID_i \bigoplus q_i\right) \tag{2}$$

$$C = h\left(A \bigoplus B \bigoplus p_i\right) \tag{3}$$

$$D = h\left(B \bigoplus C\right) \bigoplus p_i \bigoplus q_i \tag{4}$$

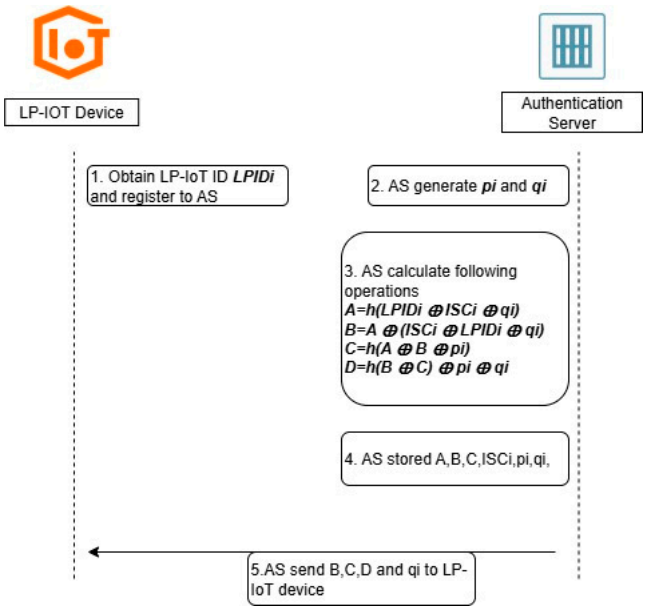


Figure 2. The Registration Phase.

After AS finishes the calculation, AS will store $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{ISC_i}$, $\boldsymbol{p_i}$ **and** $\boldsymbol{q_i}$, **and send the** $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, and $\boldsymbol{q_i}$ to $\boldsymbol{LP_i}$. Then the registration phase is accomplished.

This phase ensures that each device is initialized with a unique identity and secret parameters before operation. By preloading these lightweight values, the mechanism

avoids expensive key negotiation during runtime, which is critical for resource-constrained LP-IoT devices.

3.2.2. Mutual Authentication Phase

As Figure 3 shows, when a LP-IoT device $\boldsymbol{LP_i}$ first deploys to an environment, $\boldsymbol{LP_i}$ must conduct a mutual authentication process between $\boldsymbol{LP_i}$ and AS. The LP-IoT device makes the following computational operations marked with a timestamp $\boldsymbol{t_1}$.

$$A^* = B \bigoplus h\left(ISC_i \bigoplus LPID_i \bigoplus q_i\right) \tag{5}$$

$$E_1 = A^* \bigoplus B = h\left(ISC_i \bigoplus LPID_i \bigoplus q_i\right) \tag{6}$$

$$F = D \bigoplus E_1 \tag{7}$$

$$E_2 = E_1 \bigoplus F \bigoplus p_i \bigoplus t_1 = D \bigoplus p_i \bigoplus t_1 \tag{8}$$

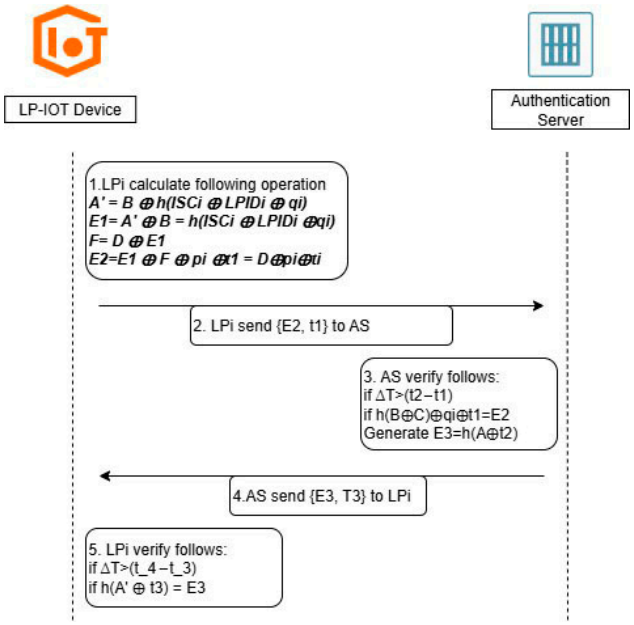


Figure 3. The Mutual Authentication Phase.

