Efficient and Anonymous Cross-Domain Authentication for IIoT Based on Blockchain

Jie Cui, *Senior Member, IEEE*, Nan Liu, Qingyang Zhang, Debiao He, *Member, IEEE*, Chengjie Gu, and Hong Zhong, *Member, IEEE*

***Abstract*—The rapid development of the Industrial Internet of Things (IIoT) has realized the intelligence of industrial manufacturing and improved production efficiency. For improved collaboration, devices from different management domains (e.g., factories) connected through various communication technologies exchange information and share resources. However, they face security and privacy issues when cross-domain communication requires authentication. The limitations of existing schemes include the risk of a single point of failure in a trusted center, leakage of device privacy, high certificate management costs, and low authentication efficiency. Because blockchain with features such as decentralization and tamper-proof can effectively solve some of these problems, we design an efficient and anonymous cross-domain authentication scheme based on blockchain to achieve reliable communication between cross-domain IIoT devices. Specifically, our scheme improves authentication efficiency while enabling device anonymity to ensure that identities are not linkable, and combines blockchain and dynamic accumulator technology to achieve fast authentication. Security analysis demonstrates that our scheme can resist common attacks, and a performance evaluation proves its feasibility and efficiency.**

***Index Terms*—Internet of Things Industrial (IIoT), cross-domain authentication, consortium blockchain, dynamic accumulator.**

I. Introduction

IN RECENT years, the Industrial Internet of Things (IIoT) [1], [2] has integrated sensors with sensing and monitoring capabilities as well as various technologies into the industrial production process [3]. The use of IIoT technology in achieving sustainable production within the management domain (e.g., smart factories) has become increasingly common. It can improve manufacturing efficiency while drastically reducing administrative costs. However, with the increase in complexity of industrial manufacturing processes, the production of a single product often requires multiple management domains to function jointly [4]. Typically, different management domains are relatively independent, and only permissioned domains can access related sensitive data in other domains [5]. Additionally, device identities in domains may leak privacy; therefore, anonymity must be guaranteed. Cross-domain authentication is required to ensure the credibility and validity of shared resources between devices.

Although a centralized facility can be used, such as a Public Key Infrastructure (PKI), to achieve cross-domain authentication [6], the Certificate Authority (CA) involved issues a digital certificate to the relying party and stores the authentication certificate on the server locally. As centralized facilities, they may have data disclosure and a single point of failure problem, making performing cross-domain authentication security impossible. Moreover, expanding the scale of the system leads to the creation of numerous certificates, which generates significant certificate management overhead [7].

Blockchain technology [8] has attracted considerable attention because of its decentralization and tamper-proof characteristics. Because the blockchain does not have a centralized governing body, the damage or loss of any part of it has no effect on the execution of the entire chain. To a large extent, it solves problems such as the vulnerability of centralized facilities to single-point attacks. A consortium blockchain [9], a type of permissioned blockchain, allows multiple organizations that may not trust each other to cooperate in maintaining distributed ledgers according to the constraints of specific contracts. Many cross-domain authentication schemes have been proposed based on consortium blockchains [10], [11], however, some challenges remain.

On one hand, the cross-domain authentication efficiency of some schemes is low [12], and multiple communication rounds result in considerable communication overhead [13]. On the other hand, many schemes require multiple updates or query operations on the blockchain. Because of the time required for the blockchain to reach a consensus, time overhead is massive, which makes it difficult to satisfy real-time requirements in the IIoT [14]. In addition, an attacker can

Manuscript received 3 July 2022; revised 3 October 2022; accepted 19 November 2022. Date of publication 24 November 2022; date of current version 23 February 2023. This work was supported in part by the National Natural Science Foundation of China under Grants 62272002, 62202005, 62202008, and U1936220, in part by the Excellent Youth Foundation of Anhui Scientific Committee under Grant 2108085J31, in part by the Natural Science Foundation of Anhui Province, China under Grants 2208085QF198 and 2208085QF196, and in part by the Special Fund for Key Program of Science and Technology of Anhui Province, China under Grant 202003A05020043. Recommended for acceptance by Dr. Yan Zhang. *(Corresponding author: Hong Zhong.)*

Jie Cui, Nan Liu, Qingyang Zhang, and Hong Zhong are with the Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei 230039, China, and also with the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China (e-mail: cuijie@mail.ustc.edu.cn; n548626@163.com; qingyang.zhang.inchina@gmail.com; zhongh@ahu.edu.cn).

Debiao He is with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Shanghai Key Laboratory of Privacy-Preserving Computation, MatrixElements Technologies, Shanghai 201204, China (e-mail: hedebiao@163.com).

Chengjie Gu is with Security Research Institute, New H3C Group, Hefei 230088, China (e-mail: gcj@ustc.edu.cn).

Digital Object Identifier 10.1109/TNSE.2022.3224453

initiate a re-identification attack by linking multiple data sources to identify the device's identity. In order to protect device privacy, anonymity is also critical [15].

To solve these problems, we propose an authentication scheme based on blockchain for cross-domain IIoT. It enables devices in different management domains to perform authentication more efficiently and negotiate session keys for resource sharing without exposing device identification information.

The main contributions are as follows:

- We propose an anonymous and efficient authentication scheme for cross-domain IIoT based on blockchain. It does not require additional costs to manage certificates, protects the privacy of devices, and uses edge devices [16] to alleviate the computational pressure on authentication servers and resource-constrained IIoT devices. Our scheme not only reduces communication rounds but also improves authentication efficiency.
- Blockchain guarantees the traceability of messages and effectively avoids the single point of failure problem. We use dynamic accumulator technology to accumulate key materials required in the identity authentication process for industrial IoT devices, and combine smart contracts to prepare for subsequent rapid authentication. Simultaneously, the device must only access the blockchain once during cross-domain authentication to ensure efficiency.
- A security analysis demonstrates that the scheme proposed is effective and can resist common attacks. A performance evaluation shows the efficiency of time and communication overhead.

The remainder of this paper is organized as follows. Sections II review the related work. The relevant preliminaries are provided in Section III. Section IV presents the system model of the scheme, and Section V introduces the cross-domain authentication scheme. Section VI provides a theoretical analysis and related security proofs to prove the security properties satisfied by the scheme. Section VII conducts performance evaluation. Finally, Section VIII concludes the paper.

II. Related Work

There are already many cross-domain authentication schemes, and we mainly divide them into two categories. One is a centralized scheme, and the other is a blockchain-based decentralized scheme.

A. Centralized Based Scheme

Typically, device-to-device authentication uses a centralized facility to provide security services, a typical one of which is PKI. Also included in PKI is a trusted third party called CA that issues and manages digital certificates for devices.

Yuan et al. [17] used the PKI-based model and access authorization credentials to realize the interconnection between the PKI domain and the Identity-Based Cryptography domain. This scheme brings a lot of computational and communication costs. Chen et al. [18] proposed a batch-verifiable cross-domain authentication protocol supporting asymmetric group keys. Zhou et al. [19] constructed a certificate authority domain based on identity encryption and secret sharing, which solved the problem of cross-domain authentication in mobile ad hoc networks and smart city construction. We cannot ignore the overhead of certificate management in these authentication mechanisms. Cui et al. [20] proposed a scheme capable of bidirectional authentication in vehicular ad hoc networks. However, a centralized facility involved in its scheme may have a single point of failure, which will affect subsequent authentication. Wazid et al. [21] proposed a scheme for authentication and key management in which users use pseudonyms to hide their real identities. However, pseudonyms are identical in all sessions, and the user's identities will be linkable.

