Multi-Heterogeneous Power Data Security Protection in Smart Grid Based on Data Aggregation and Paillier Homomorphic Encryption Algorithm

Binyuan Yan*, Zeyuan Zhou, Yun Fu and Yang Su

Guizhou Power Grid Co. Ltd., Guiyang, Guizhou 550000, China
E-mail: yanbinyuan3@gmail.com
**Corresponding Author*

Received 12 March 2026; Accepted 09 May 2026

Abstract

Multi-heterogeneous power data in smart grid refers to power data that includes multiple types, modalities, and sampling frequencies, such as user electricity consumption, equipment operation, and grid scheduling. The diverse and heterogeneous power data in the smart grid is related to the stable operation of the grid and user privacy. Without effective protection, it is easy to cause risks such as information leakage and scheduling failure. Therefore, targeted security protection solutions need to be constructed. However, there are problems with the loss of information granularity, high risk of privacy leakage, and limited data analysis in the current smart grid power data aggregation and sharing. To enhance the security protection effect of power data, a multi-dimensional data security protection scheme based on data aggregation and Paillier homomorphic encryption is proposed. Firstly, a three-tier system model for multivariate heterogeneous power data in smart grids is constructed (smart meters, data collection stations, and blockchain

Journal of Cyber Security and Mobility, Vol. 15_4, 1087–1132.
doi: 10.13052/jcsm2245-1439.15411

nodes). Subsequently, the Paillier homomorphic encryption algorithm is integrated to encrypt and aggregate users' multi-dimensional electricity consumption data. At the same time, data aggregation and consortium chain technology have been introduced. Experimental results demonstrate that this scheme offers significant advantages over traditional Rivest-Shamir-Adleman (RSA) encryption schemes, traditional Advanced Encryption Standard (AES) encryption schemes, Elgamel encryption schemes, and traditional Transmission Control Protocol/Message Queuing Telemetry Transmission Protocol transmission schemes in terms of computational and communication overhead. When the number of users reaches 5000, the computational overhead at data collection stations is only 35.6% of that in traditional RSA methods, and the communication overhead is merely 28.7% of traditional transmission control protocol methods. Additionally, when transmitting power data from 5000 users simultaneously, the information accuracy rate exceeds 92%, and the packet loss rate remains below 0.5%. In conclusion, the proposed scheme provides an efficient and reliable technical pathway for the secure transmission of multivariate heterogeneous power data in smart grids.

Keywords: Smart grid, data aggregation, Paillier homomorphic encryption, multivariate heterogeneous data, security protection, computational overhead.

1 Introduction

The smart grid, as a core component of the energy Internet, relies on the real-time collection, transmission, and analysis of diverse and heterogeneous power data for its efficient operation [1, 2]. This data encompasses various types of information, including user electricity consumption details, equipment operating statuses, and grid dispatching instructions, all of which hold significant importance for the efficient functioning of the smart grid. In the absence of effective security protection mechanisms for this data, a range of severe risks may arise, such as frequent marketing harassment of users, inaccurate grid load forecasting, line overloading, and even large-scale power outages, as well as the leakage of commercial secrets [3, 4]. Therefore, implementing security protection for diverse and heterogeneous power data in the smart grid is an inevitable requirement for ensuring stable grid operation and safeguarding user rights and social public interests. Currently, commonly used methods for data security protection include traditional encryption techniques, data aggregation technologies, blockchain technology, and access

control mechanisms [5]. Meanwhile, numerous scholars have also conducted research on data security protection issue.

Guo et al. proposed an application scheme for cross-domain data circulation collaborative protection technology based on data processing units, targeting the vulnerability risks in data interaction and sharing within the new-type power system. Additionally, this study utilized data plane programmable technology. The results indicated that this scheme could establish ubiquitous security boundaries and enhance the security of cross-domain power data circulation [6]. Niu et al. introduced a blockchain-driven system to address data privacy and security risks in healthcare systems. This system integrated technologies such as Secure Hash Algorithm 256 (SHA-256), asymmetric encryption algorithms, and Elliptic Curve Digital Signature Algorithm (ECDSA). The results demonstrated that the system had an average latency of 15.3 milliseconds for 10 transactions on a single node, with a 100% success rate in data integrity [7]. Kesavan et al. designed a new power system security model to tackle data security issues in power grids. This model leveraged blockchain technology to enhance data storage and verification security and incorporated Support Vector Machine (SVM) algorithms. The results showed that the model achieved an overall security level of 96.34%, with a false positive rate of only 1.82%, demonstrating excellent performance in enhancing power system security [8]. Pathan et al. focused on the security of energy transaction data and the lack of decentralized management in smart grids. They proposed the integration of blockchain technology into smart grid architecture and established relevant energy paradigms, with a focus on blockchain based smart grid security. This paradigm relied on the tamper proof and distributed accounting characteristics of blockchain, which could ensure data security during clean energy transactions. The results showed that this scheme could effectively avoid the security risks of traditional centralized management, provide a key technical path for the construction of smart grid security system, and perform outstandingly in data security and decentralized security management [9].

Anandh et al. proposed a data security private framework based on an improved Advanced Encryption Standard (AES) algorithm to address the vulnerability of data transmitted in cloud computing to security threats. This framework added a second round of encryption using different keys based on 128-bit AES technology and allowed the use of AES with various key lengths. The results revealed that this architecture could process 1000 blocks per second and reduced power consumption by 13.23% [10]. Can et al. analyzed novel cryptographic methods based on genetically generated

robust sub-keys and robust cryptographic techniques based on homologous genetics to gain insights into data security in cloud computing. Additionally, this study reviewed several gene cryptography-based methods, their applications, and drawbacks. The results indicated that these genetics-based cryptographic methods provided ideas for improving cloud security and held certain research value in the field of cloud computing data security [11]. Li et al. proposed a method using the AES algorithm to optimize the process of power grid data security identification to ensure the security and confidentiality of power grid system data. Moreover, this study explored the application of AES in enhancing data protection and improving the accuracy and efficiency of security identification technologies. The results demonstrated that AES-based security optimization contributed to improving data security in power grid operations [12]. Gaikwad et al. proposed a solution to the issue of privacy data security protection in cloud computing by applying homomorphic encryption and secure multi-party computation technology. Among them, homomorphic encryption supported direct computation of encrypted data, ensuring privacy and security in data processing. Secure multi-party computation achieved multi-party joint data analysis without leaking a single dataset through decentralized computation of multiple entities. The results showed that the scheme had good application effects and could better adapt to the privacy protection needs of cloud computing [13].

