frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 27 January 2025
DOI 10.3389/fphy.2025.1522170

OPEN ACCESS

EDITED BY
Hui-Jia Li,
Nankai University, China

REVIEWED BY
Jinlong Ma,
Hebei University of Science and Technology, China
Ge Gao,
Beijing Sport University, China

*CORRESPONDENCE
Liang Chen,
20051224@ppsuc.edu.cn

RECEIVED 04 November 2024
ACCEPTED 03 January 2025
PUBLISHED 27 January 2025

CITATION
Xiao Y and Chen L (2025) Efficient and secure electronic evidence exchange scheme for internet of things.
Front. Phys. 13:1522170.
doi: 10.3389/fphy.2025.1522170

Efficient and secure electronic evidence exchange scheme for internet of things

Yulong Xiao and Liang Chen*

College of Criminal Investigation, People's Public Security University of China, Beijing, China

With the rapid development of information technology, Internet of Things (IoT) is profoundly impacting various fields of the socio-economic landscape, driving the transformation of traditional industries towards intelligence. However, the widespread application of IoT has also led to a surge in electronic evidence, whose importance in the judicial field is increasingly prominent, but its characteristics such as ease of replication and leakage have posed new challenges for privacy protection. This paper focuses on the security and privacy issues of electronic evidence in IoT and proposes an efficient and secure interaction scheme based on chebyshev chaotic map, hash functions and XOR operations. Through a secure two-factor authentication mechanism, this scheme achieves identity verification between the user and the storage center, as well as confidentiality during the data transmission process. This has significant implications for the healthy development of IoT, judicial fairness and personal privacy protection. Experimental and theoretical analysis shows that the proposed scheme not only effectively resists various known attacks, but also performs excellently in terms of communication and computation costs, making it well-suited for IoT.

KEYWORDS

internet of things, electronic evidence, privacy protection, authentication, security

Highlights

- A secure authentication scheme is designed for electronic evidence transmission in IoT.
- Security analysis shows that the scheme provides enhanced security.
- The scheme exhibits higher computational efficiency and lower overhead.

1 Introduction

In recent years, Internet of Things (IoT) has become an important driving force for the development of modern science and technology [1]. IoT integrates various information sensing devices with the Internet through intelligent sensing, identification technologies, and pervasive computing, forming a vast network that connects objects, thereby enabling efficient information exchange between people and objects, as well as between objects themselves [2]. However, with the widespread adoption of IoT applications, the volume of electronic evidence generated has also grown exponentially. The vast amount of electronic evidence data is increasingly valuable and useful [3]. In the judicial field, electronic data has increasingly been used in recent years as a new form of evidence to prove the facts of a case. The concept of electronic evidence has emerged, and the perception of judicial

proof is gradually changing [4]. Electronic evidence, which is generated by the application of electronic information technology and can be used to prove case facts, includes electronic materials and their derivatives. Due to its characteristics of easy collection, convenient preservation, efficient transmission, and small space requirements, electronic evidence has gradually gained importance in the judiciary and, in many cases, carries the same legal weight as traditional evidence [5]. The extensive use of electronic evidence in the digitization of the legal system has gradually revealed its inherent flaws and limitations, which are becoming increasingly influential. First, electronic evidence can appear in multimedia forms such as text, images, audio, and video, which places higher demands on storage, extraction, and identification methods. Additionally, electronic evidence exists in the non-continuous form of binary code, and its transmission and storage rely on computer technology and specialized equipment. Non-experts find it difficult to identify and examine such evidence. If the transmission medium or storage device is compromised, the integrity of the electronic evidence may be altered, resulting in a loss of evidentiary value. Finally, in all stages of electronic evidence collection, identification, storage, and application, it is susceptible to tampering due to computer errors, virus attacks, or deliberate technical manipulation. This process is difficult to detect or trace, which directly compromises the authenticity of the electronic evidence [6–9].

Meanwhile, the privacy issues related to electronic evidence are receiving increasing attention. As electronic evidence, in its digital form, is easily replicated, accessed, and leaked, it often contains private information of states, enterprises, and individuals, whose disclosure would lead to privacy security issues [10–12]. The privacy issues associated with electronic evidence are of significant importance to both the state and the general public.

On the other hand, since electronic evidence is a form of electronic data, its transmission, download, and upload processes are easily executed. However, the flow of this data is difficult to record, making it challenging to trace the entities involved and the sequence of its transfer. Critical information such as the entity handling the electronic evidence and the time of operation is often unobtainable. Once a privacy breach occurs during the transfer of electronic evidence, it becomes difficult to trace the specific stage at which the breach happened, complicating accountability and posing significant challenges to privacy protection [13–15]. In this context, it is crucial to implement identity verification between users and storage centers while ensuring secure communication between nodes. A feasible security solution is to deploy an authenticated key agreement scheme, which verifies the true identity of communicating entities before sharing any sensitive information over unsecured wireless channels [16–18]. Mutual authentication can be used to verify the true identity of communication participants before transmitting data, eliminating the need to send sensitive information over unsecured channels. After participants have mutually confirmed their identities, the AKA scheme can negotiate a shared session key to encrypt subsequent transmission messages. Therefore, users and storage centers can authenticate each other, allowing only users with the session key to access the collected electronic evidence, while unauthorized users cannot. Researching efficient and secure interaction schemes for electronic evidence in IoT is of great significance for promoting the healthy development of IoT technology, upholding judicial fairness, and protecting personal privacy. Therefore, this paper proposes an efficient and secure interaction scheme for electronic evidence in the IoT. This scheme achieves rapid authentication of entity identity and ensures confidentiality during data transmission. This scheme not only has provable security and can resist various mentioned attacks, but it is also suitable for IoT environments with limited resources and energy, offering lower computational and communication overhead. Our contributions are as follows:

(1) A secure two-factor authentication scheme is designed for the security of electronic evidence transmission in IoT. The scheme employs a pseudonym mechanism, hiding the pseudonym within the transmission message to achieve user identity anonymity and ensure identity security. Additionally, chebyshev chaotic map, hash functions and XOR operations are utilized to complete identity authentication between users and storage centers, achieving strong authentication security and scalability.
(2) The proposed scheme satisfies security under formal proof, also meeting mutual authentication security and key agreement security. Informal security analysis shows that the scheme provides enhanced security, and resists various known attacks such as man-in-the-middle attacks and impersonation attacks.
(3) In terms of costs, the scheme exhibits higher computational efficiency and lower overhead compared to other schemes.

The organization of the rest is as follows. A comprehensive summary of existing researches in the relevant field are conducted in Section 2. In Sections 3, 4, the fundamental theoretical framework supporting the proposed scheme is thoroughly explained and the specific details of the scheme are introduced. In Section 5, we conducted the proposed scheme. Section 6 presents the performance experiments. Section 7 concludes the paper.

2 Related work

Identity authentication is one of the most crucial components in IoT systems, especially in wireless networks, where it is indispensable. This function prevents security issues such as data theft and identity spoofing. Many researchers have proposed their own security schemes for IoT identity authentication. Table 1 shows a comparative analysis of relevant protocols.

Sandeep et al. [19] presented a protocol for multi-server architectures. However, it fails to resist impersonation attacks and stolen smart card attacks. Butun et al. [20] designed a cloud-centric multi-layer framework. The entities included users, wearable devices, wearable device network coordinators and cloud service providers. It then provided multi-level authentication, such as authentication between users and cloud service providers, between cloud service providers and wearable device network coordinators and between wearable network coordinators and wearable devices. The scheme used the digital signature and identity authentication between cloud service providers and users. The algorithm is used during the initialization phase for negotiating the key for the message authentication code algorithm between different entities. The algorithm was used to compute the hash authentication code of data packets between entities. The extensive use of digital certificate

TABLE 1 Comparative analysis.

