1-1-2023

Identity-based edge computing anonymous authentication protocol

Naixin Kang

Zhenhu Ning

Shiqiang Zhang

Sadaqat ur Rehman

Muhammad Waqas
Edith Cowan University

10.32604/cmc.2023.029711
Kang, N., Ning, Z., Zhang, S., Rehman, S.& Waqas, M. (2023). Identity-based edge computing anonymous authentication protocol, 74(2), 3931-3943. https://doi.org/10.32604/cmc.2023.029711

Computers, Materials & Continua
DOI: 10.32604/cmc.2023.029711
Article

Identity-Based Edge Computing Anonymous Authentication Protocol

Naixin Kang[1], Zhenhu Ning[1,*], Shiqiang Zhang[1], Sadaqat ur Rehman[2] and Waqas[1,3]

[1]Beijing University of Technology, Beijing, 100124, China
[2]Department of Natural and Computing Science University of Aberdeen, UK
[3]School of Engineering, Edith Cowan University, Perth, 6027, Australia
*Corresponding Author: Zhenhu Ning. Email: nzh41034@163.com
Received: 10 March 2022; Accepted: 25 May 2022

Abstract: With the development of sensor technology and wireless communication technology, edge computing has a wider range of applications. The privacy protection of edge computing is of great significance. In the edge computing system, in order to ensure the credibility of the source of terminal data, mobile edge computing (MEC) needs to verify the signature of the terminal node on the data. During the signature process, the computing power of edge devices such as wireless terminals can easily become the bottleneck of system performance. Therefore, it is very necessary to improve efficiency through computational offloading. Therefore, this paper proposes an identity-based edge computing anonymous authentication protocol. The protocol realizes mutual authentication and obtains a shared key by encrypting the mutual information. The encryption algorithm is implemented through a thresholded identity-based proxy ring signature. When a large number of terminals offload computing, MEC can set the priority of offloading tasks according to the user's identity and permissions, thereby improving offloading efficiency. Security analysis shows that the scheme can guarantee the anonymity and unforgeability of signatures. The probability of a malicious node forging a signature is equivalent to cracking the discrete logarithm puzzle. According to the efficiency analysis, in the case of MEC offloading, the computational complexity is significantly reduced, the computing power of edge devices is liberated, and the signature efficiency is improved.

Keywords: Identity authentication; anonymous authentication; edge computing

1. Introduction

With sensor technology and wireless communication technology development, the application range of edge computing has become more extensive [1]. In an edge computing system, the computing power of edge devices such as wireless terminals may become the bottleneck of system performance. It is often necessary to offload to improve computing efficiency. When many terminals are offloading computing, the MEC server must process the offloaded task according to priority [2–4]. However,

the data of some terminals have the characteristics of information sensitivity and timeliness, which requires faster offloading of computing tasks and higher priority [5]. Such terminals are privileged users. Since wireless terminals are bound to user identities, privileged users will authorize signatures to other terminals in order to complete the signatures together more efficiently [6]. How to protect the privacy of the wireless terminal's identity while completing the data transmission between the wireless terminal and the MEC, which has essential research significance [7,8]. At present, the common methods mainly include group signature, ring signature, proxy signature, etc.

An identity-based proxy threshold ring signature for edge computing is proposed in this paper. The original signature scheme is optimized, and the proxy signature is combined with the ring signature to improve the efficiency of signatures and ensure the identity privacy of the proxy signer and use the threshold method prevents the influence of a single node's malicious actions on the signature; combined with edge computing, the computing power of the MEC server is used to reduce the burden on the wireless terminal further.

The arrangement of the remaining chapters of this article: Section 2 introduces the research work related to this article and briefly introduces and analyzes these results. Section 3 describes the authentication process between the original signer, the proxy signer, and the MEC server. Section 4 describes in detail the identity-based anonymous authentication protocol in the context of edge computing. Sections 5 and 6 analyze the scheme from three aspects: correctness, security and computational efficiency. The Section 7 summarizes the content of the full text, and puts forward the research direction of the follow-up work.

2 Related Work

Edge computing is a distributed service architecture that migrates computing and storage resources from the cloud platform to the network edge. It consists of multiple edge nodes located between cloud servers and local devices to complete data analysis tasks. Because it is closer to the local device, it can provide services with less latency, such as autonomous driving, virtual reality, smart cities, etc. But since edge nodes are usually located in untrusted environments, they also face various security and privacy threats. For example, the local device may add poisoned samples or send low-quality data to the edge node, and the edge node may speculate the data privacy of the local device, or tamper with the calculation result to destroy the execution of the protocol. Therefore, it is very important to build a more robust privacy protection and information security mechanism. The following mainly introduces the literature related to privacy protection and anonymous authentication in the edge computing environment.

