Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 02, PP. 311-324-, 2025
DOI: https://doi.org/10.54216/JISIoT.170220

Enhanced Lightweight Cryptography-based Authentication Protocol for IoT Devices

Sanâ Elaoudi[1,*], Marouane Sebgui[1], Slimane Bah[1]
[1]Mohammed V University in Rabat - Ecole Mohammadia d'Ingenieurs, ERSC research Team, Morocco
Emails: sanaelaoudi@research.emi.ac.ma; sebgui@emi.ac.ma; slimane.bah@emi.ac.ma

Abstract

The rapid advancement of telecommunication infrastructures and endpoint technologies has led to a significant incorporation of Internet of Things devices in modern lifestyles. IoT involves a wide range of applications, such as connected video surveillance systems for security, wearable body sensors for health monitoring, and temperature sensors for environmental control in agricultural fields. These devices are essential for gathering and transmitting data in real-time. However, data acquisition and transmission processes are often exposed to serious security threats, particularly concerning data integrity, user privacy, and communication reliability. Conventional security mechanisms are typically inappropriate to resource constrained IoT devices. Thus, to overcome these challenges, extensive research has been devoted to developing secure communication frameworks, with a particular focus on robust authentication and key agreement protocols. Authentication is essential to guarantee the legitimacy of the information source, and many proposed AKA schemes rely on asymmetric cryptographic techniques. In this paper, we introduce an Enhanced Lightweight Cryptography-based Authentication Protocol for IoT devices, conceived to meet the computational constraints of IoT devices by employing simple XOR and hashing operations. The protocol enables mutual authentication between IoT devices and routers without the need to share credentials directly. Prior to authentication, an offline registration phase is conducted through an Authentication Server (AS), which generates unique key parameters based on the identifiers of the devices and routers. These parameters are securely distributed to both parties. Authentication is then performed using these pre-shared parameters in a computationally efficient yet secure manner that safeguards against common security threats. Theoretical analysis demonstrates that the proposed protocol is resistant to several common attacks, including man-in-the-middle, impersonation, session key disclosure, replay, and eavesdropping attacks. Additionally, the protocol ensures device anonymity and data privacy while maintaining lightweight performance suitable for constrained IoT environments.

Received: January 09, 2025 Revised: March 12, 2025 Accepted: June 10, 2025

Keywords: IoT device; Modular exponentiation; Authentication and Key Agreement; Hash function; Cryptography

1. Introduction

The Internet of Things also denoted Internet of Everything (IoT) enables traditionally non-internet-connected devices to deliver services over the internet, facilitating automation, monitoring, and intelligent decision-making across diverse sectors. These devices include, but are not limited to video surveillance cameras, which support remote security monitoring; smart home lighting systems, which allow for automated and energy-efficient lighting control; smart grids, which integrate devices like smart meters to optimize energy distribution; and connected vehicles, which utilize IoT for navigation, diagnostics, and autonomous driving features. Through such applications, IoT links the physical and digital worlds, enabling seamless interaction and real-time data exchange. [1]

The data collected by IoT devices is exploited to improve and track an individual's surroundings in order to support their well-being. However, inaccurate or tampered data can lead to misguided decisions or inappropriate actions.

In contrast, accurate data captured and transmitted in real time enables faster analysis and more informed decision-making. Consequently, data exchange within an Internet of Things (IoT) network is both time-sensitive and demands strong security measures.[2] Indeed, privacy and security are critical components of any IoT application. [3]

Security concerns in IoT networks involve a wide range of malicious attacks that aim to compromise system integrity, confidentiality, and availability. These include eavesdropping, impersonation, jamming, replay attacks, man-in-the-middle (MITM) attacks, tampering, and other forms of intrusion. [4]

To tackle the complex security challenges in IoT systems, particular attention must be directed toward key aspects such as confidentiality, integrity, authentication, privacy, non-repudiation, and availability. [5], [6].

Fundamentally, the core pillars of IoT security are commonly recognized as authentication and key agreement. Authentication ensures that legitimate entities are solely allowed access to the network and its resources, thereby preventing unauthorized usage. Key agreement, on the other hand, is necessary for establishing secure communication channels, as it guarantees the privacy, confidentiality, and integrity of the data exchanged between devices. [2]

The scientific research community has significantly contributed to the IoT field by developing various categories of authentication schemes, which can be broadly classified into five types:

- One Time Password (OTP): the authentication password is produced for a single session and becomes invalid after use,
- Zero knowledge proof: authentication is achieved without revealing the actual credentials, thus preserving privacy,
- Mutual authentication: both communicating parties verify each other's identities before initiating communication,
- Public key cryptography: the IoT device generates a pair of Public and Private Keys for authentication,
- and Digital Signature: Authentication relies solely on the IoT device's private key to verify identity. [7]

These authentication types generally follow one of two models: the first category depends on a centralized authority that maintains user/device credentials and validates authentication requests accordingly. While the second form adopts a decentralized approach, allowing devices to authenticate each other directly through mutual verification. [8].

