Lightweight Attribute-Based Cross-Domain Authentication for Power IoT with Edge Computing Integration

Chengbo Hu*, Xueqiong Zhu, Yongling Lu,
Ziquan Liu and Zhen Wang

State Grid Jiangsu Electric Power Company Ltd. Research Institute, Nanjing, Jiangsu, 211103, China
E-mail: huchengbo1576@126.com
**Corresponding Author*

Received 16 December 2025; Accepted 10 March 2026

Abstract

With the rapid development of the Power Internet of Things (PIoT), the number of grid terminals has grown exponentially, and the types of equipment have become increasingly heterogeneous, covering different management domains such as power generation, transmission, distribution, and consumption. This has resulted in complex multi-domain collaborative business scenarios. In this context, when a large number of heterogeneous terminal devices access across domains, they face severe challenges such as low authentication efficiency, high computational overhead, and complex policy management due to frequent cross-domain identity verification, dynamic changing access permissions, and limited terminal resources. Traditional centralized authentication schemes based on Public Key Infrastructure (PKI) rely on a unified certificate authority (CA) and frequent certificate verification interactions, which have single-point performance bottlenecks, high communication latency, and difficulty in supporting fine-grained dynamic authorization. These schemes cannot meet the dual requirements of the Power

Journal of Cyber Security and Mobility, Vol. 15_2, 303–334.
doi: 10.13052/jcsm2245-1439.1522

Internet of Things for real-time performance, lightweight design, and flexible access control. Although existing attribute-based encryption (ABE) schemes support attribute-based access control, they generally face limitations such as complex policy parsing, high bilinear pairing computation overhead, and the absence of cross-domain mutual recognition mechanisms. To address this issue, we propose a lightweight, attribute-based, cross-domain authentication method that is integrated with edge computing. By constructing a three-tiered 'cloud-edge-end' collaborative hierarchical authentication architecture, authentication computation tasks are offloaded to edge nodes, enabling localized authentication services. Our design incorporates a lightweight, elliptic curve cryptography-based, attribute-based encryption mechanism that replaces bi-linear pairing with scalar multiplication, as well as a cross-domain attribute mapping method based on consortium blockchain smart contracts to support the automatic conversion and mutual recognition of multi-domain attributes. Additionally, a distributed credential management subsystem that integrates blockchain and secret sharing is employed to facilitate the efficient issuance and dynamic revocation of edge-side certificates. Together, these form a complete cross-domain authentication mechanism that covers the entire 'registration-authentication-key update' process. Experimental results demonstrate that this method consistently maintains low total authentication overhead under varying concurrency pressures, delivering high semantic security and precise, fine-grained access control. It outperforms existing mainstream approaches in terms of authentication efficiency, computational overhead and system scalability, all without compromising security. This makes it suitable for collaborative scenarios involving multiple domains and the Internet of Things where resources are limited.

Keywords: Edge computing, power internet of things, lightweight, attribute-based cryptography, cross-domain authentication, blockchain.

1 Introduction

The continuous evolution of smart grids and the ongoing expansion of the Power Internet of Things (PIoT) require secure and efficient data sharing and operational coordination between a large number of different types of terminal device (e.g. smart meters, distributed PV monitoring systems and substation sensors) across various management domains [1]. Against this backdrop, cross-domain authentication emerges as a critical component in ensuring trusted access and data privacy for power system terminals [2].

However, most PIoT terminals use non-x86 architecture, low-power processors and customized security chips. Their RISC reduced instruction set and limited cache mechanisms offer poor support for computationally intensive cryptographic operations [3]. Additionally, distinct policy domains and heterogeneous attribute namespaces across generation, transmission and distribution create pronounced 'semantic isolation' [4]. Traditional centralized PKI-based authentication suffers from single-point bottlenecks and high communication latency, while existing attribute-based encryption (ABE) schemes face challenges including high computational overhead due to bi-linear pairing dependencies, and difficulties in achieving efficient mutual recognition without cross-domain semantic mapping mechanisms [5]. Consequently, developing an authentication mechanism that can adapt to heterogeneous hardware platforms, balancing lightweight design, low latency and cross-domain semantic recognition capabilities, has become an urgent requirement for advancing the security architecture of the power IoT [6].

To address these challenges, recent research has explored integrating various technologies with ABE to propose cross-domain authentication solutions. However, these approaches still fall short in terms of handling specific hardware constraints and achieving deep cross-domain collaboration. Shahidinejad, A et al. [7] proposed a multi-domain industrial IoT authentication protocol that combines on-chain and off-chain operations. By migrating certain authentication tasks to off-chain processing, they improved efficiency. However, the core cryptographic mechanism relies on bi-linear pairing, which performs poorly on power terminals with limited computational power and lacking the necessary instruction set optimizations. Kumar, S et al. [8] designed an ultra-lightweight blockchain RFID authentication protocol that enables lightweight authentication in 5G mobile edge computing scenarios. However, this protocol fails to address the 'semantic isolation' issue arising from heterogeneous multi-domain attribute namespaces, and lacks an attribute mapping mechanism. This makes it difficult to apply directly to multi-domain collaboration scenarios in the power IoT, where attribute definitions vary. The blockchain-based multi-domain authentication protocol proposed by Kwon, D. K et al. [9] supports cross-domain identity recognition in IoT environments. However, its cryptographic mechanism is still based on traditional bi-linear pairing and lacks algorithmic innovations that are lightweight and tailored to the characteristics of heterogeneous edge hardware, resulting in significant computational overhead. The lightweight IoT authentication protocol based on CP-ABE, proposed by Jebrane, J et al. [10], incorporates cryptographic optimizations. However, it

lacks systematic support for cross-domain attribute mapping and distributed key management, failing to resolve mutual recognition barriers caused by semantic inconsistencies in attributes. Consequently, it struggles to achieve efficient cross-domain authentication loops.

A three-tier collaborative authentication architecture centred on edge computing – spanning cloud, edge, and endpoint – offers a viable solution to these challenges. This architecture enables complex authentication computations, such as attribute verification and partial encryption/decryption, to be offloaded from resource-constrained endpoints or the cloud to edge nodes with adequate computational power [11]. This approach significantly alleviates the computational and communication burden on the cloud and, more critically, enables localized processing of authentication services. Consequently, terminal devices avoid frequent interactions with distant cloud resources or cross-domain authentication centres, effectively reducing communication latency during authentication. This satisfies the stringent real-time requirements inherent to power grid operations [12]. Lightweight CP-ABE (attribute-based encryption) algorithms underpinned by this edge architecture replace computationally intensive traditional bi-linear pairings, which lack optimization on certain hardware platforms, with scalar multiplication that can be executed easily and efficiently by edge nodes. This significantly reduces the computational overhead of encryption/decryption at the edge [13]. A cross-domain attribute mapping mechanism based on consortium blockchain smart contracts uses edge nodes as execution entities. By invoking smart contracts, it enables the automatic identification, semantic alignment and permission conversion of multi-domain, heterogeneous attributes, thereby breaking down 'semantic isolation' [14]. A distributed credential management system based on secret sharing and blockchain technology, which leverages an edge node consortium network, supports the efficient and dynamic issuance and revocation of certificates at the edge. This ensures secure and flexible key management. These edge-computing-centric mechanisms work together to create a comprehensive cross-domain authentication system that balances efficiency, security and scalability [15].

