TYPE Original Research
PUBLISHED 09 June 2025
DOI 10.3389/fphy.2025.1579521

Check for updates

OPEN ACCESS

EDITED BY
Hui-Jia Li,
Nankai University, China

REVIEWED BY
Jinlong Ma,
Hebei University of Science and Technology, China
Jun Hu,
Inner Mongolia University, China

*CORRESPONDENCE
Xuefan Zhou,
✉ 202120928@gzcc.edu.cn

RECEIVED 19 February 2025
ACCEPTED 28 April 2025
PUBLISHED 09 June 2025

CITATION
Zhou X and Zhuang Z (2025) An anonymous secure authentication method for tourist attraction network-based edge computing. *Front. Phys.* 13:1579521.
doi: 10.3389/fphy.2025.1579521

An anonymous secure authentication method for tourist attraction network-based edge computing

Xuefan Zhou[1]* and Zhaoyu Zhuang[2]

[1]College of Tourism Management, Guizhou University of Commerce, Guiyang, China, [2]Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

An elliptic curve cryptography (ECC)-based anonymous authentication mechanism is designed to meet the demand for lightweight, anonymous, and trustworthy authentication for tourist attraction networks in edge computing environments. This mechanism uses pseudo-randomly generated identities to cover the real identity of the tourists, which ensures the anonymity of the scheme. The security of mutual authentication between the tourist and the edge computing server is increased with the help of smart card technology. At the same time, the mechanism also has the ability to guarantee security in case of smart card theft. The introduction of timestamps effectively enhances the scheme's ability against a replay attack. The security of the scheme is analyzed using Burrows—Abadi—Needham (BAN) logic and non-formal analysis methods. Finally, the results of a comprehensive analysis and comparison show that the scheme has high practical value.

KEYWORDS

anonymous, edge computing, secure, authentication, tourist attraction

1 Introduction

With the rapid development of information technology, tourism has ushered in unprecedented changes. Smart tourism, as a product of the deep integration of tourism and information technology, is gradually changing people's tourism mode and experience [1]. Edge computing, an emerging distributed computing technology, has been widely used in the field of smart tourism with its low latency and high efficiency. However, with the popularization of edge computing, the security authentication problem of tourist attraction networks has become increasingly prominent. How to realize anonymous and trustworthy security authentication in edge computing environment has become an important issue that needs to be solved in the current smart tourism field. Edge computing is a technology that pushes computing and data storage tasks from the centralized cloud to the edge of the network. This distributed computing model realizes data processing and analysis close to the edge of the network by deploying computing nodes at the edge of the network, thus greatly reducing the delay of data transmission and improving the response speed and efficiency of the system.

Edge computing is particularly widespread in the field of smart tourism [2–4]. For example, tourist attractions can collect real-time information such as tourist traffic, environmental data, and facility status by arranging sensors, cameras, and other devices in the scenic area. Through edge computing technology, these devices can initially process and analyze the data locally, and then upload the key data to the cloud for more in-depth analysis and mining. This distributed computing model not only improves the speed and efficiency of data processing but also reduces the cost and risk of data transmission [5]. However, the distributed nature of edge computing brings new security challenges. As the digitization and intelligence of tourist attractions continue to increase, network security issues are becoming more and more prominent. Especially on the edge side of the network, traditional security authentication methods often find it difficult to meet demand due to factors such as large data volumes, long transmission distances, and diverse devices. Because data are processed and stored at edge nodes, once these nodes are attacked or tampered with, a tourist's private information will be at risk of leakage [6]. In addition, the wide variety of devices in the edge computing environment has varying security protection capabilities, which also increases the possibility of the system being attacked. Therefore, realizing secure, efficient, and anonymous tourist authentication in the edge computing environment has become a key problem to be solved in the field of smart tourism [7].

Currently, the network security authentication of a tourist attraction relies on the traditional centralized authentication mechanism. This mechanism verifies the identity of tourists through a centralized authentication server, which guarantees the security of tourist identity to a certain extent but has many shortcomings [8–10]. First, the traditional centralized authentication mechanism is susceptible to a single point of failure. Once the authentication server fails or is attacked, the entire authentication system will be paralyzed, resulting in tourists being unable to complete authentication and access services. Second, the traditional authentication mechanism has security risks in the process of data transmission. Data that are transmitted between the client and the authentication server are susceptible to threats such as man-in-the-middle attacks and data tampering. Finally, traditional authentication mechanisms often neglect the protection of tourist privacy. During the authentication process, the personal information of the tourist may be leaked to a third party or used for improper purposes, which not only violates the relevant laws and regulations but also damages the legitimate rights and interests of the tourist [11].

Therefore, under the edge computing environment, the security authentication of a tourist attraction network must meet the new demands of anonymity, trustworthiness, and efficiency. The realization of this anonymous and trustworthy security authentication method is of great significance for enhancing the security of a tourist attraction network, protecting user privacy, and promoting the healthy development of the tourism industry [12]. It can not only effectively prevent all kinds of network attacks and data leakage risks but also enhance the trust and satisfaction of users in the tourist attraction network and promote the tourism industry in a more intelligent and personalized direction. In summary, an edge computing-based tourist attraction network needs an anonymous and trustworthy security authentication method that can guarantee the security of tourist identity as well as protect the privacy of the tourist. For the lightweight authentication and key negotiation needs in the edge computing environment of a tourist attraction, an anonymous secure authentication method is proposed for tourist attraction network-based edge computing. The contributions of this paper include the following aspects.

(1) A lightweight anonymous authentication mechanism based on elliptic curve cryptography (ECC) is designed for the needs of tourist attraction networks in edge computing environments. It protects the privacy of tourists through pseudo-random identities, guarantees the security of authentication by combining with smart card technology, and introduces timestamps to defend against replay attacks to efficiently protect the privacy and security of tourists' information. This scheme not only has high security but also utilizes lightweight ECC to guarantee high efficiency.

(2) The security of the scheme is verified using Burrows–Abadi–Needham (BAN) logic and informal analysis. In the performance evaluation session, the scheme is compared and analyzed with other schemes of the same category in two dimensions: communication cost and computation cost. It reveals that the scheme balances performance and security and is practical.

The following is the structural arrangement of the subsequent contents of this paper. Section 2 outlines the current research status of edge computing. Section 3 introduces the related preparatory knowledge. Section 4 details the design process of the scheme in this article. Section 5 conducts the security analysis. Section 6 conducts the performance evaluation. Section 7 summarizes the article.

2 Research status

In recent years, due to the promotion of smart transportation, Internet of Things, and cloud computing technologies, the field of mobile computing research has experienced a change from a centralized mobile cloud computing model to a mobile edge computing model. It has attracted the attention of research scholars due to the emergence of edge computing models.