Overall, centralized facilities in cross-domain authentication schemes are prone to the risk of a single point of failure [22]. Besides, the cross-domain authentication in the scheme is inefficient, requires additional costs to manage the authentication certificate, and easily leaks the identity privacy of the device.

B. Decentralized Blockchain-Based Scheme

Owing to the decentralization and tamper-proof characteristics of the blockchain itself, it can prevent a single point of failure problems. Therefore, more and more cross-domain authentication schemes have introduced blockchain.

Wang et al. [23] proposed a cross-domain authentication mechanism and built a blockchain network based on the existing PKI system to enable users to share resources across domains. Nevertheless, their scheme's authentication efficiency is lower. To solve the problems of medical information sharing and user data privacy protection, Dong et al. [24] proposed a blockchain-based scheme for cross-domain authentication between doctors and users. They store certificates distributed across devices and then introduce stealth addresses in cryptocurrencies within the cross-domain authentication field. The proposed authentication protocol has higher communication rounds. For the identity authentication of drones in 5 G networks, Feng et al. [25] used blockchain and threshold-shared multiple signatures to build identity trust for collaborative domains to enable cross-domain authentication. The high communication rounds in the scheme bring great communication overhead. In Vehicle-to-grid (V2G), Liu et al. [26] proposed a cross-domain scheme based on the SM9 digital signature algorithm and blockchain. The hashes of user certificates in the domain are stored in the blockchain. However, the scheme has problems such as a cumbersome certificate distribution process and high certificate storage overhead. Chen et al. [27] designed a Bidm system that uses blockchain to maintain identity information in different trust domains, which solves the problems of traditional decentralized identity management mechanisms that are inefficient and difficult to transmit decentralized trust widely. However, the client needs higher storage communication capability to store the identity information. Shen et al. [28] proposed a secure blockchain authentication scheme BASA in the cross-domain IIoT. They designed an identity management mechanism to protect entity

privacy and introduced a trusted platform consortium blockchain to share resources. However, frequent server data exchange increases communication overhead and requires additional blockchain write and query latency.

In general, the existing blockchain-based cross-domain authentication schemes still face some difficulties, such as high overhead for storing blockchain certificates, low cross-domain authentication efficiency, multiple communication rounds, and high communication overhead. Frequent blockchain operations on limited devices can also cause much latency.

III. Preliminary Knowledge

A. Blockchain and Smart Contract

The blockchain is equivalent to a decentralized share ledger [29], which uses cryptography to ensure that it cannot be tamper-proof. Numerous blockchain nodes use consensus to store transaction records in chronological order. The full node is a node with a complete blockchain ledger, which can independently verify whether the transaction is valid.

As a type of blockchain, a consortium blockchain [30] refers to a chain formed by multiple parties reaching an agreement according to certain constraints. This structure is similar to the partnership in different factories. Moreover, they do not trust each other, but they have to work together to complete the manufacture of the same product. Therefore, we can use the consortium blockchain as the supporting technology.

A smart contract in the blockchain [31] is essentially a program that automates the processing of traditional contracts in the form of computer instructions. Simply put, everyone prescribes the contract content in advance, and when the conditions for triggering the contract are met, the program will automatically execute the contract content. Its characteristics are that the rules are open and transparent, the data in the contract and all transactions are publicly visible to the outside world, and there will be no false or hidden transactions.

B. Dynamic Accumulator

A dynamic accumulator is a cryptographic tool that accumulates a set of input values into a value. We can prove whether a given input is in the accumulated value. The dynamic accumulator [32] allows the operator to arbitrarily add or delete a value so that the cost of the operation is independent of the number of members being accumulated; that is, the cost is independent of the accumulated value. Meanwhile, the dynamic accumulator can simultaneously add or delete multiple values to improve efficiency.

We classify dynamic accumulators as those based on strong RSA assumptions, those based on bilinear maps, or those based on Merkle trees. We use a dynamic accumulator based on strong RSA assumptions to accumulate key materials required in cross-domain authentication, reducing storage overhead on the blockchain. And it is deployed in the blockchain's smart contract, and the authentication server can automatically call the contract to achieve related functions.

C. RSA and StrongRSA Assumption

In RSA public key encryption, A uses B's public key (n, e) to encrypt plaintext M into ciphertext C. The calculation method is $C = M^e(\ mod\ n)$, where n is the product of two large prime numbers, $e \geq 3$ and is a prime number. B can decrypt the plaintext $M = C^d(\ mod\ n)$ according to the private key (n, d), $de = 1\ mod\ ((p-1)(q-1))$. The adversary knows the public key (n, e) and can steal the ciphertext C, but to calculate the plaintext M, the adversary must find the factor of n. We assume that the RSA problem is intractable, which is the RSA assumption.

The StrongRSA assumption differs from the RSA assumption because the adversary can choose the public exponent e. The task of an adversary is to get the plaintext M from the ciphertext C, $C = M^e(\ mod\ n)$. It means that the StrongRSA assumption is more robust than RSA, and the StrongRSA assumption is the basis for many cryptographic constructs.

D. Elliptic Curve Cryptography and Related Computational Problems

- Elliptic Curve Cryptography (ECC) is an asymmetric encryption technology based on elliptic curve theory. The main advantage of ECC is that it provides a comparable or higher level of security in some cases than other methods using more minor keys (such as the RSA encryption algorithm).
- Elliptic Curve Computational Diffie-Hellman (ECDHP) Problem: Given random points $Q_1 = aP$, $Q_2 = bP$ and P, where a, $b \in Z_q^*$ and $P \in G$. output abP, which is computationally difficult.

IV. System Overview

A. System Model

Fig. 1 depicts that the system model comprises a trusted key generation center, authentication server, edge device, IIoT devices and blockchain.

1) $IIoT\ Devices$: $IIoT\ devices$ are various such as sensors and thermometers. Typically, devices can only sense and transmit simple data, with weak computing and storage capabilities and limited energy, and cannot perform complex operations and data processing.
2) $Edge\ Device$: ED has strong computing and storage capabilities, which can help D for some calculations to alleviate its calculation amount.
3) $Authentication\ Server$: AS acts as a full node in the blockchain. It calls smart contracts to assist devices in cross-domain authentication and performs data upload and query operations. Authentication servers of all domains jointly maintain the consortium blockchain.
4) $Key\ Generation\ Center$: KGC is assumed to be wholly trusted, no attacker can destroy, and generates its public and private keys for devices in the domain.

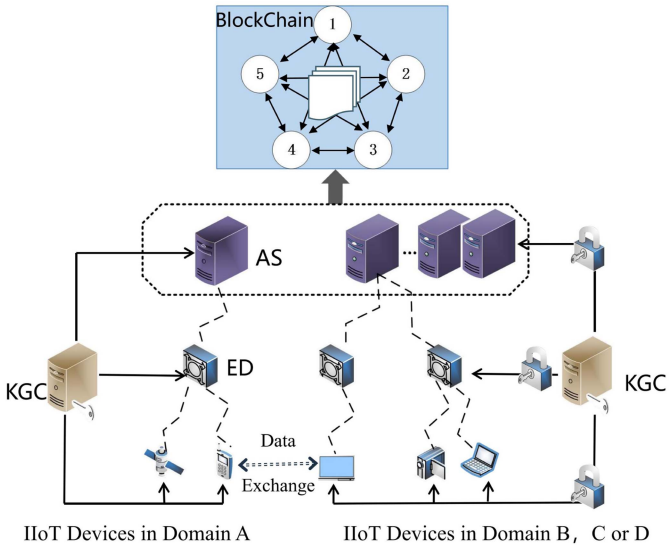


Fig. 1. Simple cross-domain system model diagram.