In summary, although a large amount of research has been conducted on the security protection of smart grid data, most of the work focuses on traditional encryption, plaintext data aggregation, or centralized blockchain systems, and has not yet formed a systematic comparative analysis of multi-source heterogeneous power data. There are obvious shortcomings in terms of ciphertext computing capability, edge device adaptability, privacy protection granularity, key management security, and compatibility with power industry standards, making it difficult to meet the engineering needs of security, efficiency, and feasibility at the same time. At the same time, the existing smart grid data security solutions still have significant limitations: traditional plaintext aggregation is prone to information granularity loss and privacy leakage. Conventional encryption algorithms do not support direct calculation of ciphertext, resulting in high privacy risks during data processing [14]. Centralized architecture poses a single point of failure hazard: single key management scheme and poor adaptability to edge devices; insufficient granularity of privacy protection, making it difficult to balance data availability and confidentiality [15]; or insufficient compatibility with power grid standards such as IEC61850. In response to these limitations,

to ensure the security of diverse and heterogeneous power data in smart grids, a three-tier system model for such power data has been developed in the research. A data transmission security protection scheme based on the Paillier algorithm has been designed and, on the basis of this scheme, a data sharing protection scheme has been constructed, namely, the ultimate Paillier encryption algorithm-based Data Transmission-and-sharing Security Protection scheme (Paillier-DTSP). This scheme adopts ciphertext aggregation to avoid information granularity loss and privacy leakage, supports direct calculation of ciphertext to reduce data processing risks, uses a distributed three-layer architecture to eliminate single points of failure, optimizes three-level key management and lightweight algorithms to improve edge device adaptability, integrates homomorphic encryption and differential privacy to balance data availability and confidentiality, and achieves compatibility with power grid standards such as IEC61850 through protocol adaptation and model extension. This study aims to carry out targeted improvements for the six major shortcomings mentioned above, with the aim of providing a comprehensive and efficient technical solution for the secure transmission, efficient aggregation, and reliable sharing of heterogeneous power data in the smart grid.

The core innovations of the research are as follows.

- Adopt a ciphertext direct aggregation mechanism to replace traditional plaintext aggregation, complete data aggregation without exposing the original data, preserving information granularity, and block privacy leakage from the source.
- Utilize Paillier homomorphic encryption to support ciphertext computation, then data can be aggregated in an encrypted state without the need for decryption during processing, significantly reducing security risks in the data processing stage.
- Adopt a distributed three-layer architecture of terminal aggregation node blockchain, this eliminates dependence on a single central node, eliminates single point of failure hazards, and enhances the system's ability to resist attacks and destruction.
- Design a three-level key management mechanism consisting of root key, region key, and device key, and combine quantum key distribution with TLS 1.3 secure transmission. Perform algorithm lightweight optimization for edge devices to solve the problems of single key management and poor edge adaptability.
- Integrate homomorphic encryption with differential privacy, adding Laplacian noise during the encryption process to protect sensitive

information of individual users while preserving the statistical characteristics of the dataset, achieving a balance between data confidentiality and availability.
- Through data format adaptation, communication protocol compatibility, and information model extension, achieve seamless integration with the smart grid IEC61850 standard, and improve the engineering feasibility and deployment compatibility of the solution in actual power systems.

2 Secure Data Aggregation for Smart Grid Using Paillier Encryption

To achieve the security protection of diverse and heterogeneous power data in smart grids, the research takes data transmission and data sharing protection as the core entry points and constructs a comprehensive scheme incorporating the Paillier homomorphic encryption algorithm. In terms of data transmission, the research devises a three-tier system model for diverse and heterogeneous power data in smart grids. Regarding data sharing, based on data transmission, the research designs a system model comprising five entities.

2.1 Multi-Heterogeneous Power System Model of Smart Grid and Power Data Transmission Process

To ensure the security of diverse and heterogeneous power data in smart grids, the research adopts a progressive approach from two perspectives, namely, data transmission and data sharing protection. In terms of data transmission, the research devises an integrated scheme that not only employs blockchain technology to prevent unauthorized tampering or loss of data but also incorporates encryption algorithms and data aggregation techniques. Specifically, the research first constructs a system model comprising smart meters, data collection stations, and blockchain nodes to clarify the roles and functional boundaries of each entity in data security protection. Subsequently, the research analyzes the power data transmission process within this system model to outline the complete path of data from generation to storage. Then, the research designs an aggregation method for diverse and heterogeneous power data to achieve efficient summarization of multi-dimensional power data and lay a technical foundation for subsequent data sharing security protection. In smart grids, the research utilizes blockchain technology, which is a distributed ledger technology with advantages such as decentralization,

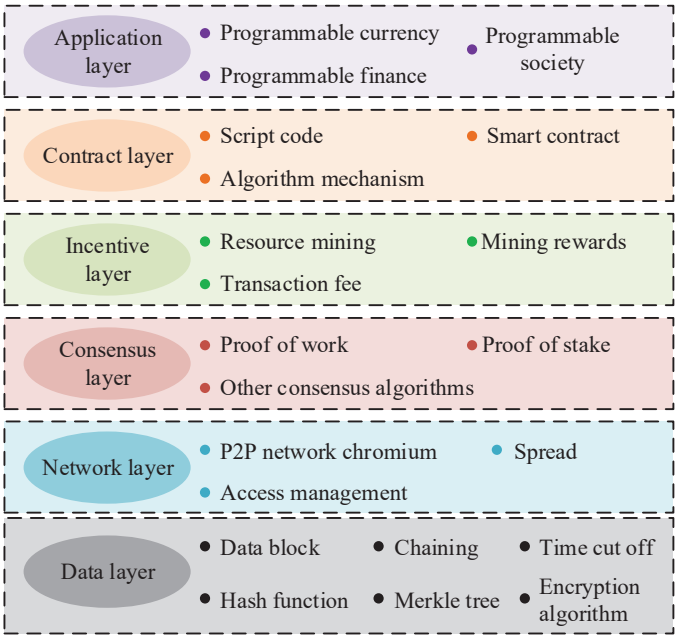

Figure 1 Hierarchical structure of blockchain.

immutability, and transparent traceability [16, 17]. The hierarchical structure of blockchain is illustrated in Figure 1.

From Figure 1, blockchain primarily consists of the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. Among them, the data layer is mainly responsible for encapsulating the fundamental data structures of blockchain, such as blocks and the chain-like structure, to ensure the immutability of data. The consensus layer, serving as the core of blockchain, guarantees data consistency across all nodes in the network through consensus algorithms. The structure of the blockchain-based data transmission protection scheme is illustrated in Figure 2.

From Figure 2, the blockchain-based data transmission protection scheme mainly comprises a power system model (which involves internal data transmission). Among them, the three-layer system model of the smart grid's heterogeneous power system is based on the core logic of "terminal collection intermediate aggregation distributed storage", covering the smart meter layer, data collection station layer, and blockchain node layer. The functions of each layer are independent and collaborative, achieving full process security protection of power data from collection to storage.

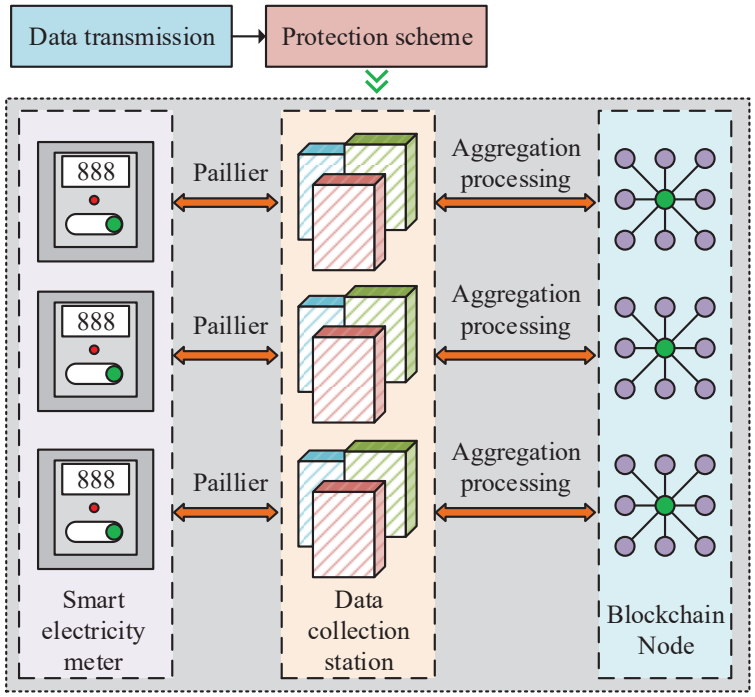

Figure 2 Structure of data transmission protection scheme based on blockchain.