After the calculation, the $\boldsymbol{LP_i}$ sends the message $\{\boldsymbol{E_2}, \boldsymbol{t_1}\}$ to AS. The AS first records the timestamp $\boldsymbol{t_2}$ when it receives the message from $\boldsymbol{LP_i}$ and then verifies whether the $\boldsymbol{LP_i}$ is trustworthy via the following process.

$$verify\ if\ \ \Delta T > (t_2 - t_1) \tag{9}$$

$$verify\ if\ h\left(B \bigoplus C\right) \bigoplus q_i \bigoplus t_1 == E_2 \tag{10}$$

$$Generate\ E_3 = h\left(A \bigoplus t_3\right) \tag{11}$$

After AS transmits the message $\{\boldsymbol{E_3}, \boldsymbol{t_3}\}$ back to $\boldsymbol{LP_i}$, the $\boldsymbol{LP_i}$ first records the timestamp $\boldsymbol{t_4}$ when it receives the message from AS and then verifies whether the AS is trustworthy via the following process.

$$verify\ if\ \Delta T > (t_4 - t_3) \tag{12}$$

$$verify\ if\ h\left(A^* \bigoplus t_3\right) == E_3 \tag{13}$$

Unlike conventional protocols that rely on expensive asymmetric operations, our mechanism only requires hash and XOR operations with timestamps. This provides freshness against replay attacks while keeping computational overhead minimal, which directly fits the low-power profile of LP-IoT deployments.

3.2.3. Data Transmission Phase

As Figure 4 shows, when the mutual authentication phase is accomplished, $\boldsymbol{LP_i}$ can transfer the targeted data $\boldsymbol{DA}$ to DCS by embedding it into the message $\boldsymbol{TD_i}$ along with a current timestamp $\boldsymbol{t_5}$.

$$TD_i = \left\{ h\left(LPID_i \bigoplus ISC_i \right) \bigoplus DA,\ t_5 \right\} \tag{14}$$

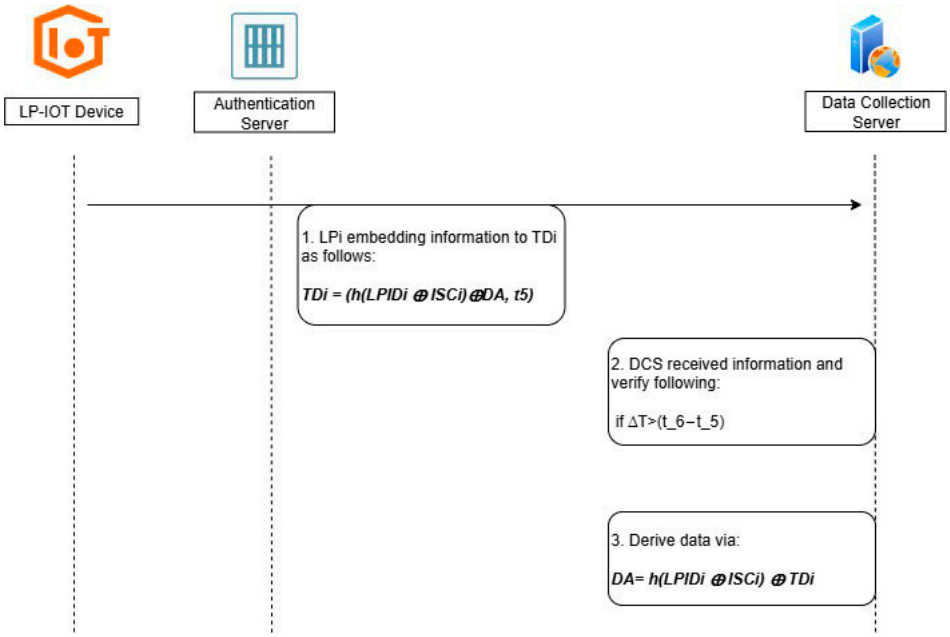


Figure 4. The Data Transmission Phase.

After DCS receives the message $\boldsymbol{TD_i}$, it first records the timestamp $\boldsymbol{t_6}$ when it receives the message from $\boldsymbol{LP_i}$ and then derives the targeted data via the following process.

$$verify\ if\ \Delta T > (t_6 - t_5) \tag{15}$$

$$Derive\ DA = h\left(LPID_i \bigoplus ISC_i \right) \bigoplus TD_i \tag{16}$$

3.2.4. Device Purge Phase

Once $\boldsymbol{LP_i}$ is no longer needed or has been lost, the user may ask AS to execute the device purge phase. The AS will delete all information related to the device identity $\boldsymbol{LPID_i}$.