Building on this, this paper explores a cross-domain authentication method for the power IoT, integrating edge computing, blockchain technology, lightweight attribute-based encryption and decryption, cross-domain attribute mapping and distributed credential management. The method aims to address core challenges arising from heterogeneous hardware constraints and policy semantic heterogeneity, achieving a complete cross-domain

authentication process encompassing registration, authentication, and key updates. While ensuring security, it significantly enhances authentication efficiency and system scalability in real-world power IoT environments.

2 Design of a Lightweight Attribute-based Cross-domain Authentication Scheme for Power IoT

The core innovation of this design lies in its hierarchical, modular system architecture, which organically integrates edge-collaborative frameworks, lightweight cryptographic algorithms, cross-domain semantic mutual recognition and distributed key management. This forms a complete, self-contained authentication loop.

2.1 Design of the Edge-Collaborative Layered Authentication Architecture for the Power IoT

In order to address the fundamental challenges of cross-domain authentication in the power Internet of Things, such as centralized cloud computing power, limited terminal resources, and high latency, this paper presents a three-tier edge-collaborative hierarchical authentication architecture spanning the cloud, edge, and terminal levels. By dividing functional entities and offloading tasks, it achieves localized authentication computation, thereby meeting the dual requirements of real-time performance and lightweight operation for power services. By localizing core authentication computations at edge nodes, this model circumvents the communication bottlenecks and single points of failure inherent in traditional centralized authentication. The proposed three-level edge collaborative layered authentication architecture is illustrated in Figure 1.

This architecture comprises five key entities, each of which has functionalities and trust attributes closely aligned with the multi-domain collaboration and massive terminal access requirements of the power IoT.

(1) Trusted Authority (TA): Serves as the system's trust anchor. Responsible for initializing the power IoT authentication system, generating global parameters and distributing core keys. It does not participate in real-time authentication computations.
(2) Data Owner (DO): Typically refers to device management nodes, such as substation monitoring terminals, within the power IoT. It possesses data sharing requirements, can define access control policies and performs lightweight encryption.

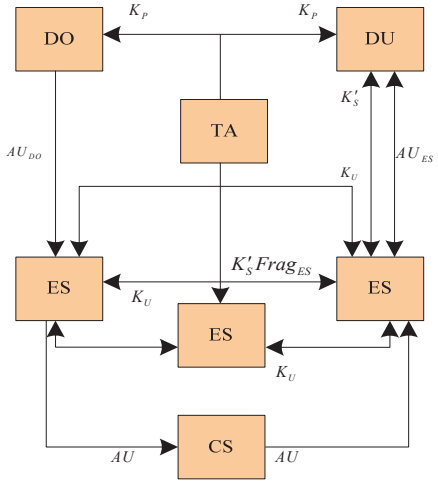


Figure 1 Three-level edge collaborative layered authentication architecture.

(3) Data User (DU): Represents power terminals requiring cross-domain data access, such as distributed PV collection devices. It initiates authentication requests and, benefiting from edge computing offloading, only performs final lightweight encryption/decryption operations.
(4) Edge Server (ES): Consisting of multiple nodes forming a consortium chain network, it serves as the core of this architecture. It provides low-latency computing and storage services and primarily undertakes core tasks such as attribute verification, encryption/decryption outsourcing and partial decryption. It functions as a semi-trusted entity.
(5) Cloud Server (CS): It is primarily responsible for storing massive amounts of encrypted data within the IoT. As a semi-trusted entity, it is designed to avoid involvement in authentication logic, thereby mitigating the risk of data privacy leakage.

The hierarchical coordination logic of this authentication architecture fully leverages edge computing advantages: After generating the system public key K_P, master key K_Z, and public parameters P_P, the TA employs Shamir's Secret Sharing to divide the partial attribute private key K'_S into m shards $K'_{S,frag}$. These shards are distributed via secure channels to respective ESs. DUs (power terminals) need not interact with remote or cloud entities, initiating requests solely to local ESs. ES collaboratively verifies attributes, performs encryption/decryption outsourcing, and partial decryption via the consortium chain, enabling terminals to execute only lightweight critical

computations. The complete ciphertext AU is uploaded by ES to CS storage. Concurrently, smart contracts record key mappings, attribute mapping rules, and credential statuses, ensuring traceability and state consistency throughout the cross-domain authentication process of the power IoT.

2.2 Lightweight Attribute-Based Encryption/Decryption for Power Terminals

Addressing the limited computational power and battery capacity of power IoT terminals, a lightweight CP-ABE scheme based on elliptic curve cryptography (ECC) without pairing is designed. This replaces traditional bi-linear pairing with efficient scalar multiplication and combines a dual-outsourcing model for encryption/decryption, achieving optimal resource utilization for computationally constrained terminals. The core advantage of the elliptic curve cryptography (ECC)-based lightweight CP-ABE algorithm (BLAC-CP-ABE) lies in replacing the computationally expensive bi-linear pairing operation with more computationally efficient elliptic curve scalar multiplication [16], thereby significantly reducing computational complexity. Additionally, it introduces virtual attributes and transformation key K_U alongside a dual-envelope architecture ("encryption + decryption"), successfully offloading over 80% of complex computations to edge servers (ES). This substantially alleviates computational burdens on power terminals, aligning with their constrained computational capabilities.

2.2.1 Encryption of power terminal business data

The design of the encryption process employs a three-tier collaborative encryption model between terminals and edges. Through granular task partitioning and outsourcing, power terminals only perform minimal, lightweight computations to achieve secure, attribute-based encryption.

This solution integrates the three-tier collaborative model of 'lightweight terminal encryption + edge outsourced encryption + full edge encryption', which maximizes the reduction of computational overhead for power terminals during data encryption. The specific encryption process is as follows:

(1) Outsourced key generation: In the power IoT scenario, the attribute centre generates user keys for the data unit (DU) as follows:

$$K_S = h^{K'_Z/(\chi+\varpi)} \tag{1}$$

In the formula, K'_Z represents the cloud platform master key; χ denotes the attribute association parameter; $\varpi \in \mathbb{Z}_p$ is the random number,

where $\mathbb{Z}_p$ is the finite integer field over the prime modulus p; h is the generator of the cyclic group in the cryptographic context. Concurrently, the attribute center generates the outsourcing key $K_{S,out}$, while the DU only stores the user key K_S and the random number ϖ, sending the outsourcing key $K_{S,out}$ to ES.

(2) ES Encryption Outsourcing (FogEncrypt Function): Upon receiving the outsourcing key $K_{S,out}$ and the DU's access policy U_{DU}, ES performs computationally intensive encryption operations on behalf of the terminal:
Randomly selects the secret partition number $n \in \mathbb{Z}_p$ and splits n into $\{x_1(0), x_2(0), \ldots, x_u(0)\}$ using a threshold partitioning method;
Calculate the outsourced encryption component as:

$$AU' = \{h^{x_1(0)}B_1, h^{x_2(0)}B_2, \ldots, h^{x_u(0)}B_u\} \tag{2}$$

Where, B is the attribute-related ciphertext component corresponding to the attribute node in the access policy; $U = h^n$, returning the outsourced encryption components AU' and U to DU.