5) *Blockchain*: We use the consortium blockchain, and the authentication servers of each domain together form the consensus nodes on the consortium blockchain.

For the reader's convenience, Table I lists some symbols used in this paper.

TABLE I
NOTATIONS

Notation	Description
p, q	Two large prime number
Fp	Prime finite field
$E(Fp)$	Elliptic curve E over Fp
G	Cyclic additive group
P	generators of group G
Z_q^*	Positive integer
KGC	Key generation center
AS^A	Authentication servers in Domain A
ED_i^A	Edge devices in Domain A
D_i^A	IIoT devices in Domain A
msk	KGC's master private in domain A
mpk	KGC's public keys in domain A
SK_i	D_i^A's private keys
PK_i	D_i^A's public keys
PID/pid	pseudonym of the device
SK_{ck}	The child private keys of the device
PK_{ck}	The child public keys of the device
SK_{EDi}	ED's private keys in domain A
PK_{EDi}	ED's public keys in domain A
H	A secure general hash function
T_i	Current timestamp
Sig/Ver	$ECDSA$ sign and verify operations

B. Model Assumptions

The model assumptions are as follows.

1) We have access to the smart contract at any time, and its record is reliable. It is because the essence of the blockchain is a jointly maintained distributed ledger, and it is difficult for an attacker to tamper with the transaction records on the blockchain.
2) In this system, the ED acts instead of the calculated node. Its identity and the public key are known to the IIoT device.
3) The critical information of the IIoT device does not need to be frequently updated or withdrawn unless it is suspected or determined to be compromised. If devices are compromised, KGC and ED will revoke the IIoT device's critical information.

C. Security Requirements

- Traceability: When performing cross-domain authentication, we are required to trace back to the records or data access behavior of device authentication. If something goes wrong, it ensures that it can be traced back to the source as quickly as possible.
- Scalability: The scalability of the blockchain is limited due to the limited throughput and transaction latency of the blockchain. Requiring us to use blockchain in our scheme will not make the final scheme less efficient or scalable.
- Forward secrecy: When negotiating session keys, disclosing long-term keys will not reveal past session keys.
- Identity anonymity: It is required not to disclose the device's identity privacy and to protect its unlinkability.
- Resist various attacks: It can resist replay attacks, impersonation attacks, Distributed Denial of Service (DDoS) attacks, and man-in-the-middle attacks.

V. Design Details

A. System Setup

1) System initialization: KGC of multiple fields jointly chooses the elliptic curve $E(Fp)$ $y^2 = x^3 + ax + b \ mod \ p$ of the finite field Fp, and then selects a cyclic addition group G with generator P and prime order q. KGC also chooses a secure hash function $H : \{0, 1\}^* \rightarrow Z_q^*$. Share global parameters on the blockchain.
2) Domain initialization: Taking domain A as an example, the KGC in the domain randomly selects $msk \in Z_q^*$ as the master private key. The master public key is $mpk = msk \cdot P$, and the master public and private key pair (msk, mpk) is obtained.

B. Registration

In the registration phase, the KGC distributes the public and private keys to the devices in the domain. Let us take the example of KGC^A registering for D_i^A. We assume a secure and private communication channel between the KGC and the device at this stage.

When D_i^A sends its identity ($ID_{D_i^A} \in \{0, 1\}^*$) to KGC^A for registration request, KGC^A firstly checks whether the device

Contract 1: Add data to accumulator.

Input: input parameters α
Output: accumulator value a

```
1: key, count := util.HashToPrime(α)
2: exists, err := ctx.GetStub().GetState(key)
3: if err != nil then
4:     return err
5: if exists then
6:     return a
7: else
8:     a.Exp(a, key,n)
9:     accr := ACC{Key:key, Count:count, A:a, }
10:    return ctx.GetStub().PutState(key)
```

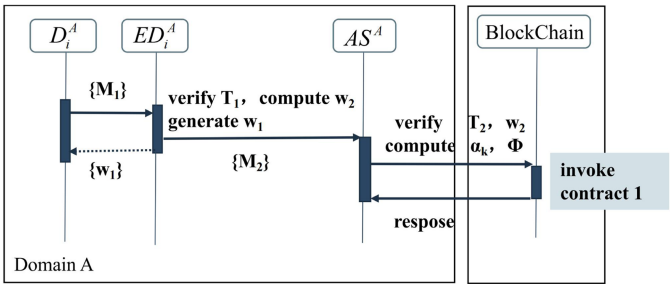


Fig. 2. Pre-authentication flowchart.

has been registered before, if so, it will stop registration. Otherwise, it will proceed:

- KGC^A randomly chooses r_1 and calculates $R_1 = r_1 \cdot P$. And KGC^A generates private key $SK_i = r_1 + H(ID_{D_i^A} \| R_1) \cdot msk$ for D_i^A, public key is $PK_i = SK_i \cdot P$, and returns to D_i^A $\{PK_i, SK_i, R_1\}$ through the secure channel.
- D_i^A calculates whether PK_i and $R_1 + H(ID_{D_i^A} \| R_1) \cdot mpk$ are equal. If the equation holds, D_i^A saves $\{PK_i, SK_i\}$ locally, otherwise registers again.

C. Pre-Authentication Process

When device D_i^A in the domain A wants to access device D_j^B in the domain B, it first needs to perform pre-authentication, as shown in Fig. 2. In this stage, ED_i^A generates relevant information for D_i^A and forwards it to the authentication server AS^A. Then AS^A uploads it to the blockchain in combination with smart contracts and dynamic accumulator technology for subsequent quick authentication operations. The contract algorithms 1-3 required in the pre-authentication and authentication process are the algorithms of smart contracts on the blockchain. Here are the detailed steps:

1) $D_i^A \rightarrow ED_i^A : M_1$=$\{T_1, ID_{D^B}, request\}$
D_i^A sends a request to $ED_i^{A'}$ to communicate with D_j^B and then returns relevant parameters for subsequent cross-domain authentication.
2) $ED_i^A \rightarrow AS^A : M_2 = \{T_2, w_2, \{PID, PK_c\}, ID_{D^B}\}$
When M_1 is received at T_1', ED_i^A firstly checks $|T_1 - T_1'| \leq \Delta T$, where ΔT is predefined threshold. After the verification is successful, ED_i^A generates relevant parameters for the subsequent authentication of D_i^A.
ED_i^A arbitrarily chooses $2n$ $(n \in Z_q^*)$ random numbers $\{b_1, b_2,..., b_n\}$ and $\{f_1, f_2,..., f_n\}$, then generates a series of pseudonyms $PID = \{pid_1, pid_2,..., pid_n\}$ and a series of sub-public and private keys $SK_c = \{SK_{c1}, SK_{c2},..., SK_{cn}\}$, $PK_c = \{PK_{c1}, PK_{c2},..., PK_{cn}\}$, where $k \in \{1, 2,..., n\}$, $pid_k = H(SK_{EDi} \| b_k)$, $SK_{ck} = H(pid_k \| f_k)$, $PK_{ck} = SK_{ck} \cdot P$.
ED_i^A signs the relevant message with its private key and forwards to AS^A, where $w_2 = Sig(SK_{EDi}, (\{PID, PK_c\}, ID_{D^B}))$. Then ED_i^A sends $w_1 = \{PID, SK_c, PK_c\}$ to $D_i^{A'}$ through the secure channel.
3) AS^A:When M_2 is received at T_2', AS^A firstly checks $|T_2 - T_2'| \leq \Delta T$, then uses ED_i^A's public key to verify the signature w_2.
After the verification is successful, AS^A processes the related messages and calculates $\alpha_k = H(pid_k \| PK_{ck} \| ID_{D^B})$ and $\Phi = \prod_{k=1}^{n} \alpha_k$. Moreover, AS^A calls Contract 1 to add Φ to the dynamic accumulator and generates a new accumulated value a for subsequent authentication.
AS^A returns a response that the addition is successful. The pre-authentication process is complete.