The purge process guarantees that once a device is decommissioned or compromised, its credentials cannot be reused. This simple step reduces the risk of long-term impersonation without introducing additional runtime costs.

4. Analyses and Discussion

In this section, we will conduct a security analysis and functional analysis to ensure that our proposed mechanism is secure and can withstand common attack scenarios, while also considering its functional purpose.

4.1. Adversarial Model

For the security analysis, we assume the following adversarial model tailored to the LP-IoT environment. This model defines the capabilities and limitations of potential attackers, providing a clear basis for the subsequent analyses.

4.1.1. Adversary Capabilities

1. Eavesdropping: The adversary can passively intercept communications between LP_i and the servers (AS, DCS).
2. Replay: The adversary may resend previously captured messages in an attempt to bypass authentication.
3. Message Injection/Modification: The adversary may inject or alter transmitted messages to impersonate a device or server.
4. Active Initiation: The adversary may actively send fabricated authentication requests to the AS or DCS.
5. Limited Compromise: The adversary may obtain local information from a single compromised LP_i, such as its $LPID_i$ or partial stored values.

4.1.2. Adversary Limitations

1. The adversary cannot reverse the on-way hash function.
2. The adversary cannot derive the global secret parameters or system master secrets held securely by the AS.
3. The initialization process is assumed to be performed in a trusted environment, ensuring each LP_i is securely provisioned with its $LPID_i$ and ISC_i.

4.1.3. Adversary Goals

1. Forge a legitimate LP_i or AS to gain unauthorized access.
2. Replay outdated messages to trick the system into accepting invalid credentials.
3. Intercept or alter transmitted data without detection.
4. Escalate a local compromise of one device into a broader system breach.

4.2. Resistance Against Common Attacks

1. Eavesdropping Attack/Passive Attack
   The eavesdropping attack focuses on collecting data in a network environment, which may result in sensitive data leakage. Our proposed mechanism involves encrypting messages and data using XOR and a hash function during transmission. When a malicious attacker sniffs network packets, all the information is encrypted and cannot be decrypted effectively. This confirms that our proposed mechanism is effective in defending against eavesdropping attacks.
2. Dictionary and Exhaustive Attack
   Dictionary and exhaustive attacks focus on systematically guessing or enumerating passcodes. These attacks are particularly effective when secret numbers lack sufficient complexity. To mitigate such risks, our proposed mechanism combines the LP-IoT device's ID with the secret number using an XOR operation, followed by encryption and hashing processes before transmission. This layered approach effectively prevents attackers from successfully performing dictionary and exhaustive attacks.
3. Credential Stuffing Attack
   The credential stuffing attack is a malicious attack where a malicious attacker utilizes a leaked valid password list to try to log in as an authorized user. Our proposed mechanism does not directly use a secret number; instead, it encrypts the secret number using the XOR of the LP-IoT device's ID and transmits it after the hashing

process. This confirms that our proposed mechanism is effective in defending against credential stuffing attacks.

4. Forgery Attack/Impersonation Attack
   A forgery attack focuses on forging the mandatory infrastructure, trying to mislead both sides into believing they are communicating with a valid device. Our proposed mechanism is designed for LP-IoT and performs mutual authentication to verify both sides are trustworthy before data transmission. This confirms that our proposed mechanism is effective in defending against forgery attacks.
5. Replay Attack
   The replay attack is a malicious attacker sniffing the valid credentials and resending the credentials to cheat the authentication mechanism as a valid user. Our proposed mechanism is attaching a timestamp in each transmission, and the AS also asks all the servers to check whether the ΔT is in a reasonable time period. This confirms that our proposed mechanism is effective in defending against replay attacks. The overhead for verifying freshness is only a single hash computation (0.12 ms in Table 3), which is negligible for LP-IoT devices.

Table 3. Computation time for different cryptographic operations [15].

Operation	Notation	Computation Time (ms)
One-way hash function	T_h	0.00032
ECC point multiplication	T_{ecm}	0.0171
ECC point addition	T_{ecca}	0.0044
Symmetric encryption/decryption	$T_{e/d}$	0.0056
Modular exponentiation operation	T_{me}	0.0192
Modular multiplication operation	T_{mul}	0.00088
Chebyshev chaotic map operation	T_{cm}	0.0171
Operation based on the Chinese Remainder Theorem	T_{crt}	0.00704
Signature generation for the elliptic curve digital signature	T_{sig}	0.02182
Verification for the elliptic curve digital signature	T_{ver}	0.03892
Message authentication code	T_{mac}	0.00032

6. Man-in-the-Middle Attack
   In a man-in-the-middle attack, an attacker intercepts and potentially alters communication between the device and the server. To defend against this, our mechanism uses mutual authentication combined with timestamp-based hash masking. Even if communication is intercepted, the attacker cannot decrypt or modify the data without being detected, as each message's integrity is verified using cryptographic hash functions and the inclusion of fresh timestamps. Since each authentication round generates new hash values bound to the current timestamp, the attacker cannot reuse old messages or maintain prolonged exposure.

