frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 23 April 2025
DOI 10.3389/fphy.2025.1540716

OPEN ACCESS

EDITED BY
Gaogao Dong,
Jiangsu University, China

REVIEWED BY
Chaker Abdelaziz Kerrache,
University of Ghardaia, Algeria
Abdelkarim Ben Sada,
University College Cork, Ireland

*CORRESPONDENCE
Zhenbo Zhang,
zhenbozhang17@outlook.com

RECEIVED 06 December 2024
ACCEPTED 20 March 2025
PUBLISHED 23 April 2025

CITATION
Zhang Z, Liu X, Gong L and Zhuang Z (2025) A signature-based secure interaction scheme for logistics management systems in the internet of things.
Front. Phys. 13:1540716.
doi: 10.3389/fphy.2025.1540716

A signature-based secure interaction scheme for logistics management systems in the internet of things

Zhenbo Zhang[1]*, Xingken Liu[1], Lijiahui Gong[2] and Zhaoyu Zhuang[3]

[1]School of Management, Guangzhou College of Technology and Business, Foshan, China, [2]School of Business, Wuhan Huaxia Institute of Technology, Wuhan, China, [3]Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

The rapid growth of e-commerce has been significantly driving the logistics industry's development, while the speed of information technology transformation has laid a solid foundation for this progress. The Internet of Things (IoT), recognized as a representative of next-generation information technology, has injected new vitality into intelligent logistics management through its powerful data collection and transmission capabilities. The importance of user access control mechanisms has become increasingly evident in logistics management systems. Therefore, this paper proposes a signature-based authenticated scheme for logistics management systems. In this scheme, the user's password, biometrics and smart card are used as the three authentication factors. During the login and authentication phase, registered users and devices in the logistics management system can securely and efficiently complete mutual authentication and key agreement. To verify the security performance of the proposed scheme, an simulation analysis is performed using the Scyther tool. Furthermore, performance evaluation demonstrates that the proposed scheme not only significantly enhances the security of the logistics management system but also maintains low costs.

KEYWORDS

internet of things, security, signature-based, logistics management systems, authentication

1 Introduction

The continuous advancement of the socio-economic landscape has made the logistics industry a crucial pillar of the economic system, profoundly influencing people's daily lives. Driven by the rapid advancements in information technology, Internet of Things (IoT) and artificial intelligence, the logistics industry is steadily advancing toward a new phase of intelligent transformation. By leveraging IoT technology, the logistics management supply chain has been constructed and optimized, establishing an integrated supply channel for goods circulation. This has not only significantly contributed to the prosperity of production and sales industries but also effectively addressed various challenges in traditional logistics, greatly enhancing distribution efficiency and service quality. The core of logistics management systems under IoT is to enable seamless interaction and sharing of diverse information, thereby effectively

reducing transportation costs, improving efficiency, and driving the intelligence of logistics decision-making and execution. Through intelligent management models, high-quality logistics services can be provided at reduced costs. The essence of IoT-based logistics management systems lies in relying on real-time and comprehensive information to emulate human intelligence, make optimal decisions, create greater value for customers, and deliver a superior service experience. Traditional logistics models have often relied on experience-based decision-making due to delayed and insufficient information. In contrast, IoT-based logistics management systems have achieved revolutionary innovation over traditional logistics, having profound impacts on the industry's structure, operating models, business models, ecological systems, and development paradigms. With the widespread application of big data technology, IoT-based logistics management systems leverage big data to process logistics information, further integrating characteristics such as informatization, digitization, networking, and visualization.

With the deep integration of IoT technology into logistics management systems, sensors, as an indispensable component of these systems, play a pivotal role [1]. They serve not only as direct perceivers of logistics environment information but also as key enablers for the intelligent and precise control of logistics processes. Sensors can accurately collect and monitor in real time various physical and chemical parameters in logistics environments, such as temperature, humidity, and pressure, providing abundant and accurate data support for logistics decision-making. These real-time data not only enhance the transparency of logistics processes but also enable managers to promptly identify and address anomalies that could affect cargo safety and quality, thereby ensuring the efficiency and security of logistics operations. In IoT-based logistics management systems, mutual authentication between sensor devices and users is important for ensuring the security and efficiency of logistics. It effectively prevents unauthorized access and operations in complex logistics environments, safeguarding the integrity and security of logistics information. Although IoT-based logistics management systems have made significant progress compared to traditional models, existing authentication schemes still have key limitations. Most current schemes rely on two-factor authentication, which is vulnerable to offline brute force attacks, device theft, and session hijacking threats in untrusted networks. Additionally, traditional schemes often overlook the computational limitations of edge devices, resulting in unacceptable delays during large-scale deployment. Based on the above discussion, the main contributions of this paper are as follows:

(1) This paper proposes a signature-based authenticated scheme for logistics management systems. The proposed scheme enables legitimate registered users to access data or tasks from devices. During the user login phase, passwords, personal biometrics and smart card are used to verify user identity. In the authentication phase, mutual authentication between the user and device is performed, and a secure session key is established to ensure the security of subsequent communications between the user and the device.
(2) Formal security analysis using Scyther has been conducted to ensure the security of the proposed scheme. Furthermore, heuristic analysis indicates that the proposed scheme can resist common attacks while maintaining user-friendliness. Experimental results show that the scheme performs excellently in terms of security strength, communication efficiency, and scalability, providing a practical and feasible security authentication framework for large-scale intelligent logistics systems.

In Section 2 and Section 3, a brief review of the relevant literature and knowledge is presented. The proposed scheme is detailed in Section 4. The security of the proposed scheme is evaluated in Section 5. Subsequently, performance analysis is conducted in Section 6. Finally, we conclude this paper.