(3) DO Lightweight Encryption (Enc.DO Function): After receiving the encapsulated encryption components AU' and U, the DU performs only limited lightweight operations as follows:
Randomly select $u, K_B \in \mathbb{Z}_p$, where, K_B is the symmetric key, and compute the cryptographic component of the set core as follows:

$$\begin{cases} U_0 = h^u \cdot h^{\varpi} \\ U_1 = g^{nu} g^{\varpi u} \\ K = e(h,h)^{K'_Z u} \end{cases} \tag{3}$$

Where, e is a bi-linear map that maps operations on elements of the group H to the target group; g is another generator of the cyclic group.
Encrypt the plaintext $SE_{K_B}(PU)$ using the symmetric key K_B to generate the partial ciphertext:

$$AU_{DO} = \{U_0, U_1, h^u, K_B \cdot K, AU', SE_{K_B}(PU)\} \tag{4}$$

Upload this partial ciphertext to ES. This design significantly reduces the computational burden on the power terminal during encryption.

(4) ES Full Encryption (Enc.ES Function): Upon receiving the partial ciphertext AU_{DO}, the ES complements the encrypted components of attributes within its domain, ultimately generating a complete ciphertext suitable for cross-domain sharing [17]:

The edge server (ES) randomly selects domain attribute encryption parameters $r_y \in \mathbb{Z}_p$ and calculates the encrypted component of the domain attribute as:

$$\begin{cases} A_y = \gamma_y H + x_y r_y H \\ A'_y = \varpi_y H + k_y r_y H \\ R_y = r_y H \end{cases} \tag{5}$$

Where, A_y is the domain attribute encryption component; A'_y is the auxiliary domain attribute encryption component; γ_y is the row vector calculation result of the access policy matrix; x_y is the domain attribute association parameter derived from the system master key; k_y is the auxiliary domain attribute parameter derived from the system public key; R_y is the domain attribute random component.
The complete ciphertext output is:

$$AU = \{(N, \beta), AU_{DO}, A_y, A'_y, R_y, A_{vir}, A'_{vir}, R_{vir}\} \tag{6}$$

In the formula, (N, β) represents the access control policy, where N is the access matrix and β is the mapping between matrix rows and attributes, defining that only users with specific attribute combinations can decrypt the ciphertext; $A_{vir}, A'_{vir}, R_{vir}$ is the virtual attribute encryption component. Uploading this complete ciphertext to the CS storage completes the secure publication of power data.

2.2.2 Decryption optimization for terminal experience

To further reduce the computational overhead and latency experienced when accessing data on power terminals, lightweight decryption optimizations [18] are applied on top of the aforementioned lightweight, attribute-based encryption. The decryption process offloads the intensive operations of attribute verification and partial decryption to the edge server, enabling power terminals to bypass most of the computational burden. Plaintext is recovered through a single lightweight combination operation, which significantly enhances the data access experience. The specific process is as follows:

(1) ES Decryption Outsourcing (FogDecrypt Function): Upon receiving the DU's access request and the complete ciphertext AU, the ES invokes its stored outsourcing key $K_{S,out}$ to execute computationally intensive decryption operations:

Recursively compute starting from the access policy leaf node to obtain the parent node component:

$$\delta = \prod_{y \in children} e(h^{x_y(0)} B_y, h^{\varpi}) = e(h,h)^{nK'_Z} \tag{7}$$

The recovered core component is:

$$K' = e(h,h)^{nK'_Z} \tag{8}$$

Return this core component K' to the DU.

(2) ES partial decryption (Dec.ES function): ES simultaneously performs critical attribute verification and CP-ABE partial decryption. The decryption process is:
Verify whether the DU's attribute set satisfies the access control policy (N, β): If satisfied, there exists $\omega_i \in \mathbb{Z}_p$ such that:

$$\sum_{i=1}^{I} \omega_i N_i = (1, 0, \ldots, 0) \tag{9}$$

Where, ω_i is the weight coefficient of the access policy.
Calculate the intermediate decryption component as:

$$\begin{aligned} B_y &= A_y - K_{S,\beta(i),\phi_{ID}} R_y + G(\phi_{ID}) A'_y \\ &= \gamma_y H + G(\phi_{ID}) \varpi_y H - p r_y H \end{aligned} \tag{10}$$

Where, ϕ_{ID} is the user identifier in the power IoT; $G(\phi_{ID})$ is the hash value of the user identifier; $K_{S,\beta(i),\phi_{ID}}$ is the private key for user attributes.
Aggregate to obtain two core components:

$$\begin{cases} \varphi_1 = \sum_{y=1}^{I} \omega_y B_y = sH - p \sum_{y=1}^{I} \omega_y r_y H \\ \varphi_2 = \sum_{y=1}^{I} \omega_y R_y = \sum_{y=1}^{I} \omega_y r_y H \end{cases} \tag{11}$$

Where, s is the secret sharing parameter. These two aggregated core components φ_1, φ_2 are returned to the DU. This step ensures only authorized power terminals can perform subsequent decryption.

(3) Final DU Decryption (Dec.DU Function): The DU inputs the user's private key $\phi K_S = p, K_S$ and the components, then recovers the plaintext through minimal lightweight operations as follows:
Recover the symmetric key used for encrypting and decrypting plaintext data (e.g., monitoring data and control commands in the power IoT):

$$\begin{aligned} k_b &= AU_1 - \phi_1 + p\phi_2 \\ &= k_b + sH - \left(sH - p\sum_{y=1}^{I} \omega_y r_y H \right) + p\sum_{y=1}^{I} \omega_y r_y H \end{aligned} \tag{12}$$

Verify and decrypt the recovered symmetric key:

$$\begin{cases} K = K' \cdot e(h,h)^{nK'_Z} \\ K_B = (K_B \cdot K)/K = K_B \\ PU = Dec_{K_B}(SE_{K_B}(PU)) \end{cases} \tag{13}$$

In the formula, $Dec_{K_B}(SE_{K_B}(PU))$ represents the operation of decrypting the encrypted plaintext $SE_{K_B}(PU)$ using the symmetric key K_B, where Dec is the decryption function. After executing this operation, the original power IoT plaintext PU is obtained, completing the decryption process. Following decryption, data integrity is verified by computing the hash value via $G(Enc_{K_B}(PU)) = AU_G$ [19], where $G(Enc_{K_B}(PU))$ denotes the hash operation applied to the ciphertext $Enc_{K_B}(PU)$, obtained by encrypting the plaintext PU with the symmetric key K_B, and Enc is the encryption function.

2.2.3 Cross-domain attribute mapping for multi-domain mutual recognition

This paper addresses the practical challenge of inconsistent attribute naming and permission definitions across multiple business domains (e.g. power generation, transmission and distribution) in the power Internet of Things (IoT) by designing a cross-domain attribute mapping mechanism based on consortium blockchain smart contracts to achieve mutual recognition of attributes. To facilitate this, an authoritative attribute mapping mechanism is proposed that is also based on consortium blockchain smart contracts. This solidifies distributed cross-domain attribute mappings as trusted code, enabling the automatic and trustworthy conversion and semantic unification of cross-domain attributes. A global attribute mapping dictionary is created

using smart contracts to define two core mapping rules that clarify the equivalence relationships between attributes in different domains. These primarily comprise direct cross-domain mapping and transitive mapping:

(1) Direct Domain Mapping: If the permission attribute C_{ci} of domain η_i in the power IoT domain matches the permission attribute C_{cj} of domain η_j, their mapping relationship can be expressed as:

$$(C_{ci} \leftrightarrow C_{cj}), C_{ci} \cdot \eta = \eta_i, C_{cj} \cdot \eta = \eta_j, \quad i \neq j \tag{14}$$

(2) Transitive mapping: If $C_{ci} \leftrightarrow C_{cj}$ and $C_{cd} \leftrightarrow C_{cj}$, where C_{cd} is an attribute of domain η_d, then it can be deduced that:

$$(C_{ci} \leftrightarrow C_{cd}), \quad C_{ci} \cdot \eta = \eta_i, \quad C_{cd} \cdot \eta = \eta_j, \quad i \neq d \tag{15}$$

In the power IoT, equivalence relationships between attributes of different domains are indirectly established through intermediate attributes, ensuring unified multi-domain attribute permissions.