Elliptic curve is a commonly used encryption method at present. It has high security, but it also consumes a lot of computation. Literature [9] proposed a lightweight anonymous authentication protocol for Internet of things terminals. The protocol uses certificateless signature, elliptic curve and signcryption technology. Through random oracle analysis, the model can realize anonymous authentication and privacy protection, and has low computing and communication costs. Literature [10] combined ring signature and elliptic curve cryptosystem and proposed a verifiable ring signature scheme using ECC anonymous sign-crypt. This scheme has the advantages of anonymity of ring signature, low computational cost, and high security of elliptic curve cryptosystem. Literature [11] combines the characteristics of group signature and threshold signature. This paper proposes a threshold group signature scheme based on the elliptic curve and realized the group members and administrators of two-way authentication. The program has anonymity and traceability also can resist collusion attacks to solve the Internet of things terminal, tampered with, such as counterfeiting threats

are easy to be tapped. According to the characteristics of group signature and threshold signature, the scheme in reference [12] proposes a threshold group signature scheme based on elliptic curve, which realizes the two-way authentication between group members and group administrators. This method has anonymity and traceability, and solves the threat that the Internet of things terminal is easy to be eavesdropped, tampered and forged. However, the improvement of security has a certain impact on the efficiency of computing and communication.

Group signature scheme is a common method of anonymous authentication. Literature [13] proposes a group signature scheme that can be modified to provide privacy protection certification. For many revocable group signature schemes, this scheme introduces a contained backward security model of the definition of safety compared with previous schemes. This scheme is efficient and scalable, and more practical in actual application. Literature [14] proposed an efficient full-dynamic group signature scheme for the group signature that allows users to register and cancel within the group. The technology uses a merkle tree to record the information of registered users and uses a trusted third party to generate public and private keys. Thus, the computational efficiency of the scheme is improved. Literature [15] proposes an anonymous authentication scheme suitable for doctor-patient relationship. The scheme uses single hash function and user behavior tracking system to protect user privacy and improve system performance. At the same time, through experimental analysis, the scheme can resist most attacks and has high security.

Proxy signature is often used to reduce the consumption of self-signature. Literature [16] puts forward a kind of according to industrial IoT environment efficiently and to prove that the proxy signature scheme based on the certificate without pairing, this scheme can solve common password scheme based on certification of identity or secret key escrow and secret key distribution problems, at the same time, at different stages of the cost and the length of the signature than other signature schemes have reduced. Reference [17] proposed a lattice-based quantum proof anonymous proxy signature. Anonymity is achieved by using ring signatures. The experimental analysis proves that the scheme has adaptive security against the stability of the selected message attack on the small integer solution problem. Reference [18] proposes a decentralized electronic reporting scheme based on proxy signature and blockchain privacy protection. The scheme uses lattice ciphers to protect privacy while also resisting quantum attacks. Reference [19] proposed an efficient heterogeneous cross-domain authentication scheme based on proxy blind signature in cloud environment. This scheme gives the authority of the third-party legal agent by introducing a trusted certification center between the clouds. The authentication process is optimized by a trusted third party, but is prone to a single point of failure.

3 Identity Authentication Protocol

3.1 Protocol Description

The specific process of the scheme is shown in Fig. 1 below.

The original signer hides his identity information by constructing a ring, sends the entrusting certificate to the proxy signer as a ring, and distributes the information that can represent his identity to the proxy signer in the way of the threshold. After receiving the entrusting certificate and key fragment, the proxy signer shares the information with the members in the ring to calculate and generate the proxy threshold ring signature.