Smart meters are mainly responsible for real-time collection and preliminary processing of users' multi-dimensional electricity consumption data, and uploading the data-to-data collection stations. In this process, the research employs the Paillier homomorphic encryption algorithm. The Paillier homomorphic encryption algorithm is a probabilistic public-key cryptosystem based on asymmetric encryption, with its core advantage being support for homomorphic addition operations. It enables aggregated computation of data without revealing plaintext, effectively protecting data privacy [18–20]. Meanwhile, the advantages of Paillier homomorphic encryption algorithm include low computational and deployment costs, probabilistic encryption, and mature engineering support, making it widely used in privacy computing and data security scenarios. The encryption and decryption processes of the Paillier homomorphic encryption algorithm mainly include key generation, encryption, decryption, and homomorphic operations (addition and scalar multiplication). In key generation, the input is the security parameter λ, and the steps can be divided into five. The specific steps are as follows: randomly

select two distinct large prime numbers p and q, calculate the public key core parameter n and the private key core parameter λ, select the generator g, calculate the private key auxiliary parameter μ, and output the public key pk and private key sk. The constraint for selecting large prime numbers is

$$\gcd(pq, (p-1)(q-1)) = 1, \quad p, q \in \mathbb{P} \tag{1}$$

where $\gcd(,)$ represents the greatest common divisor, and $\mathbb{P}$ is the set of large prime numbers. The calculation of the public key core parameter n and the private key core parameter λ is

$$\begin{cases} n = pq \\ \lambda = \mathrm{lcm}(p-1, q-1) \end{cases} \tag{2}$$

where $\mathrm{lcm}(,)$ represents the least common multiple. The constraint for selecting the generator g is

$$\begin{cases} g \in \mathbb{Z}_{n^2}^* \\ \gcd(L(g^{\lambda} \bmod n^2), n) = 1 \end{cases} \tag{3}$$

where $\mathbb{Z}_{n^2}^*$ is the multiplication group of modulo n^2 and $L(\cdot)$ is the auxiliary function. The calculation of private key auxiliary parameters is

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n \tag{4}$$

The public/private key output is

$$\begin{cases} pk = (n, g) \\ sk = (\lambda, \mu) \end{cases} \tag{5}$$

In the encryption process, the input consists of a public key $pk = (n, g)$ and a plaintext $m \in [0, n-1]$. The steps are mainly divided into three: randomly select an encryption random number $r \in \mathbb{Z}_n^*$ (r is an integer coprime with n); calculate the ciphertext c; output ciphertext. The calculation of ciphertext c is

$$c = g^m \times r^n \bmod n^2 \tag{6}$$

In the decryption process, the input consists of a private key $sk = (\lambda, \mu)$ and a ciphertext c. This step is divided into three parts: define an auxiliary function $L(x) = \frac{x-1}{n}$ (valid only when $x \equiv 1 \bmod n$); calculate the plaintext m; output plaintext. The expression of auxiliary function is

$$L(x) = \frac{x-1}{n} \tag{7}$$

Auxiliary functions are only valid when $x \equiv 1 \bmod n$. The calculation of plaintext m is

$$m = L(c^{\lambda} \bmod n^2) \times \mu \bmod n \tag{8}$$

The Paillier homomorphic encryption algorithm used in this paper is an additive homomorphic encryption algorithm that supports homomorphic addition and scalar multiplication operations, but does not support fully homomorphic multiplication. In the scenario of smart grid data aggregation, it is only necessary to perform summation class aggregation calculation on user electricity data, and addition homomorphism can fully meet the requirements. The implementation method of ciphertext aggregation calculation is as follows: without decrypting the ciphertext of a single user, the data collection station completes homomorphic accumulation of ciphertexts uploaded by multiple smart meters through Equation (9), and directly outputs the aggregated ciphertext. The blockchain node can use the private key to decrypt the aggregated ciphertext once to obtain the total electricity consumption, achieving a secure process of "ciphertext transmission, ciphertext calculation, and decryption results".

The data collection station serves to receive encrypted electricity consumption data uploaded by multiple smart meters, perform aggregation processing on this data, and then send the processed results to the blockchain nodes of the power system model. Among them, data aggregation technology is a technique that combines encrypted data from multiple users into a single aggregated ciphertext through specific operations, which can reduce data transmission volume and enhance privacy protection [21, 22]. The expression of the encrypted data merging operation in the data aggregation process is

$$C = \prod_{i=1}^{k} c_l \bmod n^2 \tag{9}$$

where k represents the number of users, i represents the serial number of user quantity, C denotes the final ciphertext generated after aggregation processing. Through this method, encrypted data from multiple users can be merged into an aggregated ciphertext without the need to decrypt individual data, thereby reducing data transmission volume and enhancing privacy protection. This aggregation operation is very useful in scenarios such as smart grids, as it allows for effective aggregation and analysis of data while maintaining data encryption. Within the power system model, blockchain nodes store the aggregated ciphertext data and relevant transaction records, and are responsible for decrypting the aggregated ciphertext. During this process, the research

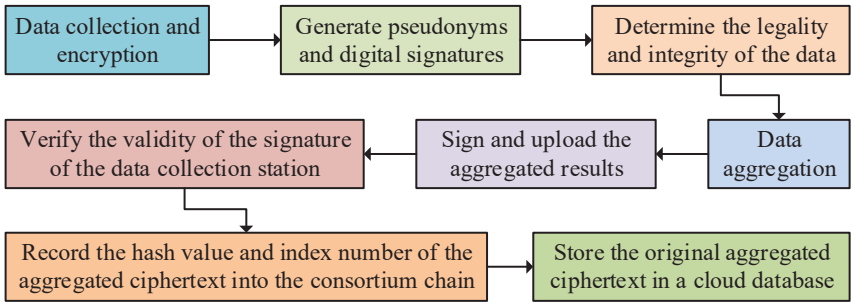

Figure 3 Specific process of power data transmission.

adopts a consortium blockchain and the Practical Byzantine Fault Tolerance consensus mechanism. The core advantage of consortium blockchain is to balance decentralized trust with high efficiency and controllability, which not only avoids the inefficiency and lack of regulation of public chains, but also solves the trust shortcomings of traditional centralized systems. In terms of data transmission, this scheme primarily involves Paillier homomorphic encryption, consortium blockchain, and cloud databases. The specific power data transmission process is illustrated in Figure 3.

From Figure 3, during the power data transmission process, smart meters first collect and encrypt the data, generating pseudonyms and digital signatures. Subsequently, data collection stations verify the legality and integrity of the data before performing data aggregation. The data collection stations then sign the aggregation results and upload them to the pre-selected nodes of the consortium blockchain. Next, the validity of the signatures from the data collection stations is verified, and information such as the hash value and index number of the aggregated ciphertext is recorded on the consortium blockchain, while the original aggregated ciphertext is stored in the cloud database. Through this process, comprehensive security protection for power data can be achieved throughout the entire process, from collection and transmission to storage.