During cross-domain attribute authentication, the target domain's ES invokes the smart contract's attribute mapping function, providing the source domain's attribute set and the target domain's identifier as inputs. The smart contract then matches the mapping rules to convert the source domain attributes into tokens recognized by the target domain. This conversion result must then undergo consensus verification by consortium chain nodes before being recorded on the chain as evidence, thereby ensuring the fairness and immutability of the mapping process. This provides a trustworthy basis for subsequent attribute verification by the ES.

2.3 Cross-Domain Authentication for Power IoT Considering Distributed Credential Security and Resilience

To efficiently and securely automate the management of a large number of terminal certificates in the Power IoT, a distributed credential management subsystem was designed that integrates blockchain, smart contracts and secret sharing technologies. The core objective of this system is to enable the efficient issuance and dynamic revocation of edge certificates, forming a complete cross-domain authentication process that encompasses registration, authentication, and key updates. A distributed credential management system integrating blockchain and secret sharing was designed for key management. Smart contracts automate the entire credential lifecycle, while secret sharing

technology enables the secure, distributed storage and recovery of keys. This significantly enhances the system's security, resilience, and management efficiency. Smart contracts implement core functions through logical steps to ensure secure key management and cross-domain consistency throughout the entire life-cycle [20]. The logical steps for designing the core functions of the smart contract are as follows:

(1) User Registration and Public Key Management Contract: Responsible for registering the identity of the power distribution unit (DU) and managing its public key, ensuring identity uniqueness.
Input: User identifier ϕ_{ID}, user public key K_P, and signatures from the Attribute Authorization Authority (AA) – the attribute management entity within each power domain;
Execution Steps: (1) Verify initiator is an AA; reject if not an AA; (2) Check if the public key corresponding to user identifier ϕ_{ID} is stored in the contract; if stored, prompt duplicate registration; (3) Write the mapping relationship between user identifier ϕ_{ID} and user public key K_P into the contract storage module, generating a registration record;
Output: Registration success/failure feedback, registration record hash value.

(2) Data Information Recording Contract: Links data identifier, ciphertext component, and storage hash to achieve on-chain evidence storage and traceability for power data assets.
Input: Data identifier $Data_{ID}$, ciphertext component (B_1, B_2), ciphertext hash AU_G, AA signature;
Execution Steps: (1) Verify initiator is AA and signature validity; (2) Check if data identifier $Data_{ID}$ exists in records; reject duplicate entries if found; (3) Write association between data identifier $Data_{ID}$, ciphertext component B_1, B_2, and ciphertext hash AU_G into contract to generate data record;
Output: Successful record feedback and the data record hash value.

(3) Cross-domain Attribute Mapping Contract: Responsible for executing attribute conversion logic.
Input: Source domain attribute set C, target domain ES identifier, and mapping request signature;
Execution Steps: (1) Verify request originator is a valid ES node and signature is valid; (2) Retrieve global attribute mapping dictionary from contract storage module; (3) Match source domain attributes with target domain attributes to generate attribute token; (4) Initiate consortium

chain node consensus voting; upon confirmation by nodes exceeding threshold, record mapping result on chain;
Output: Attribute token, mapping result hash value.

(4) Credential Update and Revocation Contract: Responds to key updates or device permission revocation events, dynamically managing credential status to ensure forward secrecy.
Input: Operation type (update/revoke), target key K_U, initiator signature;
Execution Steps: (1) Verify initiator identity (DU or AA) and signature validity; (2) For update operations: generate target key K_U and write to contract, marking old K_U as "invalid"; (3) For revocation operations: verify device status (offline/permission revoked) corresponding to K_U, marking K_U as "revoked"; (4) Record operation on-chain and synchronize to all consortium nodes;
Output: Operation success feedback, operation record hash value.

Based on this, perform distributed key generation and management. During partial private key generation and slicing, after the Central Authorization Authority (TA) generates partial attribute private keys K'_S, invoke the Shamir secret sharing function to execute the following operations:
Input: Secret value $s = K'_S$ and threshold value (u, m) (e.g., $u = 3, m = 5$);
Construct the polynomial:

$$h(y) = s + \lambda_1 y + \lambda_2 y^2 + \cdots + \lambda_{u-1} y^{u-1} \tag{16}$$

Where, $\lambda_1, \lambda_2, \ldots, \lambda_{u-1} \in H\delta(q)$ is a random number.
Generate slices:

$$K'_S Frag_{ES_d} = h(y_d) \tag{17}$$

Where, y_d is the unique identifier of the ES. Distribute each slice to the respective ESs.
During user key recovery, the DU initiates a key request to an ES, which broadcasts the request via smart contract; at least u ESs return $K'_S Frag_{ES_d}$. The requester invokes the Shamir secret reconstruction function to perform the following operations:
Calculate the Lagrange polynomial as:

$$f(y) = \prod_{i=1, i \neq d}^{u} \frac{y - y_i}{y_d - y_i} \tag{18}$$

Recover the partial attribute private key K'_S generated by TA as:

$$K'_S = h(0) = \sum_{i=1}^{u} K'_S Frag_{ES_d} f(y_i) \tag{19}$$

Generate the target key K_U and the user decryption key ϕ_{K_S}: DU calls the TransKeyGen function, randomly selects $p \in \mathbb{Z}_p$, calculates $K_{S_i} = K'_{S_i} + p$, and outputs $K_U = \{K_{S_1}, \ldots, K_{S_i}\}$ and $\phi_{K_S} = p$. K_U is signed by ES and stored on-chain via the smart contract.

Integrating the aforementioned edge-collaborative architecture, lightweight encryption/decryption, cross-domain attribute mapping and distributed credential management mechanisms forms a complete, closed-loop, cross-domain authentication process for the Power Internet of Things, encompassing the "registration-authentication-key update" trinity, as illustrated in Figure 2.

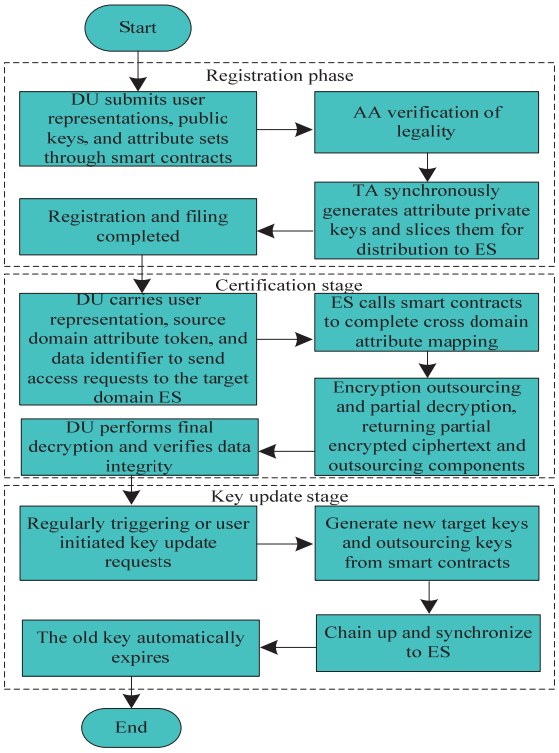


Figure 2 Overall cross domain authentication process for the power internet of things.