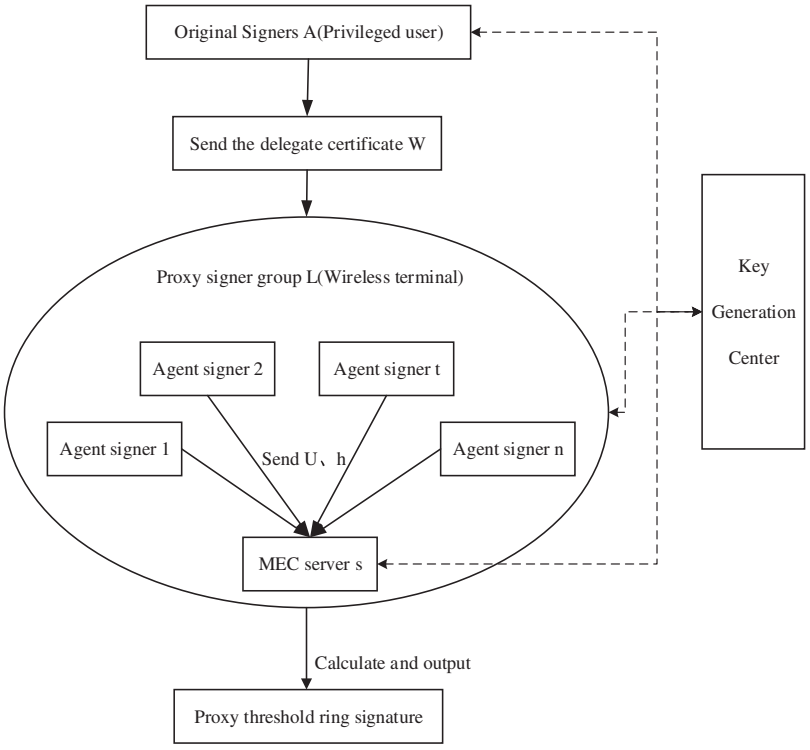

Figure 1: Anonymous authentication protocol structure diagram

Privileged member A, proxy signature terminal N, edge computing server MEC and key generation center (KGC) have shared keys, but they do not have identity authentication keys between them. Therefore, through the following protocol process, privileged members can be made A shared identity key k_{an} is obtained between A and the proxy signature terminal N, and a shared identity key k_{mn} is obtained between the proxy signature terminal N and the edge computing server MEC. The specific process is as follows:

(1) Privileged member A sends his identity information ID_A and request $req1$ to obtain the shared identity key to the proxy signature terminal N.
(2) N packs the received information of A with its own identity information ID_N and request $req2$ and sends it to the edge server MEC.
(3) MEC packs the received information of N with its own identity information ID_M and request $req3$ and sends it to the key generation center KGC.
(4) After the KGC receives the information from the MEC, it generates three random numbers r_{K1}, r_{K2}, r_{K3} and returns it to the MEC. The MEC keeps one of its own and sends the remaining two to N, and N repeats the above steps. MEC, N, and A obtain the random number r_{K3}, r_{K2}, r_{K1} generated by KGC, respectively.
(5) A generates a random number r_A, encrypts the shared identity key information that it wants to obtain with the shared key between KGC and sends it to N together with the random number. N is the same as above, packs its random number r_N, encrypted information, and received information to MEC. MEC sends $\{r_{K1}||r_A||ID_A||ID_N\}_{K_{ak}}, r_A, \{r_{K3}||r_M||ID_M||ID_N\}_{K_{mk}}, r_M, \{r_{K2}||r_N||ID_N||ID_A||ID_M\}_{K_{nk}}, r_N$ to KGC.

(6) After receiving the information, the KGC obtains the needs of different users through decryption and returns the requested information $\{r_A||k_{an}||ID_K\}_{K_{ak}}, \{r_N||k_{an}||k_{mn}||ID_K\}_{K_{nk}}$, $\{r_M||k_{mn}||ID_K\}_{K_{mk}}$ to the MEC.
(7) After MEC receives the information, it sends the information to N and A layer by layer.
(8) After A, N, and MEC decrypt the received information, they obtain the identity keys k_{an} and k_{mn}.

3.2 Safety Analysis

The security analysis of this scheme can be proved by formal methods (including BAN logic, model checking (CSP), theorem-proof (string space) and other methods). BAN logic is mainly used to analyze whether the cryptographic protocol can normally work, what content has been completed by the protocol, the assumptions required by the protocol, and the rationality of the assumptions [20]. BAN logic is a logical analysis method based on knowledge and belief. The BAN logic definition and derivation formula used in the proof of this article are as follows.

3.2.1 Protocol Description

$A->N: ID_A, req1$

$N->M: ID_A, req1, ID_N, req2$

$M->K: ID_A, req1, ID_N, req2, ID_M, req3$

$K->M: r_{K1}, r_{K2}, r_{K3}$

$M->N: r_{K1}, r_{K2}$

$N->A: r_{K1}$

$A->N: \{r_{K1}||r_A||ID_A||ID_N\}_{K_{ak}}, r_A$

$N->M: \{r_{K1}||r_A||ID_A||ID_N\}_{K_{ak}}, r_A, \{r_{K2}||r_N||ID_N||ID_A||ID_M\}_{K_{nk}}, r_N$

$M->K: \{r_{K1}||r_A||ID_A||ID_N\}_{K_{ak}}, r_A, \{r_{K2}||r_N||ID_N||ID_A||ID_M\}_{K_{nk}}, r_N\{r_{K3}||r_M||ID_M||ID_N\}_{K_{mk}}, r_M$