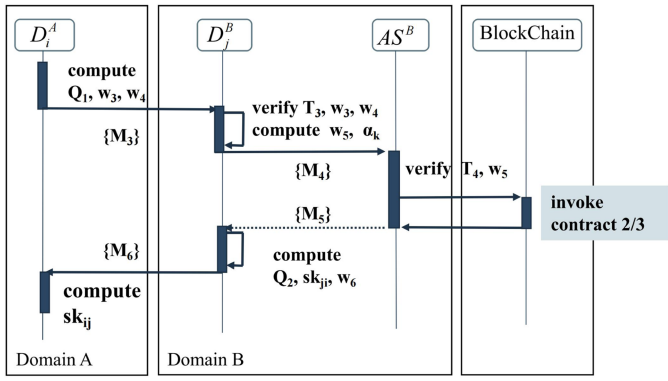


Fig. 3. Cross-domain authentication flow chart.

D. Cross-Domain Authentication Process

As shown in Fig. 3, in this phase, D_i^A negotiates the session key while authenticating with D_j^B. D_i^A knows D_j^B's public key PK_j.

1) $D_i^A \rightarrow D_j^B : M_3 = \{T_3, w_3, w_4, Q_1, pid_k, PK_{ck}\}$
D_i^A selects pid_k and PK_{ck} from a series of $\{PID, PK_c\}$, $k \in \{1, 2,..., n\}$. Then D_i^A selects a random number d_1, calculates $Q_1 = d_1 \cdot G$, $w_3 = H(T_3 \| Q_1 \| pid_k \| PK_{ck})$ and $w_4 = SK_{ck} \cdot w_3 + d_1$.
2) $D_j^B \rightarrow AS^B : M_4 = \{T_4, w_5, \alpha_k\}$
D_j^B receives M_3 at T_3', firstly checks $|T_3 - T_3'| \leq \Delta T$, then calculates $w_3' \stackrel{?}{=} H(T_3 \| Q_1 \| pid_k \| PK_{ck})$, and verifies $w_4 \cdot P \stackrel{?}{=} PK_{ck} \cdot w_3 + Q_1$.
After the verification is successful, D_j^B saves Q_1 locally, and calculates $\alpha_k = H(pid_k \| PK_{ck} \| ID_{D^B})$, $w_5 = Sig(SK_j, \alpha_k)$. D_j^B sends a message M_4 to $AS^{B'}$ to query whether α_k is in the blockchain.

Contract 2: Verify data.

```
Input: input parameters α
Output: Verification result: true or false
key, count := util.HashToPrime(α)
result := big.NewInt(1)
for k, count := range accr.data do
    if k!=key then
    prime := util.HashToPrimeWithNonce(k, count)
    witness :=result.Mul(result, prime)
result.Exp(witness, key, n)
if result.Cmp(accumulatorState) == 0 then
    return true
else
    return false
```

Contract 3: Delete data from accumulator.

```
Input: input parameters α
Output: new accumulator value a′
key, count := util.HashToPrime(α)
exists, err := ctx.GetStub().GetState(key)
if err != nil then
    return err
if !exists then
    return a
else
    ctx.GetStub().DelState(key) //calculate the product of nonce of
    elements except key itself.
    product = iterateAndGetProduct(x)
    a′ := math.Pow(a,product)
    return a′
```

3) $AS^B \rightarrow D_j^B : M_6 = \{T_5, querysuccess\}$
AS^B receives M_4 at T_4', firstly checks $|T_4 - T_4'| \leq \Delta T$, then verifies w_5 with D_j^B's public key.
Moreover, AS^B calls Contract 2 and quickly checks whether it is in the dynamic accumulator according to the value α_k, and sends a response message to D_j^B if it exists. Meantime, AS^B calls Contract 3 to delete α_k from the dynamic accumulator.
4) $D_j^B \rightarrow D_i^A : M_6 = \{T_6, Q_2, w_6\}$
D_j^B chooses random numbers d_2, and calculates $Q_2 = d_2 \cdot G$. Meanwhile, D_j^B calculates $w_6 = Sig(SK_j, Q_2)$ and sends a message M_6 to the D_i^A.
5) D_i^A : When M_6 is received at T_6', D_i^A firstly checks $|T_6 - T_6'| \leq \Delta T$, if it is established, then verifies w_6. At last, D_i^A calculates the session key $sk_{ij} = H(pid_k||d_1 \cdot Q_2)$. D_j^B also calculates the session key $sk_{ji} = H(pid_k||d_2 \cdot Q_1)$.
In the next step, D_i^A and D_j^B encrypt data when sharing information according to the negotiated session key $sk_{ij} = sk_{ji}$, and the cross-domain authentication process is complete.
In addition, the expiration time T_e of the session key is determined in advance between IIoT devices. After time T_e, if D_i^A wants to access D_j^B again, it must only select pid_m and PK_{cm} from a series of $\{PID, PK_c\}$, repeats the above cross-domain authentication process and negotiates a new session key.

E. Key Agreement

After successfully cross-domain authentication, IIoT devices must perform key negotiations for subsequent secure communication. The scheme adopts the key exchange based on ephemeral elliptic curve (ECDHE) technology, which can calculate the public and final session keys with less computation. In this process, the private keys of both parties are generated randomly and temporarily and are not public. Even if we use public information (elliptic curve, public key, base point G), it is hard to get the private key.

We embed it in a cross-domain authentication scheme that can authenticate while exchanging public keys to determine the legitimacy of the public key received by an entity to prevent ECDHE from man-in-the-middle attacks.

VI. Security Proof

In this section, we evaluate the security of attacker A against known attacks against this scheme through formal and informal security analysis. Note that widely used formal methods (e.g., random oracle models) fail to capture some structural errors. Therefore, an informal security analysis is required to ensure that our proposed scheme is secure against various attacks with high probability.

A. Formal Security Analysis

1) Security Model : We propose a suitable security model for our proposed authentication scheme based on [33], [34], [35]. First we define three participants in our authentication process: AS, ED and IIoT device(D). They all have instances (I) named oracles, denoted by $\prod_{AS}^i$, $\prod_{ED}^j$, $\prod_D^k$ to represent i, j and k instances (i, j and $k \in Z$) of AS, ED and D, respectively. We define an adversary A that interacts with the participants by implementing the following query.