2 Literature review

Authentication serves as the first line of defense in logistics management systems. For sensor devices, mutual authentication with users is conducted to validate the legitimacy of user identities while also verifying whether the devices themselves are authorized to read or write specific information. This bidirectional authentication mechanism significantly enhances system security and mitigates the risks of data breaches or damages caused by malicious attacks or operational errors.

In industrial scenarios or smart logistics contexts, numerous authentication key agreement protocols have been proposed by researchers [2–5]. Chang et al. [6] discovered that Kalra et al.'s scheme [5] failed to achieve the claimed mutual authentication and session key agreement. An improved protocol was proposed. However, Wang et al. [7] demonstrated that Chang et al.'s [6] scheme remained insecure. Subsequently, the protocol was improved, and its security was formally proven. Later, Pham et al. [8] optimized Wang et al.'s [7] protocol to support mutual authentication between devices. Despite its advantages in security and efficiency, the scheme lacked privacy protection mechanisms for devices due to identity exposure during authentication. Pham et al. [9] further improved the aforementioned protocol, and a privacy-preserving authentication protocol was proposed to support secure communication between devices in distributed network architectures. Amin et al. [10] propose a scheme that incurs significant computational overhead. Li et al. [11] proposed a scheme based on ECC, but it involves sunstantial. Wazid et al. [12] proposed an identity authentication scheme vulnerable to forgery threats, while Li et al. [13] introduced a privacy-preserving data aggregation protocol susceptible to impersonation threats. To reduce overhead, Sodorov et al. [14] proposed an RFID-based ultra-lightweight identity verification key exchange for intelligent supply chains. Later, Sergi et al. [15] introduced a secure authentication algorithm for smart logistics and IoT systems. In recent years, to address the growing demand for secure communications in industrial IoT, researchers have conducted extensive studies on authentication and key management. Zhou et al. [16] proposed a two-factor authentication mechanism utilizing hash functions and XOR operations, which emphasized lightweight properties. However, subsequent studies revealed its susceptibility to replay attacks and key leakage issues. To address these shortcomings, Ali et al. [17] introduced a three-factor authentication approach incorporating hash functions, XOR operations, and AES encryption. Despite these enhancements, the scheme failed to counter man-in-the-middle (MITM) attacks and did not achieve the expected

level of secure authentication, as noted in related research [18]. In practice, approaches relying solely on lightweight operations often face challenges in maintaining robust security. To mitigate this, public key cryptography [5] has been employed to strengthen protocol security. Das et al. [19] proposed a certificate-based device access control mechanism known as LACKA-IoT. Nevertheless, its significant computational and communication overhead restricts its effectiveness in resource-constrained industrial settings. Meanwhile, Chatterjee et al. [20] designed a protocol that leverages identity-based encryption alongside hash functions, but it fell short in ensuring sufficient forward secrecy.

Identity-Based Cryptography (IBC) eliminates the need for extensive digital certificate exchanges in secure applications, making it more lightweight and easier to deploy. Under an IBC framework, a device's private key is generated based on its unique identifier, removing the requirement for PKI-provided certificate support. This significantly broadens the application scope of public key cryptography while substantially reducing the costs associated with certificate maintenance. Over time, identity-based key algorithms have undergone numerous advancements [21–24]. Li et al. introduced a decentralized multi-signature protocol [25] that integrates identity-based signatures with the Schnorr scheme under the elliptic curve discrete logarithm problem. This protocol addresses the challenges of security and efficiency in IoT identification within centralized signature schemes. Fang et al. utilized IBS to prevent data alteration and reduce the overhead of third-party authentication [26]. Heo et al. [27] designed an identity-based mutual authentication scheme for power line communication, effectively simplifying the deployment and management of authentication credentials by eliminating the need for public key certificates. Li et al. [28] proposed a cloud-based identity authentication scheme designed for asymmetric mutual authentication between cloud servers and device users. Jin et al. [29] focused on data security and privacy in wireless body area networks by designing a privacy-preserving scheme based on biometric identities. In this scheme, user identities are constructed from biometric traits. Based on this, the authors developed an access control scheme. Subsequently, many researchers [30–32] have proposed identity-based authentication schemes in Vehicular Ad hoc Networks (VANET) to improve the communication efficiency of VANET. Existing research has made significant progress in the design of authentication protocols for logistics and industrial scenarios, but limitations remain. Most schemes struggle to balance security and lightweight requirements. Lightweight protocols are often vulnerable to replay attacks or key leakage risks due to simplified computations, while schemes that introduce public-key cryptography improve security but incur high overhead due to certificate management or complex computations, making them difficult to adapt to resource-constrained industrial environments.

3 Preliminaries

3.1 System model

In IoT-based logistics management systems, sensors capture detailed information about objects, including location, temperature, orientation, and other parameters. Any authenticated user can access the status of these objects. The system model proposed is illustrated in Figure 1, with the following participants:

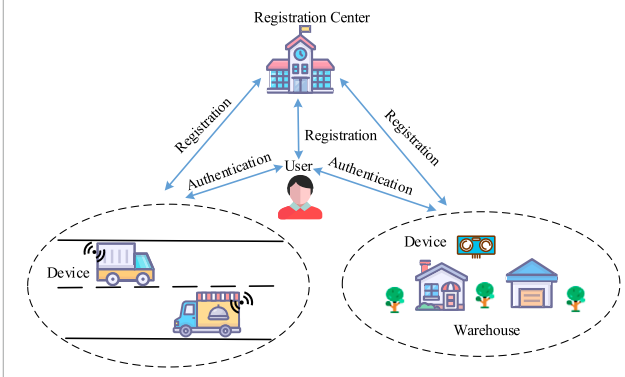

FIGURE 1
System model.

3.1.1 Registration center (RC)

RC is responsible for initializing the system and handling the registration of users and service providers. RC distributes secret information associated with each registrant. Notably, in this scheme, the RC is not involved during the mutual authentication phase.