$K->M: \{r_A||k_{an}||ID_K\}_{K_{ak}}, \{r_N||k_{an}||k_{mn}||ID_K\}_{K_{nk}}, \{r_M||k_{mn}||ID_K\}_{K_{mk}}$

$M->N: \{r_A||k_{an}||ID_K\}_{K_{ak}}, \{r_N||k_{an}||k_{mn}||ID_K\}_{K_{nk}}$

$N->A: \{r_A||k_{an}||ID_K\}_{K_{ak}}$

3.2.2 Inference Rules

(1) Message meaning rules

$$\frac{P|\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\} K}{P|\equiv Q \sim X} \tag{1}$$

(2) Temporary value validation rules

$$\frac{P|\equiv \#(X), P|\equiv Q| \sim X}{P|\equiv Q|\equiv X} \tag{2}$$

(3) Arbitration rules

$$\frac{P|\equiv Q| \Rightarrow P, P|\equiv Q|\equiv X}{P|\equiv X} \tag{3}$$

(4) Freshness rules

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X, Y)} \tag{4}$$

According to the logic initialization hypothesis:

(1) $A|\equiv A \overset{K_{ak}}{\longleftrightarrow} K$

(2) $K|\equiv A \overset{K_{ak}}{\longleftrightarrow} K$

(3) $N|\equiv N \overset{K_{nk}}{\longleftrightarrow} K$

(4) $K|\equiv N \overset{K_{nk}}{\longleftrightarrow} K$

(5) $M|\equiv M \overset{K_{mk}}{\longleftrightarrow} K$

(6) $K|\equiv M \overset{K_{mk}}{\longleftrightarrow} K$

(7) $K|\equiv \#(r_{K1})$

(8) $K|\equiv \#(r_{K2})$

(9) $K|\equiv \#(r_{K3})$

(10) $A|\equiv \#(r_A)$

(11) $N|\equiv \#(r_N)$

(12) $M|\equiv \#(r_M)$

(13) $A|\equiv K| \Rightarrow A$

(14) $N|\equiv K| \Rightarrow N$

(15) $M|\equiv K| \Rightarrow M$

3.2.3 Logical Inference

(1) Proof of $K|\equiv A \overset{k_{cn}}{\longleftrightarrow} N$:

$K \lhd \{r_{K1}||r_A||ID_A||ID_N\}_{K_{ak}}, \{r_{K2}||r_N||ID_N||ID_A||ID_M\}_{K_{nk}}$

From the initialization assumptions (2), (4) and rule (1), we can get:

$K|\equiv A \sim \{r_{K1}||r_A||ID_A||ID_N\}$ $K|\equiv N \sim \{r_{K2}||r_N||ID_N||ID_A||ID_M\}$

From the initialization assumptions (7), (8) and rule (4), we can get:

$K|\equiv \#\{r_{K1}||r_A||ID_A||ID_N\}$ $K|\equiv \#\{r_{K2}||r_N||ID_N||ID_A||ID_M\}$

From the above results and rule (2), we can get:

$K|\equiv A|\equiv \{r_{K1}||r_A||ID_A||ID_N\}$ $K|\equiv N|\equiv \{r_{K2}||r_N||ID_N||ID_A||ID_M\}$

So: $K|\equiv A \overset{k_{cn}}{\longleftrightarrow} N$

(2) Proof of $K|\equiv M \overset{k_{mn}}{\longleftrightarrow} N$:

$K \lhd \{r_{K2}||r_N||ID_N||ID_A||ID_M\}_{K_{nk}}, \{r_{K3}||r_M||ID_M||ID_N\}_{K_{mk}}$

From the initialization assumptions (4), (6) and rule (1), we can get:

$K|\equiv N \sim \{r_{K2}||r_N||ID_N||ID_A||ID_M\}$ $K|\equiv M \sim \{r_{K3}||r_M||ID_M||ID_N\}$

From the initialization assumptions (8), (9) and rule (4), we can get:

$K|\equiv \#\{r_{K2}||r_N||ID_N||ID_A||ID_M\}$ $K|\equiv \#\{r_{K3}||r_M||ID_M||ID_N\}$

From the above results and rule (2), we can get:

$K|\equiv N|\equiv \{r_{K2}||r_N||ID_N||ID_A||ID_M\}$ $K|\equiv M|\equiv \{r_{K3}||r_M||ID_M||ID_N\}$

So: $K|\equiv M \overset{k_{mn}}{\longleftrightarrow} N$

(3) Proof of $M|\equiv M \overset{k_{mn}}{\longleftrightarrow} N$:

$M \lhd \{r_M||k_{mn}||ID_K\}_{K_{mk}}$

From the initialization assumptions (5) and rule (1), we can get:

$M|\equiv K \sim \{r_M||k_{mn}||ID_K\}$

From the initialization assumptions (12) and rule (4), we can get:

$M|\equiv \#\{r_M||k_{mn}||ID_K\}$

From rule (2), we can get:

$M|\equiv K|\equiv M \overset{k_{mn}}{\longleftrightarrow} N$

From the initialization assumptions (15) and rule (3), we can get:

$M|\equiv M \overset{k_{mn}}{\longleftrightarrow} N$

(4) Proof of $N|\equiv M \overset{k_{mn}}{\longleftrightarrow} N, N|\equiv A \overset{k_{an}}{\longleftrightarrow} N$:

$N \lhd \{r_N||k_{an}||k_{mn}||ID_K\}_{K_{nk}}$

From the initialization assumptions (3) and rule (1), we can get:

$N|\equiv K \sim \{r_N||k_{an}||k_{mn}||ID_K\}$

From the initialization assumptions (11) and rule (4), we can get:

$N|\equiv \#\{r_N||k_{an}||k_{mn}||ID_K\}$

From rule (2), we can get:

$N|\equiv K|\equiv M \overset{k_{mn}}{\longleftrightarrow} N \quad N|\equiv K|\equiv A \overset{k_{an}}{\longleftrightarrow} N$

From the initialization assumptions (14) and rule (3), we can get:

$N|\equiv M \overset{k_{mn}}{\longleftrightarrow} N \quad N|\equiv A \overset{k_{an}}{\longleftrightarrow} N$

(5) Proof of $A|\equiv A \overset{k_{an}}{\longleftrightarrow} N$:

$A \lhd \{r_A||k_{an}||ID_K\}_{K_{ak}}$

From the initialization assumptions (1) and rule (1), we can get:

$A|\equiv K \sim \{r_A||k_{an}||ID_K\}$

From the initialization assumptions (10) and rule (4), we can get:

$M|\equiv \#\{r_A||k_{an}||ID_K\}$

From rule (2), we can get:

$A|\equiv K|\equiv A \overset{k_{an}}{\longleftrightarrow} N$

From the initialization assumptions (13) and rule (3), we can get:

$A|\equiv A \overset{k_{an}}{\longleftrightarrow} N$

4 Signature Scheme

4.1 Key Generation Algorithm

Let q be a large prime number, point P be the generator of the additive cyclic group G_1 of order q, G_2 be the multiplicative cyclic group of the same order, and bilinear mapping e : $G_1 \times G_1 \to G_2$. $Hash : H_1\{0,1\}* \to G_1$, $Hash : H_2\{0,1\}* \to Z_q^*$ is a hash function, H_1 maps any bit string to a point in the group G_1, H_2 maps any bit string to a number in G_1. Select s as the primary key and $P_{pub} = sP$ as the system public key randomly. Expose the system parameter $< G_1, G_2, e, q, P, P_{pub}, H_1, H_2 >$.

The signer can send his identity information to the Key Generation Center (KGC) to obtain his private key. After KGC confirms his identity, it hashes the ID, $Q_{ID} = H_1(ID)$, which can be used as his public key, and then calculates his private key $S_{ID} = sQ_{ID}$. KGC sends the public and private key pair (Q_{ID}, S_{ID}) to the corresponding member through the private channel.

4.2 Agent Generation Algorithm

4.2.1 Pretreatment Stage

The original signer A is a privileged user whose identity information is ID_0. The proxy signer is a wireless terminal device. The ring $L = \{ID_1, \ldots, ID_n\}$ has n members and consists of a wireless terminal device. The identity information of L is $ID_s = H_1(ID_1|| \ldots ||ID_n)$. At this time, the private keys of the original signer and the proxy signer are $S_{ID_0} = sQ_{ID_0}, S_{ID_s} = sQ_{ID_s}$. N members hold a private key fragment of the proxy signer's private key in a threshold manner. The KGC selection threshold polynomial is generated as follows:

$$f(x) = S_{ID_c} + \left(\sum_{i=2}^{t} a_{i-1}x^{i-1}\right)Q_{ID_c} = \left(s + \sum_{i=2}^{t} a_{i-1}x^{i-1}\right)Q_{ID_c} \tag{5}$$

Each proxy signer $ID_i (i = 1, \ldots, n)$ gets the corresponding key fragment $f(ID_i)$.

4.2.2 Agent Phase

(1) The signature information is m, and the original signature is generated into a delegation certificate m. The delegation certificate includes the ring's information where the original signer

and the proxy signer are, the time stamp, the information of the file to be signed, etc. The timestamp is used to limit the validity of the signature. Calculate $h = H_2(m||W||L)$.