- $Execute(\prod_{AS}^i, \prod_{ED}^j, \prod_D^k)$
This query is used to simulate a passive attack. An adversary A can eavesdrop on the messages delivered when the participants are honestly implementing the scheme by executing this query.
- $Reveal(\prod_D^k)$
In this query, attacker A can use this query to obtain the session key in the current session.
- $Send(\prod_{AS}^i, \prod_{ED}^j, \prod_D^k, m)$
Through this query, the adversary A can launch an active attack on $\prod_{AS}^i$, $\prod_{ED}^j$, $\prod_D^k$ and A pretends to be $\prod_D^k$ sending message m to $\prod_{AS}^i$ or $\prod_{ED}^j$. According to our scheme, if the message m is real and effective, A will query the relevant feedback message. Otherwise, the query will abort.
- $Test(\prod_D^k)$
Under this query, we model the semantic security of session keys between $\prod_D^k$ with a coin c. Before the test,

we randomly and secretly generate a bit c, and then A performs this test. When c = 1 when the session key is leaked, the instance $\prod_D^k$ will return the real session key. In addition, when it returns a random number with the same length as the session key; otherwise, the output is empty ($\perp$).

In the proposed model, the adversary A must differentiate whether the key between instances is real or random. The adversary A can do a polynomial degree test to get the query result c and then guess a bit c'. When $c' = c$, it means that A wins the game. If we denote by Succ that A wins the game, the probability that A breaks the semantic security of our proposed scheme ρ is:

$$Adv_\rho(A) = |2\mathrm{Pr}[\mathrm{Succ}] - 1| = |2\mathrm{Pr}[\mathrm{c}' = \mathrm{c}] - 1| \quad (1)$$

where $Pr[H]$ represents the probability of event H occurring. ρ in this model is safe only if $Adv_\rho(A)$ is ignorable.

A probabilistic machine Δ running at time t can be treated as a $(t, \varepsilon) - ECDHP$ attacker in G, where

$$Suc\prod_G^{ECDHP}(\Delta) = \Pr_{xy}[\Delta(\eta P, \vartheta P) = \eta\vartheta P] \geq \varepsilon \quad (2)$$

Where P is a generator on the elliptic curve $E(Fp)$, the probability takes the random number η and the random number ϑ.

Theorem 1: Given a finite field cyclic group G and a password pool of size |D|. q_{send}, q_{exe}, q_h, q_e, τG and l represents the count of Send queries, Execute queries, Hash queries, Encrypt/Decrypt queries, the scalar multiplication time in G, and the length of the hash respectively. The advantage of any PPT adversary resolving the ECDHP problem is Adv_G^{ECDHP}. Therefore, the adversary's advantage in breaking the semantic security is as (3).

$$\begin{aligned} Adv_{\rho,D}(A) \leq & \frac{2q_{send}}{|D|} + \frac{q_h^2}{2^l} + 2Adv_{Ex}^{se}(t) \\ & + \frac{2q_{send} + (q_{send} + q_{exe})^2}{n} \\ & + 2q_h Adv_G^{ECDHP}(t + (q_{send} + q_{exe} + 1) \cdot \tau G) \end{aligned} \quad (3)$$

Proof: From $G0$ to $G8$ is a series of real games. Δi denotes the distance between games Gi and $G(i+1)$; after that, (4) is:

$$\begin{aligned} Adv_{\rho,D}(A) &= 2Pr[Succ_n] - 1 \\ &\quad + 2(Pr[Succ_0] - Pr[Succ_n]) \\ &\leq 2Pr[Succ_n] - 1 + 2\sum_{i=0}^{n-1} \Delta i \end{aligned} \quad (4)$$

This formula demonstrates that if the probability of success Δi between any two successive games differs, the opponent's advantage in game $G0$ and the last game $G5$ is almost the same. From another point of view, if it can be proved from outside that $Pr[Succ_5]$ is a negligible value, then so are $Pr[Succ_0]$ and $Adv_{\rho,D}(A)$. ■

1) Game $G0$
The real attack in the random oracle model is game $G0$. It is defined as, $Adv_{\rho,D}(A) = 2Pr[Succ_0] - 1$.
2) Game $G1$
We simulate the hash oracle H in $G1$ and Encrypt/Decrypt oracles. We can implement these simulations by maintaining a list of hash values $\Lambda\Gamma_H$ and a list of encrypted values $\Lambda\Gamma_E$. We ran a series of queries that an attacker could only distinguish from an actual attack by breaking the one-way hash function and encryption function. Therefore, $\Delta 0 \leq Adv_{Ex}^{se}(t)$.
3) Game $G2$
We simulate all the oracles of the authentication phase. According to the birthday paradox, we have $\Delta 1 \leq \frac{(q_{send}+q_{exe})^2}{2n} + \frac{qh^2}{2^{l+1}}$. In particular, M_3 and M_6 can be obtained by executing $Send$ and $Execute$ queries. The size of the collision set does not exceed $q_{send} + q_{exe}$. The number of successful collisions is about $(q_{send} + q_{exe})^2$, because if a collision occurs (such as $\{T_6, w_6, Q_2\} = \{T_6', w_6', Q_2'\}$), then we must have $T_6 = T_6'$, indicating that timestamps also form collisions. The probability of hash collision is $\frac{q_h^2}{2^{l+1}}$ and the analysis is similar.
4) Game $G3$
In this game, execution is stopped if the attacker is lucky enough to guess the authentication values w_3 and w_4. Unless the device rejects a valid authentication value, we cannot distinguish between games $G3$ and $G2$; we can get $\Delta 2 \leq \frac{q_{send}}{n}$.
5) Game $G4$
We use the personal oracle H' to take the place of H to calculate α_k, so that α_k is independent of H. When executing the query, we can get $\alpha_k = H(pid_k \| PK_{ck} \| ID_{D_j^B})$. $G4$ and $G3$ are indistinguishable unless Ask_4 occurs, where Ask_4 means the attacker queries the hash event on $pid_k \| PK_{ck} \| ID_{D_j^B}$ in game $G4$. Similarly, we use Ask_5 to denote an adversary querying event in $G5$, which can be seen below. The result of b in the Test query is random, and the selection of b is performed independently of all sessions. Wherefore, we have $\Delta 3 \leq Pr[Ask_4]$ and $Pr[Succ_4] = \frac{1}{2}$.
6) Game $G5$
In $G5$, we use the stochastic autoreduction of the $ECDHP$ problem to simulate execution, given a (A, B), we randomly choose $a, b \in Z_q^*$, and compute $d_1 = a \cdot A$ and $d_2 = b \cdot B$. Since Ask_4 means that the adversary queries H, we can get $ECDHP(d_1, d_2) = abECDHP(A, B)$, which represents a degraded solution to instance $ECDHP$. Therefore, we have:

$$\begin{aligned} Pr[Ask_5] \geq & q_h Adv_G^{ECDHP}(t + (q_{send} + q_{exe} + 1) \cdot \tau G) \\ & + \frac{q_{send}}{|D|} \end{aligned} \quad (5)$$

Among them, the cardinality of queries related to offline dictionary attacks and the adversary's advantage in solving a given$ECDHP$ instance (A, B) will have

an impact on the probability of event Ask_5. From the above formula, we can easily deduce formula (6) which is the same as Theorem 1.

$$\begin{aligned} Adv_{\rho,D}(A) &\leq 2Pr[Succ_4] - 1 + 2(\Delta 0 + \Delta 1 + \Delta 2 + \Delta 3) \\ &\leq \frac{(q_{send} + q_{exe})^2}{n} + \frac{q_h^2}{2^l} + \frac{2q_{send}}{n} + 2Pr[Ask_4] \\ &\leq \frac{2qsend + (q_{send} + q_{exe})^2}{n} + \frac{q_h^2}{2^l} \\ &\quad + 2Adv_{Ex}^{se}(t) + 2Pr[Ask_5] \end{aligned} \tag{6}$$

The proof is complete.