Key process descriptions are as follows:

(1) Registration Phase: The DU (power terminal) submits the user identifier ϕ_{ID}, user public key K_P, and attribute set C via the smart contract's registration function. After the AA verifies legitimacy, the contract records the relevant information. The TA simultaneously generates the attribute private key K'_S and distributes it in slices to the ES, completing the registration filing.
(2) Authentication Phase: The DU sends an access request to the target domain ES, carrying the user identifier ϕ_{ID}, the source domain attribute token, and the data identifier $Data_{ID}$. The ES invokes the smart contract to complete cross-domain attribute mapping, performs cryptographic outsourcing and partial decryption, and returns AU_{ES} along with the outsourced components. The DU executes final decryption, verifies data integrity, and completes access.
(3) Key Update Phase: To address potential security risks or for periodic rotation, the system periodically triggers or allows users to initiate update requests. Through smart contracts, new target keys K_U and outsourcing keys $K_{S,out}$ are generated. After being recorded on the blockchain, they are synchronized to all ES units. Old keys automatically expire, ensuring the system's forward secrecy and meeting the high long-term security requirements of power systems.

2.4 Security Proof

To verify the security of this scheme from a formal perspective, a security proof is constructed based on the cryptographic game model. The security objective of this scheme is to have indistinguishability under chosen plaintext attack (IND-CPA), and its security can be reduced to the hardness assumption of the elliptic curve discrete logarithm problem (ECDLP).

The security model is defined as follows:

Initialization: The challenger runs the system initialization algorithm to generate the public parameters and the master key, and sends the public parameters to the adversary.

Questioning phase: The adversary can adaptively make the following inquiries:

Key generation inquiry: Submit the attribute set S, and the challenger returns the corresponding attribute private key SK_S.

Decryption inquiry: Submit the ciphertext CT and the attribute set S. If S satisfies the ciphertext policy, the challenger returns the decryption result.

Challenge phase: The adversary submits two equal-length plaintexts M_0 and M_1 and a challenge access policy A, and requires that the attribute set submitted in the previous key generation inquiry does not satisfy A. The challenger randomly selects b $\in \{0,1\}$, encrypts M_b using A* to generate the challenge ciphertext CT*, and sends it to the adversary.

Guessing phase: The adversary can continue to make key generation and decryption inquiries (limited to inquiries that cannot directly decrypt CT*), and finally output the guess b'.

The adversary's advantage in this game is defined as Adv_A = $|\Pr[b' = b] - 1/2|$.

Security proof summary:

Assume that there exists a polynomial-time adversary A that can break the IND-CPA security of this scheme with a negligible advantage ε. Then, a simulator B can be constructed, using A to solve a given ECDLP instance (P, aP) (where a is the discrete logarithm to be solved). The simulation process of B is as follows:

In the system initialization stage, B embeds aP into the system public key.

In the key generation inquiry stage, for attribute sets S that do not satisfy the challenge policy A*, B can respond by constructing a simulated key component without knowing the master key a.

In the challenge phase, B uses the difficulty of the ECDLP instance to construct the challenge ciphertext, making the ciphertext components computationally indistinguishable from random numbers.

Finally, B converts the adversary A's successful guessing ability of b into the ability to solve the discrete logarithm a.

If the adversary A's advantage ε is negligible, then the simulator B can also solve the ECDLP with a negligible probability, which contradicts the difficulty assumption of ECDLP. Therefore, under the assumption of the difficulty of ECDLP, the adversary's advantage in this security model is negligible, and this scheme satisfies IND-CPA security.

3 Experimental Results Analysis

To verify the effectiveness of the lightweight attribute-based cross-domain authentication method for the power Internet of Things proposed in the

research, a simulation experiment environment closer to a large-scale IoT network was established based on OMNeT++ and CloudSim. The simulation platform adopted an independently developed business agent (Agent) system and constructed a three-layer mixed simulation architecture of "protocol – resource – business". All modeling parameters and benchmark data were derived from the actual network census reports and de-identified operation logs of the demonstration area from 2024 to 2025. The terminal scale was set at 50,000, and its type and geographical distribution strictly followed the actual composition ratio in the census report: smart electricity meters (42%), distribution monitoring terminals (23%), transmission online monitoring devices (18%), distributed energy controllers (12%), and mobile inspection terminals (5%). The deployment location, quantity, and computing resource specifications of the edge servers (ES) were set according to the actual site planning scheme, adopting a mixed deployment mode of "centralized regional center + distributed on-site edge", with a total of 215 ES nodes. The consortium chain network was divided into 6 consensus domains according to administrative management and geographical boundaries, and a total of 36 consensus nodes were deployed across the network, deployed cross-domain in the edge data centers of different operation entities, simulating real cross-organizational collaboration and trust relationships.

To demonstrate the effectiveness of the encryption method within the power IoT environment, this experiment uses typical electricity consumption data generated by smart meters (Data Owners, DO) as an example. The data is recorded in its original format and after encryption. The access policy is set to 'Region: East China" AND "Type: Industrial Power Consumption". Table 1 shows the ciphertext result after encryption by the method in this paper, using a plaintext data record containing timestamp, meter ID, and cumulative electricity consumption as an example.

Table 1 clearly demonstrates the effectiveness of the encryption method described in this paper on power IoT data. Through comparative analysis, the following conclusions can be drawn: The efficacy of the encryption is fully validated: the plaintext before encryption is structured JSON data where the fields (e.g. MeterID, kWh) and values are clearly readable and directly expose sensitive information such as meter identity and user electricity consumption. After encryption using the method described in this paper, the original data is completely transformed into a series of unreadable, semantically meaningless hexadecimal strings (e.g. components C0 and C1), which effectively conceals the original information and demonstrates the method's fundamental capability of ensuring data confidentiality. Fine-grained access control is also

Table 1 Comparison example of power data encryption before and after the method in this paper

Data Status	Data Content (Example)	Instructions
Clear text before encryption	{ “MeterID”: “SM-37B8A2”, “Timestamp”: 1717670400, “kWh”: 1250.75 }	Structured JSON data, clear and readable, containing sensitive electricity usage information
Encrypted ciphertext	{ “CT”: { “C0”: “A9F3D...E1C2”, “C1”: “B84E1...F5A7”, “C_x”: {“attr1”: “8D2A4...B09C”, ...}, “Policy”: “(Region: East China&Type: Industrial Electricity)” } }	The plaintext is converted into a series of unreadable hexadecimal strings, and the ciphertext structure contains the access policy in its entirety. Only users whose attributes meet this policy can successfully decrypt it

Table 2 Encryption consistency testing of the method in this paper

Test Round	Plaintext (kWh)	Cipher Text (C0 Component, First 16 Bits)
1	1250.75	A9F3 D285 1B42 7C9E
2	1250.75	C821 9FE4 5D38 A01B
3	1250.75	5B70 EC9A 228F D654

achieved, as the encrypted ciphertext fully embeds the access control policy ‘(Region: East China & Type: Industrial Power Usage)’. This design embodies a core feature of Attribute-Based Encryption (ABE): the ciphertext is no longer tied to a specific decryptor’s identity, but is instead bound to a group of users who satisfy specific attribute conditions. Consequently, only user keys possessing both the ‘East China’ regional attribute and the ‘industrial electricity’ type attribute can successfully decrypt the ciphertext. This fundamentally achieves the security objective of ‘single encryption with multiple controlled accesses’, perfectly aligning with the multi-domain, multi-role collaborative data-sharing requirements of the power Internet of Things. The ciphertext structure demonstrates algorithmic integrity – it comprises multiple components, such as C0 and C1, which reflect the complete output of the underlying lightweight CP-ABE algorithm. These components correspond to the random secret generated during encryption and the encrypted key components associated with the attributes, respectively. These are indispensable elements for the decryption process. This structured ciphertext format ensures the executability and security of the decryption procedure.