Tsai et al. [13] proposed an authentication mechanism for distributed mobile cloud computing, which aims to ensure that a mobile user and service provider can verify each other's identities and protect user anonymity. However, Jiang et al. [14] demonstrated that Tsai et al.'s scheme failed to meet their proposed security criteria and improved it. Jiang et al. introduced advanced cryptographic techniques such as homomorphic encryption to enhance the protection of user anonymity, as well as to ensure that service providers are able to verify the legitimacy of a user without having to know the user's true identity. Xiong et al. [15] designed an authentication scheme for distributed mobile cloud computing in order to reduce the computational overhead while increasing the functionality of user revocation and reregistration. However, this scheme requires secure key transfer between multiple nodes, which increases the complexity of key management and is prone to key leakage. Irshad et al. [16] utilized a bilinear pair mapping algorithm to design an authentication optimization strategy for multi-server environments. However, applying the bilinear pair mapping algorithm leads to an increase in computational overhead. Cui et al [17] proposed an information authentication method based on edge computing. The edge nodes assist the roadside unit in accomplishing the information verification task. With the growth of open applications, edge nodes are responsible for the authenticity verification of information and participate in the intelligent connected vehicle system as an edge device, but the real-time performance is relatively low. Dewanta et al. [18] designed a method for switching the authentication of mobile terminals by using a cloud server. When a mobile terminal wants to access the services of an edge node, it must send a request to the cloud server. The cloud server then assists in the authentication process between the mobile terminal and the edge node. However, storing the authentication credentials on a cloud server results in a high overhead for the authentication process.

In 2020, Jia et al [19] designed an anonymous identity authentication scheme for mobile edge computing based on the principle of edge-end architecture. It has a privacy protection function, but this scheme cannot effectively defend against user impersonation attacks and temporary secret information leakage attacks. Mishra et al. [20] designed a mobile terminal authentication scheme for the multi-access edge computing (MEC) environment. This scheme is based on the bilinear pair mapping algorithm, thus incurring a high computational cost. Lai et al. [21] designed a multiuser access and anonymous switching authentication mechanism that integrates the detection capability of the aggregate message authentication code (AMAD) technology. However, this mechanism does not consider the pre-switching process, which leads to high signaling and computational costs during switching, and it has difficulty meeting the real-time requirements. Li et al. [22], in order to improve the lack of forward security and user anonymity of security authentication schemes, designed an anonymous identity-based key negotiation scheme, which is able to provide perfect security features such as forward security. However, the analysis of Shamshad et al. [23] found that Li et al.'s scheme is also unable to resist an MEC server impersonation attack or a user impersonation attack. Therefore, a new and improved scheme is proposed. Rakeei et al. [24] proposed a scheme with several security features, such as two-way authentication. However, due to the bilinear pair technique, this scheme is unsuitable for some IoT end devices with limited performance. Xu et al. [25] designed a lightweight authentication key negotiation scheme for mobile edge computing without the intervention of a trusted third party, and verified its security under the stochastic predicate machine model. However, the scheme fails to ensure user anonymity and results in high overhead due to the application of bilinear pairs.

Zhang et al. [26] designed an authentication framework in order to enhance the security of Internet of Things environments supported by edge computing. The goal of this framework is to secure the communication between devices and between devices and edge servers. By integrating a portion of the local private key during registration and combining it with a distributed blockchain network, this authentication framework achieves secure communication and authentication functions among edge computing-enabled IoT devices and between devices and edge servers. Nodes in a blockchain network typically need to constantly synchronize their data to maintain consistency, which creates a significant communication overhead. Tian et al. [27] designed a mobile edge computing-based scheme that ensures untraceability and full anonymity of information by virtue of a one-time pseudonym protection, while strengthening the security of key management and communication process by applying one-time public-private key pairs to verify identity. In addition, the parallel processing mechanism enables two independent processes to be executed synchronously, thus reducing the overall time cost. However, the pseudonym update mechanism of this scheme is not timely enough, and the user's identity remains unchanged for a long period of time, which increases the risk of being traced. Zhang et al. [28] proposed a secure and verifiable multimedia data search scheme based on cloud-assisted edge computing, which is based on bilinear pairing, and a secure, flexible, and efficient keyword search mechanism was achieved. Bilinear pairing involves complex mathematical operations with high computational overhead.

In summary, edge computing reduces the pressure on data centers and improves data processing efficiency by performing data processing at the device side. However, it also brings about the problem of balancing security and efficiency. On the one hand, the edge computing environment involves a large number of devices, which increases the vulnerability of network security and may lead to data leakage and device attacks. On the other hand, edge computing requires real-time data processing, which puts higher demands on the data processing capacity and efficiency. Therefore, it must be optimized from the perspectives of security and system performance in light of the actual situation to achieve secure and efficient anonymous trusted security authentication for tourist attraction networks in edge computing environments. The scheme in this paper shows significant advantages in realizing security and smaller computation and time overhead. These advantages are due to the high efficiency of ECC, the assistance of smart card technology, and the optimized authentication process design. First, the scheme in this paper ensures the anonymity of the scheme by masking the real identity of tourists with pseudo-randomly generated identities. This reduces the risk of users' identities being tracked or leaked and enhances user privacy protection. Combined with smart card technology, even if the tourists' passwords are leaked, the attackers cannot directly utilize this information to forge legitimate identities. Furthermore, ECC, as a public key cryptography algorithm, offers higher security and smaller key lengths than traditional algorithms. ECC requires fewer computational resources, which reduces computational overhead. Smart cards typically can process and store data quickly, which can accelerate computational operations during the authentication process. In addition, smart cards can pre-store some necessary keys or parameters to reduce the amount of online computation.

3 Prerequisite knowledge

3.1 Elliptic curve

Elliptic curve cryptography (ECC) is a public key cryptography technique whose security is built on the elliptic curve discrete logarithm problem. Compared with the Rivest–Shamir–Adleman (RSA) algorithm, ECC can achieve the same level of security with a shorter key length, so it is often used in areas such as digital signatures and key exchange [29].

Definition 1: In a finite field F, it defines the points according to the equation $y^2 = x^3 + ax + b \; mod \; q$, forming a set to form an elliptic curve E of order prime q, where $x, y, a, b \in F_q, \left(4a^3 + 27b^2\right)\ mod\ q \neq 0$. O is defined as the point of infinity. Then, O and the points on the elliptic curve E form an additive cyclic group G. It has the following properties:

(1) Addition: P and Q are two points on group G. If $P \neq Q$, then $P + Q = R$ means that the line between points P and Q intersects another point R of the curve E.

(2) Scalar multiplication: the point product on an elliptic curve is defined as $mP = P + P + \cdots + P$ (m times), where $\in Z_p^*, m > 0$.

3.2 Difficult question hypothesis

Definition 2: Discrete logarithmic problems on elliptic curves (ECDLP) [30].

Let G be a finite cyclic group defined on an elliptic curve, and $P, Q \in G$ are given. It is difficult to solve $x \in Z_p^*$ in polynomial time, such that $Q = xP$ holds.

Definition 3: The Diffie–Hellman problem on elliptic curves (ECDHP).

Let G be a cyclic group defined on an elliptic curve, and $P, aP, bP \in G$ are given. It is difficult to compute $abP \in G$ in polynomial time.

3.3 Adversary model and security requirement

Adversary $\mathcal{A}$ has the following capabilities:

(1) Adversary $\mathcal{A}$ has absolute control over the public communication channel.

(2) Adversary $\mathcal{A}$ is able to obtain the previous session key.

(3) Adversary $\mathcal{A}$ is able to obtain the long-term key of the edge computing server and the data stored in the database.

The following analyzes the security features that must be present in the method of this paper [31–35].

(1) Man-in-the-middle attack: After taking control of the communication path, the adversary manages to intervene in the communication between the tourist and the edge computing server by disguising himself as the object of direct communication between the two parties, so that the tourist and the edge computing server mistakenly believe that they are communicating directly with each other.