4.3. Cryptographic Security

1. Data Freshness and Hash-based Protection
   The authentication server (AS) does not distribute long-term session keys; instead, it relies on lightweight hash functions combined with timestamps to ensure data freshness. Even if a past message is intercepted, the bound timestamp and hash values prevent it from being reused in future sessions, thereby achieving forward protection against replay and forgery attempts.
2. Low Computational Overhead
   The mechanism avoids computationally expensive operations, such as public-key cryptography, and instead relies on lightweight hashing and XOR operations. This

makes it feasible for LP-IoT devices with limited processing power.
As shown in Table 3, each masking step requires only one XOR and one hash operation, with combined latency below 0.15 ms, which is significantly lighter compared to RSA- or ECC-based protocols that require tens to hundreds of milliseconds per operation.

3. Resistance to Side-Channel Attacks
The mechanism is designed to mitigate the risks of side-channel attacks by minimizing the exposure of cryptographic computations to an external observer. Since the mechanism utilizes XOR and a hash function rather than complex modular arithmetic, it reduces the likelihood of timing attacks and power analysis attacks. Furthermore, the authentication process incorporates randomized elements, ensuring that each execution path varies slightly, making pattern analysis more difficult for adversaries.

4.4. Device and Communication Security

1. Mutual Authentication
Unlike traditional IoT authentication mechanisms that only verify client-side legitimacy, our mechanism ensures that both the LP-IoT device and the authentication server authenticate each other before any data transmission occurs. The proposed lightweight authentication mechanism for low-power IoT devices demonstrably upholds the property of mutual authentication by ensuring that both the device LP_i and the Authentication Server (AS) verify each other's legitimacy before any data exchange occurs. In the mutual authentication phase, the LP_i first generates authentication values (E_2, t_1) derived from its unique ID, secret number, and time-sensitive parameters, which the DCS verifies for validity and timeliness. This prevents replay attacks and confirms the device's authenticity. Subsequently, the DCS responds with its own authentication token (N, t_3), computed using shared secret components and a fresh timestamp, which the LP_i validates through cryptographic checks. This bidirectional verification process, coupled with the use of lightweight hash and XOR operations, ensures that neither party proceeds without confirming the trustworthiness of the other.
In contrast, schemes using ECC incur approximately 15–20 ms per scalar multiplication, which is more than two orders of magnitude heavier than our approach.
2. Minimal Local Secrets
The LP-IoT device stores only minimal security information (such as its device ID and a hashed value tied to its secret number). All authentication values are generated dynamically for each session using lightweight hash and XOR operations with fresh timestamps, eliminating the need for long-term session keys and further reducing the risk of key compromise.

4.5. Functional Analysis

1. Suitability for LP-IoT Devices
The proposed mechanism executes all complex calculations on the server side during the registration phase. The LP-IoT devices only store mandatory information generated by AS, which significantly reduces their computational loading. In the authentication phase, the devices execute only XOR operations, which is a simple logical function that requires minimal computational resources and power. This design aligns with the limited processing power and energy constraints of LP-IoT devices, ensuring efficient performance without overloading hardware.
2. Lightweight Storage Requirements
Our proposed mechanism requires minimal storage on LP-IoT devices. Only essential credentials, such as device IDs and hashed secret keys, are stored locally, reducing

memory usage. This is particularly advantageous compared to mechanisms like ECC-based protocols, which require complex key management and large storage capacities.