2.2 Design of Power Data Security Protection Based on Data Aggregation and Paillier Homomorphic Encryption Algorithm

The research has devised a data security protection scheme tailored for the data transmission process. However, the security protection of power data also encompasses safeguards during the data sharing process. Data sharing

is conducted on the premise that data transmission has been completed and the data has been securely stored, with data transmission serving as the prerequisite and foundation for data sharing. Therefore, building upon the data security protection scheme based on data aggregation and the Paillier homomorphic encryption algorithm, the research has designed a data sharing protection scheme to form a comprehensive method for protecting power data security. Given the issues of prominent risks in centralized architectures and low sharing efficiency in traditional data sharing approaches, the research introduces a consortium blockchain, aiming to leverage its immutability to ensure traceability of data sharing operations. Additionally, the Paillier homomorphic encryption algorithm is adopted to enhance sharing efficiency. The model of the data sharing protection scheme is illustrated in Figure 4.

From Figure 4, the data sharing protection scheme involves five types of entities. The first entity is the data requester, who needs to interact with the blockchain to obtain decryption keys and index numbers, and download homomorphically encrypted ciphertext from the cloud database. The second

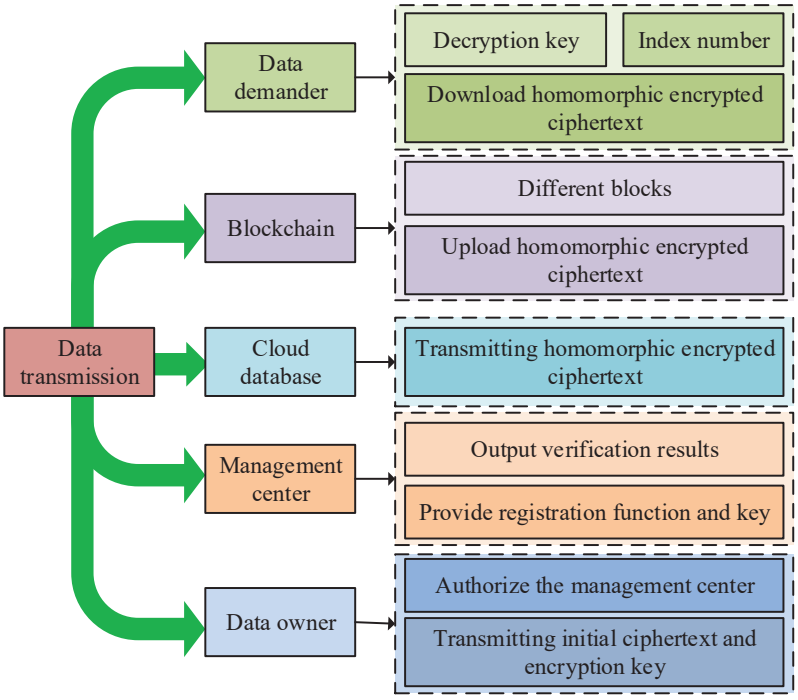

Figure 4 Model of data sharing protection scheme.

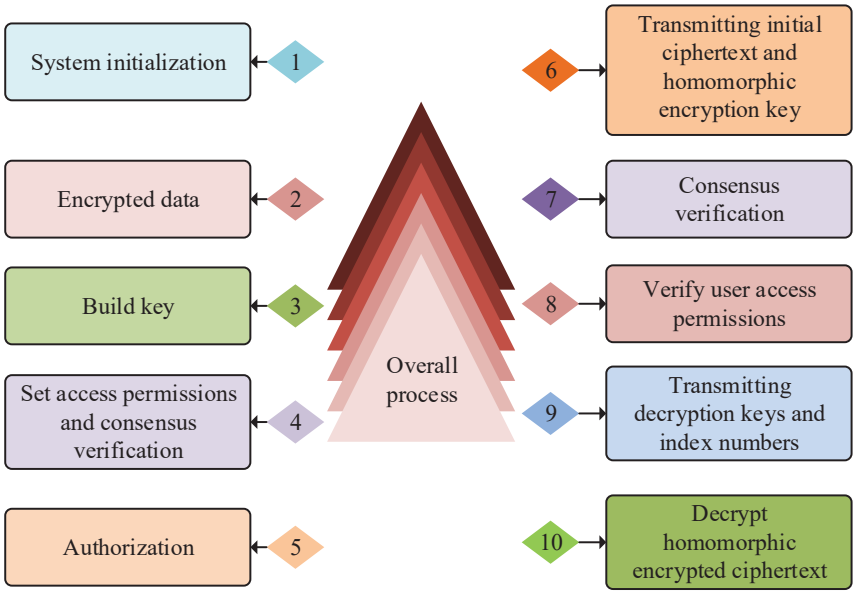

Figure 5 Overall process of data sharing protection scheme.

entity is the blockchain, which consists of different blocks and is required to upload homomorphically encrypted ciphertext to the cloud database. The third entity is the cloud database, while the fourth entity is the management center. The management center needs to output verification results to the blockchain and provide registration functions and keys to both the data requester and the owner, respectively. The fifth entity is the data owner, who needs to authorize the management center and transmit the initial ciphertext and encryption keys to the blockchain. The overall process of the data sharing protection scheme is illustrated in Figure 5.

From Figure 5, the process of this method encompasses system initialization, data encryption, key generation, access permission setting, and consensus verification, among others. Among them, system initialization ensures the correctness and security of system parameters, while the stages of data encryption and key generation provide core support for data privacy protection. Through this series of processes, the research can enhance the efficiency and reliability of data sharing. The construction details of the data sharing protection scheme are shown in Figure 6.

From Figure 6, system initialization includes determining security parameters, generating public-private key pairs, and user registration. Data

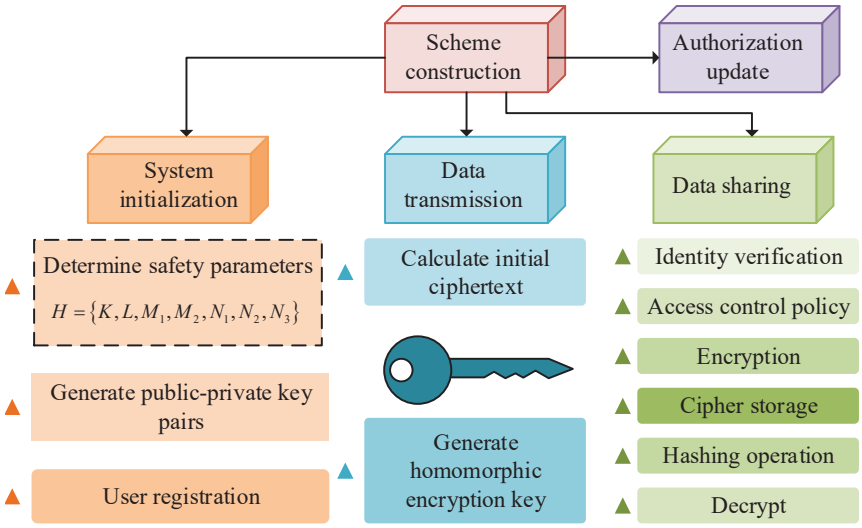

Figure 6 Construction details of data sharing protection scheme.