3.1.2 User (U_i)

Users can directly access sensory data collected by devices, allowing them to obtain real-time information about the environment, devices, or target objects. This sensory data can include various types of information such as light intensity, location, and motion status, depending on the type of sensor and the application scenario. By accessing this data, users or applications can accurately track specific target objects, such as the current location and condition of a package during logistics transportation.

3.1.3 Device (D_i)

Sensor devices deployed in warehouses and on vehicles efficiently read item-related information, including identity, status, and other relevant parameters. This may involve unique identifiers, transportation conditions, and location records for the goods being tracked.

3.2 Elliptic curve cryptography

Definition 1: Elliptic Curve Discrete Logarithm Problem (ECDLP):

E_q is an elliptic curve group over the prime field F_p. P is a generator of E_q. Computing $W = sP$ is relatively easy for given $s \in Z_q^*$ and $W \in E_q$. However, given W, P, to find an integer such s that $W = sP$ is computational hard.

Definition 2: Elliptic Curve Diffie- Hellman Problem (ECDHP):

Let P, εP and γP are points over an elliptic curve. It is computational infeasible to solve $\varepsilon\gamma P$ without knowledge of ε and γ.

TABLE 1 Symbols.

Notations	Definitions
RC	Registration Center
ID_i	Identity for user
DID_j	Identity for Device
SK	session key
T_i	Current Timestamp
$H(\cdot)$	Hash function
$\oplus$	Nonequivalence Operation
k	System Private Key

3.3 Adversary model

In our proposed scheme, we adopt the widely recognized Dolev-Yao threat model (DY model) to assess potential security risks. The DY model assumes a powerful adversary with full control over the communication channel, capable of eavesdropping, tampering with, injecting, or replaying any transmitted message [33–35]. We assume the following capabilities for an adversary (denoted as A):

(1) It is assumed that $\mathcal{A}$ can intercept, block, and alter messages transmitted over public channels.
(2) It is assumed that $\mathcal{A}$ numerate all possible identity-password pairs within the dictionary space.
(3) In three-factor authentication system, it is assumed that $\mathcal{A}$ could potentially compromise any two of the authentication factors.

4 Proposed protocol

We propose a signature-based authenticated scheme for logistics management systems. It comprises three types of participants: the registration center (RC), sensor devices (D_j), and users (U_i). Table 1 shows the symbols.

4.1 System setup

E is an elliptic curve defined over F_p, and the RC selects a cyclic additive group G on $E(F_p)$ with an order of q, where q is a prime number. The generator of G is P. RC randomly selects $k \in Z_q^*$ as the system's master key, and the system's public key is $P_{pub} = kP \in G$. RC chooses a secure hash function $H()$. RC securely stores the master key k and publishes parameters $\{G, Q.P, P_{pub}, H()\}$.

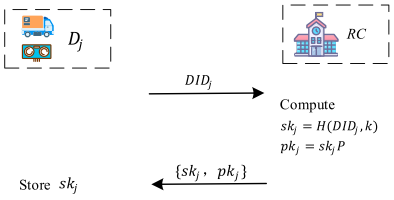

FIGURE 2
Device registration process.

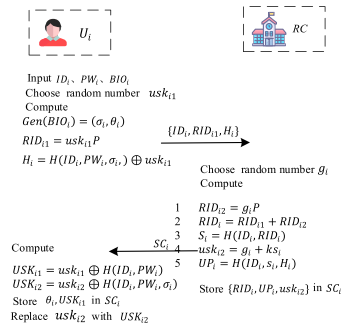

FIGURE 3
User registration process.

4.2 Registration phase

4.2.1 Device registration

(1) D_j sends its identity value DID_j to RC.
(2) Upon receiving the identity value of D_j , RC calculates $sk_j = H(DID_j, k)$ and $pk_j = sk_j P$. The RC then sends $\{sk_j, pk_j\}$ to D_j via a credible channel.
(3) D_j stores sk_j securely and publicly shares pk_j.The registration process is as illustrated in Figure 2.

4.2.2 User registration

(1) U_i chooses its identity ID_i, a password PW_i, and inputs biometric BIO_i. Then, U_i generates a random number usk_{i1} and computes $Gen(BIO_i) = (\sigma_i, \theta_i)$, $RID_{i1} = usk_{i1}P$, $H_i = H(ID_i, PW_i, \sigma_i) \oplus usk_{i1}$. Finally, U_i sends $\{ID_i, RID_{i1}, H_i\}$ to RC.
(2) Upon receiving $\{ID_i, RID_{i1}, H_i\}$, RC checks whether ID_i exists in its authentication list. If it does, the user is considered a duplicate registrant, and the server rejects the request. If ID_i does not exist, the RC stores ID_i in its authentication list. Then, RC selects a random number g_i, and computes $RID_{i2} = g_i P$, $RID_i = RID_{i1} + RID_{i2}$, $S_i = H(ID_i, RID_i)$, $usk_{i2} = g_i + ks_i$, $UP_i = H(ID_i, s_i, H_i)$. Finally, RC stores $\{RID_i, UP_i, usk_{i2}\}$ in smart card SC_i and issues to U_i via reliable channel.
(3) Upon receiving SC_i, U_i computes $USK_{i1} = usk_{i1} \oplus H(ID_i, PW_i)$, $USK_{i2} = usk_{i2} \oplus H(ID_i, PW_i, \sigma_i)$, replaces usk_{i2} with USK_{i2}, and stores θ_i and USK_{i1} in SC_i.

The user registration process is as illustrated in Figure 3.

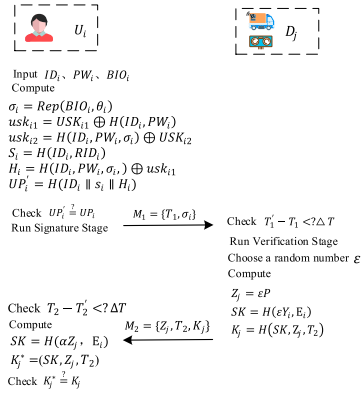

FIGURE 4
Login and mutual authentication process.