3. Flexibility Across IoT Applications
   Unlike protocols designed for specific industries (e.g., healthcare or smart grids), our mechanism is highly adaptable to various LP-IoT applications, including automobile insurance, supply chain management, and environmental monitoring. Its generic design ensures ease of integration into diverse IoT environments without significant architectural modifications.
4. Reduced Communication Overhead
   Our proposed mechanism minimizes the number of communication steps during the authentication phase, thereby significantly reducing bandwidth consumption. This is particularly beneficial in LP-IoT environments where devices often operate under low-bandwidth or intermittent network conditions.
5. Scalability in a dynamic IoT environment
   The proposed mechanism is designed for operation in dynamic IoT settings, where the number of devices may frequently fluctuate. The registration phase has been designed to accommodate these changes, allowing the system to maintain its efficiency and security even in highly variable environments. This scalability ensures long-term usability across diverse IoT deployments.
6. Enhanced Energy Efficiency
   The mechanism limits calculations on the LP-IoT device to XOR and hash functions. According to Table 3 [13], these operations require minimal computation time compared to other cryptographic methods. This ensures the mechanism is both fast and resource-efficient, meeting the performance requirements of LP-IoT devices while maintaining robust security.
   The performance evaluation demonstrates that our mechanism consumes only 1.56 ms per authentication cycle (as derived from Table 3). This value is substantially lower than other schemes that require more than 30 ms on average.
7. Strong Security with Minimal Resource Consumption
   Despite its lightweight design, the mechanism provides robust security guarantees against common attack vectors, including reply attacks, impersonation attacks, and man-in-the-middle attacks. This balance between security and efficiency distinguishes our mechanism from traditional IoT security protocols.

4.6. Computation Time Analysis

Zhao et al. [15] has provided a list of time consumption for various cryptographic operations, as shown in Table 3. Theoretically, assuming a constant power supply, a shorter computation time corresponds to lower overall energy consumption.

Table 4 compares the computation time required for a single execution of cryptographic operations across several authentication schemes. Zhao et al. [15] and Peivandizadeh et al. [17] reported similar execution times (approximately 0.0171 ms) for Chebyshev chaotic mapping and ECC point multiplication, respectively. Thakare et al. [16] included ECC point multiplication, hash, and XOR operations, resulting in a computation time of 0.01742 ms. In contrast, Zhou et al. [18] achieved a significantly reduced computation time of 0.00032 ms by leveraging cloud computing resources to offload the heavy ECC operations. Similarly, Das et al. [19] utilized lightweight operations such as hash and XOR to attain the same level of performance. Our proposed method, based solely on XOR and hash functions, also achieves a computation time of 0.00032 ms—without relying on any cloud-based acceleration, thereby offering comparable efficiency with greater deployment flexibility in resource-constrained environments.

Table 4. Comparison of the computation time among existing authentication schemes and our scheme.

Authentication Solution	Applied Operations	Approximate Computation Time (ms)
Zhao et al. [15]	Chebyshev chaotic mapping	0.0171
Thakare et al. [16]	ECC point multiplication + Hash + XOR	0.01742
Peivandizadeh et al. [17]	ECC point multiplication	0.0171
Zhou et al. [18]	Cloud-assisted ECC + Hash + XOR	0.00032 (with cloud computing ability)
Das et al. [19]	Hash + XOR (Session Key)	0.00032
Ours	XOR + Hash	0.00032

These findings emphasize the need for cryptographic mechanisms that minimize power consumption while maintaining robust security and scalability in LP-IoT environments. Our proposed solution fulfills this need by combining XOR and hash functions. It achieves computational efficiency comparable to the most lightweight authentication schemes, without relying on ECC-based operations or cloud-assisted infrastructure.

5. Conclusions

In this study, a secure mutual authentication mechanism tailored for low-power IoT (LP-IoT) devices is proposed. The proposed mechanism ensures secure communication between LP-IoT devices and data collection servers, enhancing data integrity and confidentiality in IoT-based applications.

Through comprehensive security analysis, this study demonstrated that the proposed mechanism effectively defends against common attack scenarios, including eavesdropping, dictionary and exhaustive attacks, credential stuffing, forgery, replay, and man-in-the-middle attacks. By leveraging lightweight cryptographic operations such as XOR and hashing, the mechanism achieves robust security without compromising the efficiency or power consumption of LP-IoT devices. In the functional analysis, we highlighted the adaptability of the mechanism across various application scenarios, such as usage-based insurance, asset tracking, and data collection for predictive analytics. Its flexible architecture supports seamless integration into existing IoT infrastructures and enables scalability, making it suitable for a wide range of IoT-dependent industries beyond financial technology, including healthcare, logistics, and smart cities.

For future work, one could explore the possibility of integrating lightweight, mutually authenticated LP-IoT devices into a Zero-Trust Architecture (ZTA) to derive a robust framework for general IoT-based applications.

In conclusion, this work helps bridge the gap between security and functionality in LP-IoT devices, offering a scalable, adaptable, and secure solution for safeguarding critical data and operations in IoT application scenarios.