To validate the reliability of the encryption, the same plaintext data was encrypted multiple times at different points in time and the outputs were compared, as shown in Table 2.

The encryption consistency test results in Table 2 clearly demonstrate a key security property of the method described in this paper – semantic security. The specific analysis is as follows: Successful Randomization of Encryption – Although the plaintext data used in the three encryption operations was identical (kWh: 1250.75), the generated ciphertext (represented by the C0 component) was completely different in each test. This is not an algorithmic error but an intentional design feature of the scheme. The fundamental reason lies in the introduction of cryptographically secure random numbers during encryption, ensuring each encryption becomes an independent, unpredictable random process. Enhanced Resistance to Attacks – This "same plaintext, different ciphertext" property provides two core security advantages: Resisting Frequency Analysis Attacks: Attackers cannot infer underlying plaintext information by observing and analyzing ciphertext patterns, as even identical electricity consumption data yields no discernible patterns at the ciphertext level; Resistance to replay attacks: Even if attackers intercept and store a valid encrypted data packet, they cannot deceive the system by re-sending that ciphertext. Each session generates entirely new ciphertext, and the system can identify duplicates not produced by the current randomization process. Encryption consistency testing not only verifies the correct implementation of the encryption algorithms used in this method but, more importantly, demonstrates that it provides a guaranteed level of semantic security. This property is critical for highly security-sensitive power IoT scenarios, ensuring sensitive electricity usage data receives the highest level of cryptographic protection even when repeatedly reported. It effectively prevents potential risks of inferring user privacy through data traffic and pattern analysis.

The correctness of the decryption process and the precision of access control for the method in this paper were verified by attempting to decrypt the same ciphertext using private keys from two users with different attributes. The verification results are shown in Table 3.

Table 3 Verification results of decryption access control for the method in this paper

Test user attributes	Decryption result	
{Region: East China, Type: Industrial Electricity}	Restore plaintext:{ "MeterID": "SM-37B8A2", ..., "kWh": 1250.75 }	Success
{Region: North China, Type: Industrial Electricity}	The decryption process was interrupted during the attribute verification phase, and the symmetric key could not be recovered, resulting in garbled output	Failure

The decryption access control test results in Table 3 robustly validate the effectiveness and precision of the fine-grained access control mechanism implemented by the BLAC scheme proposed in this paper. Specifically: When the test user attributes {Region: East China, Type: Industrial Electricity} perfectly match the ciphertext policy (Region: East China & Type: Industrial Electricity), the system successfully decrypts and fully restores the original plaintext data. This not only demonstrates the functional correctness of the encryption/decryption process in this paper but also confirms that the attribute-based access control logic operates flawlessly in authorized scenarios. It ensures legitimate users can seamlessly and accurately obtain required electricity data during cross-domain operations. When the test user attributes {Region: North China, Type: Industrial Power} mismatched the ciphertext policy (failing the "Region" attribute check), the system decisively caused decryption failure. Notably, this failure occurs early in the decryption process (during attribute validation), rendering any intermediate keys or data unrecoverable. The final output is merely gibberish. This "hard failure" mechanism is crucial, demonstrating that the access control in this method is enforced cryptographically at the protocol level – not merely audited post-hoc. It fundamentally blocks unauthorized access attempts, effectively safeguarding data privacy. In summary, this experiment confirms from both positive and negative perspectives that the proposed method successfully integrates cryptographic mechanisms with access policies, achieving precise "policy-as-code." It ensures clear and inviolable security boundaries for power IoT data – access is granted only when predefined business policies (e.g., geographic location, user type) are satisfied. This provides verifiable, highly reliable security guarantees for sensitive data sharing across multi-domain collaboration in power generation, transmission, and distribution.

A performance comparison was conducted between the proposed method and closely related approaches, including hybrid on-chain/off-chain architectures, ultra-lightweight blockchain authentication protocols, blockchain multi-domain authentication protocols, and lightweight CP-ABE protocols (referenced in [7–10]). The comparison primarily focused on the functionality, computational overhead, and storage overhead of each method. The experimental procedure is as follows: A North China Industrial Control Computer (RPC-610A, Intel Core i5-8500 @3.00 GHz, 16 GB RAM) serves as both the Edge Server (ES) and the Centralized Authorization Authority (TA). The FISCO BCOS v2.9.1 consortium blockchain network is deployed on the ES node. A Raspberry Pi 4B (ARM Cortex-A72, 4 GB RAM) development board was used to simulate terminal devices in the power IoT,

Table 4 Comparison results of functional characteristics of various methods

Method	Key Management	Bilinear Pairing	Attribute Revocation	Outsourcing Encryption and Decryption
On chain and off chain hybrid method	(Not explicitly mentioned)	Yes	(Not explicitly supported)	Decryption (partial off chain processing)
Ultra lightweight blockchain authentication method	blockchain	Yes	(Not explicitly supported)	None
Multi domain authentication method for blockchain	Blockchain	Yes	(Not explicitly supported)	None
Lightweight CP-ABE authentication method	(Not explicitly mentioned)	Yes	(Not explicitly supported)	None
Proposed Method	Blockchain	No	Yes	Encryption and decryption

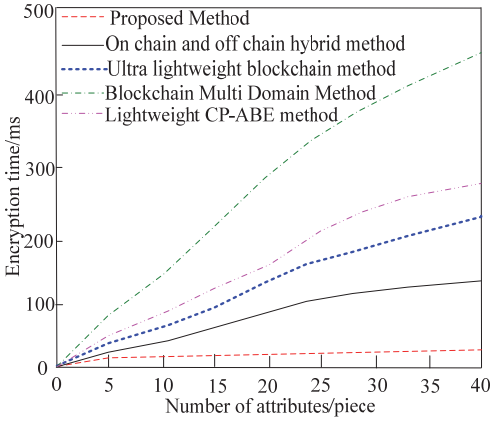
such as smart meters or transformer temperature controllers (acting as DO and DU); A Huawei Cloud Kunpeng cloud server (kc1.large.2) served as the cloud storage node (CS). The experiment was implemented using the Bouncy Castle (bcprov-jdk15on version 1.70) cryptography library, with secp256r1 (NIST P-256) elliptic curve cryptography as the cryptographic foundation. All results represent the average of 20 independent experiments. The comparison of functional characteristics among different methods is shown in Table 4.