4.3 User login

U_i enters ID_i、 PW_i and imprints BIO_i. Next the smart card performs the following calculations: $\sigma_i = Rep(BIO_i, \theta_i)$, $uski_1 = USKi_1 \oplus H(ID_i, PW_i)$, $uski_2 = H(ID_i, PW_i, \sigma_i) \oplus USKi_2, S_i = H(ID_i, RID_i), H_i = H(ID_i, PW_i, \sigma_i,) \oplus usk_{i1}, UP_i' = H(ID_i \| s_i \| H_i)$, and verifies whether $UP_i' = UP_i$. If $UP_i' \neq UP_i$, the session terminates. If $UP_i' = UP_i$, the smart card proceeds to the next step.

4.4 Mutual authentication

Figure 4 shows the mutual authentication process between the device and the user, where the user completes the signing process and the device verifies the signature. The process uses a signature scheme that signs messages with pre-generated private keys. Figure 5 is verification algorithm. The detailed steps are as follows:

(1) U_i forms current timestamp T_1. The user generates a signature: $\sigma_i = (G_i, RID_i, Y_i, \mathrm{F}_i, PID_i)$ according to the signing algorithm shown in Figure 6. Finally, the user sends: $M_1 = \{\sigma_i, T_1\}$ to D_j over a public channel.

(2) Upon receiving $\{\sigma_i, T_1\}$, D_j verifies the freshness of the timestamp T_1. If the check holds, D_j executes the signature verification algorithm to check its validity. If successful, D_j selects a random number ε, computes $Z_j = \varepsilon P$, $SK = H(\varepsilon Y_i, \mathrm{E}_i), K_j = H(SK, Z_j, T_2)$ and sends $\{Z_j, K_j, T_2\}$ to the user, which T_2 is current timestamp.

(3) Upon receiving $\{Z_j, K_j, T_2\}$, the smart card checks the freshness of the timestamp T_2. If the check holds, the smart card computes $SK = H(\alpha Z_j, \mathrm{E}_i)$, $K_j^* = (SK, Z_j, T_2)$. The smart card verifies whether $K_j^* = K_j$. If they match, mutual authentication is successfully completed, and the session key SK is established.

4.5 Password and biometric update

User U_i can update their password and biometric data offline by following these steps:

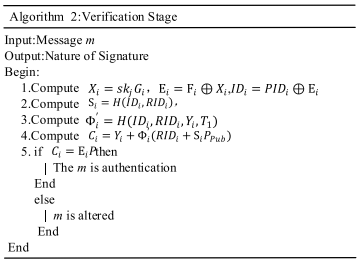
Algorithm 2:Verification Stage
Input:Message m
Output:Nature of Signature
Begin:
1.Compute $X_i = sk_j G_i$, $\mathrm{E}_i = \mathrm{F}_i \oplus X_i, ID_i = PID_i \oplus \mathrm{E}_i$
2.Compute $S_i = H(ID_i, RID_i)$,
3.Compute $\Phi_i^{'} = H(ID_i, RID_i, Y_i, T_1)$
4.Compute $C_i^{'} = Y_i + \Phi_i(RID_i + S_i P_{Pub})$
5. if $C_i = \mathrm{E}_i P$then
| The m is authentication
End
else
| m is altered
End
End

FIGURE 5
Verification algorithm.

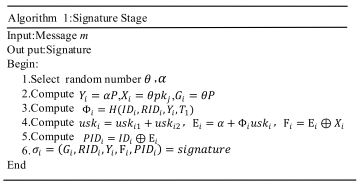
Algorithm 1:Signature Stage
Input:Message m
Out put:Signature
Begin:
1.Select random number θ, α
2.Compute $Y_i = \alpha P, X_i = \theta pk_j, G_i = \theta P$
3.Compute $\Phi_i = H(ID_i, RID_i, Y_i, T_1)$
4.Compute $usk_i = usk_{i1} + usk_{i2}$, $\mathrm{E}_i = \alpha + \Phi_i usk_i$, $\mathrm{F}_i = \mathrm{E}_i \oplus X_i$
5.Compute $PID_i = ID_i \oplus \mathrm{E}_i$
6. $\sigma_i = (G_i, RID_i, Y_i, \mathrm{F}_i, PID_i) = signature$
End

FIGURE 6
Signing algorithm.

(1) U_i inputs ID_i、 PW_i, and imprints BIO_i, then performs the following calculations: $\sigma_i = Rep(BIO_i, \theta_i), usk_{i1} = USK_{i1} \oplus H(ID_i, PW_i), usk_{i2} = H(ID_i, PW_i, \sigma_i) \oplus USK_{i2}, S_i = H(ID_i, RID_i), H_i = H(ID_i, PW_i, \sigma_i,) \oplus usk_{i1}, UP_i' = H(ID_i, s_i, H_i)$. The smart card verifies whether $UP_i' = UP_i$. If $UP_i' \neq UP_i$, the smart card rejects the request. Otherwise, U_i is prompted to input a new password PW_i^{new} and new biometric data B_i^{new}.

(2) U_i inputs PW_i^{new} and B_i^{new}, and then the smart card performs the following calculations: $(\sigma_i^{new}, \theta_i^{new}) = Gen(B_i^{new})$, $H_i^{new} = H(ID_i, PW_i^{new}, \sigma_i^{new}) \oplus usk_{i1}$, $USK_{i2}^{new} = usk_{i2} \oplus H(ID_i, PW_i^{new}, \sigma_i^{new})$, $USK_{i1}^{new} = usk_{i1} \oplus H(ID_i, PW_i^{new})$.