Nevertheless, IoT devices are unable to use authentication based on computationally advanced cryptography due to their limited resources. Thus, lightweight authentication using simple operations like Hash and XOR is more suitable. [9]

Indeed, due to the constrained computational resources of IoT devices, authentication protocols commonly employ lightweight cryptography techniques such as XOR and hash functions. However, relying solely on simple cryptographic operations is insufficient to achieve a high level of security, especially in the face of increasingly sophisticated and frequent malicious attacks. Thus, to enhance security, multifactor authentication schemes integrate multiple mechanisms; typically combining XOR operations, hash functions, and biometric parameters; to construct robust and efficient authentication protocols suitable for IoT environments. [10]

Therefore, an authentication protocol is considered optimized only when it achieves a balance between security and efficiency, enhancing protection against threats while reducing energy consumption, computational overhead and execution time. [11]

Subsequently, when designing IoT authentication protocols, different critical parameters must be considered:

- Time cycle, which refers to the frequency at which authentication processes occur,
- Latency, the delay between initiating and completing the authentication,
- Reliability, which ensures consistent and error-free authentication under varying network conditions [12],
- Secrecy which helps ensure that sensitive information remains confidential, further supporting the integrity and reliability of the authentication process [13],
- Resistance to several security attacks for instance man-in-the-middle, impersonation, replay attack, provision of a secure key agreement process to protect subsequent communications [14]
- and mutual authentication [15].

Other parameters are associated with the resource-constrained nature of IoT devices. Accordingly, protocols are typically evaluated based on three key metrics: communication cost (measured in milliseconds), computation cost (in bits), and storage cost (in bits). [16] These parameters are essential to maintaining both the performance and security of IoT systems. However, other conditional parameters are to be considered like environmental conditions and real-world deployment constraints. [17]

Throughout this paper, we introduce an innovative lightweight authentication protocol tailored for Internet of Things (IoT) environments, utilizing fundamental cryptographic operations such as one-way hashing, XOR, and

modular exponentiation. The proposed scheme is designed to reinforce security against prevalent attacks including replay, impersonation, and man-in-the-middle while ensuring the preservation of privacy, data integrity, and operational efficiency.

By leveraging computationally efficient primitives, our protocol achieves robust security with minimal resource consumption, making it specifically appropriate for resource-constrained IoT devices. Comprehensive evaluations demonstrate that our approach offers enhanced security features with reduced computational complexity, communication overhead, and storage requirements compared to existing solutions.

In intelligent IoT systems that process sensitive data often about users and locations, our approach enhances data privacy by ensuring device anonymity, so real identity is not traceable. By employing pseudo identity instead of real device identity, the scheme enables privacy-preserving AI algorithms to learn from different devices without exposing device information.

Compared to existing protocols, such as the one in [21], the proposed protocol not only strengthens security aspect but also reduces resource computation, memory and storage overheads, thereby freeing resources for intelligent IoT systems to perform advanced processing and accelerating system responses.

Furthermore, the proposed protocol addresses security issues in previous protocols including session key disclosure in [20] and vulnerability to Man-In-The-Middle Attack in [22], positioning the proposed scheme as robust security mechanisms that support privacy and data integrity required by Intelligent IoT Systems. The protocol is able to ensure only authorized devices can join the network.

Unlike the approach in [23], the proposed scheme eliminates the need for a persistent secure channel between devices and the gateway/router, which is particularly advantageous for intelligent IoT systems that often rely on a massive device population.

The article is arranged in eight sections: Section II states the problem to solve. Section III recapitulates related work. Section IV. Reintroduces mathematical preliminaries. Section V delivers a summary of the proposed protocol. Section VI describes the security evaluation of the scheme. Section VII depicts a comparative analysis with various authentication schemes. Finally, Section VIII concludes the article.

2. Problem statement

Authentication is a critical security concern in the Internet of Things (IoT) domain that demands focused attention from both academic researchers and industry practitioners. There is a urgent need to develop robust authentication protocols that not only ensure secure access but also prevent the excessive consumption of limited IoT resources.

A significant body of research has been dedicated to developing authentication protocols that strengthen the security of existing mechanisms; however, many of these solutions require high computational power or introduce substantial communication overhead. Conversely, other studies have prioritized minimizing resource consumption, but often at the cost of reduced security, leaving the protocols vulnerable to various malicious attacks.

Striking an effective balance between authentication security and resource efficiency remains a promising area of research, offering opportunities to enhance the adoption of IoT devices and technologies while minimizing associated constraints and limitations.

Our approach aligns with this research direction by first enhancing the security level of selected existing solutions in [20] and [22], which are exposed to attacks such as Man-in-the-Middle, eavesdropping, Unlinkability, and session key disclosure. Second, we aim to optimize resource consumption compared to other existing proposals in [21] and [23].

The main contributions of the proposed scheme are:

a. No Clock Synchronization Required

The proposed authentication mechanism eliminates the need for clock synchronization among devices such as smart sensors, routers, and authentication servers. This is achieved by employing a nonce-based authentication approach, wherein each session utilizes a unique, randomly generated number (nonce) to ensure the freshness and uniqueness of the communication. Unlike timestamp-based methods, i.e [18], that require synchronized clocks to prevent replay attacks, nonce-based protocols inherently provide replay protection without relying on time-based data.[19] This design choice simplifies implementation and enhances reliability, particularly in resource-constrained IoT environments where maintaining synchronized clocks can be challenging.

b. Fast Error Detection

Within the proposed authentication process, the router promptly verifies the authenticity of the sensor by verifying the provided sensor A_{IDi}. If an adversary attempts to authenticate using an incorrect or unauthorized sensor A_{IDi}, the router detects the difference immediately and terminates the authentication attempt. This early detection mechanism ensures that only legitimate devices proceed to subsequent stages, such as session key establishment, thereby conserving computational resources and mitigating potential security threats at an early stage. Hence enhancing the deployment of Artificial Intelligence and Machine Learning algorithms on resource-constrained devices, such as sensors and edge nodes.