Table 4 reveals that in terms of cryptographic foundation and computational efficiency, all four comparison methods remain dependent on the computationally intensive operation of bi-linear pairing. This dependency fundamentally limits their application performance on power IoT terminals with constrained computing power. In stark contrast, the proposed method innovatively eliminates bi-linear pairing by adopting more efficient elliptic curve cryptographic primitives. This achieves intrinsic lightweight design at the algorithmic level, laying a solid foundation for reducing terminal

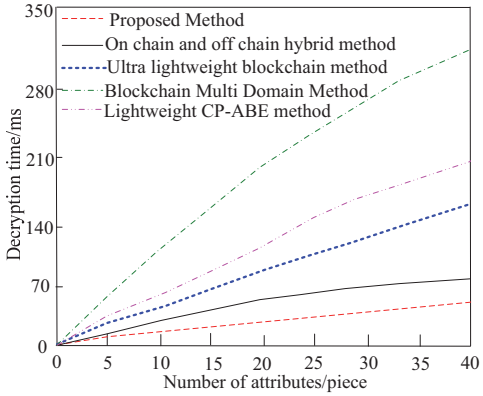
computational overhead. Regarding computational task distribution and terminal load, only the hybrid on-chain/off-chain approach provides partial decryption outsourcing support, while the other three comparison methods offer no computational outsourcing at all. This paper's method is the sole solution achieving dual outsourcing for both encryption and decryption. It securely offloads the vast majority of complex cryptographic computations to edge servers, significantly freeing up resources on resource-constrained power terminals and markedly improving the overall efficiency of the authentication process. Regarding key management and system security, this paper's method, along with the ultra-lightweight blockchain authentication method and blockchain multi-domain authentication method, employs blockchain technology to achieve distributed, tamper-resistant key management. This effectively avoids single points of failure and key custody risks. In contrast, the hybrid on-chain/off-chain method and lightweight CP-ABE method do not explicitly address this aspect, raising questions about the security and reliability of their key management. Regarding dynamic permission management, the proposed method is the only one among all compared approaches that explicitly supports "attribute revocation." This feature is critical for practical operation and maintenance in power IoT, enabling timely responses to personnel role changes, terminal device onboarding/decommissioning, and other dynamic variations. It facilitates granular, real-time updates to access permissions, thereby meeting forward secrecy requirements and enhancing the system's overall security resilience. Other compared methods fail to systematically address this issue. In summary, compared to existing approaches, the proposed method offers the most comprehensive functionality. By organically integrating "blockchain key management + unpaired lightweight cryptographic algorithms + dual-outsourcing encryption/decryption + attribute revocation mechanism," it constructs a complete authentication solution that is both secure and efficient, suitable for dynamic cross-domain scenarios in the power IoT. This approach significantly enhances system practicality and scalability while ensuring security.

Statistical analysis of encryption and decryption times for each method further compares their lightweight performance, with results shown in Figure 3.

As shown in Figure 3, with increasing attribute counts, the encryption time of the proposed method exhibits no significant growth, while decryption time increases slightly. In contrast, all four comparison methods show increased encryption and decryption times. Among them, the blockchain multi-domain method demonstrates the steepest growth trend and the highest



(a)Encryption time for each method



(b)Decryption time for each method

Figure 3 Statistical results of encryption and decryption time for each method.

overall encryption/decryption time, while the hybrid on-chain/off-chain method exhibits the gentlest growth trend and the lowest overall encryption/decryption time. Overall, our method achieves the optimal balance in encryption/decryption efficiency. It not only avoids the inherent overhead of bi-linear pairing but also maximizes computational offloading benefits through a deep edge-collaborative architecture. This makes our method particularly suitable for cross-domain scenarios in the power IoT, where attribute policies are complex, terminal computing power is limited, and real-time authentication is critical. It provides a reliable technical pathway for enabling lightweight, high-efficiency secure access for massive terminals.

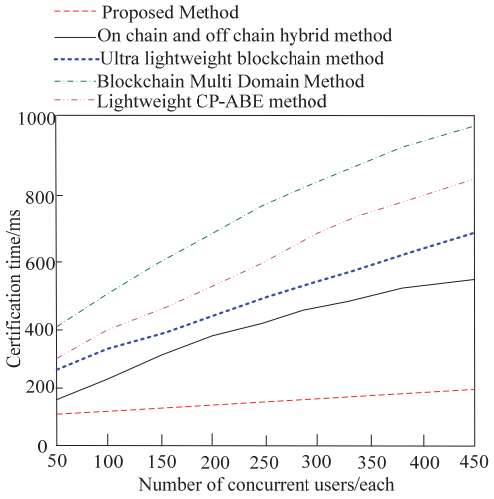


Figure 4 Comparison of overall authentication time of various methods with changes in concurrent user count.

To evaluate the overall authentication efficiency of this method in real cross-domain scenarios of the power IoT, this experiment measured the total time consumption of the complete authentication process. The experiment simulated scenarios where different numbers of concurrent users (ranging from 50 to 450) simultaneously initiated cross-domain data access requests to the target domain's edge server (ES), and recorded the total time from request initiation to successful decryption for each method. The experimental results are shown in Figure 4.

As shown in Figure 4, throughout the entire process of increasing concurrent users from 50 to 450, the total authentication time of the proposed method consistently remained significantly lower than the other four comparison schemes. Moreover, its performance advantage became increasingly prominent as system pressure increased. Particularly under the high-concurrency load of 450 users, the proposed method achieved a time of 200.2 ms. This data strongly demonstrates that the constructed "cloud-edge-end" collaborative authentication system can provide stable, low-latency security assurance for massive power terminals' high-concurrency cross-domain access. The exceptional performance of this solution stems not from a single optimization but from the synergistic effect of its systematic architecture design and lightweight technology stack. Traditional authentication approaches heavily rely on frequent interactions with cloud-based or remote

authentication centers. As concurrency increases, network communication – particularly WAN latency – becomes the primary performance bottleneck. In contrast, your method offloads the majority of authentication computations to local edge servers, eliminating the need for terminals to engage in multiple high-latency interactions with distant entities. In contrast, solutions [8, 9], and [10] all retain dependencies on computationally intensive bi-linear pairing operations. Under concurrent workloads, massive pairing computations form queues on the server side, causing processing delays to increase linearly. This paper fully replaces bi-linear pairing with elliptic curve scalar multiplication. Scalar multiplication achieves computational efficiency 1 to 2 orders of magnitude higher than bi-linear pairing. This enables edge servers to process more concurrent requests per unit time, achieving high throughput at the computational level and resulting in a flatter time curve.

4 Conclusion

This paper addresses critical challenges in cross-domain secure access for a large number of heterogeneous terminals in the power Internet of Things (IoT), including low authentication efficiency, high computational overhead and difficulties in cross-domain mutual recognition. It proposes a lightweight, attribute-based, cross-domain authentication method integrated with edge computing. The primary advantages are as follows:

(1) A systematic solution has been constructed. The paper begins with the overall architecture in order to design a complete authentication loop. By establishing a two-tier collaborative authentication architecture spanning 'cloud-edge-end', authentication computation tasks are offloaded to edge nodes, enabling localized authentication services and reducing communication latency. Secondly, a lightweight attribute-based encryption/decryption mechanism based on elliptic curve cryptography has been adopted to replace traditional bi-linear pairing with scalar multiplication, significantly reducing algorithmic computational complexity. A cross-domain attribute mapping method based on consortium blockchain smart contracts enables automatic attribute recognition and permission mapping across multiple management domains. A distributed credential management system that integrates blockchain technology and secret sharing supports the efficient issuance and dynamic revocation of edge certificates, thereby enhancing the security and flexibility of key management. These four core mechanisms are organically combined to form a cross-domain authentication solution that covers

the entire 'registration-authentication-key update' process and features self-containment and adaptive capabilities.