(3) The smart card updates $H_i, USK_{i1}, USK_{i2}, \theta_i$ with $H_i^{new}, USK_{i1}^{new}, USK_{i2}^{new}, \theta_i^{new}$.

5 Security evaluation

5.1 Informal security analysis

Here, we conducted a comprehensive evaluation of potential security risks through heuristic analysis. By simulating real-world attack scenarios, we validated the scheme's ability to defend against informal attacks [36–42].

5.1.1 Mutual authentication

Devices authenticate users by verifying $C_i = \mathrm{E}_i P$. User generates the signature using usk_i. Only users with usk_i can compute a valid signature. Additionally, the user authenticates devices based on $X_i = \theta pk_j$. During the signing process, the user encrypts E_i using X_i. Only devices with the key sk_j can compute X_i and recover E_i, ensuring that K_j^* equals K_j, and successfully establish the session key.

5.1.2 Session key agreement

User and device generate $SK = H(\varepsilon Y_i, \mathrm{E}_i) = H(\varepsilon\alpha P, \mathrm{E}_i)$. The session key consists of $\varepsilon\alpha P$ and E_i, where $\varepsilon\alpha P$ is derived from the elliptic curve Diffie-Hellman key exchange. E_i, generated using usk_i, ensures resistance against attacks targeting session-specific temporary information.

5.1.3 Perfect forward secrecy

Assume $\mathcal{A}$ obtains the user's and device's long-term secrets and intercepts information. $\mathcal{A}$ attempts to recover SK, but SK is protected by random numbers α and ε, where εY_i (αZ_j) is generated using the Diffie-Hellman key exchange. Even if the attacker gains long-term secrets, they cannot retrieve $\varepsilon\alpha P$ from Y_i and Z_j.

5.1.4 User impersonation attack

$\mathcal{A}$ attempting to impersonate U_i needs to create a legitimate login request by generating s_i and H_i. These values require the ID_i, PW_i, BIO_i, and the information stored in SC_i. Only with all these elements can an attacker successfully generate a legitimate login request.

5.1.5 Device impersonation attack

$\mathcal{A}$ attempting to impersonate D_j needs to create a valid response message by computing E_i: $\mathrm{E}_i = \mathrm{F}_i \oplus X_i$, $X_i = sk_j G_i$. Since attacker $\mathcal{A}$ lacks knowledge of $\mathcal{A}$, they cannot compute E_i. Additionally, $\mathrm{E}_i = \alpha + \Phi_i usk_i$. To derive E_i, the attacker would also need the user's usk_i. Thus, $\mathcal{A}$ cannot produce a valid response message.

5.1.6 User-friendliness

During the authentication phase, the registration center remains offline, allowing users to directly access devices without RC. The proposed scheme supports password and biometric updates, which can be completed without further communication with the RC. Therefore, the proposed scheme demonstrates excellent user-friendliness.

5.1.7 Resistance to insider attack

In insider attacks, privileged users such as system administrators may attempt to access legitimate users' accounts. However, in this scheme, the user's PW_i and biometric σ_i are concatenated, and the concatenation is processed using hash function H, XORed with the parameter usk_{i2}. Neither insiders nor the registration center can retrieve the original password.

5.1.8 Stolen smart card attack

In the proposed scheme, if $\mathcal{A}$ steals a smart card, they may attempt to impersonate a legitimate user. However, $\mathcal{A}$ cannot log into system because they must also provide the user's ID_i, password PW_i, and biometric BIO_i. While the smart card is tamper-resistant, $\mathcal{A}$ could extract all stored information. Nevertheless, $\mathcal{A}$ cannot derive the user's password or biometric data.

5.1.9 Temporary secret leakage attack

If the random numbers α and ε are accidentally or maliciously exposed to an attacker $\mathcal{A}$, they can compute $\varepsilon\alpha P$. However, $\mathcal{A}$ still cannot derive $SK = H(\varepsilon Y_i, \mathrm{E}_i) = H(\varepsilon\alpha P, \mathrm{E}_i)$. This is because $\mathcal{A}$ cannot retrieve E_i without access to the user's private key or the device's private key.

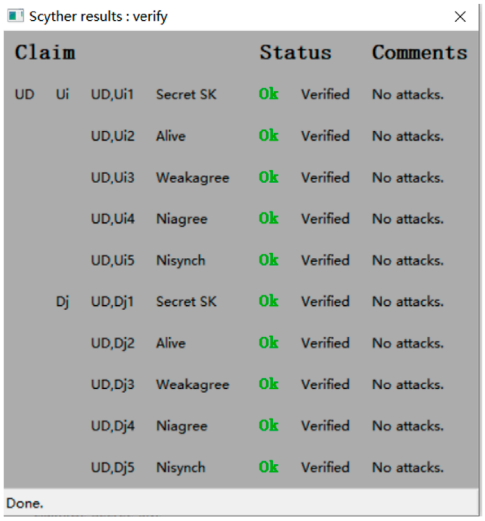

FIGURE 7
Scyther results.

5.1.10 Man-in-the-middle attack

$\mathcal{A}$ forges valid user authentication and responses messages to convince participants that the information is legitimate. To do so, $\mathcal{A}$ would need to compute relevant parameters. However, $\mathcal{A}$ cannot access the user's and device's private keys, password PW_i, or biometric BIO_i. As a result, $\mathcal{A}$ cannot forge valid authentication and response messages.

5.1.11 Replay attack

According to the proposed scheme, the user and the device generate new random numbers and T_i during the authentication phase, and the information recipient verifies the timestamp. Therefore, the proposed new protocol can effectively defend against replay attacks.

5.2 Scyther verification

The proposed scheme was subjected to an in-depth security analysis using Scyther, with the results presented in Figure 7. During the verification process, multiple security properties of the protocol were evaluated, including key confidentiality (Secret SK), liveness (Alive), weak agreement (Weakagree), non-interactive agreement (Niagree), and synchronization (Nisynch). All verification results were marked as "Ok," with a status of "Verified" and no attacks detected, indicating that no potential vulnerabilities were identified under the current verification conditions.