c. Independent Session Key Generation

A sensor and a router generate the session key (SK) using a combination of cryptographic hash functions and random numbers unique to each session. This method ensures that each session key is independent of previous keys, providing forward secrecy. Consequently, although a session key is compromised, it does not affect the security of precedent or upcoming sessions. The sensor can initiate the generation of a new session key without relying on previously established keys, thereby maintaining the integrity and confidentiality of the communication.

d. Resource efficiency

The proposed protocol employs simple operations like one-way hashing, XOR, and modular exponentiation that are resource preserving in terms of computation, memory and energy. This efficiency renders the authentication process lightweight compared to traditional cryptography authentication techniques. The lightweight nature of the protocol frees up resources for advanced processing tasks, thus promoting the execution of Artificial Intelligence and Machine Learning algorithms that runs on resource-constrained devices i.e sensors and edge nodes.

e. IoT Network scalability

Intelligent IoT systems, edge computing architectures and autonomous decision-making processes rely usually on a large number of interconnected IoT devices continuously collecting and sharing data. Since authentication is the first step to join an IoT Network, it should be both lightweight and secure. The proposed lightweight authentication scheme ensures robust security while enabling the large-scale onboarding of IoT devices without overloading the system.

f. Time effectiveness

Intelligent IoT systems often require real-time decision making which renders them highly time sensitive. The proposed lightweight authentication scheme accelerates the authentication process enabling rapid response from Artificial Intelligence-driven models while simultaneously reducing the latency in secure data exchange.

3. Related Work

Although numerous studies have focused on the authentication of IoT devices, existing protocols still fall short of meeting all performance requirements. This is primarily because of the diversity of IoT devices and their limited resources, the wide range of security threats, and the diverse real-world conditions in which these devices are deployed. The research community tries to find an optimal balance among these factors to design a secure, efficient and lightweight authentication process for IoT devices. In [20] Esfahani et al. proposed an authentication scheme for machine-to-machine communication in an Internet of Things environment, based uniquely on hash and XOR operations. The proposed system ensures authentication by utilizing hash values generated from the sensor ID and a random value, with the assistance of an intermediary authentication server. A malicious entity cannot replicate the same hash value, as it lacks access to both the sensor ID and the random value. However, the scheme exposes sensitive data to potentially untrusted sensors, especially the secret key of the router and the session key established between the router and a sensor. Barnana Baruah and Subhasish Dhal, present in [21] an authentication scheme for secure communication between a sensor and a router in an Industrial IoT environment. While the scheme offers adequate security and protection against various types of attacks, it incurs high computational overhead. Al-Turjman and David, [22] proposed a privacy-preserving authentication scheme designed to interoperate across diverse devices within an IoT environment. The scheme resists forgery, insider threats, masquerade attacks, eavesdropping and denial-of-service (DoS). Furthermore, it provides traceability, anonymity, and secret key updates. Nevertheless, it remains vulnerable to man-in-the-middle attacks.

In [23], Arwa Badhib and al. proposed an authentication protocol that incorporates two authentication phases: a static phase and a continuous authentication phase. While the scheme enhances security by continuously verifying sensor identity and status, it introduces several limitations. Specifically, the protocol requires efficient memory management at the gateway to store a wide range of sensor parameters, including sensor ID, battery level, location, and secure range. Additionally, a secure channel between the gateway and each sensor must be maintained, which

may not be feasible in highly dynamic or resource constrained IoT environments. Furthermore, the protocol imposes a high computational overhead, particularly due to the large number of hash operations required.

4. Preliminaries

a. Cyclic Groups

A cyclic group is a type of group where all elements are generated by applying the group operation repetitively to a single element, called the generator. When there is an element $g \in G$ such as that every element $a \in G$ can be written as $a=g^k$ (for an integer k). Then G is a cyclic group, and g is considered the generator of the group.
Cyclic groups are used in modular exponentiation, which strengthens cryptographic protocols like ElGamal encryption and Diffie–Hellman key exchange. Indeed, these protocols rely on the hardness of the discrete logarithm problem in cyclic groups (i.e., given g^x, it is hard to find x). [24].
In IoT authentication, these groups allow secure key generation and verification using lightweight mathematical structures that can run even on constrained devices. [25]
In the proposed scheme we use cyclic group G of generator g to perform modular exponentiation in resource constrained sensors.

b. Exponentiation on resource constrained IoT devices

Given the resource constraints of many IoT devices, researchers have explored various methods to optimize authentication protocols for efficient and secure communication. Modular exponentiation is a fundamental operation used in cryptographic protocols, including those used for authentication in Internet of Things (IoT) devices to protect data during transmission. [26], Modular exponentiation is a computational operation in number theory where an integer base a is raised to an integer exponent b, and the result is reduced modulo an integer m.
The mathematical representation of modular exponentiation is defined as: "$c = a^b \bmod m$" where: a is the base (typically a secret or public key component), b is the exponent (often a nonce, private key, or session variable) and m is the modulus (usually a large prime or composite number). The result of the modular exponentiation c is the result of elevating a to the power b, modulo m.