(2) The original signer A randomly selects $r \in Z_q^*$, calculates and publishes the rP, then calculates the rP_{pub} and sends it to the member MEC server ID_c.
Original signer selection threshold polynomial:

$$h(x) = rP_{pub} + \left(\sum_{i=2}^{t} a_{i-1}x^{i-1}\right) Q_{ID_P} \tag{6}$$

Each proxy signer $ID_i (i = 1, \ldots, n)$ obtains the corresponding fragment $h(ID_i)$.

4.3 Signature Generation Algorithm

(1) The proxy signer $ID_i (i = 1, \ldots, t, i \neq c)$ participating in the signing selects $U_i \in G_1$ and calculates $h_i = H_2(m||W\|L\|U_i), \forall i \in \{1, \ldots, t\}\backslash\{c\}$.

(2) MEC server ID_c selects a random $r_c \in Z_q^*$, calculates $U_c = r_c Q_{ID_c} - \sum_{i \neq c} \left\{U_i + h_i Q_{ID_i}\right\}$ and $h_c = H_2(m\|W\|L\|U_c)$. The MEC calculates $r_c + h_c$ and returns it to the proxy signer ID_i.

(3) Proxy signer ID_i calculates $V_i = (r_c + h_c) f(ID_i) + h(ID_i)$ and sends it to MEC server ID_c.

(4) The MEC server ID_c calculates $V = \sum_{i=1}^{t} \lambda_i V_i$ and λ_i as Lagrange multipliers and outputs the proxy signature σ of the message m:$\sigma = \left\{U_{i=1}^{t}\{U_i\}, V\right\}$.

5 Signature Verification

The MEC performs the following verification after receiving the signature information:

Verify that $e\left(P_{pub}, \sum_{i=1}^{t}\left(U_i + h_i Q_{ID_i}\right) + rP\right) = e(P, V)$ is valid. If yes, the signature is accepted. The specific process is as follows:

$$\begin{aligned} & e\left(P_{pub}, \sum_{i=1}^{n}\left(U_i + h_i Q_{ID_i}\right) + rP\right) \\ & = e\left(P_{pub}, \left(U_c + h_c Q_{ID_c}\right) + \sum_{i=1, i\neq c}^{n}\left(U_i + h_i Q_{ID_i}\right) + rP\right) \\ & = e\left(P_{pub}, r_c Q_{ID_c} + h_c Q_{ID_c} + rP\right) \\ & = e(P, V) \end{aligned} \tag{7}$$

6 Performance Analysis

6.1 Security Analysis

The scheme in this paper is based on the typical Shamir threshold and bilinear technique to construct the signature. According to the characteristics of the threshold, the following conclusions can be drawn: any node whose weight sum is less than the threshold value cannot complete the signature, and any node whose weight sum is greater than or equal to the threshold value can complete the signature. Therefore, the scheme can resist the collusive attack of any member whose sum is less than the threshold. At the same time, a typical security analysis scheme is adopted, and the security of this scheme can be reduced to a discrete logarithm problem. The difficulty of the proposed scheme is equivalent to solving the discrete logarithm problem.

Discrete logarithm problem: given a random number $Z \in G$, the finding $r(r > 1)$ makes $rP = Z$ difficult for the group. The variant form is as follows: Given $R \in G, h \in Z_q$, it is difficult to find $T \in G$ that satisfies $h = e(R, T)$.

Theorem 1: Suppose there is an adaptive selection message and identity of the attacker F with a non-negligible probability ε to break the scheme within PPT time. Then, algorithm C solves the discrete logarithm problem with a non-negligible probability $\varepsilon' = O(\varepsilon)$ in PPT time. Where $O(\varepsilon)$ represents the quantity that ε is not less than a certain constant (which is related to the capability of the random predictor q_{H_1}, q_{H_2}, q_L, but independent of the safety parameter K).

Proof: Assuming C is a challenger, C's goal is to call F to solve the discrete logarithm problem eventually.

(1) Setup: C runs the setup algorithm. C maintains T signature $ID_1, \ldots, ID_N$ public keys and constructs two predictors H_1 and H_2 (see the structure below for the structure of H_1 and H_2). C sends data $\{ID_1, \ldots, ID_N, H_1, H_2\}$ to attacker F as a public parameter.
(2) H_1 Query: C maintains a list ${H_1}^L$ with the array $\{ID_i, Q_i\}$. C prepared q_{H_1} responses $Q_1, \ldots, Q_{q_{H_1}}$ randomly. When F accesses the value H_1 of ID_i, C retrieves $\{ID_i, Q_i\}$ from the list ${H_1}^L$ and sends Q_i to F.
(3) H_2 Query: C maintains a list ${H_2}^L$ with $\{ID_i, m_j, U_i, h_i\}$. C prepared q_{H_2} responses to $h_1, \ldots, h_{q_{H_2}}$ randomly. When F accesses H_2 value of ID_i, m_j, U_i, C retrieves $\{ID_i, m_j, U_i, h_i\}$ from the list ${H_2}^L$ and sends h_i to F.
(4) Signature Query: C maintains a list L^L containing q_L an array L^L. F makes a signature query to m_i, C first checks whether m_i is in the list ${H_2}^L$, then restores $\{m_i, \sigma_i\}$ and sends σ_i to F.