(2) Offline password guessing attack: The adversary intercepts all the communication messages between the tourist and the edge computing server, generates a candidate password by utilizing the saved communication messages, and examines whether a matching password exists.

(3) Replay attack: When the tourist sends a request message to the edge computing server, it is assumed that the adversary intercepts the communication message and resends this message to the edge computing server by pretending to be a legitimate tourist.

(4) Tourist impersonation attack: The adversary steals information and pretends to be a legitimate tourist to communicate.

(5) Privileged internal attack: The adversary accesses the edge computing server pretending to be a tourist by stealing the parameter, identity, and password information of the attacked tourist.

(6) Forward security: It is assumed that the adversary has already mastered the session key of the current session but is also unable to compute the relevant parameters and cannot compute the session key of the previous sessions.

(7) Anonymity: It is assumed that the adversary has stolen the relevant communication messages, but due to the lack of relevant parameters, it is impossible to calculate the real identity of the visitor.

4 Method design

4.1 System model

The design of the anonymous secure authentication method for tourist attraction network-based edge computing includes the following entities: tourist T_i, edge computing server ECS_j, and trusted agency TA. The three entities realize secure authentication and key negotiation through a series of operational processes.

4.1.1 Tourist

The tourist accomplishes registration, authentication, key negotiation, and password update. The visitor generates key information by selecting random numbers and passphrases, sends registration information to the edge computing server, and saves the received parameters. In the authentication and key negotiation phase, the visitor generates random numbers and timestamps to ensure message freshness, sends authentication information to the edge computing server, verifies its response, and then computes the session key to support encrypted communication. When an update of the password is required, the tourist selects a new password and random number, sends an update request to the edge computing server, and processes its response to update the encrypted parameters.

4.1.2 Edge computing server

The edge computing server receives and stores the encrypted parameters of the tourist in the registration phase and computes and sends the response parameters. In the authentication and key negotiation phase, it verifies the identity of the tourist, ensures message freshness, computes the session key to support encrypted communication, and confirms success to the tourist. In the password update phase, it receives and decrypts the update request from the visitor, updates the stored parameters, and confirms the success of the password update to the tourist.

4.1.3 Trusted agency *TA*

The trusted agency TA is responsible for the initialization and parameterization of the system, ensuring that all entities in the system have access to the necessary public information.

The specific operation process of this system model is as follows: first, in the system initialization phase, the trusted agency

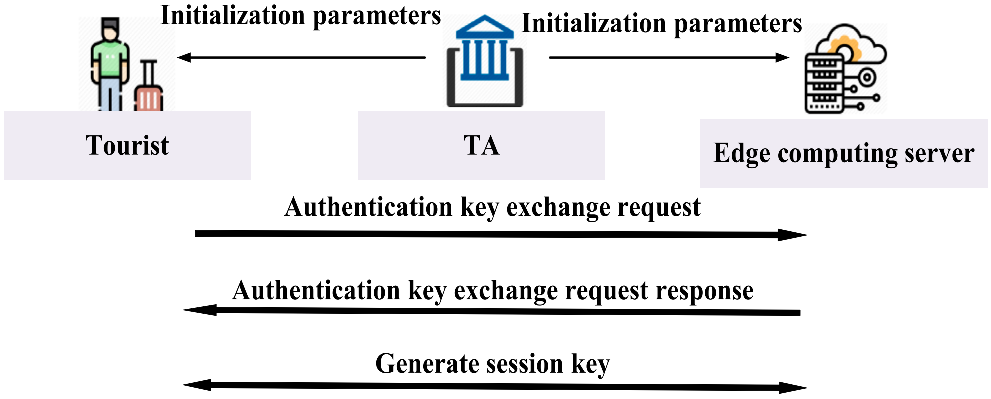
Initialization parameters
Initialization parameters
Tourist
TA
Edge computing server
Authentication key exchange request
Authentication key exchange request response
Generate session key

FIGURE 1
Model architecture.

TA generates and releases the system parameters. Then, in the tourist registration phase, the tourist initiates a registration request to the edge computing server, which completes the identity registration of the tourist and returns the corresponding authentication credentials. Then, in the authentication key negotiation phase, the tourist initiates an authentication key negotiation request to the edge computing server, and the edge computing server receives the relevant message to authenticate the identity legitimacy of the tourist, generates the key negotiation message and the session key, and responds to the request of the tourist. The tourist receives the response message to authenticate the identity of the edge computing server and generates a session key consistent with the tourist based on the key negotiation information sent by the edge computing server. Finally, in the password update phase, the tourist computes and sends the current session key encrypted with the current session key to the edge computing server, which decrypts the stored parameters and sends the updated part of the parameters encrypted to the tourist for replacement. The model architecture is shown in Figure 1.

TABLE 1 Definition of symbols.

Symbol	Connotation
$E_p(a,b)$	Elliptic curve
P	The base point of an elliptic curve
$h()$	One-way hash function
y_1,y_2,y_3	Keys for the edge computing server
K_j	Public key of the edge computing server
PW_i	Tourist's password
ID_i	Identification of tourists
x_i,w_i,z_j	Random numbers
$\oplus$	Different or converse operation
$\|$	Concatenation operator

4.2 The methodology process

The definitions of the symbols used in this section are shown in Table 1.

This scheme includes four processes: system initialization, tourist registration, authentication and key negotiation, and password update, and its specific flow is shown in Figure 2.

4.2.1 System initialization

The trusted agency *TA* chooses an elliptic curve $E_p(a,b)$, and selects the n th order base point P on this elliptic curve. Then, *TA* chooses a one-way hash function $h()$ and selects three random numbers $y_1,y_2,y_3 \in Z_p^*$. *TA* assigns the identity ID_i to the tourist T_i and computes the public key $K_j = y_2P$ of the edge computation server ECS_j. Finally, the ECS_j saves y_1,y_2,y_3 as its key, and the *TA* discloses the public parameter $\{E_p(a,b),n,P,h(),K_j\}$.

4.2.2 Tourist registration

(1) First, T_i selects a random number $x_i \in Z_p^*$ and password PW_i. Then, it obtains identity ID_i and a biometric feature BC_i, and then T_i calculates the parameter $C_i = h(h(ID_i) \oplus PW_i \oplus x_i \oplus BC_i)$. Finally, T_i sends the message $MG(ID_i,C_i)$ to ECS_j through the secure channel.

(2) After receiving the message, ECS_j first calculates the parameters $D_j = C_i \oplus h(y_2)$, $E_j = h(C_i \| y_1 \| y_3)y_2^{-1}P$, and $F_j = h(ID_i \| D_j \| y_1 \| y_3)$. Then, ECS_j saves the parameters D_j,F_j , and ECS_j saves the parameter E_j to the smart card. ECS_j sends the smart card to T_i through the secure channel.

(3)T_i receives the smart card and inputs a biometric message BC_i. T_i calculates $(\sigma_i,\tau_i) = GEN(BC_i)$, $BM_j = h(ID_i \| PW_i \| \sigma_i \| x_i)$ and saves the parameters (E_j,x_i,BM_j,τ_i) into the smart card.