In the context of IoT authentication protocols, modular exponentiation is employed to enable secure key exchanges, digital signatures, and mutual authentication through cryptographic primitives such as Diffie-Hellman key exchange and RSA. It ensures computational infeasibility of deriving secret keys from public parameters due to the hardness of the discrete logarithm or integer factorization problems. [27] For exponentiation on constrained IoT devices, the recommended finite group is a prime-order subgroup of $Zp*$, where: p is a small (but secure) prime (e.g., 160–256 bits) and $p=2q+1$, a safe prime. Exponentiation is done as $g^x \bmod p$, with small, optimized g.

Hence, we use modular exponentiation in our scheme since it's:

- Efficient enough for 8-bit / 32-bit microcontrollers,
- Secure against basic attacks. Security based on the Discrete Logarithm Problem,
- Simple to implement (no elliptic curve math),
- Well understood and audited.

In fact, a part of our algorithm is inspired by the hard inverse computational Diffie Hellman problem widely used to secure communication over an insecure network. [28]

5. Proposed protocol

The protocol is structured into two primary phases: the Offline Registration Phase, during which entities are initially enrolled in the system, and the authentication and key agreement phase, where mutual authentication and secure session key establishment are performed.

Figure 1 exhibits the registration phase of the proposed protocol, Figure 2 illustrates the process flow for authentication and session key agreement, while Table 1 specifies a list of the symbols, and their corresponding definitions used throughout the scheme.

Table 1: Symbols and definitions

Symbols	**Definitions**
AS	Authentication Server
x	Authentication Server secret Key
ID_i	Unique Identifier of Sensor i
A_{IDi}	Anonymous Identity of Sensor i
A_{IDj}	Anonymous Identity of Router j
f_{1i}	Sensor i secret parameter $f_{1i} = h(ID_i \| x)$
f_{2ij}	Sensor i secret parameter for router j $f_{2ij} = P_{SKj} \oplus f_{1i}$
P_{SKj}	Router j preshared session key
Z_p	Finite group-prime order subgroup of Z_p^*
s, r	Random Number
M_1, M_2, M_3, M_4, M_5	XOR and Hash values
Message 1, Message 2, Message3	Authentication messages
$\oplus$	XOR Operation
$\|$	Concatenation operation
T_{XOR}	XOR execution time
T_h	Hash execution time
T_{ran}	Random Number generation time
T_{expo}	Modular Exponentiation execution time

a. Registration

Let consider a cyclic group G of prime order p, with g its generator. The initialization of parameters for the Authentication Server (AS), routers, and sensors involves the following steps (Figure 1):

1. **Sensor Initialization**: Sensor S_i chooses a random number as its identifier ID_i and sends it over a secure channel to AS.
2. **Parameter Generation**:

The AS generates necessary cryptographic parameters required for secure communication:

Step 1. The Authentication server (AS) generates its secret key x.

Step 2. The Authentication server (AS), generates pre-shared key P_{SKj} for each router j.

Step 3. The Authentication server (AS) computes secret parameters f_{1i} and f_{2ij} for each sensor i and router j as explained in equations (a) and (b):

$$f_{1i} = h(IDi \parallel x) \qquad (a)$$

$$f_{2ij} = P_{SKj} \oplus f_{1i} \qquad (b)$$

3. **Distribution to Routers and Sensors**: Each router receives its unique set of parameters (P_{SKj}) from the AS, enabling them to authenticate devices and facilitate secure data transmission within the network.

Similarly, every sensor i receives its credentials f_{1i} and all f_{2ij} for the same sensor but different routers.

This structured initialization ensures that all entities within the IoT network can engage in secure and authenticated communications, leveraging the mathematical properties of cyclic groups and the efficiency of lightweight cryptographic operations.

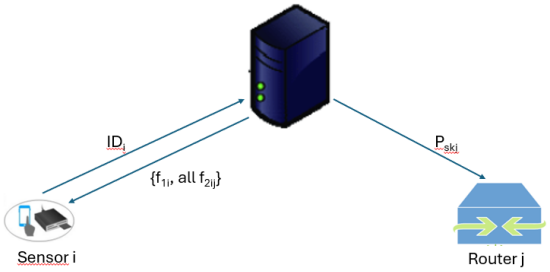

Figure 1. Registration phase

b. Authentication and session Key Agreement

During this phase, sensor i and router j engage in communication over an unsecured channel, which is susceptible to diverse security threats for example eavesdropping, tampering, and replay attacks. To mitigate these risks, the proposed authentication protocol incorporates robust cryptographic mechanisms designed to secure data transmission even in the absence of a secure communication medium. Figure 2 illustrates the procedural flow of this phase, detailing the steps involved in establishing a secure and authenticated session between the sensor and the router.

The proposed authentication protocol functions over an insecure communication channel between a sensor i and router j. The protocol comprises the following steps:

Step 1: Sensor Initialization and Message Transmission

Sensor i selects a random nonce $s \in Zp$ and computes:

- $M_1 = f_{2ij} \oplus f_{1i} \oplus s$
- $A_{IDi} = s \oplus ID_i^s$
- $M_2 = h(M_1 \parallel A_{IDi} \parallel ID_i^s)$

Sensor i then sends the authentication request Message 1 = $\{M_1, M_2, A_{IDi}\}$ to router j.