6 Performance analysis

This section will provide a comparative performance analysis, including comparisons of computational and communication overhead. This section focuses on the performance comparison during the login and authentication phases. The performance comparison in this section focuses solely on elliptic curve addition, point multiplication, and hash operations. XOR operations are

TABLE 2 Security comparison.

Feature	[35]	[36]	[37]	[38]	Our
Mutual authentication	✓	✓	✗	✓	✓
Key Agreement	✓	✓	✓	✓	✓
Forward Security	✓	✓	✗	✗	✓
User Friendliness	✓	✓	✗	✓	✓
Replay Attack	✓	✓	✓	✓	✓
Impersonation Attack	✓	✓	✓	✓	✓
Man-in-the-Middle Attack	✓	✓	✓	✓	✓
Temporary Secret Leakage Attack	✓	✓	✓	✓	✓
Stolen Smart Card Attack	✓	✓	✓	✓	✓
Privileged Insider Attack	✓	✗	✓	✓	✓
Three-factor authentication	✗	✗	✗	✓	✓

considered negligible in terms of computational time, and thus bitwise XOR operations are excluded from the time analysis.

6.1 Security comparison

A detailed comparison between the proposed scheme and other related schemes has been carried out. The outcomes of this evaluation are summarized in Table 2. In the table, ✓ signifies the presence of a specific feature or functionality, whereas × denotes its absence.

6.2 Computation overhead comparison

The computational overhead of the proposed protocol is compared with the protocols presented in Refs. [35–38], as shown in Table 3. The symbols T_H, T_{eca}, and T_{ecm} represent the time required to execute a single hash function, elliptic curve addition, and elliptic curve point multiplication, respectively. The following times (in milliseconds) for cryptographic operations are used [40, 41]: $T_h \approx 0.056ms$, $T_{ecm} \approx 13.405ms$, $T_{eca} \approx 0.081ms$, $T_{bp} = 32.713ms$.

During the user login phase, 4 hash operations are performed, along with 3 elliptic curve point multiplications and 1 hash operation for the signature algorithm. Additionally, when the device receives a message, 1 elliptic curve point multiplication and 2 hash operations are performed. During the authentication phase, the device verifies the signature algorithm, requiring 4 elliptic curve point multiplications, 1 elliptic curve addition, and 2 hash operations, along with 2 more hash operations and 2 elliptic curve point multiplications. Therefore, the total computational cost of the proposed scheme is $11T_h + 10T_{ecm} + T_{eca}$.

As shown in Table 3 and Figure 8, the proposed scheme demonstrates significant optimization in computational cost and execution time compared to other protocols. The total

TABLE 3 Computation overhead.

Protocol	Computation overhead	Time (ms)
[35]	$10T_{ecm} + 7T_h + 4T_{eca}$	134.766
[36]	$15T_{ecm} + 17T_h$	211.027
[37]	$3T_{ecm} + 2T_h + 2T_{eca} + 5T_{bp}$	204.054
[38]	$12T_{ecm} + 33T_h + 5T_{eca}$	163.113
Our	$11T_h + 10T_{ecm} + T_{eca}$	134.747

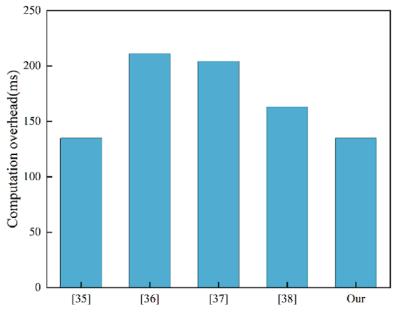

FIGURE 8
Computation overhead.

execution time of the proposed scheme is 134.747 ms, which is significantly lower than the protocols in [36, 37]. Compared to the protocol in [38], the execution time of the proposed scheme is reduced by approximately 17.4%. Additionally, the scheme reduces the number of hash operations and minimizes the computationally expensive elliptic curve point multiplication operations. This indicates that the proposed scheme strikes a better balance between performance optimization and computational complexity, showcasing superior efficiency.

6.3 Communication overhead comparison

To evaluate the communication cost, it is assumed that the user identity, random number, timestamp, hash output, and elliptic curve point (P_x, P_y) require 160 bits, 160 bits, 32 bits, 160 bits, and 320 bits, respectively, where P_x and P_y are the x- and y-coordinates of the elliptic curve point P.

In the proposed protocol, the total length of the exchanged information during the login and authentication phases is calculated as $1984bits$. The communication costs of other protocols are summarized in Table 4. From the comparison, it is evident that the proposed scheme incurs a lower communication overhead. Additionally, the amount of information transmitted during the authentication phase is relatively small. This demonstrates that the proposed scheme achieves higher security and functionality while minimizing communication costs.

As shown in Table 4 and Figure 9, the proposed scheme offers a significant advantage in terms of both communication cost and the amount of transmitted information compared to other protocols. In

TABLE 4 Communication overhead.

Protocol	Communication overhead (bits)
[35]	2,560
[36]	4,832
[37]	3,488
[38]	3,200
Our	1984

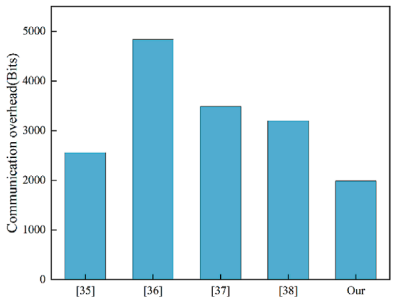

FIGURE 9
Communication overhead.

contrast to protocols, the proposed scheme requires only 2 messages to be transmitted, significantly fewer than the 3 to 5 messages needed by other protocols. This reduction in communication rounds enhances the efficiency of the protocol. In terms of communication cost, the proposed scheme has the lowest overhead at 1984 bits. This indicates that the proposed scheme effectively reduces information transmission costs through optimized communication, significantly improving the overall performance of the protocol, particularly in scenarios where high communication efficiency is required, ensuring the scalability of the protocol in large-scale scenarios.