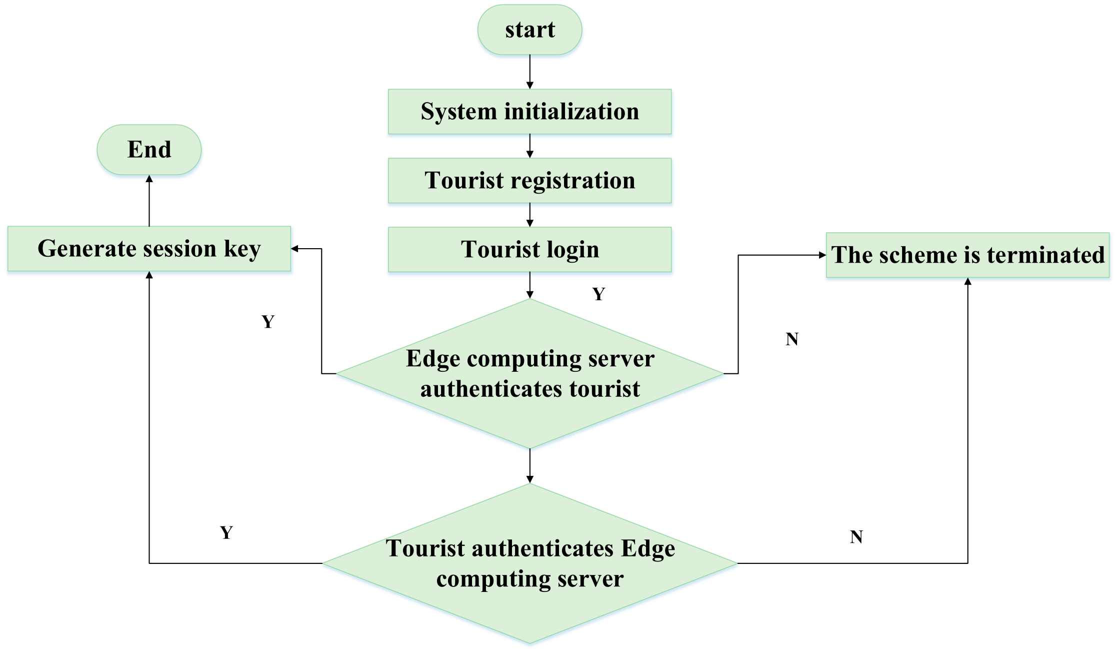

FIGURE 2
Scheme flow.

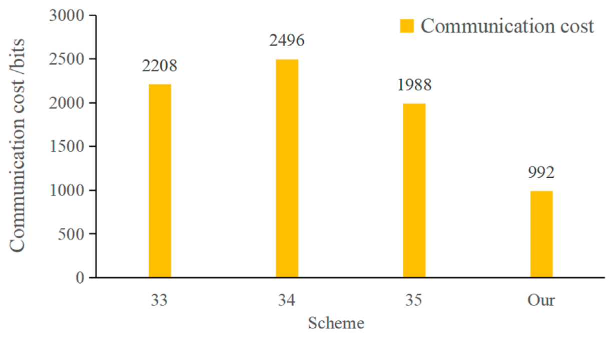

FIGURE 3
Communication cost.

4.2.3 Authentication and key negotiation

(1) T_i inserts the smart card and inputs the corresponding ID_i, password PW_i , and biometric value BC_i. Then, the smart card calculates $\sigma_i = Rep(BC_i, \tau_i)$ and $BM_j' = h(ID_i \| PW_i \| \sigma_i \| x_i)$.

(2) The smart card judges whether BM_j' and BM_j are equal. If they are equal, the smart card logs in successfully by verifying the legitimacy of T_i; otherwise, the smart card ends this session.

(3) T_i first chooses a random number $w_i \in Z_p^*$ and generates a timestamp t. Then, T_i calculates the parameters $C_i = h(h(ID_i) \oplus PW_i \oplus x_i \oplus BC_i)$, $L_i = h(C_i \| E_j \| w_i P \| t)$, $O_i = w_i E_j = w_i h(C_i \| y_1 \| y_3) y_2^{-1} P$, and the pseudo-identity $PID_i = ID_i \oplus C_i \oplus t$. Finally, T_i sends the message $MG(PID_i, O_i, L_i, t)$ to ECS_j.

(4) After receiving the message, ECS_j first obtains the current timestamp t' and checks whether the timestamp is valid by judging $t' - t < \Delta t$. If the timestamp t is invalid, ECS_j terminates the session. Otherwise, ECS_j computes the tourist identity $ID_i' = D_j \oplus h(y_2) \oplus PID_i \oplus t$. Then, it computes the parameter $F_j' = h(ID_i' \| D_j \| y_1 \| y_3)$ and compares F_j' and F_j to see if they are equal. If they are not equal, the session is terminated directly. If equal, ECS_j can pair the received identity ID_i and the stored parameter D_j. Then, ECS_j computes $C_i' = D_j \oplus h(y_2)$, $E_j' = h(C_i' \| y_1 \| y_3) y_2^{-1} P$ and $S_j = O_i \cdot y_2 \cdot h^{-1}(C_i \| y_1 \| y_3) = w_i P$. ECS_j computes the parameter $L_i' = h(C_i' \| E_j' \| S_j \| t)$ and compares whether L_i' is equal to L_i. If they are not equal, the session is terminated directly. If they are equal, ECS_j successfully authenticates T_i. Then, ECS_j selects a random number $z_j \in Z_p^*$ and computes $U_j = z_j S_j = w_i z_j P$. It selects a random number $r_j \in Z_p^*$ and computes the session key $SK = h(ID_i \| C_i' \| U_j \| r_j)$ and $V_j = z_j P, H_j = h(SK \| S_j \| r_j \| C_i')$. Finally, ECS_j sends the message $MG(V_j, r_j, H_j)$ to T_i.

(5) After T_i receives the message, T_i first calculates the parameter $S_j' = w_i P$, $U_j' = w_i V_j = w_i z_j P$ and the session key $SK = h(ID_i \| C_i \| U_j' \| r_j)$. T_i then calculates the parameter $H_j' = h(SK \| S_j' \| r_j \| C_i)$. T_i compares whether H_j' is equal to the received H_j. If they are not equal, the session is terminated. If they are equal, T_i completes the authentication to the edge computing server. The authentication and key negotiation phases are shown in Figure 3.

4.2.4 Password update

(1) T_i inserts the smart card and then inputs the unique identity ID_i , password PW_i , and biometric value BC_i. The smart card calculates $\sigma_i = Rep(BC_i, \tau i)$, $BM_j' = h(ID_i \parallel PW_i \parallel \sigma_i \| x_i)$ and verifies whether BM_j' is equal to BM_j. If they are not equal, the smart card terminates the session. Otherwise, T_i can input a new password.

(2) T_i first chooses a random number $x_i^* \in Z_p^*$ and a new password PW_i^*. Then, T_i calculates the parameters $C_i^* = h(h(ID_i) \bigoplus PW_i^* \bigoplus x_i^*), B_i = E_j \bigoplus C_i^*$ and updates $BM_j^* = h(ID_i \parallel PW_i^* \parallel \sigma_i \| x_i)$. T_i then encrypts the message $E^{SK}(B_i \parallel C_i \parallel ID_i)$ with the current session key SK, and T_i sends it to ECS_j.