transmission involves calculating the initial ciphertext and generating homomorphic encryption keys. Data sharing encompasses identity verification, access control policy implementation, encryption, ciphertext storage, hash computation, and decryption. Among them, the set of system parameters is

$$H = \{K, L, M_1, M_2, N_1, N_2, N_3\} \tag{10}$$

where M_1 and M_2 represent cyclic groups, L is the generator of the cyclic group N_1, N_2, and N_3 are hash functions. Additionally, N_1 combines SHA-256 with elliptic curve mapping to ensure the irreversibility of identity information. N_2 is primarily used for generating verifiable tags, while N_3 is responsible for the mapping transformation of attribute sets. By incorporating a triple-hash mechanism, the aim is to reduce the risk of collisions. In user registration, the generation expression for the pseudonym O'_P is [23]

$$O'_P = O_P \oplus N_1(Q_P R_P) \tag{11}$$

where P represents the data owner, Q_P denotes a temporary private key, R_P is the public key, $\oplus$ stands for the exclusive-OR operation, and O_P represents the real identity identifier. The expression for the temporary public key S_P is [24]

$$S_P = Q_P L \tag{12}$$

The verifiable hash tag U_P is

$$U_P = N_2(O'_P \| O_P \| S_P V_A) \tag{13}$$

where V_A represents a timestamp and $\|$ is a concatenation symbol. By comparing the real identity identifier with the hash computation result, the management center can verify the validity of the user's identity. During data transmission, the research employs data aggregation and the Paillier homomorphic encryption algorithm, with the homomorphic encryption key generated through public key interaction by the data owner. Regarding the access control policy, the policy set is

$$W = \langle W_1, W_2, W_3, \ldots, W_x \rangle \tag{14}$$

where W_x represents the xth policy subset, $x \in [1, X]$, and X denotes the total number of policies. Generally, an access request can only be approved if at least one policy subset is satisfied. Furthermore, the expression for W_x is

$$W_x = \langle Y, Z, g, t, r \rangle \tag{15}$$

where Y represents a set of attributes, Z indicates the minimum number of attributes that must be satisfied, r denotes environmental variables, g refers to the specific operations performed on P, and t represents the duration for which the data is operated upon. The process of Paillier-DTSP scheme is shown in Figure 7.

From Figure 7, the process of Paillier-DTSP scheme mainly includes system initialization, key generation, data collection, data encryption, aggregation stage, consensus verification and fault tolerance stage, blockchain

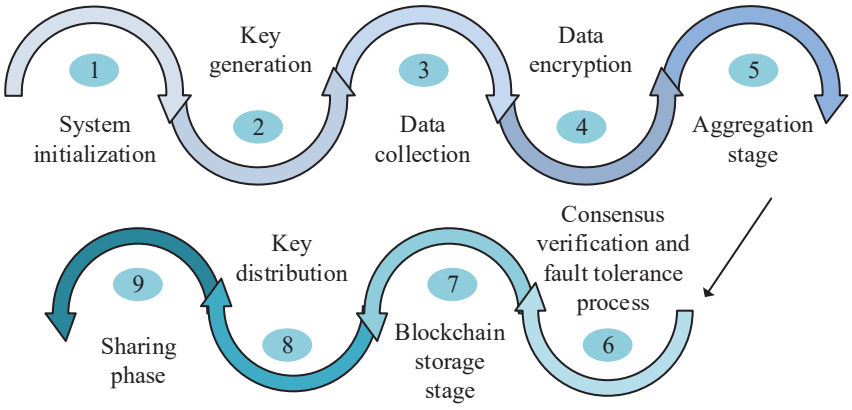

Figure 7 Process of Paillier-DTSP scheme.

storage stage, key distribution, and sharing stage. Among them, the system initialization process is led by the management center, which determines the set of security parameters including loop groups and hash functions. In the key generation process, the smart meter autonomously generates Paillier homomorphic encrypted local public and private key pairs based on the security parameters determined by system initialization. The public key is used for subsequent data encryption and synchronized to the management center for filing, while the private key is kept locally to avoid leakage. Through these processes, a full chain protection can be built from parameter security configuration, data encryption aggregation to blockchain authentication and controllable sharing, providing technical support for efficient processing and secure application of smart grid data while ensuring the privacy of diverse heterogeneous power data. The calculation of communication overhead is

$$\partial = \beta + \chi + \delta + \varepsilon \tag{16}$$

where ∂ represents communication overhead, β represents data transmission volume, χ represents protocol overhead, δ represents encryption overhead, and ε represents transmission loss.

3 Performance Analysis of Paillier-based Data Aggregation

To verify the performance of the data protection scheme designed in the research, an experimental environment was constructed, followed by a comparison of different schemes. Regarding the comparison metrics, the research took into account communication overhead, computational overhead, data transmission performance, and data security performance, among others.

3.1 Construction of Experimental Environment

To verify the performance advantages of the "Encryption Aggregation Chain Integration" architecture, this study constructed a fair and fully controlled evaluation environment to ensure that Paillier DTSP was compared with all baseline schemes (traditional RSA, AES, ElGamal encryption, TCP/UDP/MQTT transmission protocols) under identical hardware, software, network, and data conditions, eliminating the interference of environmental differences on performance results. The specific control conditions are as follows.

The experiment was conducted on an Ubuntu 22.04 LTS server cluster consisting of 12 Dell PowerEdge R750 servers. Each server was configured

with dual Intel Xeon Gold 6330 processors (28 cores at 2.1 GHz), 128 GB of DDR4 ECC memory, and a 1 TB NVMe SSD, interconnected via 10 Gigabit Ethernet. The software environment included JDK 17, Python 3.10, and Go 1.20. The Paillier cryptosystem was implemented using Python-Paillier 1.3, blockchain nodes were based on Hyperledger Fabric 2.5 with the Practical Byzantine Fault Tolerance consensus algorithm, and smart contracts were written in Go. The network layer was constructed using Mininet to create a three-tier topology: 5000 smart meters (simulated by Raspberry Pi 4B devices), 20 data collection stations, and five consortium blockchain nodes. All experiments were repeated 10 times, and the average values were taken. The testing tools included Locust for generating concurrent traffic, and Wireshark and iPerf3 for collecting network metrics. Computational overhead, latency, and throughput were monitored in real time using Prometheus and Grafana.

In the Paillier-DTSP scheme, the assumption between smart meters and data stations was that the meters were pre-authenticated by a trusted root institution, only legitimate devices could access them, encrypted data were transmitted with a private key signature and, once verified, the data were deemed not tampered with and the meters complied with encryption and reporting logic. Assumption between data station and blockchain nodes is as follows. Only authorized entities deployed nodes, and the data station's upload of evidence information with a valid signature was considered authentic. There was no direct interaction between smart meters and blockchain nodes. Assume that the meters indirectly trust the certificate through the on-chain results forwarded by the data station, and the key update instructions forwarded by the data station came from legitimate nodes. The sampling frequency of smart meter data is 15 minutes per time, and the collection time points are aligned with Beijing time 00:15, 00:30,. . . ,23:45. The meter register data is read through Modbus TCP protocol, and the data cache adopts a circular queue (capacity of 100). For data encryption and upload, the delay of electricity meter encryption is controlled within 5 ms. After encryption is completed, a 2-byte checksum is added and uploaded to the data collection station through the MQTT3.1.1 protocol with a QoS level of 2. The simulation power dataset and simulation parameter details are as follows.

The synthetic dataset was generated based on the typical daily electricity characteristics of a provincial power grid in 2024, covering five types of users, namely residential, commercial, industrial, photovoltaic, and energy storage, with a total of 100,000 devices. Each device had a sampling frequency of 15 minutes per time, and a single data contained timestamp, device ID,

active power (0.2–500 kW), reactive power (0.1–200 kVar), and voltage (220–380 V) fields. It was generated through Python code, and the code included parameter configuration comments. The simulation environment was an Ubuntu 22.04 system, with a Central Processing Unit (CPU) of Intel Xeon Gold 6330 (2.0 GHz), 64 GB of memory, and encryption operations based on the OpenSSL library. Information accuracy refers to the consistency rate between decrypted data and the original collected data. The calculation formula is as follows.