7 Conclusion

This paper proposes a signature-based authentication scheme designed to meet the security requirements of logistics management systems in the Internet of Things (IoT). The proposed scheme effectively reduces the complexity of elliptic curve operations and the number of communication exchanges, thus achieving a dual reduction in both computational cost and communication overhead. Additionally, the scheme incorporates a three-factor authentication mechanism to enhance system security. To comprehensively evaluate the effectiveness of the proposed protocol, it has been validated through heuristic evaluation, and testing with the Scyther tool. Compared to current mainstream protocols, the proposed scheme shows significant advantages in terms of communication efficiency and operational performance. It not only ensures the effectiveness of identity authentication and maintains data integrity but also provides robust protection against various attacks. The proposed scheme is suitable for various logistics scenarios, such as ensuring that only authorized personnel or devices can operate the system in large warehouses, preventing unauthorized operations or data tampering. Additionally, real-time identity verification is carried out using biometrics (such as fingerprints) and smart cards, ensuring that only designated personnel can unlock or access order information, reducing the risk of cargo theft during transportation. This scheme is particularly well-suited for logistics management scenarios requiring high security and efficiency, providing an efficient and reliable solution for secure communication in logistics.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

ZeZ: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Supervision, Visualization, Writing–original draft. XL: Data curation, Investigation, Methodology, Software, Supervision, Validation, Visualization, Writing–original draft. LG: Conceptualization, Methodology, Project administration, Validation, Writing–review and editing. ZaZ: Data curation, Investigation, Resources, Software, Validation, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Chen J, Li T, Zhang Y, You T, Lu Y, Tiwari P, et al. Global-and-Local attention-based reinforcement learning for cooperative behaviour control of multiple UAVs. *IEEE Trans Vehicular Technology* (2024) 73(3):4194–206. doi:10.1109/tvt.2023.3327571

2. Miao J, Wang Z, Miao X, Xing L. A secure and efficient lightweight vehicle group authentication protocol in 5G networks. *Wireless Commun Mobile Comput* (2021) 2021:1–12. doi:10.1155/2021/4079092

3. Xiao N, Wang Z, Sun X, Miao J. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Eng J* (2024) 86:631–43. doi:10.1016/j.aej.2023.12.021

4. Khelloufi A, Ning H, Naouri A, Sada AB, Qammar A, Khalil A, et al. A multimodal latent-features-based service recommendation system for the social Internet of Things. *IEEE Trans Comput Social Syst* (2024) 11:5388–403. doi:10.1109/tcss.2024.3360518

5. Kalra S, Sood SK. Secure authentication scheme for IoT and cloud servers. *Pervasive Mobile Comput* (2015) 24:210–23. doi:10.1016/j.pmcj.2015.08.001

6. Chang CC, Wu HL, Sun CY. Notes on secure authentication scheme for IoT and cloud servers. *Pervasive Mobile Comput* (2017) 38:275–8. doi:10.1016/j.pmcj.2015.12.003

7. Wang KH, Chen CM, Fang W, Wu TY. A secure authentication scheme for internet of things. *Pervasive Mobile Comput* (2017) 42:15–26. doi:10.1016/j.pmcj.2017.09.004

8. Pham DMC, Nguyen LPT, Dang TK. Resource-constrained IoT authentication protocol: an ECC-based hybrid scheme for device-to-server and device-to-device communications. In: *Proceedings of the 6th international conference on future data and security engineering (FDSE 2019)*. Berlin: Springer (2019). p. 27–9.

9. Pham CD, Dang TK. A lightweight authentication protocol for d2d-enabled IoT systems with privacy. *Pervasive Mobile Comput* (2021) 74:101399. doi:10.1016/j.pmcj.2021.101399

10. Amin R, Islam SH, Biswasi GP, Giri D, Khan MK, Kumar N. A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments. *Security Commun Networks* (2016) 9(17):4650–66. doi:10.1002/sec.1655

11. Li X, Niu J, Bhuiyan MZA, Wu F, Karuppiah M, Kumari S. A robust ECC-based provable secure authentication protocol with privacy protection for industrial internet of things. *IEEE Transaction Ind Inf* (2018) 14(8):3599–609. doi:10.1109/TII.2017.2773666

12. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M. Design of secure user authenticated key management protocol for generic IoT networks. *IEEE Internet Things J* (2018) 5(1):269–82. doi:10.1109/jiot.2017.2780232

13. Li X, Liu S, Wu F, Kumari S, Rodrigues JJPC. Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications. *IEEE Internet Things J* (2019) 6(3):4755–63. doi:10.1109/jiot.2018.2874473

14. Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access* (2019) 7:7273–85. doi:10.1109/access.2018.2890389

15. Sergi I, Montanaro T, Benvenuto FL, Patrono L. A smart and secure logistics system based on IoT and cloud technologies. *Sensors* (2021) 21(6):2231. doi:10.3390/s21062231

16. Zhou L, Li X, Yeh K, Su C, Chiu W. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Syst* (2019) 91:244–51. doi:10.1016/j.future.2018.08.038

17. Ali Z, Hussain S, Rehman R, Munshi A, Liaqat M, Kumar N, et al. An improved three-factor symmetric-key based secure AKA scheme for multi-server environments. *IEEE Access* (2020) 8:107993–8003. doi:10.1109/ACCESS.2020.3000716

18. Esfahani A, Mantas G, Matischek R, Saghezchi FB, Rodriguez J, Bicaku A, et al. A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet Things J* (2019) 6(11):288–96. doi:10.1109/jiot.2017.2737630

19. Das A, Wazid M, Yannam A, Rodrigues J, Park Y. Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access* (2019) 7:55382–97. doi:10.1109/access.2019.2912998

20. Chatterjee U, Govindan V, Sadhukhan R, Mukhopadhyay D, Chakraborty R, Mahata D, et al. Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. *IEEE Trans Dependable Secure Comput* (2019) 16(3):424–37. doi:10.1109/tdsc.2018.2832201

21. Shamir A. Identity-based cryptosystems and signature schemes. *Lect.notes Comput* (1985) 196(2):47–53. doi:10.1007/3-540-39568-7_5

22. Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing. In: *Proc. Of the 2000 symposium on cryptography and information security*. Okinawa, Japan (2000).