(3) ECS_j first decrypts the ciphertext with the session key SK and computes $D_{SK}(B_i \parallel C_i \| ID_i), C_i^* = B_i \bigoplus E_j$. Then, ECS_j computes the parameters $E_j^* = h(C_i^* \parallel y_1 \parallel y_3)y_2^{-1}P$, $D_j^* = C_i^* \bigoplus h(y_2)$, and $F_j^* = h\left(ID_i \parallel D_j^* \parallel y_1 \parallel y_3\right)$. Finally, ECS_j replaces the parameter pair $\left(D_j^*, F_j^*\right)$ with the parameter pair $\left(D_j, F_j\right)$ in the database. ECS_j sends the parameter $E_{S\kappa}\left(E_j \bigoplus E_j^* \bigoplus C_i^*\right)$ to T_i.

(4) T_i then decrypts the ciphertext with the session key SK and computes $D_{SK}\left(E_j \bigoplus E_j^* \bigoplus C_i^*\right), E_j^* = E_j \bigoplus E_j^* \bigoplus C_i^* \bigoplus E_j \bigoplus C_i^*$. T_i replaces E_j with the parameter E_j^*.

5 Security analysis

5.1 Proof of BAN logic

In this section, the BAN logic [31] will be utilized to formally validate the secure authentication process for the anonymous secure authentication method. The prescribed entities are described as follows: tourist T_i and edge computing server ECS_j.

(1) The messages involved in the authentication process are idealized and described as follows:

1) $T_i \rightarrow ECS_j{:}\{w_i\}_{T_i \overset{E_j}{\leftrightarrow} ECS_j}, < ID_i >_{T_i \overset{C_i}{\leftrightarrow} ECS_j}, (w_i P, t)_{T_i \overset{C_i, E_j}{\leftrightarrow} ECS_j}, \left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_j P\right)_{T_i \overset{C_i}{\leftrightarrow} ECS_j}$

2) $ECS_j \rightarrow T_i{:}\left(T_i \leftrightarrow ECS_j, w_i P, r_j\right)_{T_i \overset{C_i}{\leftrightarrow} ECS_j}$

(2) The final objectives of this method are as follows:

$$G1.\, T_i| \equiv \left|ECS_j\right| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j$$

$$G2.\, T_i| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j$$

$$G3.\, ECS_j| \equiv T_i| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j$$

$$G4.\, ECS_j| \equiv T_i \equiv T_i \overset{SK}{\leftrightarrow} ECS_{j.}$$

(3) In order to derive the final objective of this method, the following initialization assumptions must be made:

$$A1. T_i| \equiv \# x_i$$

$$A2. T_i| \equiv \# w_i$$

$$A3. ECS_j| \equiv \# z_j$$

$$A4. T_i| \equiv T_i \overset{C_i}{\leftrightarrow} ECS_j$$

$$A5. ECS_j| \equiv T_i \overset{C_i}{\leftrightarrow} ECS_j$$

$$A6. T_i| \equiv T_i \overset{E_j}{\leftrightarrow} ECS_j$$

$$A7. ECS_j| \equiv T_i \overset{E_j}{\leftrightarrow} ECS_j$$

$$A8.\, T_i| \equiv ECS_j| \Rightarrow \left(T_i \overset{SK}{\leftrightarrow} ECS_j\right)$$

$$A9.\, ECS_j| \equiv T_i| \Rightarrow \left(T_i \overset{SK}{\leftrightarrow} ECS_j\right).$$

(4) The logical reasoning process is as follows:

According to assumption $A4$, the idealized description (2) and the message meaning rule, it can be obtained:

$$\frac{T_i| \equiv T_i \overset{C_i}{\leftrightarrow} ECS_j, T_i \lhd \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right)_{T_i \overset{C_i}{\leftrightarrow} ECS_j}.}{T_i| \equiv ECS_j| \sim \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right)} \tag{1}$$

By assumption $A2$ and the message freshness rule, it can be obtained:

$$\frac{T_i| \equiv \# w_i}{T_i| \equiv \# \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right).} \tag{2}$$

According to Equations 1, 2, and the temporary value validation rule, it can be obtained:

$$\frac{T_i| \equiv \# \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right), T_i| \equiv ECS_j| \sim \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right).}{T_i| \equiv ECS_j| \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right)} \tag{3}$$

From Equation 3 and the belief rule, it can be obtained:

$$\frac{T_i| \equiv ECS_j| \left(T_i \overset{SK}{\leftrightarrow} ECS_j, w_i P, r_j\right).}{T_i| \equiv ECS_j \equiv T_i \overset{SK}{\leftrightarrow} ECS_j} \tag{4}$$

In summary, objective $G1$ is achieved.

According to Equation 4, assumption $A8$, and the jurisdiction rule, it can be obtained: 8

$$\frac{T_i \left|\equiv ECS_j\right| \Rightarrow \left(T_i \overset{SK}{\leftrightarrow} ECS_j\right), T_i \left|\equiv ECS_j\right| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j.}{T_i| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j} \tag{5}$$

In summary, objective $G2$ is achieved.

According to assumption $A5$, the idealized description (1), and the message meaning rule, it can be obtained:

$$\frac{ECS_j| \equiv T_i \leftrightarrow C_i ECS_j, ECS_j \lhd \left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_j P\right)_{T_i \overset{C_i}{\leftrightarrow} ECS_j}}{ECS_j| \equiv T_i| \sim \left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_j P\right)} \tag{6}$$

According to assumption $A3$ and the message freshness rule, it can be obtained:

$$\frac{ECS_j| \equiv \# z_j}{ECS_j| \equiv \# \left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_j P\right)} \tag{7}$$

According to Equations 6, 7, and the temporary value validation rule, it can be obtained:

$$\frac{ECS_j| \equiv \#\left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_jP\right), ECS_j| \equiv T_i| \sim \left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_jP\right)}{ECS_j| \equiv T_i|\left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_jP\right)} \tag{8}$$

According to Equation 8 and the belief rule, it can be obtained:

$$\frac{ECS_j| \equiv T_i|\left(T_i \overset{SK}{\leftrightarrow} ECS_j, z_jP\right)}{ECS_j| \equiv T_i|T_i \overset{SK}{\leftrightarrow} ECS_j} \tag{9}$$

In summary, objective $G3$ is achieved.

According to Equation 9, assumption $A9$, and the jurisdiction rule, it can be obtained:

$$\frac{ECS_j| \equiv T_i| \Rightarrow T_i \overset{SK}{\leftrightarrow} ECS_j, ECS_j| \equiv T_i|T_i \overset{SK}{\leftrightarrow} ECS_j}{ECS_j| \equiv T_i \overset{SK}{\leftrightarrow} ECS_j} \tag{10}$$

In summary, objective $G4$ was achieved.

In summary, according to Equations 4, 5, 9, and 10, objectives are achieved. Hence, the proposed approach facilitates mutual authentication between the tourist and the edge computing server and enables session key negotiation.

5.2 Informal analysis

5.2.1 Resisting a man-in-the-middle attack

A man-in-the-middle attack may be more likely to occur in edge computing due to the decentralization of nodes. Suppose adversary $\mathcal{A}$ intercepts and steals message $MG(PID_i, O_i, L_i, t)$ and message $MG\left(V_j, r_j, H_j\right)$. However, because adversary $\mathcal{A}$ does not know the parameters E_j and C_i, adversary $\mathcal{A}$ cannot successfully calculate the relevant parameters PID_i, O_i , and L_i. Therefore, adversary $\mathcal{A}$ cannot disguise itself as a legitimate tourist to deceive the edge computing server. Meanwhile, because the key y_1, y_2, y_3 of the edge computing server is not known, adversary $\mathcal{A}$ cannot calculate the correct parameters $S_j = w_iP$ and $U_j = z_jS_j = w_iz_jP$, so adversary $\mathcal{A}$ cannot disguise itself as the edge computing server to deceive the tourist, either. Therefore, this scheme is resistant to a man-in-the-middle attack.