Information accuracy = (number of correctly decrypted data entries/total number of data entries) $\times$ 100%. The judgment standard is that a numerical error of $\leq$3% is considered correct. The success rate indicator of this paper strictly follows IEEE Std 1687-2014, defined as the ratio of the number of successful attacks to the total number of experiments. Calculation formula is attack success rate = (number of successful attacks/total number of experiments) $\times$ 100%. The experimental environment is an Ubuntu 22.04 server cluster, repeat the experiment four times, and take the average value. Attack scenarios include internal threats, collusion attacks, replay attacks, and differential privacy breaches. Judgment criteria are: (a) Internal threat: Obtaining plaintext data from unauthorized users with an error of $\leq$3%; (b) Collusion attack: $\geq$3 semi-trusted nodes collude to decrypt aggregated ciphertext; (c) Replay attack: Repeatedly sending intercepted data and passing verification; (d) Differential privacy breach: Accurately infer specific user electricity usage patterns with an error of $\leq$5%. The experimental scenario parameters are shown in Table 1.

For the gradient of experimental user scale, the study referred to the typical user scale of China's provincial power grid and selected a 500$\sim$6000 user gradient that can cover small and medium-sized pilot scenarios. The scalability verification of the scheme is shown in Table 2.

From Table 2, it can be seen that as the user base gradually expands from 500 households to 6000 households, the performance indicators of the scheme show a steady trend of change: the computational cost increases from 28.6 m/s/batch to 64.8 m/s/batch, the communication cost increases from 89.2 KB/10 minutes to 267.9 KB/10 minutes, and the end-to-end latency increases from 42.3 ms to 85.7 ms, all of which show a linear growth and a moderate growth rate; The accuracy of data transmission slowly decreased from 99.1% to 97.3%, the packet loss rate gradually increased from 0.12% to 0.45%, and the core performance indicator attenuation was controlled within a reasonable range. This data fully verifies the excellent scalability of the Paillier DTSP scheme. With a 12-fold increase in user scale, there is no

Table 1 Experimental scenario parameters

Experimental Scenario	Number of Nodes	Hardware Specifications	Measurement Setup
Small-scale performance verification (5000 devices)	Smart electric meters: 5000 units Data collection stations: 20 Consortium chain nodes: 5	Smart meter: Raspberry Pi 4B (Broadcom BCM2711 quad-core processor, 4 GB LPDDR4 memory) Data collection station/consortium chain node: Dell PowerEdge R750 server (dual Intel Xeon Gold 6330 processors, 28 cores at 2.1 GHz, 128 GB DDR4 ECC memory, 1TB NVMe SSD)	Network environment: Stable LAN (10 Gbps fixed bandwidth) Test duration: 30 minutes/group Number of repetitions: 10 times (average value taken) Measurement indicators: computation overhead, communication overhead, encryption/decryption delay
Large-scale data transmission verification (100,000 devices)	Simulation equipment: 100,000 units Data acquisition stations: 20 Edge computing nodes: 8 Number of consortium chain nodes: 8	Simulation equipment: Dell PowerEdge R750 server cluster for distributed simulation	Network environment: Hybrid network (LAN+WAN, bandwidth fluctuating between 1-10 Gbps) Test duration: 24 hours/group (covering peak and off-peak electricity usage periods) Number of repetitions: 10 times (average value taken) Measurement indicators: transmission accuracy, packet loss rate, and data integrity verification success rate

Table 2 Scalability verification of the scheme

User Scale/ Household	Calculation Cost (Data Collection Station, ms/batch)	Communication Expenses (KB/10 minutes)	End to End Latency/ms	Data Transmission Accuracy/%	Packet Loss Rate/%
500	28.6	89.2	42.3	99.1	0.12
1000	32.1	105.7	47.5	98.8	0.15
2000	38.5	136.4	55.8	98.5	0.21
3000	45.2	168.9	63.4	98.2	0.27
4000	51.7	201.3	70.6	97.9	0.33
5000	58.3	234.6	78.2	97.6	0.39
6000	64.8	267.9	85.7	97.3	0.45

Table 3 Code for generating synthetic datasets

```
import pandas as pd
import numpy as np
from datetime import datetime
np.random.seed(42)
ts = pd.date_range(datetime(2024,1,1), datetime(2024,1,2), freq='15min')[:-1]
u = {"res":(40000,(0.2,5),(220,230)),"com":(25000,(5,50),(225,235)),"ind":(20000,(50,500),
(380,380)),"pv":(10000,(0.5,100),(220,240)),"es":(5000,(10,200),(230,240))}
d=[]
for tpe,(cnt,ap,v) in u.items():
    for dev in range(1,cnt+1):
        for tm in ts:
            bap = np.random.uniform(*ap)
            apv = bap*(1.3 if (tpe=="res" and (7<=tm.hour<=9 or 18<=tm.hour<=22))
else 1.4 if (tpe=="com" and 9<=tm.hour<=21) else 1.7 if (tpe=="pv" and 10<=tm.hour
<=14) else 0.8 if tpe=="es" else 1.0)
            d.append([tm,f"{tpe}_{dev:05d}",round(apv,2),round(apv*0.5,2),round
(np.random.uniform(*v),1)])
pd.DataFrame(d,columns=["timestamp","device_id","active_kW","reactive_kVar",
"voltage_V"]).to_csv("grid_2024_data.csv",index=False)
```

sudden change in key performance indicators, and performance degradation remains at a low level, fully meeting the deployment needs of small-scale pilot scenarios in smart grids. The generation code for the synthetic dataset is shown in Table 3.

Based on the above fair and controlled environment, subsequent comparative experiments were conducted under the condition of no additional variable

interference, ensuring that the performance difference between Paillier DTSP and the baseline scheme is only due to architecture design and algorithm optimization, rather than environmental factors, thus effectively verifying the core advantages of the "encryption aggregation on chain integration" architecture.

3.2 Comparative Analysis of Communication and Computing Overhead of Different Schemes

To verify the computational efficiency advantages of the proposed Paillier-homomorphic-encryption-based data aggregation scheme, the research employed a comparative experimental approach. It conducted a comprehensive comparison of the computational overhead of the Paillier-DTSP scheme against traditional Rivest-Shamir-Adleman (RSA) encryption, traditional AES encryption, and ElGamal encryption schemes under varying user scales. The results are shown in Figure 8.