B. Other Security Analysis

Analyze the security requirements previously proposed:

1) Traceability: The blockchain is essentially a trusted public ledger. It can achieve traceability by recording transaction changes and access behavior. The AS in the scheme uploads or revokes the relevant data by initiating a smart contract, and attackers cannot tamper and manipulate the data on the blockchain. We can track the data through the blockchain to ensure its authenticity.
2) Scalability [36]: One of the difficulties facing identity authentication with blockchain is the issue of scalability, processing data while reducing transaction processing speed or latency as much as possible. Due to the consensus mechanism of the blockchain, transactions are delayed, and if devices frequently authenticate through the blockchain, it will consume many resource costs. In this solution, the device only needs to upload the corresponding data to the blockchain in the pre-authentication stage. In the subsequent authentication, we can query data from the local backup of the ledger without the need for transaction verification and node consensus on the blockchain.
3) Forward secrecy [37]: Since $sk_{ij} = H(pid_k||d_1 \cdot Q_2)$ and $H(pid_k||d_2 \cdot Q_1) = sk_{ji}$, the attacker can only generate a correct session key by solving the $ECDHP$ problem to obtain random numbers d_1, d_2. That is, our scheme satisfies forward secrecy.
4) Identity anonymity: In the proposed scheme, D_i^A uses pseudonyms [38] to authenticate with D_j^B instead of its real identity. It can effectively protect D_i^A's identity privacy and realize the unlinkability of identity.
5) Resist various attacks: The proposed scheme can resist replay attacks, impersonation attacks, DDoS attacks, and man-in-the-middle attacks.

- Replay Attacks: The proposed scheme can defend against replay attacks with timestamp T [39]. When the receiver receives the timestamp T, it will immediately check the freshness of the timestamp. If the attacker processes the message repeatedly, the time difference will exceed the time threshold set in advance. The receiver will discard the message if $|T_1 - T_1'| \geq \Delta T$, which is a good defense against replay attacks.

TABLE II
WANG'S TIME COSTS (IN SECONDS) OF THE SMART CONTRACT

Operations	**Update**	**Query**
Max Time	2.681	0.312
Min Time	1.989	0.138
Average Time	2.335	0.225

- Impersonation attack: An adversary A can simulate a legitimate device to generate an efficacious signature without exposing it. We make A pretend to be a legitimate edge device, which generates the signature $w_4 = SK_{ck} \cdot w_3 + d_1$ without knowing the private key of the device and sends it to D_j^B. Nevertheless, if the adversary A can forge the signature. It means that the $ECDHP$ problem can be solved, but the $ECDHP$ problem has been proved difficult.
- DDoS attack: It refers to multiple attackers in different locations launching attacks on one or several machines simultaneously. Our scheme employs valid timestamps T to verify the timeliness of received messages. In the blockchain, due to its consensus mechanism, the premise of DDoS attackers destroying the security of the blockchain system is to hold more than 51% of the node rights, which is unrealistic in terms of feasibility and probability.
- Man-in-the-middle attack: An attacker acts as an intermediary between two honest communicating parties to pass information [40]. If the attacker tries to intercept the message $\{w_3, w_4\}$ between D_i^A and D_j^B, and modify it to another valid authentication message $\{w_3', w_4'\}$ according to its own private key. The attacker must have the subkey of D_i^A to be able to crack the $ECDHP$ hard problem. Obviously, the attacker cannot obtain its private key value.

VII. PERFORMANCE ANALYSIS

A. Experimental Setup

Wang et al. [41] built a consortium blockchain using Hyperledger Composer version V0.20.7 on an x86_64 GNU/Linux system with 1 core and 2 GB RAM to evaluate smart contract operations. We directly refer to the relevant experimental data in their protocol for comparison, and their experimental results are summarized in Table II.

Additionally, a desktop computer performs the operations of the devices, and its configuration is an Intel(R) Core(TM) i7-10700 CPU @2.90 GHz, with 16.0 GB of memory. Windows 10 64-bit OS and JDK 11.0.13 are installed on the desktop computer. The comparison experiment has a bilinear pairing operation; therefore, we complete the experimental simulation under the JPBC library and select the Type-F elliptic curve.

B. Computational Costs

1) Theoretical Analysis
We first evaluate the computational cost in device authentication by theoretical analysis of time-consuming operations.

TABLE III
THE TOTAL COMPUTATIONAL COST OF D_i^A IN THE PROCESS OF ACCESSING D_j^B

Costs / *Device* / *Scheme*	D_i^A	AS^A	D_j^B	AS^B
[25]	$2Enc + Dec + BCW + 2BCR$	-	$2Enc + Dec + BCW + 2BCR$	-
[28]	$3SM + Exp_T$	$2SM + SM_T + PA + 2Exp_T + BP + BCW$	$3SM + Exp_T$	$2SM + SM_T + PA + 2Exp_T + BP + BCR$
Ours	$Ver + SM$	-	$2Sig + SM$	$Ver + BCR$

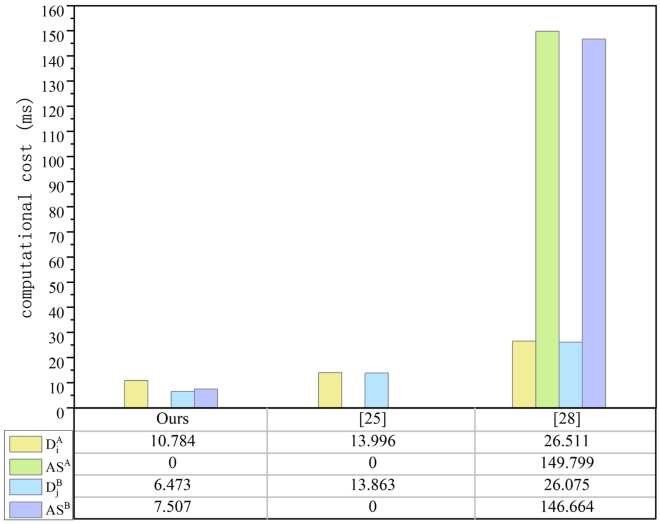


Fig. 4. Computational cost comparison of each device (ms).

Other lightweight operations such as XOR, hash, and integer addition take very little time and are not considered here. The specific symbols are listed below.

SM: The cost of performing a scalar multiplication operation in G; SM_T: The cost of performing a scalar multiplication operation in G_T; PA: The costs of performing a point addition; Exp_T: The cost of performing an exponential operation in G_T; BP: The cost of performing a bilinear pairing; BCR/BCW: The cost of performing a read/write operation on the blockchain; Sig/Ver: The cost of performing an ECDSA signature/verification; Enc/Dec: The cost of performing an Elgamal asymmetric encryption and decryption.

In Table III, we can see the total computational overhead that the IIoT device D_i^A in each scheme needs to undertake in authentication and key negotiation with D_j^B. Among them, the scheme [25] does not indicate the asymmetric encryption and decryption algorithm used, so we use ECC instead.