Attacker F interacts with attacker C and C outputs based on the preceding policy.

When F stops asking, F outputs a signature σ_j about m_j (whose signature was never asked) that satisfies $Ver(m_j, \sigma_j) = 1$. C restores $\{ID_i, m_j, U_i, h_i\}$ from the list ${H_2}^L$ and $\{ID_i, Q_i\}$ from the list ${H_1}^L$. Set $h = e\left(P_{pub}, \sum_{i=1}^{n}\left(U_i + h_i Q_{ID_i}\right) + rP\right)$, then $e(P, V) = h$. Since h has not been asked, the discrete logarithm problem is solved correctly.

If h is equal to some value that has already been queried, the probability is $\frac{q_L}{2^n}$ according to the drawer principle. So the probability that C successfully solves the discrete logarithm problem is still $\varepsilon' = O(\varepsilon) + \frac{q_L}{2^n} = O(\varepsilon)$.

6.2 *Efficiency Analysis*

Tab. 1 shows the time complexity of each operation.

Comparison data refer to reference [21]. And P represents the bilinear pair operation, S represents the scalar multiplication operation on the elliptic curve, A represents the addition operation of two points on the elliptic curve, E represents the power multiplication operation, and M represents the dot multiplication operation. Reference [22] tested the calculation time of number multiplication on an elliptic curve on a 900 KHz sensor is about 2.6 s. Considering the intelligent terminal of the latest CortexA9 1.2 GHz microprocessor, the calculation time of number multiplication on the elliptic curve is about 0.00195 s (1S). The efficiency of each stage of the scheme is as Tab. 1.

Table 1: Comparison of various operation time complexity

Operation	Time complexity
Scalar multiplication operation S	$1S \approx 29$ M
The addition of points A	$1A \approx 0.11$ M
Bilinear pair operation P	$1P \approx 87$ M
Power by computing E	$1E \approx 21$ M
Ordinary hash operation H	Ignore

It can be seen from Tab. 2 that the calculation time of the key generation stage is linear with the total number of members. When the number of members increases, the calculation time also increases. The calculation time of the signature generation and verification stage has a linear relationship with the threshold value. The larger the threshold value is, the longer the calculation time is. The calculation time of the agent stage is certain and has nothing to do with the total number of members and the threshold value.

Table 2: Comparison of various operation time complexity

Phase	Computational complexity	Total time consuming (M)	Time (ms)
Key generation phase	$n(H+S)$	29n	1.95n
Agent generation phase	$2A+4S+H$	116.22	7.8
Signature generation phase	$t\,(H+3S+2A)$	87.22t	5.86t
Attestation phase	$2P+t(A+S)$	$174+29.11t$	$12+1.95t$

The performance comparison between the proposed scheme and the node without edge computing server is given below to evaluate better the influence of proxy threshold signature in the edge computing environment. As can be seen from Tab. 3, edge computing offloading optimizes the computing structure of the original signature scheme, offloads some high-consumption computations to edge computing servers, and greatly improves the computing efficiency of terminal nodes.

Table 3: Influence of offload on efficiency

Scheme	Computational complexity	Total time consuming (M)	Time (ms)
Our scheme	$S(n+4t)+tA+H(n+t)$	$29n+145.11t$	$1.95n+7.81t$
No MEC offload scheme	$S(n+8t)+A(2+3t)+H(n+t)+2P$	$29n+116.33t+290.22$	$1.95n+15.6t+11.7$

7 Conclusion

An identity-based anonymous authentication protocol for edge computing is proposed in this paper. This scheme combines proxy signature and ring signature, and at the same time, incorporates (t, n) threshold into it. And through correctness verification and security analysis, it is concluded that the signature has the characteristics of unforgeability and resistance to collusion attacks, which can

provide timely response to information with timeliness and other characteristics, improve the efficiency of the signature, and ensure the identity of the proxy signer privacy. Through efficiency analysis, it can be seen that applying the solution in this paper to an edge computing system can make full use of the computing power of the MEC server, reduce the burden on wireless terminals, and improve system performance. Although the solution in this paper further releases the computing power of the terminal under the premise of ensuring anonymity, ensuring anonymity is redundant and complicated and not concise enough. We will further optimize the program to achieve better efficiency in the future.