Step 2: Router Processing and Response Generation

Upon receiving Message 1, router j performs the following computations:

- $ID_i^{s'} = A_{IDi} \oplus M_1 \oplus P_{SKj}$

Since

- $f_{2ij} = P_{SKj} \oplus f_{1i} \rightarrow P_{SKj} = f_{2ij} \oplus f_{1i}$
- $M_1 = f_{2ij} \oplus f_{1i} \oplus s$
- $A_{IDi} = s \oplus ID_i^s$
- $ID_i^{s'} = s \oplus ID_i^s \oplus f_{2ij} \oplus f_{1i} \oplus s \oplus P_{SKj}$

- $ID_i^{s`} = ID_i^s$

Router j confirms the integrity of the received message by verifying whether:

- $h\ (M_1 \| A_{IDi} \| ID_i^s) =? M_2$

If the check fails, the authentication request is declined. Otherwise, router j proceeds by selecting random value r ∈ Zp and computes:

- $SK=(ID_i^s)^r$
- $A_{IDj}= r \oplus P_{SKj}$
- $M_3=SK \oplus ID_i^s$
- $M_4=h\ (M_3 \| A_{IDj} \| ID_i^s)$

Router j then sends the authentication reply Message 2 = $\{M_3, M_4, A_{IDj}\}$ to sensor i.

Step 3: Sensor Verification and Session Key Computation

Upon receiving Message 2, sensor i confirms the legitimacy of the response by ensuring whether:

- $h\ (M_3 \| A_{IDj} \| ID_i^s) = ?\ M_4$

If the check fails, the authentication response is declined. Otherwise, sensor i computes the session key:

- $SK= M_3 \oplus ID_i^s$

Sensor i then computes :

- $M_5=f_{2ij} \oplus f_{1i} \oplus SK$

and sends Message 3 =$\{M_5\}$ to router j.

Step 4: Router Final Verification

Upon receiving Message 3, router j confirms the validity of the session key by ensuring if:

- $SK = ?\ M_5 \oplus P_{SKj}$

If the check successes, the session key SK is accepted for subsequent secure communications. Otherwise, the authentication processes is declined.

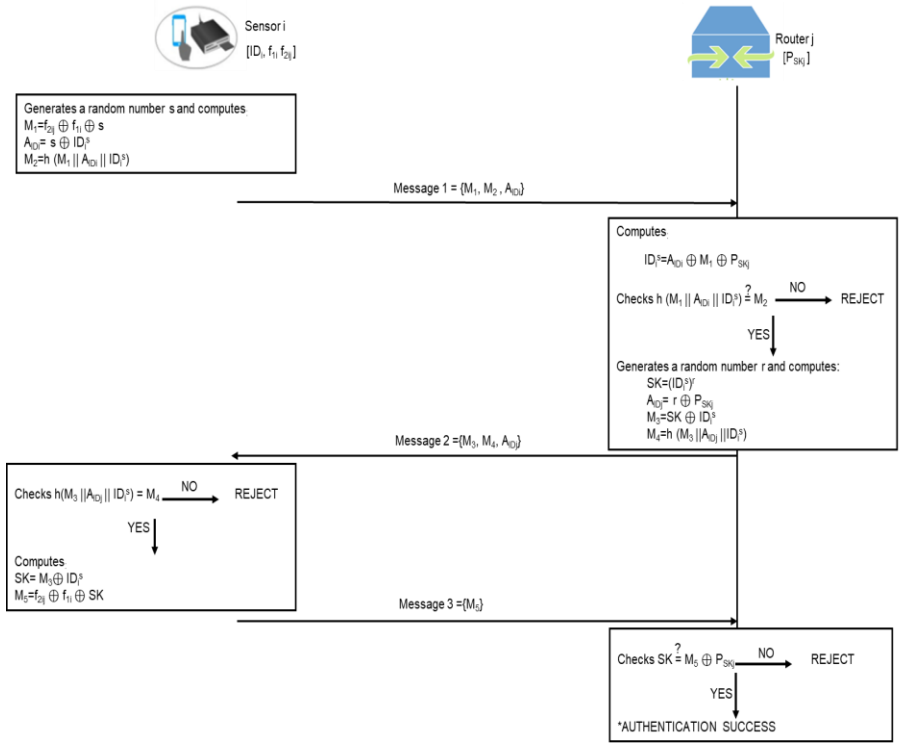

Figure 2. Authentication and Session Key Agreement phase

6. Security analysis

This chapter gives a comprehensive analysis of the security and performance aspects of the proposed Authentication Protocol and compares its features with those of existing authentication schemes referenced in [20], [21] and [22]. As mentioned in Table 2, the proposed protocol demonstrates improved security capabilities relatively to the compared schemes.

Table 2: Key characteristics of existing authentication protocols

Schemes	Alireza Esfahani et al. [20]	Barnana Baruah et al. [21]	Fadi AL-Turjma et al. [22]	Proposed Scheme
Mutual authentication	√	√	√	√
Anonymity	√	√	√	√
Unlinkability	x	√	√	√
Replay attack	√	√	√	√
Man-In-The-Middle Attack	√	√	x	√
Eavesdropping Attack	x	√	√	√
Impersonnation	√	√	√	√
Session Key Disclosure Attack	x	√	x	√

The key security properties of the proposed scheme include:

a. Mutual authentication

The smart sensor and the router authenticate mutually in the authentication phase of the proposed protocol, through the exchange and verification of specific messages.