Author Contributions: Conceptualization, N.-W.L., T.-C.Y. and J.-J.H.; methodology, N.-W.L., T.-C.Y. and J.-J.H.; validation, N.-W.L., T.-C.Y. and J.-J.H.; formal analysis, N.-W.L., T.-C.Y. and J.-J.H.; writing—original draft preparation, T.-C.Y.; writing—review and editing, J.-J.H.; supervision, N.-W.L.; project administration, N.-W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Grag, A.; Demirezen, E.M. Hsing Kenneth Cheng. Financial Sustainabilitiy of IoT Platforms: The Role of Quality and Security. *Prod. Oper. Manag.* **2024**, *2*, 412–431. [CrossRef]
2. Manral, J. IoT enabled Insurance Ecosystem—Possibilities Challenges and Risks. *arXiv* **2015**, arXiv:1510.03146.
3. Elicegui, I.; Carrasco, J.; Escribano, C.P.; Gato, J.; Becerra, A.; Politis, A. Usage-Based Automotive Insurance. In *Big Data and Artificial Intelligence in Digital Finance: Increasing Personalization and Trust in Digital Finance Using Big Data and AI*; Springer International Publishing: Cham, Switzerland, 2022; pp. 295–311.
4. Tyagi, S.K.S.; Boyang, Q. An Intelligent Internet-of-Things-Aided Financial Crisis Prediction Model in FinTech. *IEEE Internet Things* **2023**, *10*, 2183–2193. [CrossRef]
5. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
6. Yang, K.; Blaauw, D.; Sylvester, D. Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey. *IEEE Micro* **2017**, *37*, 72–89. [CrossRef]
7. Sasi, T.; Lashkari, A.H.; Lu, R.; Xiong, P.; Iqbal, S. A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanism and Challenges. *J. Inf. Intell.* **2024**, *2*, 455–513. [CrossRef]
8. Allioui, H.; Mourdi, Y. Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive survey. *Sensors* **2023**, *23*, 8015. [CrossRef] [PubMed]
9. New York State Department of Financial Services. 23 NYCRR-Part 500 Cybersecurity Requirements for Financial Services Companies. 2017. Available online: https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf (accessed on 17 November 2024).
10. Hong Kong Monetary Authority. Cybersecurity Fortification Initiative. 2016. Available online: https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi/ (accessed on 17 November 2024).
11. Monetary Authority of Singapore. Cyber Hygiene Notice. 2018. Available online: https://www.mas.gov.sg/regulation/cybersecurity (accessed on 17 November 2024).
12. Cook, J.; Rehman, S.U.; Khan, A. Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions. *IEEE Access* **2023**, *11*, 39295–39317. [CrossRef]
13. Kumar, D.; Shen, K.; Case, B.; Garg, D.; Alperovich, G.; Kuznetsov, D.; Gupta, R.; Durumeric, Z. All Things Considered: An Analysis of IoT Devices on Home Networks. 2019. Available online: https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak (accessed on 20 September 2025).
14. Lazzaro, S.; De Angelis, V.; Mandalari, A.M.; Buccafurri, F. A black-box assessment of authentication and reliability in consumer IoT devices. *Pervasive Mob. Comput.* **2025**, *110*, 102045. [CrossRef]
15. Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L. Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. *Electronics* **2023**, *12*, 1812. [CrossRef]
16. Thakare, A.; Kim, Y.-G. Secure and Efficient Authentication Mechanism in IoT Environments. *Appl. Sci.* **2021**, *11*, 1260. [CrossRef]
17. Peivandizadeh, A.; Molavi, B. Compatible Authentication and Key Agreement Protocol for Low Power and Lossy Network in Iot Environment. SSRN. 2023. Available online: https://www.researchsquare.com/article/rs-2085426/v1 (accessed on 18 October 2025).
18. Wang, C.; Wang, D.; Duan, Y.; Tao, X. Secure and Lightweight User Authentication Mechanism for Cloud-Assisted Internet of Things. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2961–2976. [CrossRef]
19. Das, S.; Singh, M.P.; Namasudra, S. A Lightweight Authentication and Key Agreement protocol for IoT-Based Smart Healthcare System. *World Conf. Commun. Comput.* **2023**, 1–5.
20. Li, X.; Zao, H.; Xu, J.; Zhu, G.; Deng, W. APDPFL: Anti-Poisoning Attack Decentralized Privacy Enhanced Federated Learning Scheme for Flight Operation Data Sharing. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 19098–19109. [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.