Protocol	Limitation
Sandeep et al. [19]	Impersonation attacks and stolen smart card attacks
Butun et al. [20]	Excessive computational overhead
Shen et al. [22]	Significant computational overhead and replay attacks
Zheng et al. [26]	The computational complexity of key calculations on the user side is too high
Lin et al. [28]	the packet loss rate in this scheme significantly increases
Sanaz et al. [30]	Significant computational overhead
Song et al. [32]	Transmission round number desynchronization
Rathore et al. [34]	High computational overhead
Hui et al. [35]	Ciphertext analysis attacks

signature algorithms and multi-tier key agreement algorithms in this scheme results in excessive computational overhead. Furthermore, the identity authentication method relied on an authentication chain, which, if disrupted at any stage, can cause the entire authentication process to fail. Ramos et al. [21] proposed a method for point and field algorithms, designed to implement access control mechanisms based on security and functionality in smart objects. Shen et al. [22] focused on efficient multi-layer authentication protocols. First, the authors proposed a group protocol. Then, the authors proposed a certificate-less authentication protocol between the personal digital assistant and application providers. In these protocols, elliptic encryption algorithms offer low computational overhead and high security. However, the excessive use of point multiplication calculations in this scheme introduces significant computational overhead. Additionally, the lack of consideration for timestamps in each data packet transmission makes it vulnerable to replay attacks. Shen et al. [23] described a lightweight and cloud-assisted protocol. During the registration phase, the user and the central server send the hash value of their device ID to the network administrator, who then uses an elliptic curve algorithm to select a random number to compute the public key for the corresponding entity. The network administrator also provides a signature value using their private key and the corresponding ID's hash value to the entity. This achieves entity identity authentication while protecting the entity's ID from being disclosed, thus enabling secure anonymous authentication in the protocol. However, the scheme's use of multiple signature algorithms increases computational overhead and fails to resist replay attacks. Gope et al. [24] described a lightweight real-time protocol for anonymous identity verification. It guarantees anonymity and ensures both forward and backward data confidentiality. However, it uses an excessive number of hash functions, making its authentication more susceptible to attacks compared to other methods. Similarly, Chifor et al. [25] proposed a scheme. The scheme utilizes the existing mobile authentication framework to achieve fast and convenient entity identity verification. However, this scheme simply leverages an existing open-source framework and its corresponding APIs for specific user authentication and authorization, rather than being a genuinely lightweight solution.

Encrypting transmitted data using a secure shared key is an effective method for establishing a secure communication channel. The secure distribution of the shared key is crucial, and key agreement is an effective way to address key distribution. However, as the sensor devices in IoT rapidly increases on a large scale, it presents greater challenges for secure transmission in the IoT context. Zheng et al. [26] presented a group key management scheme, which has the advantage of minimizing parameter broadcasts. However, the computational complexity of key calculations on the user side is too high. In the same year, Guo et al. [27] presented a secure data scheme. In this scheme, a single public key is linked to multiple groups of private keys, making it easy for attackers to identify the group sending the message but difficult to trace the sender's specific message. Lin et al. [28] presented a scheme based on ordered message authentication. In this scheme, a vehicle first sends a hash chain to nearby vehicles, which then generate message authentication codes based on elements of the hash chain. Nearby vehicles can use this information to authenticate the sender. However, due to the need for the sender to frequently broadcast its hash chain in large-scale networks, the packet loss rate in this scheme significantly increases. In recent years, the transmission efficiency and security of devices in the IoT environment have garnered widespread attention. Vijayakumar et al. [29] proposed a data security transmission protocol. The protocol used bidirectional authentication to ensure identity verification and employed a group key algorithm for key agreement. However, this scheme required re-negotiating the group key every time a user joins or leaves, which incurs a certain computation overhead on the secure transmission of the entire model. Sanaz et al. [30] presented a scheme within the context of mobile smart healthcare networks. This scheme achieved secure and efficient identity authentication and authorization for end users. It incorporates a key renegotiation mechanism, which reuses previous parameters to save on the cost of parameter negotiation, while the cross-regional transition mechanism effectively addresses the issue of patient identity authentication during spatial movements. However, because it is a traditional communication protocol that uses certificate mechanisms for identity authentication, it results in significant computational overhead, making it unsuitable for smart home environments. Tarun et al. [31] demonstrated through capability and performance analysis that ECDH is more suitable for IoT. The authors tested the time required for ECDH and RSA encryption and decryption using specific code, and conducted detailed energy consumption analyses using industry-standard test suites. They also made precise comparisons with other algorithms and ultimately applied the ECDH scheme to image encryption. Song et al. [32] described an improved protocol for IoT devices. This protocol employs a dual-key encryption mechanism, with one key used for plaintext encryption and another for computing MAC. The shared encryption key and MAC key are generated by a chaotic logistic map system. Instead of using a device authentication code mechanism for identity authentication, this scheme relies on a simple MAC-based approach. The mechanism adopted in this scheme is a one-time pad, where each data encryption is

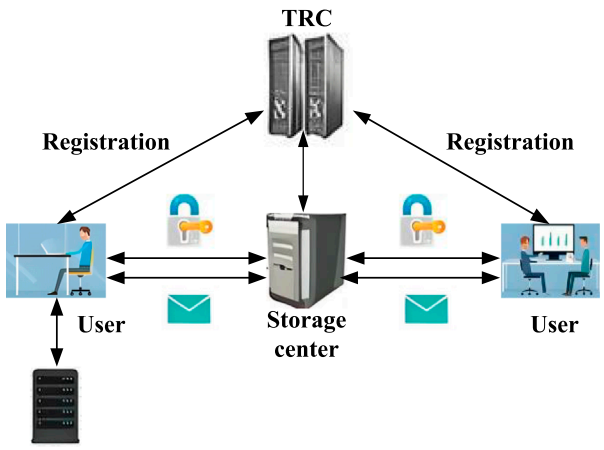

FIGURE 1
System model.

accompanied by a transmission round number. Although a one-time pad significantly enhances data security, it also introduces the problem of transmission round number desynchronization, leading to decryption confusion in the smart home transmission scheme, which could be a critical issue. Shen et al. [33] focused on secure data uploading. They proposed an improved scheme, which ensured the integrity of cloud-verified data while preventing data theft and modification by malicious home gateways. Rathore et al. [34] proposed a high-speed real-time scheme. The scheme is divided into four stages: registration, key exchange, key revocation, and data transmission. Although the scheme achieves real-time high-speed data transmission with careful consideration of details like timestamps, it employs a large number of signature algorithms and asymmetric encryption algorithms to ensure data integrity, data identity authentication, and secure key agreement. This results in high computational overhead for the entire smart city system. Hui et al. [35] proposed a novel data transmission scheme for Industrial IoT, based on a chaotic system and utilizing a linear n-shift encryption mechanism, which also includes a synchronization mechanism. However, this scheme lacks a reliable key update mechanism, making it vulnerable to ciphertext analysis attacks.

3 Preliminaries

3.1 Model

This paper delves into the secure interaction mechanisms for electronic evidence, with the core objective of ensuring the privacy and security of electronic evidence during its transfer, thereby upholding the dual requirements of judicial fairness and data protection. As shown in Figure 1, this electronic evidence interaction model is meticulously constructed and consists of three core components: the trust registration center (TRC), user, the storage center.

As the cornerstone of the model, TRC acts as a trusted third party. Its primary responsibility is system initialization, including generating the necessary security parameters and related configurations, laying a solid foundation for subsequent secure interactions. Additionally, TRC is responsible for the registration management of users and storage centers, ensuring that only legitimate and trusted entities can join the system through rigorous identity verification processes. In the electronic evidence interaction model, the user base is extensive and diverse, encompassing key judicial and law enforcement agencies such as courts, public security departments, procuratorates, forensic identification centers, arbitration committees, and notary offices. These users not only perform core operations such as uploading, forwarding, downloading, and reviewing evidence within the model but also ensure the legality and validity of the electronic evidence transfer through their expertise and authority. Notably, when interacting with the storage center, users, with the assistance of the TRA, use the key agreement mechanism to jointly generate a shared session key with the storage center. This key is used to encrypt all subsequent communications, ensuring the confidentiality and integrity of data transmission.

As the centralized platform for storing and managing electronic evidence, the storage center plays a crucial role. It stores the received electronic evidence to prevent unauthorized access and tampering. The storage center also enforces strict access control policies, precisely regulating user access to electronic evidence based on their permissions and identity. Additionally, to mitigate the risks of potential data loss or damage, the storage center employs strategies such as multi-replica storage, regular backups, and disaster recovery, ensuring high availability and durability of electronic evidence data. When providing upload and download services to users, the storage center uses the session key previously negotiated with the user to encrypt and decrypt the transmitted data, thus achieving secure end-to-end interaction.

In our security model, we assume that the TRC is a trusted entity with sufficient computational power to resist various known security attacks. TRC communicates with other entities through wired or secure channels and does not exhibit malicious behavior towards users during the registration process. The storage center is assumed to be a semi-trusted entity, meaning it is curious about the user's privacy and is motivated to obtain it, but it will not conduct malicious attacks and will adhere to the protocol to execute the corresponding operations. The user is assumed to communicate with the storage center via an insecure wireless channel, which may be subject to various network security attacks from attackers. We consider the user to be an untrusted entity, meaning there may be malicious entities, such as compromised electric vehicles, that could carry out tampering, replay, delay, and other network security attacks on the system.