5.2.2 Resisting an offline password guessing attack

Suppose adversary $\mathcal{A}$ can obtain parameters PID_i, O_i, L_i, V_j, r_j and H_j from the public channel. However, adversary $\mathcal{A}$ does not know the parameters x_i, w_iP, w_iz_jP, y_1, y_2, y_3, so adversary $\mathcal{A}$ cannot guess the password from the public channel by calculating the parameters $h\left(SK \| w_iP \| r_j \| h(h(ID_i) \bigoplus PW_i \bigoplus x_i)\right)$ and the parameter $h\left(h(h(ID_i) \bigoplus PW_i \bigoplus x_i) \| E_j \| w_iP \| t\right)$ to verify that the password matches. It is also assumed that the adversary can obtain BM_j from the smart card through an attack, but the ability of the adversary to guess the two secret parameters, password and identity, is computationally infeasible in polynomial time, so the adversary cannot extract the identity ID_i and password PW_i from BM_j.

5.2.3 Resisting a replay attack

In edge computing, a replay attack may intercept authentication messages and send them repeatedly. When the tourist sends a request message to the edge computing server, adversary $\mathcal{A}$ intercepts the request message $MG(PID_i, O_i, L_i, t)$ and then pretends to be the legitimate tourist to resend this message to the edge computing server. However, without knowing the parameters C_i and E_j, if adversary $\mathcal{A}$ tampers with the timestamp t, the edge computing server can find the message invalid. If adversary $\mathcal{A}$ sends the request message $MG(PID_i, O_i, L_i, t)$ to the edge computing server directly, by verifying the timestamp, the edge computing server can detect whether it is invalid in the request message and subsequently terminate the session. Consequently, this approach can defend against a replay attack.

5.2.4 Resisting a tourist impersonation attack

In edge computing, edge nodes hijack or remotely control other nodes to forge multiple identities to interfere with the authentication process and steal private information from tourists. Assuming that adversary $\mathcal{A}$ impersonates a legitimate tourist, adversary $\mathcal{A}$ can intercept the message $MG(PID_i, O_i, L_i, t)$ of the attacked tourist. At this time, adversary $\mathcal{A}$ can compute the parameter $C_i = ID_i \oplus PID_i$. However, because y_1 is unknown to adversary $\mathcal{A}$ and the difficulty of the elliptic curve discrete logarithmic problem exists, adversary $\mathcal{A}$ cannot correctly compute parameter $E_j = h(C_i \| y_1 \| y_3)y_2^{-1}P$. Adversary $\mathcal{A}$ uses its own parameter C_i' and the identity ID_i of the impersonated tourist to compute the parameter $PID_i = ID_i \bigoplus C_i' \bigoplus t$. Then, $\mathcal{A}$ utilizes E_j' with C_i' to compute $L_i' = h\left(C_i' \| E_j' \| S_j \| t\right)$ and attempts to impersonate tourist T_i. However, the edge computing server verifies that parameter D_j is matched with parameter C_i and identity ID_i when it verifies that the equation $F_j' = h\left(ID_i' \| D_j \| y_1 \| y_3\right)$ is equal to F_j. So, the equation is not valid. Therefore, this scheme is resistant to a tourist impersonation attack.

5.2.5 Resisting a privileged insider attack

Suppose adversary $\mathcal{A}$ acts as a privileged insider tourist and obtains the parameter C_i, identity ID_i and password PW_i of the attacked tourist T_i. Adversary $\mathcal{A}$ tries to impersonate tourist T_i to access the edge computing server. Because parameter E_j is stored in the memory of the tourist, and because adversary $\mathcal{A}$ cannot obtain the keys y_1, y_2, y_3 of the edge computing server, adversary $\mathcal{A}$ is unable to compute the correct parameter E_j. When adversary $\mathcal{A}$ requests the service by pretending to be tourist T_i, the validation $L_i' = h\left(C_i' \| E_j' \| S_j \| t\right) = L_i$ will not pass. Therefore, this scheme is resistant to a privileged internal attack.

5.2.6 Forward security

Assuming that adversary $\mathcal{A}$ already has the session key $SK = h\left(ID_i \| C_i' \| U_j \| r_j\right)$ for the current session and obtains the password PW_i for the tourist and y_2, y_3 for the key of the edge computation server, due to the ECDLP problem, adversary $\mathcal{A}$ cannot compute the values of the parameters w_i and z_j. Meanwhile, because $C_i = h(h(ID_i) \bigoplus PW_i \bigoplus x_i \bigoplus BC_i)$, BC_i is stored as a biometric encryption in a smart card, and C_i cannot be obtained, it is impossible to compute the session key of the previous session. Therefore, this scheme has forward security.

TABLE 2 Length size of various operations.

Definition	Length
Identification	160 *bits*
Random number	160 *bits*
Hash function	160 *bits*
ECC point multiplication	160 *bits*
Timestamp	32 *bits*

TABLE 3 Communication cost.

Scheme	Communication cost
[33]	2,208 *bits*
[34]	2,496 *bits*
[35]	1988 *bits*
Our	992 *bits*

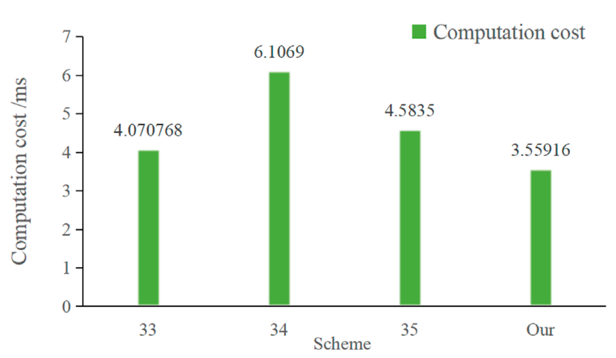

FIGURE 4
Computation cost.

TABLE 4 Operation runtime.

Symbol	Definition	Time
T_h	Hash function	0.00038 *ms*
T_{ecm}	ECC point multiplication	0.5078 *ms*
T_{fe}	Fuzzy extractor generation	0.5078 *ms*

5.2.7 Anonymity

Suppose adversary $\mathcal{A}$ obtains message $MG(PID_i, O_i, L_i, t)$ and message $MG\left(V_j, r_j, H_j\right)$. Because the parameter C_i, $\mathcal{A}$ cannot be obtained, adversary $\mathcal{A}$ cannot calculate the tourist identity $ID_i = PID_i \bigoplus C_i \bigoplus$t. Even if the tourist's long-term private key U_j is leaked, the session key cannot be computed because the tourist utilizes smart card technology to achieve password and biometric encryption preservation, while the tourist ID_i is encrypted through a pseudonym. In addition, the temporary session key passphrase PW_i is updated, which in turn realizes the update of the visitor's identity and cuts off the session key correlation, so it is not possible to infer the tourist's identity through the session key correlation. Therefore, this scheme can realize anonymity. On the other hand, because the tourist uses the random number w_i to calculate the parameters O_i and L_i in each session, adversary $\mathcal{A}$ can not trace through the communication messages to identify who is communicating with the server, realizing untraceability and guaranteeing anonymity.