2) Experimental Simulation Results

We perform the simulations for this experiment under the experimental environment configuration described in Section VII-A. The system initialization and pre-authentication phases are performed in advance, and the cross-domain authentication phase does not include their computational overhead. To show the advantages of the scheme in terms of efficiency, we compare it with Feng et al. [25], and Shen et al. BASA [28] under the same setting. We negotiated a session key during the authentication process.

TABLE IV
COMPARISON OF TIME AND COMMUNICATION OVERHEAD WITH OTHER SCHEMES

	Communication Rounds	Communication Overhead (bytes)
[25]	12	1099
[28]	10	1509
Ours	4	737

Here we compare the computational overhead of various devices in the cross-domain authentication process. Firstly, Fig. 4 demonstrates that the time consumption of our scheme in IIoT devices D_i^A and D_j^B is 10.784 ms and 6.473 ms, respectively, during cross-domain authentication. Our devices are the least time-consuming of the comparison options and are suitable for resource-constrained IIoT devices. The time consumption of the scheme [25] in D_i^A and D_j^B during cross-domain authentication is 13.996 ms and 13.863 ms, respectively. Moreover, [25] performs most of its operations on the blockchain. When extensive IIoT devices perform cross-domain authentication, numerous read and write operations will consume much time, making the authentication time longer and the efficiency worse. Finally, the scheme [25] does not use the authentication server, and our computational cost of AS^B is 7.507 ms. Moreover, AS^B in [28] has time-consuming operations such as bilinear pairing. The AS^B computational overhead is 146.664 ms, about 20 times in our scheme. And [28] The time consumption in D_i^A, and D_j^B is 26.511 ms and 26.075 ms respectively. The time consumption is the most in the comparison scheme.

C. Communication Overhead

In this section, we calculate the communication overhead of the scheme. Similar to the computational cost analysis, we

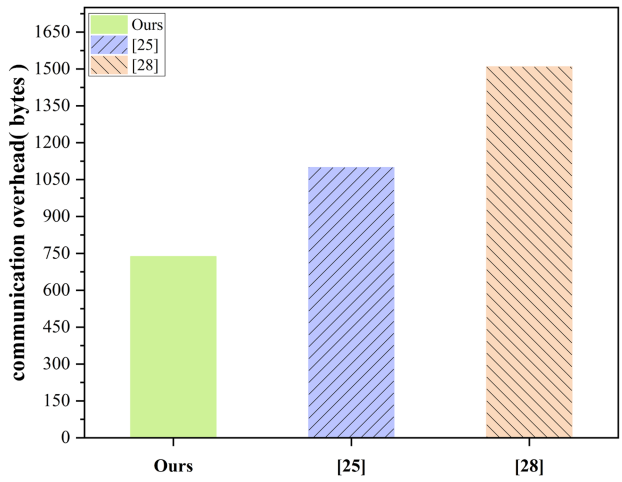


Fig. 5. Communication overhead.

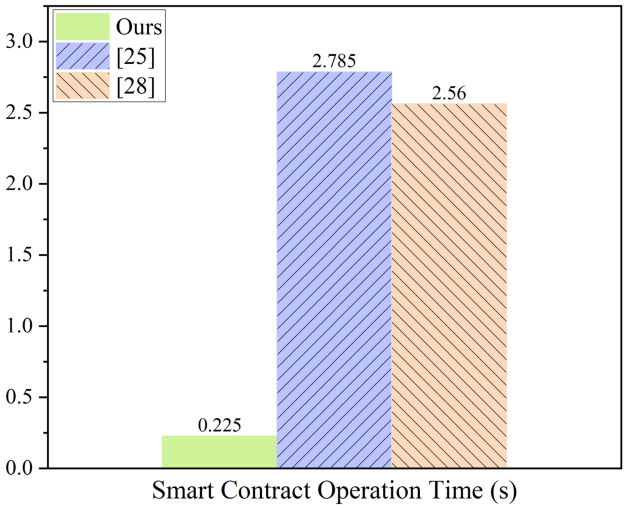


Fig. 6. On-chain time cost comparison.

consider the total communication cost of the cross-domain authentication and key agreement phases. We set T to be 4 bytes, the pseudonym length to be 32 bytes, the hash function used to be SHA-256, and the point size in the group G to be 128 bytes. D_i^A calculates the 128 bytes message of w_3 and w_4, and then sends the 420 bytes message M_3 to D_j^B. D_j^B calculates the 32 bytes α_k, generates a 72 bytes signature, and sends the 108 bytes message M_4 to AS^B to query related information; after that, D_j^B converts the 128 bytes public message to AS^B. D_i^A receives the key and the 72 bytes signature. D_i^A and D_j^B calculate the same session key after authentication. After calculation, the communication cost of the proposed scheme is 737 bytes. Table IV shows that the communication overhead of the scheme is reduced by 362 bytes compared with [25]. While the communication cost of [28] is more than doubled compared with this scheme. Fig. 5 can see the difference in communication overhead between schemes.

Besides, we also compare the communication rounds with these two schemes. We can see from Fig. 3 that our scheme only needs 4 rounds of message exchange in the cross-domain authentication protocol. However, we can see in Table IV that schemes [25] and [28] require 12 and 10 message exchanges, respectively. This scheme is significantly less than the other two comparison schemes regarding communication rounds.

D. On-Chain Related Operation Time

Since both the scheme and the comparison scheme in this paper involve using smart contracts to perform some operations on the blockchain, we refer to the experimental data of Wang et al. [41] for comparison. It can be known from Table II that the cost of query operation is much lower than that of update and undo, about 0.225 s, while, the time of update and undo operations is about 2.335 s and 2.338 s. When storing data on the blockchain, it must go through the consensus confirmation stage, which takes a long time. When querying data, it only needs to read from the blockchain copy data saved by the node, and the query time is much faster. After analysis, the scheme uses the authentication server to perform a blockchain read operation during the authentication process. In contrast, [28] uses the AS to perform a write and read operation during the cross-domain authentication phrase. Meantime, the devices in the scheme [25] must perform one write and two read operations, which does not apply to devices with limited resources. Fig. 6 can see the comparison time. It should be aware that this operation time includes the time of transaction publishing, verification, and synchronization.

VIII. Conclusion

In this study, we proposed a lightweight cross-domain authentication scheme suitable for most models and designed a blockchain-based device authentication protocol for cross-domain IIoT. Owing to the flexible application of dynamic accumulators in smart contracts, we can quickly add and delete the information required for authentication between devices. This scheme can alleviate the low authentication efficiency between devices while ensuring anonymity. Performance evaluations demonstrated that our scheme has low computational overhead and fewer communication rounds. Future research will now focus on solving secure cross-domain authentication when devices encounter capture attacks in an IIoT environment.

Acknowledgment

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

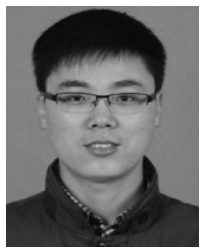
[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Inform.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[2] J. Cui, F. Wang, Q. Zhang, Y. Xu, and H. Zhong, "Anonymous message authentication scheme for semitrusted edge-enabled IIoT," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12921–12929, Dec. 2021.

[3] M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, "Significance of sensors for industry 4.0: Roles, capabilities, and applications," *Sensors Int.*, vol. 2, 2021, Art. no. 100110.

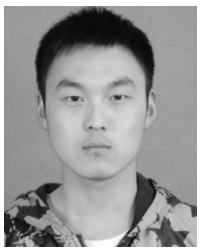
[4] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," *IEEE Access*, vol. 6, pp. 6505–6519, 2018.