3.2 Chebyshev chaotic map

In this scheme, we employ an extended Chebyshev polynomial with enhanced security [36]. It is defined as follows:

Definition 1: Let n be an integer and $x \in [-1, 1]$, chebyshev polynomial is defined as Equations 1, 2

$$T_n(x) = cos(n \cdot arccos(x)) \quad (1)$$

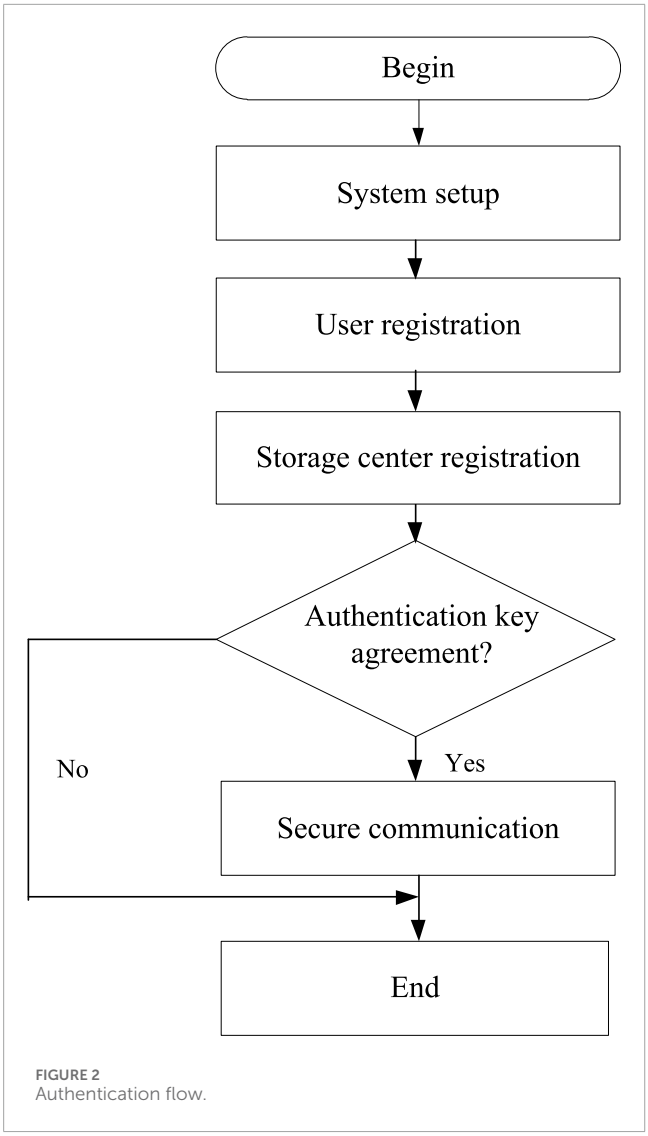

FIGURE 2
Authentication flow.

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)(modp) \quad (2)$$

Zhang [37] demonstrated that the semigroup property of chebyshev polynomials also holds.

Definition 2: (Chaotic Map-Based Diffie-Hellman Problem (CMBDHP)): Given x, $T_s(x)$ and $T_r(x)$, it is almost impossible to find $T_{rs}(x)$.

4 Proposed protocol

This paper proposes an interaction scheme for electronic evidence in IoT. Figure 2 shows the authentication flow.

4.1 System setup phase

At this stage, TRC generates its master private key and other public system parameters.

1. TRC selects a large prime number p and a hash function $H(\cdot)$. Simultaneously, TRC chooses s and x from $(-\infty, +\infty)$, where s serves as its master private key, and computes the public key $S_{pub} = T_s(x)$.
2. TRC securely and confidentially stores the private key s, and publicly releases the system parameters $P = \{p, x, S_{pub}\}$.

4.2 User registration

1. U_i first selects their identity identifier ID_i and password PW_i. Then it randomly selects a number w_i, computes $IDW_i = H(ID_i, PW_i, w_i)$ and sends $\{ID_i, IDW_i\}$ to the TRC.
2. Upon receiving $\{ID_i, IDW_i\}$, TRC calculates $PID_i = H(ID_i, s)$ and $A_i = H(ID_i, IDW_i, s)$, and securely stores (ID_i, A_i, PID_i) in its database. TRC then securely sends $\{PID_i, A_i\}$ to U_i. Otherwise, TRC rejects the request.
3. Upon receiving the response message $\{PID_i, A_i\}$, U_i computes $A_i^* = \mathrm{H}(ID_i, PW_i) \oplus A_i$ and $PID_i^* = h(ID_i, PW_i, A_i) \oplus PID_i$. Finally, U_i securely stores $\left(A_i^*, PID_i^*\right)$.

4.3 Storage center registration

1. SC_j selects its identity identifier ID_j and sends it to TRC.
2. Upon receiving SC_j's request, TRC randomly selects a number n_j, calculates $SID_j = H\left(ID_j, n_j\right)$ and $B_j = H\left(ID_j, s\right)$, and securely stores $\left(ID_j, SID_j\right)$. Finally, TRC sends $\left\{SID_j, B_j\right\}$ to SC_j via a secure channel.
3. Upon receiving the response message $\left\{SID_j, B_j\right\}$, SC_j stores $\left\{SID_j, B_j\right\}$ in a secure storage area and publicly discloses SID_j.

4.4 Authentication key agreement phase

1. As shown in Figure 3, U_i first inputs their identity identifier ID_i and password PW_i into their mobile device. Then it computes $A_i = \mathrm{H}(ID_i, PW_i) \oplus A_i^*$ and the pseudonym $PID_i = H(ID_i, PW_i, A_i) \oplus PID_i^*$. U_i then randomly selects two numbers c_i, y_i and current timestamp T_1, computes the following message, and sends an authentication request message $\{V_1, V_3, V_4, V_5, V_6, T_1\}$ to TRC via a public channel.