6 Performance evaluation

6.1 Communication cost

The communication cost of this scheme is compared with other schemes [33–35] to make a uniform assumption in the communication overhead comparison. The length settings for each operation are given in Table 2.

In this paper, the authentication and key negotiation phases of the scheme, the transmitted messages $MG(PID_i, O_i, L_i, t)$ and $MG\left(V_j, r_j, H_j\right)$, respectively, require 512 *bits* and 480 *bits*. Therefore, the total communication cost of this scheme is 992 *bits*. The total communication cost of [33] is 2208 *bits*.The total communication overhead of [34] is 2496 *bits*.The total communication overhead of [35] is 1988 *bits*.The results of the comparison of the communication cost with other schemes are shown in Table 3 and Figure 4.

The results of Table 3, Figure 3 show that the proposed scheme in this paper is significantly better than schemes [33–35] in terms of communication cost. This can greatly reduce the communication cost of an anonymous secure authentication method for tourist attraction network-based edge computing and is suitable for the lightweight communication requirements of the edge computing tourist attraction network scenarios. In practical applications, the method in this paper can effectively reduce the amount of data transmission, accelerate the speed of secure authentication, and reduce bandwidth consumption and device energy consumption, so as to enhance the tourists' travel experience while safeguarding their privacy and security.

6.2 Computation cost

The computational cost of this scheme is compared with that of other schemes [33–35]. Some operations with a large computation cost are considered in this paper and the rest, such as XOR operations, have negligible computation time. The different operations and their execution times are shown in Table 4.

In this paper, the computation cost of the tourist T_i is $5T_h + 3T_{ecm} + T_{fe}$, and the computation cost of the edge computing server is $7T_h + 3T_{ecm}$, so the total computation cost of this scheme is $12T_h + 6T_{ecm} + T_{fe} \approx 3.55916\,ms$. The computation cost of [33] is $22T_h + 8T_{ecm} \approx 4.070768\,ms$. The computation cost of [34] is $35T_h + 10T_{ecm} + 2T_{fe} \approx 6.1069\,ms$. The computation cost of [35] is $35T_h + 9T_{ecm} \approx 4.5835$ *ms*. Table 5 and Figure 4 show the computation costs of the relevant schemes.

TABLE 5 Computation cost.

Scheme	Computation cost	Time
[33]	$22T_h + 8T_{ecm}$	$4.070768\,ms$
[34]	$35T_h + 10T_{ecm} + 2T_{fe}$	$6.1069\,ms$
[35]	$35T_h + 9T_{ecm}$	$4.5835\,ms$
Our	$12T_h + 6T_{ecm} + T_{fe}$	$3.55916\,ms$

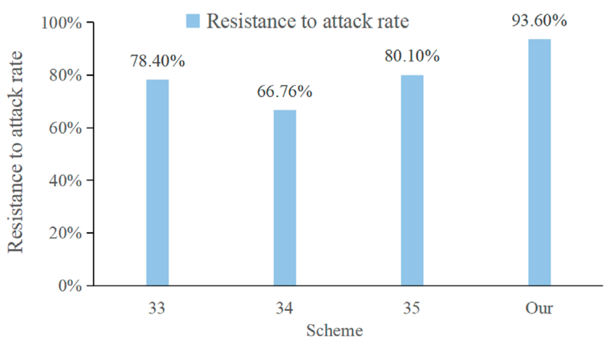

FIGURE 5
Resistance to attack rate.

The comparison results show that the computation cost of this paper's scheme is relatively low. Although [33] achieves lower computation overhead, this scheme cannot resist the fake attack and lacks anonymity analysis, so the proposed scheme outperforms [33] in terms of security attributes. The computational cost of the scheme presented in [34] is approximately 1.72 times higher than that of our proposed scheme, while the cost of [35] is slightly higher at about 1.29 times. Overall, both schemes exhibit relatively elevated computational costs compared to ours. Therefore, the computation cost of this scheme is relatively low while providing better security. This scheme can effectively shrink the amount of data transmission, reduce the network bandwidth occupation, and increase the transmission speed of authentication information. This scheme significantly improves the security authentication efficiency of the tourist attraction network in the edge computing environment, while safeguarding the privacy of the tourists and the security of the data.

6.3 Resistance to attack rate

Assuming that this experiment is tested under the same kind of attack, due to more types of attacks, we select the more typical replay attack, man-in-the-middle attack, and impersonation attack in edge computing, and compare the resistance to attack rate of this scheme with the other schemes [33, 34], and [35] under the three kinds of attacks. The experimental results are shown in Figure 5.

It can be seen from the experiments that the overall resistance to attack rate of this paper's scheme is 93.6%. The overall resistance to attack rate of [33] is 78.4%, and this scheme cannot resist a man-in-the-middle and an impersonation attack well. The overall resistance to attack rate of [34] is 66.76%; this scheme lacks the analysis of a replay attack. The overall resistance to attack rate of [35] is 80.1%, and this scheme cannot effectively resist a replay attack. In summary, the overall resistance to attack rate for this paper's scheme is higher and the security strength is stronger than that of other schemes.

7 Conclusion

Edge computing, a distributed computing paradigm, migrates data processing and application services from centralized data centers to the edge of the network to reduce latency and increase responsiveness. However, edge computing brings new challenges, especially in terms of security authentication. The large number and diverse types of devices in edge computing environments, and the often resource-constrained nature of the devices, require efficient, lightweight, secure, and reliable authentication mechanisms for tourist attraction networks. The scheme proposed in this paper is based on ECC, which ensures the anonymity of the scheme through a pseudo-random identity. At the same time, the mechanism also has the ability to guarantee security even when the smart card is stolen. BAN logic is used for formal analysis and combined with non-formal evaluation tools for comprehensive security consideration. In terms of performance evaluation, the focus is on comparing communication and computation costs, as well as resistance to attack rate, and the results show that the scheme achieves a good balance between performance and security by maintaining high efficiency while also achieving high security standards. In terms of future research prospects, it will continue to innovate the authentication mechanism, optimize the authentication process, and improve security and efficiency through the integration with emerging technologies such as 5G, IoT, and blockchain.

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

XZ: Conceptualization, Funding acquisition, Investigation, Methodology, Project administration, Software, Writing – original draft. ZZ: Data curation, Formal analysis, Projectadministration, Resources, Supervision, Validation, Visualization, Writing – review and editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. From the Guizhou

University of Commerce Research and Interpretation of the Spirit of the Third Plenary Session of the 20th Central Committee of the Communist Party of China Special Project Funding: "Coupling Mechanism and Collaborative Enhancement Path of Urban Digital Economy and High-Quality Development of Exhibition" (No. 2024XJFSDZD10).