- **Sensor Authentication:**

Upon receiving Message 1 parameters M_1, M_2 and the anonymized identifier (A_{IDi}), the router computes the hash value
h ($M_1 \| A_{IDi} \| ID_i^s$) and checks whether this computed value matches the received M_2.

If the values are equal, the router authenticates the smart sensor as legitimate.

- **Router Authentication:**

Similarly, when the smart sensor receives Message 2 parameters M_3, M_4 and the anonymized identifier (A_{IDj}) from the router, it computes the hash value: h ($M_3 \| A_{IDj} \| ID_i^s$).

It then verifies whether the computed hash matches the received M_4.

If the values are equal, the smart sensor authenticates the router as legitimate.

b. Anonymity/identity confidentiality

In the proposed Secure Authentication Protocol, each sensor utilizes a pseudonymous identifier (IDi) instead of its real identity. Hence, adversaries cannot deduce the sensor's identity, thereby enhancing privacy. Furthermore, the protocol generates distinct pseudonymous identities for both the sensor and the router, which are unknown to each

other. This strategy effectively prevents information leak between the device and the router. Consequently, the protocol mechanism upholds the principles of anonymity and identity protection.

c. Unsinkability

In the proposed authentication protocol, consider an adversary intercepting two distinct instances of the same message transmitted by a sensor i during separate sessions. In session y, sensor i sends Message $1^y = \{M_1^y, M_2^y, A_{IDi}^y\}$, where the identity-related components are randomized as $M_1 = f_{2ij} \oplus f_{1i} \oplus s$ and $A_{IDi} = s \oplus ID_i^s$ using a session specific nonce s_y. Similarly, in session z, the sensor transmits Message$1^z = \{M_1^z, M_2^z, A_{IDi}^z\}$, utilizing a different nonce s_z. Due to the incorporation of a unique nonce in each session, the identity parameters differ across sessions, i.e.$\{M_1^y, M_2^y, A_{IDi}^y\} \neq \{M_1^z, M_2^z, A_{IDi}^z\}$. Consequently, an adversary cannot correlate these messages to a specific sensor, thereby achieving unlinkability within the proposed scheme.

d. Resistance to Replay attack

We suppose an adversary intercepted Message 1 and attempts to launch a replay attack by repeating this message, the router will decline the authentication request. This is due to the anonymous identity A_{IDi} that is computed with a hash function incorporating a random number s, which is exclusively known to sensor i. Without knowledge of s, the adversary cannot generate a valid A_{IDi}, rendering the replayed message invalid.

Similarly, if an adversary tries to reply Message 3, the sensor will reject the replayed message since A_{IDj} is computed using a hash function that incorporates a random number s, exclusively known to sensor i.

This mechanism ensures that each authentication session is unique and resistant to replay attacks. By integrating pseudonymous identifiers derived from unpredictable random values, the proposed protocol effectively safeguards against unauthorized access attempts through message replay.

e. Resistance to Man-In-The-Middle Attack

Even if a malicious entity obtains the smart sensor's identity (IDi), he/she cannot launch a Man-In-The-Middle attack or calculate the session key (SK) without access to the secret key x, that is securely deposited in the Authentication Server (AS) and at no time disclosed to any other entity. Additionally, the malicious entity cannot impersonate a trusted router and authenticate other sensors, as it lacks the pre-shared secret key (PSK) required for such authentication.

f. Resistance to Eavesdropping Attack

An adversary A may intercept transmitted messages within the network. However, the sensor's identity parameters are randomized into components $M_1 = f_{2ij} \oplus f_{1i} \oplus s$ and $A_{IDi} = s \oplus ID_i^s$ through the application of XOR operations with session specific random nonce. Additionally, sensitive information such as nonces s and r, essential for session key generation, are similarly protected using XOR operations. This approach ensures that even if A captures the messages, the underlying sensitive data remains concealed, rendering the extraction of meaningful information infeasible. Consequently, the proposed scheme demonstrates robustness against eavesdropping attacks.

g. Resistance to Impersonation and Session Key Disclosure attacks

Consider a scenario where a malicious sensor k, attempts to impersonate another sensor i. Despite any efforts, sensor k cannot derive the session key (SK_{ij}) established between sensor i and the router j. This is because SK_{ij} is generated using random number s and r, which are uniquely created and securely stored by sensor i and router j. Without access to s and r, sensor k lacks the necessary information to compute the correct session key.

This mechanism ensures that each authentication session is unique and resistant to impersonation attacks. By integrating pseudonymous identifiers derived from unpredictable random values and safeguarding critical cryptographic keys, the proposed protocol effectively defends against unauthorized access attempts through impersonation and session key disclosure.

h. Resistance to Modification attack

By producing a unique hash value for a given message, the one-way hash function h () ensures data integrity. Any alteration to the original message, even by a single bit, results in a significantly different hash output. Consequently, if an adversary modifies a message during transmission, the router/sensor can detect this tampering by recalculating the hash and comparing it to the received hash value. A mismatch between these values indicates that the message has been altered, prompting the router/sensor to reject it. This mechanism effectively safeguards against unauthorized modifications and ensures the authenticity of the transmitted data.

7. Performance analysis

In this section, we assess the performance of the proposed authentication mechanism by analysing its communication overhead, computational cost, and storage requirements.

a. Communication Cost

To weigh the communication overhead of the proposed authentication scheme, we refer to the parameter settings outlined in Table 3. These parameters define the size of various cryptographic elements and identifiers used within the protocol. Based on these settings, the total bandwidth overhead can be calculated by summing the sizes of all messages exchanged during the authentication process.