$$V_1 = T_{c_i}(x)\, mod p$$

$$V_2 = T_{c_i}\left(S_{pub}\right) mod p$$

$$V_3 = H(V_2, T_1) \oplus PID_i$$

$$V_4 = H(PID_i, V_2, T_1) \oplus y_i$$

$$V_5 = H(PID_i, V_2, y_i, T_1) \oplus SID_j$$

$$V_6 = H\left(SID_j, ID_i, V_2, y_i, A_i, T_1\right)$$

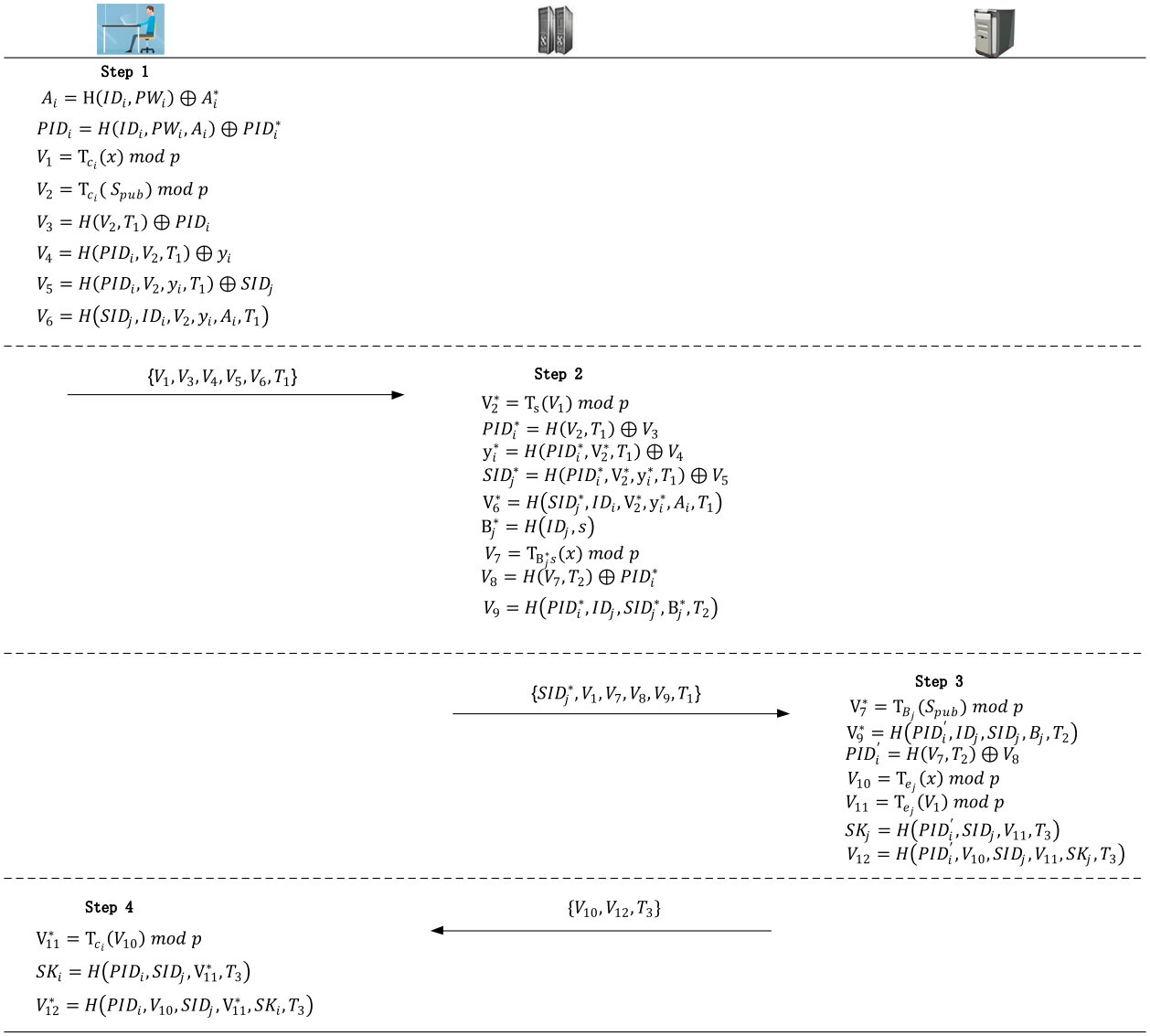

FIGURE 3
Authentication key agreement phase.

2. Upon receiving the authentication request message $\{V_1, V_3, V_4, V_5, V_6, T_1\}$ from U_i, TRC first verifies the validity of the timestamp T_1. If the received authentication request message is valid, TRC proceeds to the next step; otherwise, TRC rejects the authentication request. TRC calculates $\mathrm{V}_2^* = \mathrm{T}_s(V_1)\, mod p$ and $PID_i^* = H(V_2, T_1) \oplus V_3$. Then, using the pseudonym PID_i^*, TRC retrieves the corresponding information (ID_i, A_i) from the database and computes the message $\left(y_i^*, SID_j^*\right)$.

$$\mathrm{y}_i^* = H(PID_i^*, \mathrm{V}_2^*, T_1) \oplus V_4$$

$$SID_j^* = H(PID_i^*, \mathrm{V}_2^*, \mathrm{y}_i^*, T_1) \oplus V_5$$

TRC further computes the verification message V_6^* using the message $\left(y_i^*, SID_j^*\right)$:

$$\mathrm{V}_6^* = H(SID_j^*, ID_i, \mathrm{V}_2^*, \mathrm{y}_i^*, A_i, T_1)$$

TRC verifies the correctness of the message $V_6^* = V_6$. If the message is validated, the TRC can authenticate that the communication requester is U_i. Otherwise, TRC rejects the authentication request. TRC retrieves the corresponding information ID_j from the database using the pseudonym SID_j^*, selects the current timestamp T_2, computes $B_j^* = H(ID_j, s)$, and generates the message $\left\{SID_j^*, V_1, V_7, V_8, V_9, T_2\right\}$. TRC sends the message $\left\{SID_j^*, V_1, V_7, V_8, V_9, T_1\right\}$ to SC_j via a public channel.

$$V_7 = \mathrm{T}_{\mathrm{B}_j^* s}(x)\, mod p$$

$$V_8 = H(V_7, T_2) \oplus PID_i^*$$

$$V_9 = H\left(PID_i^*, ID_j, SID_j^*, \mathrm{B}_j^*, T_2\right)$$

3. Upon receiving the message $\left\{SID_j^*, V_1, V_7, V_8, V_9, T_1\right\}$ from TRC, SC_j first verifies T_2. Then SC_j retrieves the corresponding information B_j from the database using SID_j^* and computes the message:

$$\mathrm{V}_7^* = \mathrm{T}_{B_j}\left(S_{pub}\right) mod p$$

$$PID_i' = H(V_7, T_2) \oplus V_8$$

SC_j calculates the verification message V_9^* using the retrieved information.

$$\mathrm{V}_9^* = H\left(PID_i', ID_j, SID_j, B_j, T_2\right)$$

4. SC_j first verifies the correctness of the message $\mathrm{V}_9^* = V_9$. If the message fails verification, SC_j rejects the communication request. Otherwise, SC_j can authenticate that the communication requester is the TRC. SC_j then selects a random number e_j and the current timestamp T_3, calculates the message $\left(V_{10}, V_{11}, SK_j, V_{12}\right)$ and sends the message $\{V_{10}, V_{12}, T_3\}$ to U_i via a public channel.

$$V_{10} = \mathrm{T}_{e_j}(x) mod p$$

$$V_{11} = \mathrm{T}_{e_j}(V_1) mod p$$

$$SK_j = H\left(PID_i', SID_j, V_{11}, T_3\right)$$

$$V_{12} = H\left(PID_i', V_{10}, SID_j, V_{11}, SK_j, T_3\right)$$

5. Upon receiving $\{V_{10}, V_{12}, T_3\}$, U_i first verifies T_3. If the received authentication request message is valid, U_i proceeds to the next step; otherwise, U_i rejects the authentication request. U_i calculates the session key using the received message V_{10}.

$$\mathrm{V}_{11}^* = \mathrm{T}_{c_i}\left(V_{10}\right) mod p$$

$$SK_i = H\left(PID_i, SID_j, \mathrm{V}_{11}^*, T_3\right)$$

Then, U_i computes the verification message V_{12}^* and verifies the correctness of $V_{12}^* = V_{12}$.

$$V_{12}^* = H\left(PID_i, V_{10}, SID_j, \mathrm{V}_{11}^*, SK_i, T_3\right)$$

If the message passes verification, U_i can authenticate that the communication requester is SC_j, and the session key is also verified. Otherwise, U_i rejects the communication request.

5 Security evaluation

5.1 Formal security analysis

Before conducting a formal safety analysis of the proposed protocol, we propose an appropriate safety model [38, 39]. First, we define three participants in the proposed protocol: U, TRC and SC. In addition, Π_U^i, Π_{TRC}^j and Π_{SC}^k respectively represent the instance i, j, and k of U, TRC and SC, which are also called the prophecy machine. Let Π be the set of instances, and Π^s be the s-th instance of Π. Define an attacker $\mathcal{A}$ can make the following queries:

$Execute\left(\Pi_U^j, \Pi_{TRC}^i, \Pi_{SC}^k\right)$: By executing this query, $\mathcal{A}$ can intercept all messages during the communication between U, TRC and SC.

$Hash(m)$: This query simulates the opponent $\mathcal{A}$ to receive the hash results by *Hash* query. After getting this query, if there are *Hash* records in the query, the result will be returned, otherwise a random number needs to be selected and returned.

$Reveal(\Pi^s)$: The current session key established between Π^s and its partner is disclosed to $\mathcal{A}$ by executing this query.

$Send(\Pi^s, m)$: This query is designed to simulate an active attack initiated by $\mathcal{A}$, where $\mathcal{A}$ pretends a legitimate instance and sends a message m. If m is the correct message, then $\mathcal{A}$ can retrieve the corresponding feedback message per protocol P. Otherwise, the query will be terminated.

$Test(\Pi^s)$: The query assesses the semantic security of the authenticated key. During the execution of protocol, $\mathcal{A}$ may initiate a test query to challenge the security of the key. Upon receiving this query, Π^j returns a genuine authentication key or a randomly generated string based on an unbiased coin flip.

5.1.1 Session key security

It defines allowing an attacker $\mathcal{A}$ to interrogate many *Test* queries. If *Test* query targets an instance of a dishonest participant paired with an honest participant or an instance of a dishonest participant whose intended partner is also dishonest, the system will return the genuine authenticated key. Otherwise, it utilizes an unbiased coin flip to decide whether to return the actual key K or a randomly generated key. $\mathcal{A}$ tries to use the *Test* query to correctly guess $c \in \{0, 1\}$. If $\mathcal{A}$ successfully guessed the bit c, where $\mathcal{A}$ is able to successfully distinguish the true K from a randomly generated string, $\mathcal{A}$ wins. $Adv_P^{SK}(\mathcal{A})$ is defined as the advantage of the event where the opponent $\mathcal{A}$ wins the game for protocol P, and if the $Adv_P^{SK}(\mathcal{A})$ is negligible, protocol P is safe.