23. Boneh D, Franklin M. *Identity-based encryption from the weil pairing* (2003). p. 213–29.

24. Deebak BD, Memon FH, Khowaja SA, Dev K, Wang W, Qureshi NMF. In theDigital age of 5G networks:seamless privacy-PreservingAuthentication forCognitive-inspired internet of medical things. *IEEE Trans IndustrialInformatics* (2022) 18(12):8916–23. doi:10.1109/tii.2022.3172139

25. Liu H, Han D, Cui M, Li K -C, Souri A, IdenMultiSig MS. Ldentity-BasedDecentralized multi-signature in internet of things. *J.EEE Trans onComputational Social Syst* (2023) 10(4):1711–21. doi:10.1109/TCSS.2022.3232173

26. Fang L, Li M, Liu Z, Lin C, Ji S, Zhou A. A secure and authenticated MobilePayment protocol against of-site attack strategy. *lEEE Trans Dependableand Secure Comput* (2022) 19(5):3564–78. doi:10.1109/TDSC.2021.3102099

27. Heo J, Hong CS, Choi MS, Ju SH, Lim YH. Identity-based mutual device authentication schemes for PLC system[C]//2008 IEEE international symposium on power line communications and its applications. *IEEE* (2008) 47–51. doi:10.1109/ISPLC.2008.4510397

28. Li H, Dai Y, Tian L, Yang H. Identity-based authentication for cloud computing. In: *2009 IEEE international conference on cloud computing*. IEEE (2009). p. 157–66.

29. Jin CH, Xu YL, Chen GH, Yu CH, Jin Y, Shan JS. EBIAC: efficient biometric identity-based access control for wireless body area networks. *J Syst Architecture* (2021) 121:102317. doi:10.1016/j.sysarc.2021.102317

30. Babu ES, Dadi AK, Singh KK, Nayak SR, Bhoi AK, Singh A. A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system. *Expert Syst – J Knowledge Eng* (2022) 39(10). doi:10.1111/exsy.12941

31. Shareeda MA, Anbar M, Manickam S, Hasbullah IH. Towards identity-based conditional PrivacyPreserving authentication scheme for vehicular *ad hoc* networks. *IEEE Access* (2021) 9:113226–38. doi:10.1109/ACCESS.2021.3104148

32. Bansal U, Kar J, Ikram A, Naik K. ID-CEPPA: identity-based computationally efficient PrivacyPreserving authentication scheme for vehicle-to-vehicle communications. *Jorunal Syst Architecture* (2022) 123:102387. doi:10.1016/j.sysarc.2021.102387

33. Ullah I, Amin NU, Khan MA, Khattak H, Kumari S. An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-Health) system. *J Med Syst* (2021) 45(1):4. doi:10.1007/s10916-020-01658-8

34. Mandal S, Bera B, Sutrala AK, Das AK, Choo KKR, Park Y. Certificateless-signcryption-based ThreeFactor user access control scheme for IoT environment. *IEEE Internet Things J* (2020) 7(4):3184–97. doi:10.1109/jiot.2020.2966242

35. Saqib M, Jasra B, Moon AH. A lightweight three factor authentication framework for IoT based critical applications. *J King SaudUniversity-Computer Inf Sci* (2022) 34(9):6925–37. doi:10.1016/j.jksuci.2021.07.023

36. Ma M, He D, Wang H, Kumar N, Choo KKR. An efficient and provably secure authenticatedkeyagreement protocol for fog-based vehicular ad-hoc networks. *IEEE Internet Things J* (2019) 6(5):8065–75. doi:10.1109/jiot.2019.2902840

37. Li F, Han Y, Jin C. Practical access control for sensor networks in the context of the Internet of Things. *Comput Commun* (2016) 89–90:154–64. doi:10.1016/j.comcom.2016.03.007

38. Sutrala AK, Obaidat MS, Saha S, Das AK, Alazab M, Park Y. Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyberphysical systems. *IEEE Trans Intell Transportation Syst* (2021) 23(3):2316–30. doi:10.1109/tits.2021.3056704

39. Malani S, Srinivas J, Das AK, Srinathan K, Jo M. Certificatebased anonymous device access control scheme for IoT environment. *IEEE Internet Things J* (2019) 6(6):9762–73. doi:10.1109/JIOT.2019.2931372

40. Wu L, Wang J, Choo K-KR, He D. Secure key agreement and key protection for mobile device user authentication. *IEEE Trans Inf Forensics Security* (2019) 14(2):319–30. doi:10.1109/tifs.2018.2850299

41. Miao J, Wang Z, Ning X, Shankar A, Maple C, Rodrigues JJ. A UAV-assisted authentication protocol for internet of vehicles. *IEEE Trans Intell Transportation Syst* (2024) 25(8):10286–97. doi:10.1109/tits.2024.3360251

42. Kerrache CA, Rathee G, Lahby M, Vegni AM, Bilal M, Ferrag MA. A secure and transparent communication mechanism based on blockchain and fuzzy evaluation matrix in metaverse industry 4.0. *Inf Security J A Glob Perspective* (2024) 1–12. doi:10.1080/19393555.2024.2353067