In [29] Alshawish and Al-Haj, assessed the communication overhead by calculating the total number of bytes transmitted during the mutual authentication process. They consider the sizes of individual messages, and the total of messages exchanged within entities such as the IoT device, authentication server, and management server.

Similarly, in [30], Xiaofeng Wu et al. analyze the communication overhead by comparing the number of signaling messages required in their proposed scheme against existing schemes. They provide a theoretical comparison of communication costs, demonstrating the efficiency of their approach in terms of reduced message exchanges.

By applying the parameter values from Table 3 to the message structures defined in the proposed mechanism, we can compute the total communication overhead. This involves calculating the size of each message based on the constituent parameters and summing these sizes across all messages exchanged during the authentication process.

This approach ensures a comprehensive assessment of the bandwidth requirements of the authentication protocol, facilitating comparisons with existing schemes and aiding in the optimization of communication efficiency.

Communication cost of our authentication protocol is equivalent to:

|Message 1| + |Message 2| + |Message 3|=**896 bits**,

While:

- $|\text{Message 1}| = |M_1| + |M_2| + |A_{IDi}| = 384$ bits
- $|\text{Message 2}| = |M_3| + |M_4| + |A_{IDj}| = 384$ bits
- $|\text{Message 3}| = |M_5| = 128$ bits

The proposed scheme incurs lower communication cost of 896 bits compared to those in [22] estimated at 1212 bits and [20], [21] evaluated at 1024 bits while enhancing the security aspect.

Table 3: Parameter settings

Parameter	**Size in bits**
ID_i	128
ID_i^s	128
A_{IDi}	128
A_{IDj}	128
f_{1i}	128
f_{2ij}	128
Hash value	128

b. Computation Cost

We estimate the computation overhead of our scheme based on the average time consumed by the main operations. T_h denotes hash function execution time, T_{ran} denotes random number generation time, T_{XOR} denotes XOR operation execution time and T_{expo} denotes modular exponentiation operation execution time.

Table 4 and table 5 highlight the computational cost associated with each of the three main components involved in the proposed authentication mechanism, namely the sensor, router, and authentication server.

In comparison to other schemes, the proposed scheme incurs the lowest computational cost during the registration phase, requiring only $T_{XOR} + T_h$.

Table 4: Registration Phase Computation Cost comparison

Schemes	Sensor	Router	AS
Alireza Esfahani et al. [20]	-------	-------	$T_{XOR} + 2 * T_h$
Barnana Baruah et al. [21]	T_{expo}	-------	$2 * T_h + 2 * T_{XOR}$
Fadi AL-Turjma et al. [22]	-------	-------	$3 * T_h + 1 * T_{XOR}$
Proposed Scheme	-------	-------	$T_{XOR} + T_h$

Throughout the authentication phase, the proposed scheme reduces the hash operation usage by introducing only two exponentiation operations. Additionally, XOR and random number generation operations are used at approximately the same frequency as in other schemes. Hence, the proposed scheme achieves more efficient computational performance while enhancing protocol security.

Table 5: Authentication Phase Computation Cost comparison

Schemes	Sensor	Router	AS
Alireza Esfahani et al. [20]	$4*T_{XOR} + 7*T_h + T_{ran}$	$6*T_{XOR} + 8*T_h + T_{ran}$	-------
Barnana Baruah et al. [21]	$5*T_{XOR} + 5*T_h + T_{ran} + T_{expo}$	$6*T_{XOR} + 6*T_h + 2*T_{ran} + 2*T_{expo}$	-------
Fadi AL-Turjma et al. [22]	$4*T_{XOR} + 7*T_h + T_{ran}$	-------	$6*T_{XOR} + 9*T_h + T_{ran}$
Proposed	$6*T_{XOR} + 2*T_h + T_{ran} + T_{expo}$	$5*T_{XOR} + 2* T_h + T_{ran} + T_{expo}$	-------

c. Storage Cost

Table 6 presents the detailed storage requirements for each component in the proposed scheme.

Table 6: Storage Cost of the proposed Scheme

Parameter	Sensor	Router	AS
ID_i	√	-	√
ID_i^s	√	√	-
A_{IDi}	√	√	-
A_{IDj}	√	√	-
f_{1i}	√	-	√
f_{2ij}	√	-	√
P_{SKj}	-	√	√
Random s	√	-	-
Random r	-	√	-
M_1	√	√	-
M_2	√	√	-
M_3	√	√	-
M_4	√	√	-
M_5	√	√	-

The storage requirements are determined based on the size of each parameter to store in the memory of each entity within the system. Table 7 illustrates a comparison of the memory requirements between the proposed scheme and existing approaches.

Table 7: Storage Cost Comparison

Scheme	**Sensor**	**Router**	**AS**
Alireza Esfahani et al. [20]	1536 Bits	1664 Bits	640 Bits
Barnana Baruah et al. [21]	1664 Bits	1536 Bits	512 Bits
Fadi AL-Turjma et al**.** [22]	1408 Bits	128 Bits	1536 Bits
Proposed	1536 Bits	1280 Bits	512 Bits

The proposed scheme demonstrates lower storage overhead compared to the schemes in [28] and [29]. Although its storage overhead is marginally higher than that of the scheme in [30], the latter is considered vulnerable to session key disclosure attack as explained in section 6-table 2.