Theorem 1: Suppose $\mathcal{A}$ represents the attackers, P, q_s, q_h, $|HASH|$ and $Adv_{\mathcal{A}}^{\mathrm{CMBDHP}}(t)$ represent the proposed protocol, the number of *Send* queries, the number of *Hash* queries, the range space of $H()$ and the advantage of $\mathcal{A}$ cracking CMBDHP in time t. The advantage of $\mathcal{A}$ in breaking the group session key security of the protocol can be estimated as Formula 3:

$$Adv_P^{SK}(\mathcal{A}) \leq \frac{q_h^2}{|HASH|} + 2Adv_{\mathcal{A}}^{\mathrm{CMBDHP}}(t) \tag{3}$$

Prove: we proved it by playing four games, Gm_i (i = 0,1,2,3). Let $Succ_{Gm_i}$ denote the success probability of $\mathcal{A}$ winning the Gm_i while guessing the correct bit c, and the response advantage probability of $\mathcal{A}$ is defined as $Adv_{Gm_i} = \Pr\left[Succ_{Gm_i}\right]$. Below is a detailed analysis for each Gm_i.

Gm_0: Gm_0 is a real attack of $\mathcal{A}$. And from the semantic security definition of the proposed protocol, Formula 4 can be obtained that:

$$Adv_P^{SK}(\mathcal{A}) = |2\Pr\left[Adv_{Gm_0}\right] - 1| \tag{4}$$

Gm_1: Gm_1 is a simulated eavesdropping attack. Under this game, $\mathcal{A}$ intercepts all the authentication information $\{V_1, V_3, V_4, V_5, V_6, T_1\}, \{SID_j^*, V_1, V_7, V_8, V_9, T_1\}, \{V_{10}, V_{12}, T_3\}$ and simulates through the *Execute* query. Then $\mathcal{A}$ performs the *Test* query to check whether its output gives the true group session key or a random value. Since the intercepted messages do not endanger the temporary/long-term secrets of any of the communication entities, the Gm_1 winning chances do not increase. Therefore, Formula 5 can be obtained that:

$$\Pr\left[Adv_{Gm_1}\right] = \Pr\left[Adv_{Gm_0}\right] \tag{5}$$

Gm_2: The difference from the previous game Gm_1 is that Gm_2 contains *Send* and *Hash* queries. Gm_2 simulates an active attack, in which $\mathcal{A}$ tries to persuade the communication entity to accept the forged message. While $\mathcal{A}$ can repeat *Hash* queries to check conflicts in authentication messages, each message set is associated with a random number, current timestamp, identity, and secret value. Therefore, $\mathcal{A}$ has little chance of collision when making *Send* queries. Therefore, according to the birthday paradox, we have Formula 6:

$$\left|\Pr\left[Adv_{Gm_2}\right] - \Pr\left[Adv_{Gm_1}\right]\right| \leq \frac{q_h^2}{2|HASH|} \tag{6}$$

Gm_3: In this final game, $\mathcal{A}$ tries to use the intercepted messages to calculate the session keys and to solve the CMBDHP problem. If $\mathcal{A}$ tries to calculate the key $SK_i = H\left(PID_i, SID_j, V_{11}^*, T_3\right)$, the secret value V_{11}^* need to be known. This means that $\mathcal{A}$ needs to solve the CMBDHP in the shortest time to obtain the session key. Therefore, Formula 7 can be obtained that:

$$\left|\Pr\left[Adv_{Gm_3}\right] - \Pr\left[Adv_{Gm_2}\right]\right| \leq Adv_{\mathcal{A}}^{ECDHP}(t) \tag{7}$$

Once all the queries are made by $\mathcal{A}$, the only guess bit c is left to win the game and we have Formula 8.

$$\Pr\left[Adv_{Gm_3}\right] = \frac{1}{2} \tag{8}$$

According to the formulas, we can get Formula 9:

$$Adv_P^{SK}(\mathcal{A}) \leq \frac{q_h^2}{|HASH|} + 2Adv_{\mathcal{A}}^{\text{CMBDHP}}(t) \tag{9}$$

Based on the above proof, $\mathcal{A}$ is unable to win the game in probability polynomial time. Therefore, the proposed protocol has been formally analyzed and proven to be secure and effective.

5.2 Scyther tool analysis

Scyther is a protocol security analysis and verification tool [16]. This tool can use the Dolev-Yao attacker model and a strong security model to detect attack paths, which are illustrated graphically when found. To standardize the description of protocols and their security properties, Scyther provides a specialized description language called SPDL [40]. The following verification will utilize the Scyther tool and the Dolev-Yao attacker model.

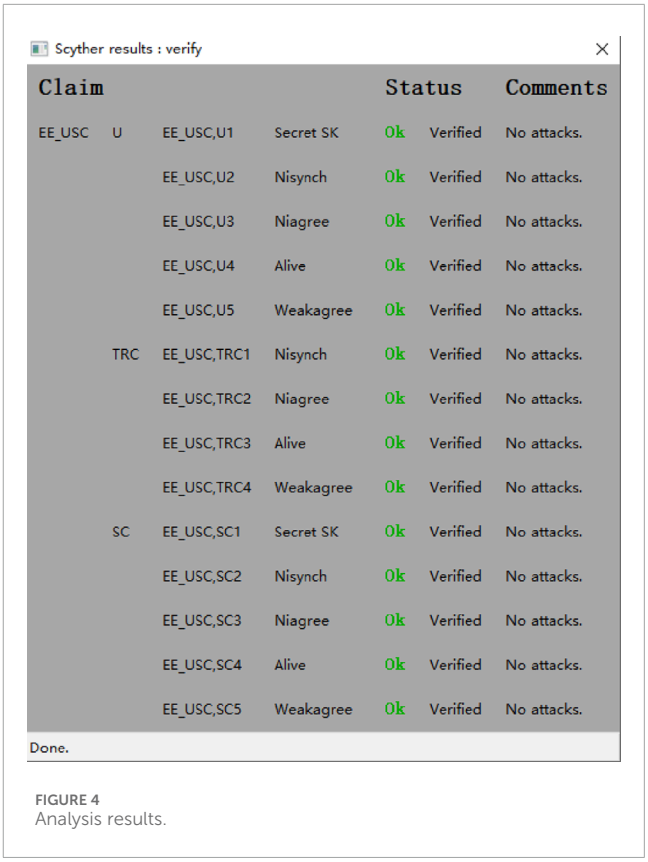

FIGURE 4
Analysis results.

In the protocol modeling of this paper, three roles are defined: U, TRC and SC, representing the tag, reader, and server, respectively. Secret, Alive, Weakagree, Niagree, and Nisynch are used to detect secret leakage, replay attacks and desynchronization attacks, respectively. The analysis results show that the Scyther tool could not identify any malicious attacks against the protocol presented in this paper, indicating that the protocol ensures the security of the secret information among the user, the trusted registration center, and the storage center. The Scyther tool analysis results are shown in Figure 4.

5.3 Informal analysis

5.3.1 User anonymity and untraceability

In the proposed scheme, on the one hand, no identity information is transmitted over the public channel. On the other hand, even if an attacker captures all the transmission information on the public channel, we use temporary identities for transmission, encrypted by $PID_i = h(ID_i, PW_i, A_i) \oplus PID_i^*$. To obtain the user's identity PID_i^*, the attacker would need to know these values, but since they are secret, the attacker cannot obtain PID_i. Even if the attacker obtains PID_i, it is only a temporary identity, not the user's real identity. Since the random numbers c_i and y_i change with each

session, and the computed authentication information is generated using these random numbers and timestamps, the information transmitted over the public channel is variable, making the user's information untraceable.

5.3.2 Privileged insider attack

Suppose a privileged insider becomes an attacker after obtaining the registration information of a legitimate user. Since the user's password is protected by secret values and hash functions, the privileged insider cannot obtain the plaintext of the user's password and cannot impersonate any party in the protocol.

5.3.3 User impersonation attack

To impersonate a legitimate U_i, the attacker would have to obtain the user's identity identifier and password plaintext or forge the request information $\{V_1, V_3, V_4, V_5, V_6, T_1\}$.First, based on the analysis of the offline password guessing attack, the attacker cannot obtain ID_i and PW_i. Second, since V_6 is derived from the concatenated hash of $SID_j, ID_i, V_2, y_i, A_i$ and T_1, the attacker cannot forge V_2 and A_i.Therefore, the proposed protocol is immune to user impersonation attacks.

5.3.4 Storage center impersonation attack

Since B_j is the long-term private key of the storage center SC_j and is unknown to adversaries, the attacker cannot compute the correct V_{11}, and thus cannot forge V_{12} to generate a legitimate response message corresponding to the user's request. Therefore, the proposed scheme is immune to storage center impersonation attacks.