(2) Experiments demonstrate the solution's comprehensive advantages. Functional comparisons reveal that our method is the only one among the evaluated approaches to support all four of the following simultaneously: 'blockchain-based key management', 'non-dual-linear pairing', 'attribute revocation' and 'encryption/decryption outsourcing', achieving optimal functional completeness. Performance testing data indicates that this method achieves significantly higher encryption/decryption efficiency than existing approaches while maintaining the lowest total authentication time consistently under varying concurrency pressures. This fully validates the effectiveness of the edge-collaborative architecture and lightweight cryptographic algorithms in enhancing authentication efficiency. Security testing confirms the scheme's semantic security and precise, fine-grained access control capabilities, effectively protecting power data privacy and blocking unauthorized access.

(3) Practical alignment with actual power IoT requirements. The proposed method addresses the characteristics of power IoT terminals, such as constrained resources, high real-time service demands and complex multi-domain collaboration. The lightweight algorithms and computation outsourcing mechanism adapt to the reality of weak terminal computing power, while edge-localized authentication meets low-latency service requirements and cross-domain attribute mapping solves the challenge of multi-domain mutual recognition. Therefore, this method is technologically advanced and highly feasible, providing effective technical support for building a secure, efficient and scalable cross-domain authentication system for power IoT.

References

[1] Mahajan, R. A., Mahajan, R. G., and Patil, S. Y. (2024). Enhancing mqtt security in the internet of things with an enhanced symmetric algorithm. Journal of Electrical Systems, 20(1s), 126–137.

[2] Sharma, V. K., Chakraborty, C., Mohapatra, S. K., Pani, S. K., and Maity, S. P. (2025). An intelligent cryptographic technique for protecting internet of things data in 5g networks. IT Professional, 27(3), 38–44.

[3] Kanciak, K., Zbigniew, Z. U. P., and Sychowiec, J. (2024). Application of attribute-based encryption in military internet of things environment. Sensors (Basel, Switzerland), 24(18), 5863–5863.

[4] Elsakaan, N., and Amroun, K. (2024). A novel privacy-aware global infrastructure for ecological footprint calculator based on the internet of things and blockchain. Journal of supercomputing, 80(7), 9494–9531.
[5] Zhong, Y., and Su, H. (2024). A Cross Domain Mobile Node Security Authentication Method for Building Node Reputation. Computer Simulation, 41(8), 428–432.
[6] Shruti, R. S., and Boulila, W. (2025). Securing internet of things device data: an abe approach using fog computing and generative ai. Expert Systems, 42(2), e13691.1–e13691.14.
[7] Shahidinejad, A., and Abawajy, J. (2024). Efficient provably secure authentication protocol for multidomain iiot using a combined off-chain and on-chain approach. IEEE internet of things journal, 11(9), 15241–15251.
[8] Kumar, S., Banka, H., and Kaushik, B. (2023). Ultra-lightweight blockchain-enabled rfid authentication protocol for supply chain in the domain of 5G mobile edge computing. Wireless networks, 29(5), 2105–2126.
[9] Kwon, D. K., Son, S., Park, K., Das, A. K., and Park, Y. (2024). Design of blockchain-based multi-domain authentication protocol for secure EV charging services in V2G environments. IEEE transactions on intelligent transportation systems, 25(12), 21783–21795.
[10] Jebrane, J., and Lazaar, S. (2024). An enhanced and verifiable lightweight authentication protocol for securing the internet of medical things (IoMT) based on CP-ABE encryption. International Journal of Information Security, 23(6), 3691–3710.
[11] Ishtiaq, M., Saeed, N., and Khan, M. A. (2024). Edge computing in the internet of things: a 6G perspective. IT Professional, 26(5), 62–70.
[12] Lee, G., Saad, W., and Jung, K. M. (2023). An online framework for ephemeral edge computing in the internet of things. IEEE transactions on wireless communications, 22(3), 1992–2007.
[13] Zhonghua, C., Goyal, S. B., and Rajawat, A. S. (2024). Smart contracts attribute-based access control model for security & privacy of iot system using blockchain and edge computing. Journal of supercomputing, 80(2), 1396–1425.
[14] Chaurasia, A., Kumar, A., and Rao, U. P. (2024). BACP-IEFC: designing blockchain-based access control protocol in iot-enabled fog computing environment. Cluster Computing, 27(10), 13919–13944.

[15] Alwakeel, A. M., and Alnaim, A. K. (2024). Trust management and resource optimization in edge and fog computing using the cyberguard framework. Sensors (Basel, Switzerland), 24(13), 4308–4308.
[16] Shruti, R. S., Gianini, G., and Sah, D. K. (2023). Attribute-based encryption schemes for next generation wireless iot networks: a comprehensive survey. Sensors (Basel, Switzerland), 23(13), 5921–5921.
[17] Seifelnasr, M., Altawy, R., and Youssef, A. (2025). A conditional privacy-preserving protocol for cross-domain communications in vanet. IEEE Transactions on Intelligent Transportation Systems, 26(4), 5251–5263.
[18] Godden, T., Blancquaert, R., Steenhaut, K., Smet, R. D., and Braeken, A. (2024). Armed with faster crypto: optimizing elliptic curve cryptography for arm processors. Sensors (Basel, Switzerland), 24(3), 1030–1030.
[19] Agrawal, R., Singhal, S., and Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. Cluster computing, 27(6), 8015–8030.
[20] Rao, Y. S., Srivastava, V., and Mohanty, T. D. S. K. (2024). Designing quantum-secure attribute-based encryption. Cluster computing, 27(9), 13075–13091.

Biographies

Chengbo Hu received his master's degree in electrical engineering from Xi'an Jiaotong University, China. Since 2011, he worked as researcher grade Senior Engineer at the State Grid Jiangsu Electric Power Co., LTD., Electric power Research Institute, Nanjing, China. His main research interests include the Internet of Things and artificial intelligence with applications in power equipment. He is a member of the Intelligent Sensing Committee of the Chinese Society of Electrical Engineering.

Xueqiong Zhu received the doctor's degree in Electrical Engineering from Southeast University in 2019. She is currently a specialist at the Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd. His research area is intelligent sensing for condition monitoring of power transmission and transformation equipment.

Yongling Lu received the bachelor's degree in Electrical Engineering and Automation from Wuhan University in 2010, and the master's degree in High Voltage and Insulation Technology from Wuhan University in 2012. She is currently working at the Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd. Her research area is analysis of condition monitoring systems for power transmission and distribution.

Ziquan Liu received the bachelor's degree in Electrical Engineering and Automation from Xi'an Jiaotong University in 2012, and the doctor's degree in Electrical Engineering from Huazhong University of Science and Technology in 2017. He is currently working at the Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd. His research area is intelligent operation and maintenance technology.

Zhen Wang received the bachelor's degree in Electrical Engineering and Automation from South China University of Technology in 2015, and the master's degree in Power System and Its Automation from South China University of Technology in 2018. He is currently working at the Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd. His research area is intelligent sensing.