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. Asghari A, Sohrabi MK. Server placement in mobile cloud computing: a comprehensive survey for edge computing, fog computing and cloudlet. *Computer Sci Rev* (2024) 51:100616. doi:10.1016/j.cosrev.2023.100616

2. Tang X, Tang T, Shen Z, Zheng H, Ding W. Double deep Q-network-based dynamic offloading decision-making for mobile edge computing with regular hexagonal deployment structure of servers. *Appl Soft Comput* (2025) 169:112594. doi:10.1016/j.asoc.2024.112594

3. Miao J, Wang Z, Wang M, Garg S, Hossain MS, Rodrigues JJ. Secure and efficient communication approaches for industry 5.0 in edge computing. *Computer Networks* (2024) 242:110244. doi:10.1016/j.comnet.2024.110244

4. Ahmed ST, Vinoth Kumar V, Mahesh TR, Narasimha Prasad LV, Velmurugan AK, Muthukumaran V, et al. FedOPT: federated learning-based heterogeneous resource recommendation and optimization for edge computing. *Soft Comput* (2024) 1–12. doi:10.1007/s00500-023-09542-6

5. Huo Y, Liu Q, Gao Q, Wu Y, Jing T. Joint task offloading and resource allocation for secure OFDMA-based mobile edge computing systems. *Ad Hoc Networks* (2024) 153:103342. doi:10.1016/j.adhoc.2023.103342

6. Wei CC. Tourist attraction image recognition and intelligent recommendation based on deep learning. *J Comput Methods Sci Eng* (2025):14727978251318805. doi:10.1177/14727978251318805

7. 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

8. Rong J, Hao H, Xu W. Big data intelligent tourism management platform design based on abnormal behavior identification. *Intell Syst Appl* (2024) 21:200312. doi:10.1016/j.iswa.2023.200312

9. 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

10. 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

11. Dogru T, Line N, Mody M, Hanks L, Abbott J, Acikgoz F, et al. Generative artificial intelligence in the hospitality and tourism industry: developing a framework for future research. *J Hospitality and Tourism Res* (2025) 49(2):235–53. doi:10.1177/10963480231188663

12. Ling EC, Tussyadiah I, Liu A, Stienmetz J. Perceived intelligence of artificially intelligent assistants for travel: scale development and validation. *J Trav Res* (2025) 64(2):299–321. doi:10.1177/00472875231217899

13. Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Syst J* (2015) 9(3):805–15. doi:10.1109/jsyst.2014.2322973

14. Jiang Q, Ma J, Wei F. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Syst J* (2016) 12(2):2039–42. doi:10.1109/jsyst.2016.2574719

15. Xiong L, Peng D, Peng T, Liang H An enhanced privacy-aware authentication scheme for distributed mobile cloud computing services. *KSII Trans Internet Inf Syst (Tiis)* (2017) 11(12):6169–87. doi:10.3837/tiis.2017.12.026

16. Irshad A, Sher M, Ahmad HF, Alzahrani BA, Chaudhry SA, Kumar R An improved multi-server authentication scheme for distributed mobile cloud computing services. *KSII Trans Internet Inf Syst (Tiis)* (2016) 10(12): 5529–52. doi:10.3837/tis.2016.12.021

17. Muniswamaiah M, Agerwala T, Tappert CC. A survey on cloudlets, mobile edge, and fog computing[C]. In: *2021 8th IEEE international conference on cyber security and cloud computing (CSCloud)/2021 7th IEEE international conference on edge computing and scalable cloud (EdgeCom)*. IEEE (2021). p. 139–42.

18. Dewanta F, Mambo M. A mutual authentication scheme for secure fog computing service handover in vehicular network environment. *IEEE Access* (2019) 7:103095–114. doi:10.1109/access.2019.2931217

19. Jia X, He D, Kumar N, Choo KKR. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. *IEEE Syst J* (2019) 14(1):560–71. doi:10.1109/jsyst.2019.2896064

20. Mishra D, Dharminder D, Yadav P, Sreenivasa Rao Y, Vijayakumar P, Kumar N. A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party. *J Inf Security Appl* (2020) 55:102648. doi:10.1016/j.jisa.2020.102648

21. Lai C, Ma Y. A novel group-oriented handover authentication scheme in MEC-enabled 5G networks[C]. *2021 Ieee/cic Int Conf Commun China (Iccc) IEEE* (2021) 29–34. doi:10.1109/ICCC52777.2021.9580296

22. Li Y, Cheng Q, Liu X, Li X. A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing. *IEEE Syst J* (2020) 15(1):935–46. doi:10.1109/jsyst.2020.2979006

23. Shamshad S, Rana M, Mahmood K, Khan MK, Obaidat MS. On the security of a secure anonymous identity-based scheme in new authentication architecture for mobile edge computing. *Wireless Personal Commun* (2022) 124(1):283–92. doi:10.1007/s11277-021-09338-7

24. Rakeei M, Moazami F. An efficient and provably secure authenticated key agreement scheme for mobile edge computing. *Wireless Networks* (2022) 28(7):2983–99. doi:10.1007/s11276-022-03005-w

25. Xu Y, Zhou Y, Yang B, Qiao Z, Wang Z, Xia Z, et al. An efficient identity authentication scheme with provable security and anonymity for mobile edge computing. *IEEE Syst J* (2022) 17(1):1012–23. doi:10.1109/jsyst.2022.3185258

26. Zhang S, Cao D. A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT. *The J Supercomputing* (2024) 80(5):6778–808. doi:10.1007/s11227-023-05696-0

27. Tian J, Wang Y, Shen Y. An ldentity-based AuthenticationScheme with full anonymity and unlinkability for MobileEdge computing. *lEEE Internet Things J* (2024). doi:10.1109/JIOT.2024.3385095

28. Zhang S, He J, Liang W, Li K. MMDS: a secure and verifiable multimedia data search scheme for cloud-assisted edge computing. *Future Generation Computer Syst* (2024) 151:32–44. doi:10.1016/j.future.2023.09.023

29. Samal K, Sunanda SK, Jena D, Patnaik S. A lightweight privacy preservation authentication protocol for IoMT using ECC based blind signature. *Int J Eng Business Management* (2025) 17:18479790251318538. doi:10.1177/18479790251318538

30. Liu G, Lu H, Wang W, Liu Z, Huang H. A cross-domain authentication scheme for vehicular networks based on mobile edge computing. *IEEE Internet Things J* (2025) 1. doi:10.1109/jiot.2025.3540162

31. Adil ZUI, Iqbal Khan M, Sanam K, Malik SUR, Moqurrab SA, Srivastava G. LightAuth: a lightweight sensor nodes authentication framework

for smart health system. *Expert Syst* (2025) 42(2):e13756. doi:10.1111/exsy.13756

32. Suneetha G, Haripriya D. An enhanced deep learning integrated blockchain framework for securing industrial IoT. *Peer-to-Peer Networking Appl* (2025) 18(1):28–0. doi:10.1007/s12083-024-01857-x

33. Zhao X, Li D, Li H. Practical three-factor authentication protocol based on elliptic curve cryptography for industrial internet of things. *Sensors* (2022) 22(19):7510. doi:10.3390/s22197510

34. Cui J, Cheng F, Zhong H, Zhang Q, Gu C, Liu L. Multi-factor based session secret key agreement for the Industrial Internet of Things. *Ad Hoc Networks* (2023) 138:102997. doi:10.1016/j.adhoc.2022.102997

35. Prasanna R, Santhakumar D, Sudhan MB, Manikandan SP, Prathaban BP, Kanna RR, et al. Smart driving licensing system and authorization of autonomous vehicle integrating wireless sensor networks and IoT. *Telecommunications Radio Eng* (2024) 83:69–85. doi:10.1615/telecomradeng.2024052539