5.3.5 Replay attack

The scheme uses random numbers and timestamps to defend against replay attacks. Suppose an attacker attempts to replay request messages $\{V_1, V_3, V_4, V_5, V_6, T_1\}$, $\{SID_j^*, V_1, V_7, V_8, V_9, T_1\}$,and $\{V_{10}, V_{12}, T_3\}$. Since the random numbers and timestamps are variable and random in each session, replayed messages cannot pass the verification by the storage center SC_j and will result in session termination. Similarly, due to the characteristics of random numbers and timestamps, replayed messages cannot pass the user's detection, leading to session termination. Additionally, even if the attacker replays previous messages, the difficult problem prevents the attacker from calculating a valid session key. Therefore, the proposed protocol is resistant to replay attacks.

5.3.6 Man-in-the-middle attack

Suppose an attacker attempts to intercept and tamper with messages $\{V_1, V_3, V_4, V_5, V_6, T_1\}$, $\{SID_j^*, V_1, V_7, V_8, V_9, T_1\}$, and $\{V_{10}, V_{12}, T_3\}$, making participants believe the received information is authentic. The attacker would need to obtain the parameters V_2 and A_i to calculate V_3, V_4, V_5, V_6 and modify the message $\{V_1, V_3, V_4, V_5, V_6, T_1\}$. Similarly, the attacker cannot modify other messages $\{SID_j^*, V_1, V_7, V_8, V_9, T_1\}$ and $\{V_{10}, V_{12}, T_3\}$. Therefore, this scheme can resist man-in-the-middle attacks.

5.3.7 Mutual authentication

In the proposed scheme, to authenticate U_i, the TRC first verifies the correctness of the message $V_6^* = V_6$. If the message passes verification, the TRC can authenticate that the communication requester is U_i. To authenticate the TRC, SC_j first verifies the correctness of the message $V_9^* = V_9$. If the message fails verification, SC_j rejects the communication request. Otherwise, SC_j can authenticate that the communication requester is the TRC. To authenticate SC_j, U_i computes the verification message V_{12}^* and verifies the correctness of $V_{12}^* = V_{12}$. If the message passes verification, U_i can authenticate that the communication requester is SC_j, and the session key is also verified. Otherwise, U_i rejects the communication request. Therefore, the proposed protocol provides mutual authentication functionality.

5.3.8 Forward security

The session key ultimately negotiated in the proposed scheme, $SK_i = H(PID_i, SID_j, V_{11}^*, T_3)$, is independently calculated by both parties in the protocol and is unrelated to the user's password or long-term private key. Even if an attacker intercepts $\{V_1, V_3, V_4, V_5, V_6, T_1\}$, $\{SID_j^*, V_1, V_7, V_8, V_9, T_1\}$, and $\{V_{10}, V_{12}, T_3\}$, they still cannot compute the session key. Moreover, due to the difficult problem, the attacker cannot derive $V_{11}^* = T_{c_i}(V_{10}) \bmod p$ from $V_{10} = T_{e_j}(x) \bmod p$. Therefore, the scheme ensures the security of the session key.

5.3.9 Session key security

Only legitimate U_i and SC_j will negotiate a session key $SK_i = H(PID_i, SID_j, V_{11}^*, T_3)$ for communication after the authentication process. Since the session key includes T_3, which indicates the freshness of each communication, even if the session key is compromised, an attacker cannot use this key to recover previous or future session keys.

6 Performance analysis

6.1 Computation overhead comparison

Table 2 summarizes the computation overhead of several protocols, where T_{ecm} represents the time for ECC point multiplication, T_{fe} represents the time for fuzzy extraction operations, T_h represents the time for a one-way hash function, $T_{E/D}$ represents the time for encryption/decryption using symmetric encryption techniques and T_{cm} represents the time for chebyshev chaotic map operation. Table 2 summarizes the computation overhead of the proposed scheme and other schemes by Chang [41], Wazid [42] and Li [43]. For the cryptographic operations involved in the proposed scheme and other related schemes, network simulation experiments were conducted on a hardware platform configured with 8GB memory, an Intel Core i7 processor, and an Ubuntu 16 system. The execution times for the relevant operations were calculated using the widely applied cryptographic PBC library. Through this experiment, the execution times of various cryptographic operations were obtained. The running times for different operations are as follows: T_{ecm} is approximately 71.23 ms, T_h is approximately 0.45 ms, T_{je} is approximately 71.23 ms, $T_{D/E}$ is approximately 6.86 ms, and T_{cm} is approximately 18.61 s.

According to the proposed scheme, the time cost for user authentication is $3T_{cm} + 8T_h$, the time cost for TRC authentication is $2T_{cm} + 7T_h$, and the time cost for SC authentication is $3T_{cm} + 4T_h$. Therefore, the total time cost for the proposed scheme is $8T_{cm} + 19T_h$. In Chang [17], the time costs for the communication

TABLE 2 Computation overhead.

Scheme	User	TRC	SC	Total
[41]	$2T_{ecm}+7T_h$	$9T_h$	$2T_{ecm}+5T_h$	$4T_{ecm}+21T_h$
[42]	$T_{fe}+7T_h+T_{D/E}$	$8T_h+2T_{D/E}$	$7T_h+T_{D/E}$	$T_{fe}+22T_h+5T_{D/E}$
[43]	$2T_{ecm}+9T_h+T_{fe}$	$9T_h+T_{ecm}$	$4T_h$	$3T_{ecm}+22T_h+T_{fe}$
Proposed	$3T_{cm}+8T_h$	$2T_{cm}+7T_h$	$3T_{cm}+4T_h$	$8T_{cm}+19T_h$

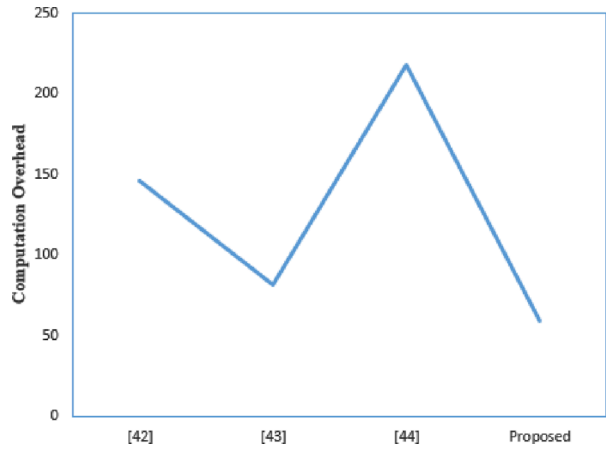

FIGURE 5
Computation overhead of user.

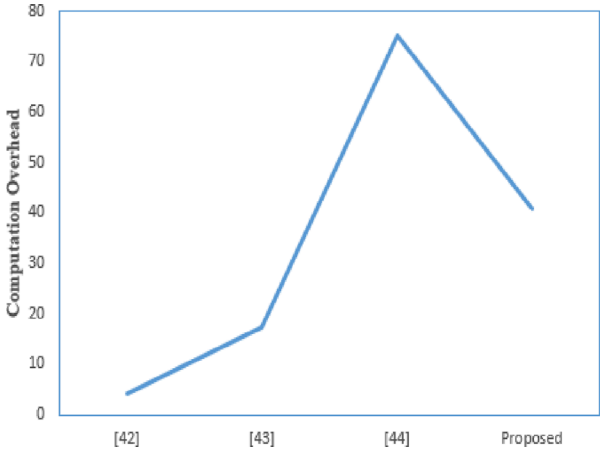

FIGURE 6
Computation overhead of TRC.

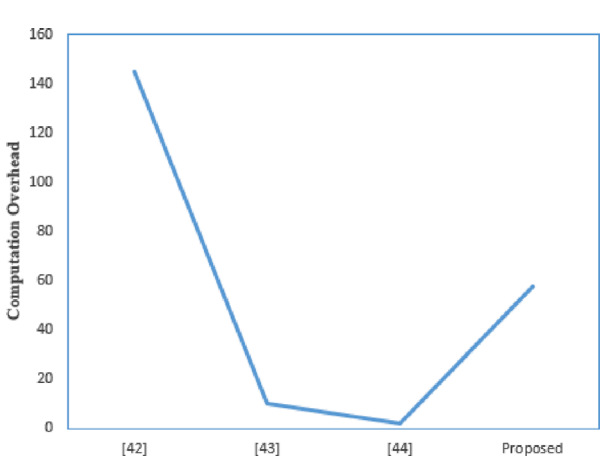

FIGURE 7
Computation overhead of SC.