[5] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial IoT," *J. Parallel Distrib. Comput.*, vol. 156, pp. 176–184, 2021.
[6] X. Zhang, M. Song, and J. Song, "A solution of electronic authentication services based on PKI for enabling e-business," in *Proc. IEEE Int. Conf. e- Bus. Eng.*, 2009, pp. 431–436.
[7] G. Li, Y. Wang, B. Zhang, and S. Lu, "Smart contract-based cross-domain authentication and key agreement system for heterogeneous wireless networks," *Mobile Inf. Syst.*, vol. 2020, pp. 1–16, 2020.
[8] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.
[9] M. Dabbagh, K.-K. R. Choo, A. Beheshti, M. Tahir, and N. S. Safa, "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities," *Comput. Secur.*, vol. 100, 2021, Art. no. 102078.
[10] Y. Zhang et al., "A lightweight authentication scheme based on consortium blockchain for cross-domain IoT," *Secur. Commun. Netw.*, vol. 2022, 1–15, 2022.
[11] C. Huang et al., "Blockchain-assisted transparent cross-domain authorization and authentication for smart city," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17194–17209, Sep. 2022.
[12] S. Guo, F. Wang, N. Zhang, F. Qi, and X. Qiu, "Master-slave chain based trusted cross-domain authentication mechanism in IoT," *J. Netw. Comput. Appl.*, vol. 172, 2020, Art. no. 102812.
[13] J. Liu, Y. Liu, Y. Lai, R. Li, S. Wu, and S. Mian, "Cross-heterogeneous domain authentication scheme based on blockchain," *J. Artif. Intell. Technol.*, vol. 1, no. 2, pp. 92–100, 2021.
[14] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *J. Ind. Inf. Integration*, vol. 21, 2021, Art. no. 100190.
[15] L. Xue, H. Huang, F. Xiao, and W. Wang, "A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 2409–2420, Sep. 2022.
[16] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020.
[17] C. Yuan, W. Zhang, and X. Wang, "EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system," *Arabian J. Sci. Eng.*, vol. 42, no. 8, pp. 3275–3287, 2017.
[18] Q. Chen, T. Wu, C. Hu, A. Chen, and Q. Zheng, "An identity-based cross-domain authenticated asymmetric group key agreement," *Information*, vol. 12, no. 3, 2021, Art. no. 112.
[19] X. Zhou, F. Miao, and Y. Xiong, "A certificate authority domain-based cross-domain authentication scheme for virtual enterprise using identity based encryption," in *Proc. IEEE 7th Int. Conf. Big Data Comput. Commun.*, 2021, pp. 144–149.
[20] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Veh. Commun.*, vol. 21, 2020, Art. no. 100200.
[21] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Gener. Comput. Syst.*, vol. 91, pp. 475–492, 2019.
[22] Y. Chen, G. Dong, J. Bai, Y. Hao, F. Li, and H. Peng, "Trust enhancement scheme for cross domain authentication of PKI system," in *Proc. IEEE Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, 2019, pp. 103–110.
[23] W. Wang, N. Hu, and X. Liu, "Blockcam: A blockchain-based cross-domain authentication model," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace*, 2018, pp. 896–901.
[24] G. Dong, Y. Chen, J. Fan, J. Bai, P. Zhang, and F. Li, "Anonymous cross-domain authentication scheme for medical PKI system," in *Proc. ACM Turing Celebration Conf.-China*, 2019, pp. 1–7.
[25] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.
[26] D. Liu, D. Li, X. Liu, L. Ma, H. Yu, and H. Zhang, "Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid," in *Proc. IEEE 2nd Conf. Energy Internet Energy Syst. Integration*, 2018, pp. 1–5.
[27] R. Chen et al., "BIDM: A blockchain-enabled cross-domain identity management system," *J. Commun. Inf. Netw.*, vol. 6, no. 1, pp. 44–58, 2021.
[28] M. Shen et al., "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, May 2020.
[29] X. Yang et al., "Blockchain-based secure and lightweight authentication for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3321–3332, Mar. 2022.
[30] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[31] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018.
[32] Y. Yu, Y. Zhao, Y. Li, X. Du, L. Wang, and M. Guizani, "Blockchain-based anonymous authentication with selective revocation for smart industrial applications," *IEEE Trans. Ind. Inform.*, vol. 16, no. 5, pp. 3290–3300, May 2020.
[33] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.
[34] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, 2021.
[35] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1382–1392, Jun. 2017.
[36] X. Huang, S. Leng, S. Maharjan, and Y. Zhang, "Multi-agent deep reinforcement learning for computation offloading and interference coordination in small cell networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9282–9293, Sep. 2021.
[37] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1654–1667, 2020.
[38] Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.
[39] L. Vishwakarma and D. Das, "SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, 2021.
[40] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, "A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain," *J. Syst. Archit.*, vol. 117, 2021, Art. no. 102112.
[41] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Inform.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.



Jie Cui (Senior Member, IEEE) was born in Henan Province, China, in 1980. He received the Ph.D. degree from the University of Science and Technology of China, Hefei, China, in 2012. He is currently a Professor and Ph.D. Supervisor with the School of Computer Science and Technology, Anhui University, Hefei, China. His research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security, and software-defined networking. He has more than 150 scientific publications in reputable journals e.g. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON CLOUD COMPUTING AND IEEE TRANSACTIONS ON MULTIMEDIA, academic books and international conferences.

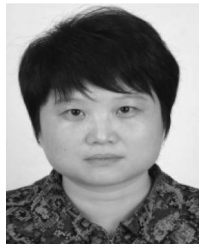
Nan Liu is currently a Research Student with the School of Computer Science and Technology, Anhui University, Hefei, China. Her research focuses on the security of the Internet of Things.



Qingyang Zhang was born in Anhui Province, China, in 1992. He received the B. Eng. and Ph.D. degrees in computer science from Anhui University, Hefei, China, in 2021. He is currently a Lecture of School of Computer Science and Technology with Anhui University. His research interests include edge computing, computer systems, and security.

Debiao He (Member, IEEE) received the Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols. He has authored or coauthored more than 100 research papers in refereed international journals and conferences, such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and Usenix Security Symposium. He was the recipient of the 2018 IEEE Systems Journal Best Paper Award and the 2019 IET Information Security Best Paper Award. His work has been cited more than 10000 times at Google Scholar. He is on the Editorial Board of several international journals, such as *Journal of Information Security and Applications*, *Frontiers of Computer Science*, and *Human-centric Computing & Information Sciences*.

Chengjie Gu received the Ph.D. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012. From 2012 to 2017, he was an Innovation Team Leader with the 38th Research Institute of CETC and conducted research and development with the communication and networking sector. He is currently a President of Security Research Institute with new H3C group. He is also studying for Postdoctoral Fellowship with the University of Science and Technology of China, Hefei, China. He is a high-level Innovation Leader of Anhui province and a cybersecurity expert of Zhejiang province in China. His research interests include network security and trusted network architecture.



Hong Zhong (Member, IEEE) was born in Anhui Province, China, in 1965. She received the Ph.D. degree in computer science from the University of Science and Technology of China, Hefei, China, in 2005. She is currently a Professor and Ph.D. supervisor with the School of Computer Science and Technology, Anhui University, Hefei, China. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security, and software-defined networking. She has more than 200 scientific publications in reputable journals e.g. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS and IEEE TRANSACTIONS ON BIG DATA, academic books and international conferences.