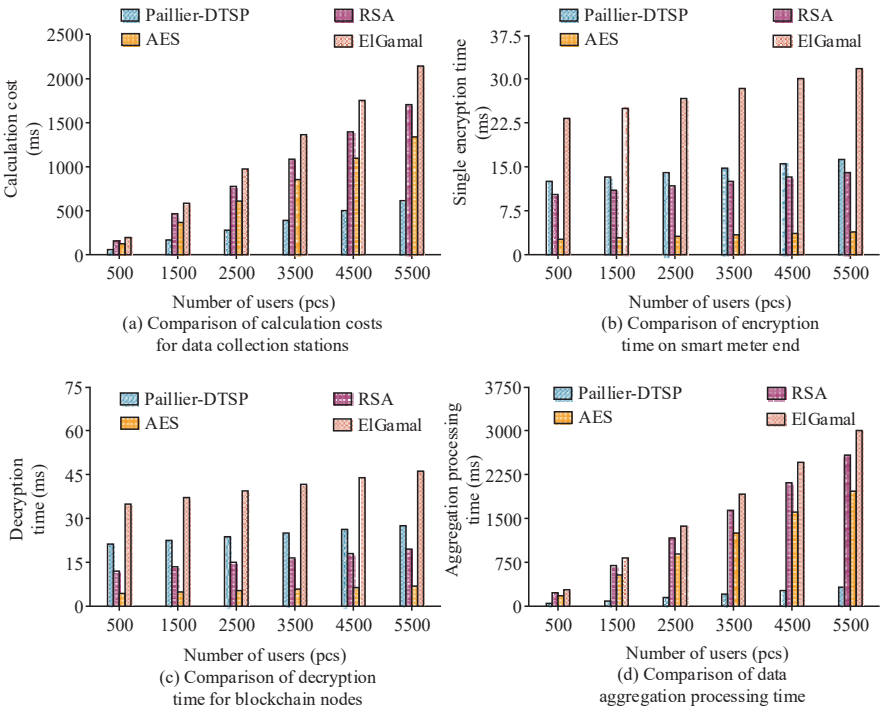

Figure 8 Comparison of computational costs of different schemes under different user sizes.

As seen in Figure 8(a), as the number of users increased from 500 to 6000, the computational overhead at data collection stations for all schemes exhibited an upward trend. However, the growth rate of Paillier-DTSP was significantly lower than that of other traditional schemes. At a user scale of 5000, the computational overhead of Paillier-DTSP was only 35.6% of that of the traditional RSA scheme, representing reductions of 62.3% and 58.7% compared to the traditional AES and ElGamal schemes, respectively. From Figure 8(b), it can be observed that in terms of encryption time at smart meter endpoints, although Paillier-DTSP had a slightly longer single-encryption time than the AES scheme, it significantly outperformed the RSA and ElGamal schemes. Figure 8(c) shows that, regarding decryption time at blockchain nodes, Paillier-DTSP, due to its homomorphic encryption properties, maintained relatively stable decryption times that did not increase linearly with the number of users, in stark contrast to traditional schemes. As depicted in Figure 8(d), the data aggregation processing time represented the greatest advantage of Paillier-DTSP. Thanks to its support for encrypted aggregation operations, the processing time was only 20–30% of that of traditional schemes. In addition, the main reason why AES has a higher computational cost than Paillier in data stations is due to different application scenarios and operation modes. AES, as a symmetric encryption algorithm, can only achieve data encryption and decryption and does not support homomorphic operations. Therefore, in data aggregation scenarios, it is necessary to decrypt each user ciphertext one by one, then perform plaintext aggregation, and finally re encrypt. Multiple encryption and decryption operations bring a lot of redundant calculations. As an additive homomorphic encryption algorithm, Paillier supports direct accumulation of ciphertexts and can complete aggregation without decrypting individual data one by one, greatly reducing the number of large number operations and repetitive operations. Therefore, in multi-user data aggregation scenarios, the overall computational cost of AES is significantly higher than Paillier.

To comprehensively evaluate the performance of different communication schemes within the three-tier architecture of smart grids, the research designed multi-dimensional communication performance testing experiments. These experiments compared the communication overhead and network latency of the proposed Paillier-DTSP with traditional schemes such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Message Queuing Telemetry Transport (MQTT) under varying network conditions. The transmission layer of all comparison schemes was unified to MQTT protocol (version 3.1.1), implemented based on TCP/IP protocol

stack, ensuring layer matching. In terms of data volume, the size of a single power data was uniformly 1 KB, including timestamp, device ID, active power, reactive power, and voltage fields, ensuring consistent data carrying capacity. In terms of message format, JSON format was used to encapsulate data, and the field naming, order, and encoding methods were completely unified. On the security layer, Transport Layer Security (TLS 1.3) was enabled. In addition, the network topology structure was the same and the same network environment was uniformly used. Comparison of communication overhead and network latency of different schemes under different network conditions is shown in Figure 9.

As seen in Figure 9(a), during the communication from smart meters to data collection stations, the proposed Paillier-DTSP reduced communication overhead by 28.7% compared to the traditional TCP scheme. From Figure 9(b), it can be observed that in the communication performance tests from data collection stations to blockchain nodes, Paillier-DTSP significantly

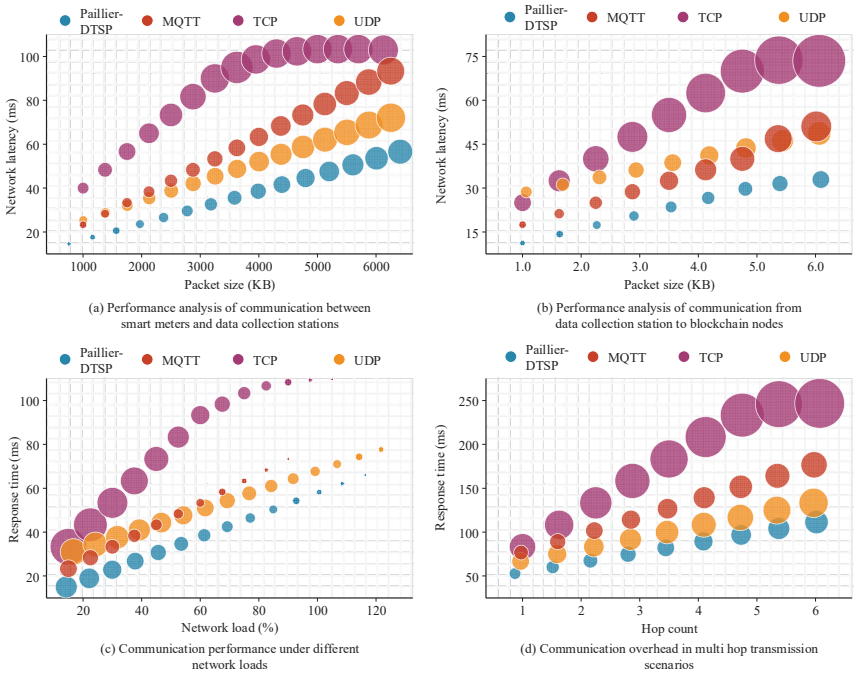

Figure 9 Comparison of communication overhead and network latency of different schemes under different network conditions. *Note*: bubble size indicates the communication cost/cumulative throughput cost.

Table 4 Comparison of the proposed solution with MQTT in terms of payload expansion, latency, and other indicators

Comparison Metrics	Paillier-DTSP	MQTT	Discrepancy Rate
Payload expansion amount (bytes/entry)	128	64	−100%
End-to-end delay (ms)	85	62	−37.10%
Throughput (MB/s) at 10% network load	4.32	3.89	11.05%
Throughput (MB/s) at 120% network load	3.15	2.07	52.17%
Multi-hop (5 hops) transmission overhead (KB)	22.5	99.8	−77.45%

reduced the volume of transmitted data through data aggregation techniques. Under the same packet size conditions, its communication overhead was 35.2% lower than that of the UDP scheme, 41.8% lower than that of the MQTT scheme, and 52.3% lower than that of the traditional TCP scheme. As depicted in Figure 9(c), under varying network load conditions, when the network load increased from 10% to 120%, Paillier-DTSP exhibited the smallest increase in average response time and maintained relatively stable data throughput. From Figure 9(d), it is evident that in multi-hop transmission scenarios, Paillier-DTSP had the lowest growth rate in communication overhead as the number of hops increased, with its communication overhead at 5-hop transmission being only 22.5% of that of the traditional TCP scheme. The comparison between the proposed scheme and MQTT in terms of payload expansion, latency, and other indicators is shown in Table 4.