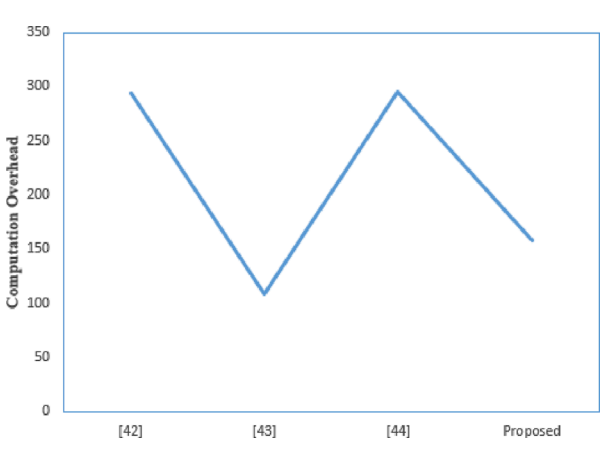

FIGURE 8
Computation overhead.

entities are $2T_{ecm}+7T_h$, $9T_h$, and $2T_{ecm}+5T_h$ respectively. Thus, the total time cost is $4T_{ecm}+21T_h$. In Wazid [19], the time costs for the communication entities are $T_{fe}+7T_h+T_{D/E}$, $8T_h+2T_{D/E}$, and $7T_h+T_{D/E}$ respectively. Thus, the total time cost is $T_{fe}+22T_h+5T_{D/E}$. In Li [18], the time costs for the communication entities are $2T_{ecm}+9T_h+T_{fe}$, $9T_h+T_{ecm}$, and $4T_h$ respectively. Thus, the total time cost is $3T_{ecm}+22T_h+T_{fe}$. Compared to the schemes by Chang [17] and Li [18], the proposed scheme has lower computational overhead. Although the proposed scheme requires more computational overhead than Wazid [19], it provides more security features. Figures 5–8 show the computational overhead for each scheme across different communication entities. As the number of user devices increases, the proposed solution becomes more acceptable.

6.2 Communication overhead comparison

The communication overhead is shown in Table 3. The proposed scheme uses a 160-bit chebyshev chaotic map, a 160-bit random number, a 160-bit identity identifier, 128-bit symmetric encryption/decryption, 160-bit hash value, and a 32-bit timestamp. The three messages transmitted in this scheme are $\{V_1, V_3, V_4, V_5, V_6, T_1\}$, $\{SID_j^*, V_1, V_7, V_8, V_9, T_1\}$, and $\{V_{10}, V_{12}, T_3\}$. The bit consumption for these three messages is 832 bits, 832

TABLE 3 Communication overhead.

Scheme	User	TRC	SC	Total
[41]	672	512	1,088	2,272
[42]	512	1,088	384	1984
[43]	1,120	1,120	320	2,560
Ours	832	832	352	2016

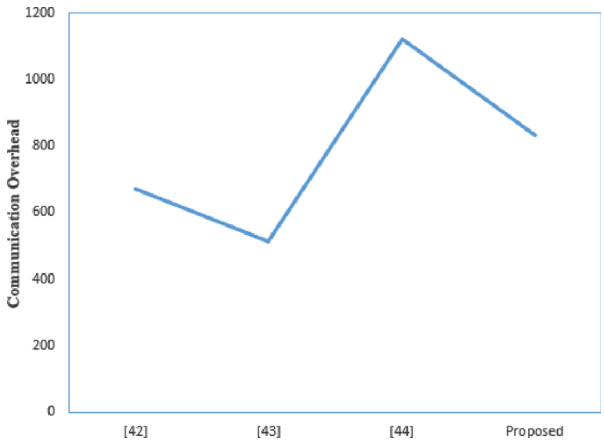

FIGURE 9
Communication overhead of user.

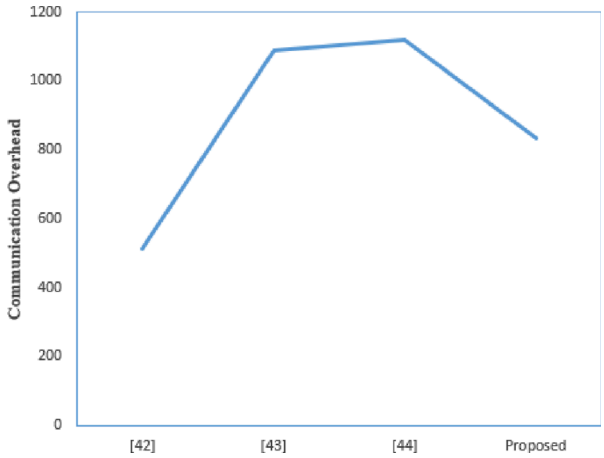

FIGURE 10
Communication overhead of TRC.

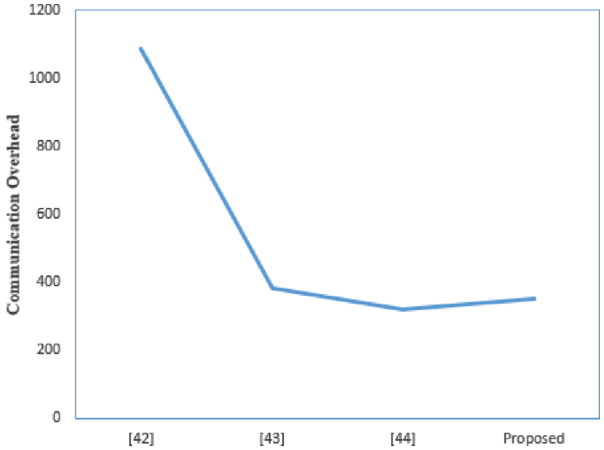

FIGURE 11
Communication overhead of SC.

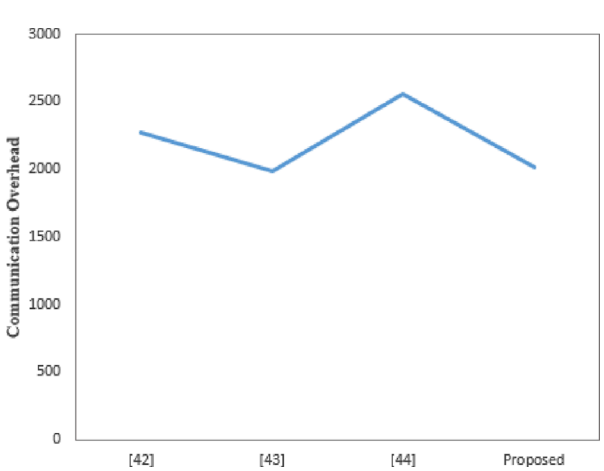

FIGURE 12
Communication overhead.

bits, and 352 bits, respectively, resulting in a total communication overhead of 2016 bits. In Chang [17], the communication costs for each entity are 672 bits, 512 bits, and 1,088 bits, respectively, with a total communication overhead of 2,272 bits. In Wazid [42], the communication costs for each entity are 512, 1,088, and 384 bits, respectively, resulting in a total communication overhead of 1984 bits. In Li [18], the communication costs for each entity are 1,120, 1,120, and 320 bits, respectively, with a total communication overhead of 2,560 bits. Wazid [42]

While meeting more security performance and resistance to attacks, the communication overhead for some nodes in this scheme is slightly higher than that of other nodes. First, Chang [41] and Wazid [42]do not support resistance to password guessing attacks, so the user's communication overhead is slightly lower than that of the proposed scheme. In order to implement this function, this consumes more communication overhead. Additionally, the proposed scheme has slightly higher communication overhead than Wazid [42]. However, Chang [41] does not support the safety requirement. Figures 9–12 visually illustrate the communication consumption of each scheme on different entities. Compared to other schemes, the communication overhead is lower. Therefore, the scheme in this article meets the practical needs of electronic evidence interaction in IoT.

7 Conclusion

This paper provides an in-depth analysis of the security and privacy issues surrounding electronic evidence in IoT. It highlights that the importance of electronic evidence in the judicial field is increasing, but its inherent vulnerabilities also pose significant privacy risks. To address this issue, this paper proposes a secure interaction scheme for electronic evidence in IoT. This scheme innovatively combines chebyshev chaotic map, hash functions and XOR operations to ensure the security of the electronic evidence transmission process. The scheme was then subjected to a security analysis using the random oracle model and the Scyther, proving its resilience against various types of attacks. Furthermore, the security analysis and performance experiment results demonstrate that the scheme optimizes authentication efficiency while ensuring security. This research not only offers new insights and methods for the secure management of electronic evidence in IoT environments but also makes a positive contribution to the healthy development of IoT technology, the maintenance of judicial fairness, and the protection of personal privacy. In the practical application, with numerous IoT devices and frequent data exchange, security risks also increase. The secure interaction scheme proposed in this paper can be applied to IoT security monitoring and management systems, achieving comprehensive monitoring and protection of device identity, data transmission, and storage processes, thereby improving the overall security of IoT systems.