8. Conclusion

Through the precedent paragraphs, we suggested a new lightweight authentication scheme for IoT environments, relying solely on simple operations like hash and Exclusive OR. The proposed solution offers low computational cost, minimal storage and communication overhead, whereas ensuring mutual authentication, device identity confidentiality, session key agreement, and robustness against various attacks, including man-in-the-middle, impersonation, replay, and session key disclosure attacks. The verification results confirm that the protocol meets essential security requirements and effectively resists various types of attacks. A comparative performance analysis with existing protocols in the literature demonstrates that the proposed solution is secure, well suited for IoT environments and lightweight. As a perspective for future work, we envisage implementing the protocol and evaluating its scalability and performance in real world IoT scenarios.

Funding: “This research received no external funding”

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

References

[1] B. Harjito and S. Han, "Wireless Multimedia Sensor Networks Applications and Security Challenges," in *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, Nov. 2010.

[2] Kumar, U. Jain, M. Hussain, M. K. I. Rahmani, and A. S. Banga, "Mechanism for Device Authentication and Session Key Generation in Industrial Internet of Things Networks," *IEEE Access*, vol. 12, Jul. 2024.

[3] P. P. Ray, D. Dash, and N. Kumar, "Sensors for internet of medical things-State-of-the-art, security and privacy, issues, challenges and future directions," *Computer Communications*, vol. 160, pp. 111-131, Jul. 2020.

[4] S. Sathasivam and M. R. Vignesh, "Healthcare Sensors Issues, Challenges & Security Threats in Wireless Body Area Network: A Comprehensive Survey," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 5, no. 4, May-Jun. 2021.

[5] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199-221, Aug. 2018.

[6] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical Layer based Message Authentication with Secure Channel Codes," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1-1, Sep.-Oct. 2020.

[7] Albalawi, A. Almrshed, A. Badhib, and S. Alshehri, "A Survey on the Authentication Techniques in Internet of Things," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, Apr. 2019.

[8] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, and H. Sun, "Secure Identity Authentication of Community Medical Internet of Things," *IEEE Access*, vol. 7, Aug. 2019.

[9] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2959-2971, May 2021.

[10] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, and N. B. A. Juma'at, "Review on Security of Internet of Things Authentication Mechanism," *IEEE Access*, vol. 7, Oct. 2019.

[11] Thakare and Y.-G. Kim, "Secure and Efficient Authentication Scheme in IoT Environments," *Applied Sciences*, vol. 11, no. 24, 2021.

[12] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," *IEEE Access*, vol. 6, Dec. 2018.

[13] K. Sahu, S. Sharma, S. S. Tripathi, and K. N. Singh, "A Study of Authentication Protocols in Internet of Things," in *2019 International Conference on Information Technology (ICIT)*, Dec. 2019.

[14] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5007-5017, Sep. 2019.

[15] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649-2656, Feb. 2022.

[16] L. Nkenyereye, A. Thakare, P. Khataniar, R. Imandi, and P. K. B. N, "Lightweight Authentication Protocol for Smart Grids: An Energy-Efficient Authentication Scheme for Resource-Limited Smart Meters," *Mathematics*, vol. 13, no. 4, p. 580, 2025.

[17] N. Paliwal, "Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for Industrial Internet of Things," *IEEE Access*, vol. 7, Sep. 2019.

[18] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things," *IEEE Access*, vol. 7, Apr. 2019.

[19] S. Khan, A. I. Alzahrani, O. Alfarraj, N. Alalwan, and A. H. Al-Bayatti, "Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices," *IEEE Access*, vol. 7, Nov. 2019.

[20] Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, and A. Bicaku, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288-296, Feb. 2019.

[21] Baruah and S. Dhal, "An Efficient Authentication Scheme for Secure Communication between Industrial IoT Devices," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2020.

[22] F. Al-Turjman and B. D. Deebak, "Seamless Authentication: For IoT-Big Data Technologies in Smart Industrial Application Systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2411-2420, Apr. 2021.

[23] Badhib, S. AlShehri, and A. Cherif, "A Robust Device-to-Device Continuous Authentication Protocol for the Internet of Things," *IEEE Access*, vol. 9, Sep. 2021.

[24] P. Vadhan, "Cyclic Groups & Cryptographic Applications," Harvard University Lecture Notes, 2009.

[25] D. Santis, A. L. Ferrara, M. Flores, and B. Masucci, "Continuous Entity Authentication in the Internet of Things Scenario," *MDPI*, 2021.

[26] S. Rath, J. Ramalingam, and C.-C. Lee, "On Efficient Parallel Secure Outsourcing of Modular Exponentiation to Cloud for IoT Applications," *Mathematics*, vol. 12, no. 5, p. 713, 2024.

[27] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Security and Communication Networks*, vol. 2017, 2017.

[28] P. Hao, X. Wang, and W. Shen, "A Collaborative PHY-Aided Technique For End-to-End IoT Device Authentication," *IEEE Access*, vol. 6, Jul. 2018.

[29] Alshawish and A. Al-Haj, "An efficient mutual authentication scheme for IoT systems," *The Journal of Supercomputing*, Apr. 2022.

[30] X. Wu, F. Ren, Y. Li, Z. Chen, and X. Tao, "Efficient Authentication for Internet of Things Devices in Information Management Systems," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.