Funding Statement: This paper was sponsored in part by Beijing Postdoctoral Research Foundation (No. 2021-ZZ-077, No. 2020-YJ-006) and Chongqing Industrial Control System Security Situational Awareness Platform, 2019 Industrial Internet Innovation and Development Project-Provincial Industrial Control System Security Situational Awareness Platform, Center for Research and Innovation in Software Engineering, School of Computer and Information Science (Southwest University, Chongqing 400175, China), and Chongqing Graduate Education Teaching Reform Research Project (yjg203032).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Shanshan, M. Waqas, S. Rehman, T. Mir, Z. Halim *et al.,* "Social phenomena and fog computing networks: A novel perspective for future networks," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 32–44, 2021.

[2] Y. Liu, Y. Ren, Q. Wang and J. Xia, "The development of proxy re-encryption," *Journal of Cyber Security*, vol. 2, no. 1, pp. 1–8, 2020.

[3] N. Ahamed and N. Duraipandian, "Secured data storage using deduplication in cloud computing based on elliptic curve cryptography," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 83–94, 2022.

[4] S. Tu, M. Waqas, S. Rehman, T. Mir, G. Abbas *et al.,* "Reinforcement learning assisted impersonation attack detection in device-to-device communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1474–1479, 2021.

[5] K. Shankar and S. Venkatraman, "A secure encrypted classified electronic healthcare data for public cloud environment," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 765–779, 2022.

[6] A. Berguiga and A. Harchay, "An IoT-based intrusion detection system approach for tcp syn attacks," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3839–3851, 2022.

[7] S. Oliver and T. Purusothaman, "Lightweight and secure mutual authentication scheme for IoT devices using coap protocol," *Computer Systems Science and Engineering*, vol. 41, no. 2, pp. 767–780, 2022.

[8] P. Ranaweera, A. Jurcut and M. Liyanage, "MEC-Enabled 5G use cases: A survey on security vulnerabilities and countermeasures," *ACM Computing Surveys*, vol. 54, no. 9, pp. 186:1–186:37, 2022.

[9] X. Ding, X. Wang, Y. Xie and F. Li, "A lightweight anonymous authentication protocol for resource-constrained devices in internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1818–1829, 2022.

[10] P. Gupta and M. Kumar, "A verifiable ring signature scheme of anonymous signcryption using ECC," *International Journal of Mathematical Sciences and Computing*, vol. 7, no. 2, pp. 24–30, 2021.

[11] B. Gong, X. Zhang, Y. Cao, Z. Li, J. Yang *et al.,* "A threshold group signature scheme suitable for the internet of things," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 13, 2021.

[12] T. Preethi and B. Amberker, "Lattice-based group signature scheme without random oracle," *Information Security Journal: A Global Perspective*, vol. 29, no. 6, pp. 366–381, 2020.

[13] X. Yue and M. Xi, "A revocable group signatures scheme to provide privacy-preserving authentications," *Mobile Networks and Applications*, vol. 10, pp. 1–5, 2020.
[14] Y. Sun, Y. Liu and B. Wu, "An efficient full dynamic group signature scheme over ring," *Cyber Security*, vol. 1, no. 1, pp. 15, 2019.
[15] J. Subramani, A. Maria, A. Rajasekaran and F. Al-Turjman, "Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3484–3491, 2022.
[16] G. Verma and B. Singh, "An efficient and provable certificate-based proxy signature scheme for IIoT environment," *Information Sciences*, vol. 518, pp. 142–156, 2020.
[17] R. Swati and P. Sahadeo, "A quantum resistant anonymous poxy signature scheme," *Sādhanā*, vol. 47, no. 1, 2022.
[18] H. Zou, X. Liu, W. Ren, T. Zhu and M. Alazab, "A decentralized electronic reporting scheme with privacy protection based on proxy signature and blockchain," *Security and Communication Networks*, vol. 2022, pp. 5424395:1–8, 2022.
[19] J. ZeTao and X. JuanJuan, "Efficient heterogeneous cross domain authentication scheme based on proxy blind signature in cloud environment," *Computer Science*, vol. 47, no. 11, pp. 60–67, 2020.
[20] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.
[21] S. Islam and G. Biswas, "A Pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks," *Annals of Telecommunications*, vol. 67, no. 11, pp. 547–558, 2012.
[22] Y. Lin, "Design and implementation of identity authentication scheme based on elliptic curve cryptography on WSN," Ph.D. Dissertation, Zhejiang University of Technology, China, 2008.