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

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

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. The authors acknowledge funding received from the following science foundations: Research on the basic theory and methodology of data investigation (2023JKF01SK08).

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

References

1. Nassereddine M, Khang A. Applications of internet of things (IoT) in smart cities. *Adv IoT Tech Appl industry 4.0 digital economy* (2024) 109–36.

2. Salam A. Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. *Internet things Sustain Community Dev wireless Commun sensing, Syst* (2024) 299–326. doi:10.1007/978-3-031-62162-8_10

3. Quick D, Choo K-KR. Big forensic data reduction: digital forensic images and electronic evidence. *Cluster Comput* (2016) 19:723–40. doi:10.1007/s10586-016-0553-1

4. Arshad H, Bin Jantan A, Abiodun OI. Digital forensics: review of issues in scientific validation of digital evidence. *J Inf Process Syst* (2018) 14(2):346–76. doi:10.3745/JIPS.03.0095

5. Losavio M, Adams J, Rogers M. Gap analysis: judicial experience and perceptionof electronic evidence. *J Digital Forensic Pract* (2006) 1(1):13–7. doi:10.1080/15567280500541462

6. Sin JM, Son HR. Dealing with the problem of collection and analysis of electronic evidence. *Int J Electron security digital forensics* (2019) 11(3):363–77. doi:10.1504/ijesdf.2019.100497

7. 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

8. Li H, Cao H, Feng Y, Li X, Pei J. Optimization of graph clustering inspired by dynamic belief systems. *IEEE Trans Knowledge Data Eng* (2024) 36(11):6773–85. doi:10.1109/tkde.2023.3274547

9. Li HJ, Feng Y, Xia C, Cao J. Overlapping graph clustering in attributed networks via generalized cluster potential game. *ACM Trans Knowledge Discov Data* (2024) 18(1):1–26. doi:10.1145/3597436

10. Xiong Y, Du J. Electronic evidence preservation model based on blockchain. In: the 3rd International Conference on Cryptography, Security and Privacy (ICCSP'19) (2019). p. 1–5. doi:10.1145/3309074.3309075

11. Chen Y, Li M, Qiu Y. A study on the current status of electronic evidence preservation in internet crime. *J Educ Humanities Social Sci* (2024) 28:541–8. doi:10.54097/reykxj59

12. Li HJ, Song S, Tan W, Huang Z, Li X, Xu W, et al. Characterizing the fuzzy community structure in link graph via the likelihood optimization. *Neurocomputing* (2022) 512:482–93. doi:10.1016/j.neucom.2022.09.013

13. 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

14. Weilbach WT, Motara YM. Applying distributed ledger technology to digital evidence integrity. *Saiee Africa Res J* (2019) 110(2):77–93. doi:10.23919/saiee.2019.8732798

15. Miao J, Wang Z, Wu Z, Ning X, Tiwari P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Syst Appl* (2024) 237:121329. doi:10.1016/j.eswa.2023.121329

16. Darbandeh FG, Safkhani M. SAPWSN: a secure authentication protocol for wireless sensor networks. *Computer Networks* (2023) 220:109469. doi:10.1016/j.comnet.2022.109469

17. Wei H, Miao J, Lv J, Chen C -M, Kumari S, Amoon M. Secure and trustworthy data management mechanism for dance-consumer electronics in AIoT. *IEEE Trans Consumer Electronics* (2024) 1. doi:10.1109/tce.2024.3471573

18. Chen S, Zhao C, Huang L, Yuan J, Liu M. Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Sci Int Digital Invest* (2020) 35:301001. doi:10.1016/j.fsidi.2020.301001

19. Sandeep S, Anil S, Kuldip S. A secure dynamic identity-based authentication protocol for multi-server architecture. *J Netw Computer Appl* (2010) 34(2):609–18. doi:10.1016/j.jnca.2010.11.011

20. Butun I, Erol-Kantarci M, Kantarci B, Song H. Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Commun Mag* (2016) 54(4):47–53. doi:10.1109/mcom.2016.7452265

21. Hernandez-Ramos JL, Jara J, Marin L, Skarmeta Gómez AF. DCapBAC: embedding authorization logic into smart things through ECC optimizations. *Int J Computer Mathematics* (2016) 93(2):345–66. doi:10.1080/00207160.2014.915316

22. Shen J, Chang S, Jun S, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Syst* (2018) 78(3):956–63. doi:10.1016/j.future.2016.11.033

23. Shen J, Ziyuan G, Ji S, et al. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J Netw Computer Appl* (2018) 106(1):117–23. doi:10.1016/j.jnca.2018.01.003

24. Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Trans Ind Electron* (2016) 63(11):7124–32. doi:10.1109/tie.2016.2585081

25. Chifor B, Bica I, Patriciu V, Pop F. A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Syst* (2018) 106(1):740–9. doi:10.1016/j.future.2017.05.048

26. Zheng X, Huang CT, Matthews M. *Chinese remainder theorem based group key management[C]//45th ACMSE Winston-Salem*. USA: ACMSE Press (2007). p. 266–71. doi:10.1145/1233341.1233389

27. Guo J, Baugh JP, Wang S. A group signature based secure and privacy preserving vehicular communication framework. *Proc IEEE INFOCOM. Anchorage: IEEE Press* (2007) 103–8. doi:10.1109/MOVE.2007.4300813

28. Lin X, Sun X, Wang X, Zhang C, Ho PH, Shen X. TSVC: timed efficient and secure vehicular communications with privacy preserving. *IEEE Trans Wireless Commun* (2008) 7(12):4987–98. doi:10.1109/t-wc.2008.070773

29. Vijayakumar P, Azees M, Kannan A, Jegatha Deborah L. Dual Authentication and key management techniques for secure data transmission in vehicular *ad hoc* networks. *IEEE Trans Intell Transportation Syst* (2016) 17(4):1015–28. doi:10.1109/tits.2015.2492981

30. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, et al. End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Syst* (2016) 64(2):108–24. doi:10.1016/j.future.2016.02.020

31. Tarun KG, Vineet S. Lightweight security algorithm for low power IoT devices. In: Proceedings of International Conference on Advances in Computing, Communications and Informatics; USA. ICACCI Press (2016). p. 12–8.

32. Song T, Ruinian L, Mei B A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet Things J* (2017) 4(1):1844–52. doi:10.1109/JIOT.2017.2707489

33. Shen J, Chen W, Tong L, et al. Secure data uploading scheme for a smart home system. *Inf Sci* (2018) 453(28):186–97. doi:10.1016/j.ins.2018.04.048

34. Rathore MM, Paul A, Ahmad A, Chilamkurti N, Hong WH, Seo H. Real-time secure communication for smart city in high-speed big data environment. *Future Generation Computer Syst* (2018) 83(4):638–52. doi:10.1016/j.future.2017.08.006

35. Hongwe H, Chengcheng Z, Shenggang X, Lin F. A novel secure data transmission scheme in industrial internet of things. *China Commun* (2020) 17(1):73–88. doi:10.23919/jcc.2020.01.006

36. Chen R, Mou Y, Li W. A provably secure multi-server authentication scheme based on Chebyshev chaotic map. *J Inf Security Appl* (2024) 83:103788. doi:10.1016/j.jisa.2024.103788

37. Zhang L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons and Fractals* (2008) 37(3):669–74. doi:10.1016/j.chaos.2006.09.047

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

39. Lee T-F, Ye X, Lin SH. Anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things. *IEEE Internet Things J* (2022) 9(16):15336–48. doi:10.1109/jiot.2022.3149117

40. Ma Y, Shi W, Li X, Cheng Q. Provable secure authentication key agreement for wireless body area networks. *Front Computer Sci* (2024) 18(5):185811. doi:10.1007/s11704-023-2548-4

41. Chang CC, Le HD. A provably secure, efficient, and flexible authentication scheme for *ad hoc* wireless sensor networks. *IEEE Trans wireless Commun* (2015) 15(1):357–66. doi:10.1109/twc.2015.2473165

42. Wazid M, Das AK, Odelu V, Kumar N, Susilo W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans Dependable Secure Comput* (2017) 17(2):391–406. doi:10.1109/tdsc.2017.2764083

43. Li X, Niu J, Kumari S, Wu F, Sangaiah AK, Choo KKR. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *J Netw Computer Appl* (2018) 103:194–204. doi:10.1016/j.jnca.2017.07.001