In terms of positive indicators of throughput, a higher value was better. However, for negative indicators such as latency, payload expansion, and multi-hop transmission overhead, a lower value was preferable. As can be seen from Table 4, in terms of throughput, the Paillier-DTSP scheme significantly outperformed the traditional MQTT scheme. For example, when the network load was 10%, the throughput of Paillier-DTSP was 4.32 MB/s, an increase of 11.05% compared to MQTT's 3.89 MB/s, demonstrating strong load resistance. In terms of negative indicators, Paillier-DTSP had a payload expansion of 128 bytes per message, a 100% increase compared to MQTT's 64 bytes per message, while its end-to-end latency was 85 ms, 37.10% higher than MQTT's 62 ms. The higher payload expansion of Paillier-DTSP compared to traditional MQTT was due to the addition of encrypted fields, but the overall transmission overhead was reduced through data aggregation technology. The slightly higher latency was a reasonable price to pay for encryption operations, and the significant throughput advantage under high load scenarios met the practical application requirements of smart grids.

3.3 Comparative Analysis of Data Transmission Performance of Different Schemes

To verify the data transmission reliability of the proposed scheme under complex network environments, the research designed a multi-dimensional heterogeneous power data transmission quality testing experiment. By comparing the transmission accuracy, packet loss rate, and data integrity verification success rate of Paillier-DTSP with those of the traditional TCP scheme under varying user scales and network conditions, the results were obtained as shown in Figure 10.

Figures 10(a)–10(c) are presented using a combination of box plots and kernel density estimation: box plots show the interquartile range and median of the data, while kernel density curves show the distribution density of the data. The box represents the upper and lower quartiles, the center line is the median, the contour line represents the normal range of data, and the outlier points are separately labeled to clearly distinguish the data dispersion and outlier values under different user sizes. As seen in Figure 10(a), as the number of

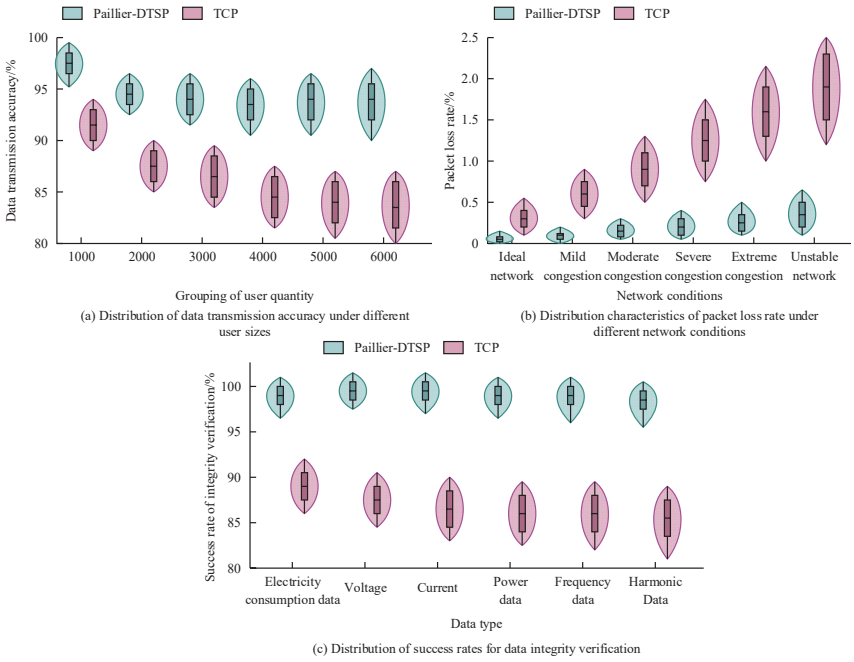

Figure 10 Comparison of transmission accuracy, packet loss rate, and data integrity verification success rate among different schemes.

users increased from 1000 to 6000, the data transmission accuracy of Paillier-DTSP consistently remained above 90%, with a relatively concentrated data distribution and a small standard deviation, indicating that the scheme offered good stability and predictability, representing an 8.5% improvement over the traditional TCP scheme. From Figure 10(b), it can be observed that under varying network congestion conditions, the packet loss rate of Paillier-DTSP was consistently controlled below 0.5%. Even in extremely congested and unstable network environments, the packet loss rate did not exceed 0.8%, significantly outperforming other schemes. As depicted in Figure 10(c), for different types of power data, the integrity verification success rate of Paillier-DTSP consistently remained above 96%. To evaluate the blockchain-based data integrity verification mechanism and fault tolerance capabilities, the research designed performance testing experiments across multiple dimensions, including Byzantine fault tolerance, data integrity verification, network partition recovery, and security attack protection, with the results shown in Figure 11.

As seen in Figure 11(a), the system maintained 100% availability when the proportion of Byzantine nodes was below 33%. When the proportion of Byzantine nodes reached the theoretical threshold of 33%, system availability began to decline significantly but still remained above 85%. From Figure 11(b), it can be observed that in the data integrity verification mechanism,

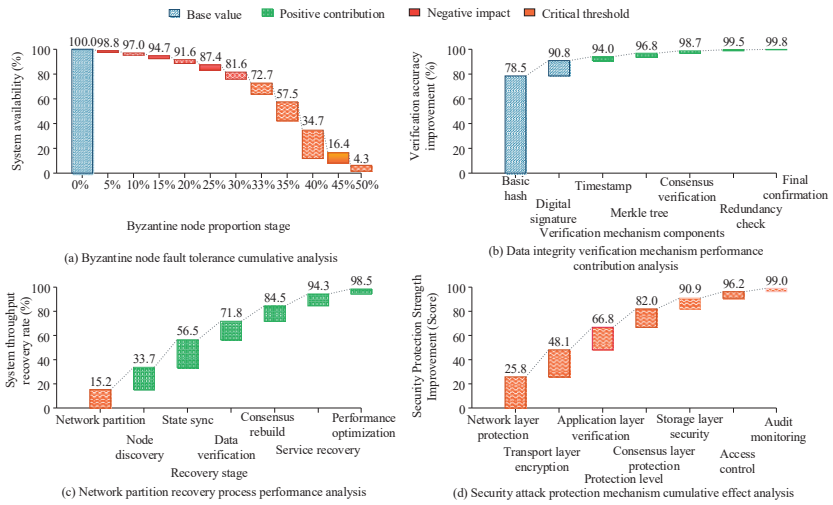

Figure 11 Performance evaluation of data integrity verification and fault tolerance mechanism based on blockchain.

basic hash verification contributed a 35% improvement in accuracy, while digital signatures and timestamps contributed 25% and 15%, respectively. Merkle tree verification contributed 12%, and consensus verification and redundancy checks contributed 8% and 5%, respectively. The synergistic effect of these components resulted in an overall verification accuracy rate of 99.8%. As depicted in Figure 11(c), during the network partition recovery process, the system was able to restore its performance within a relatively short time, demonstrating good self-healing capabilities. From Figure 11(d), it is evident that among the multi-layered security protection mechanisms, transport layer encryption and consensus layer protection were the most critical measures, contributing security strength improvements of 30 points and 25 points, respectively.

3.4 Comparative Analysis of Data Security Performance of Different Schemes

To thoroughly assess the security performance of the Paillier homomorphic encryption algorithm, we conducted a series of security strength tests targeting various attack methodologies. In terms of threat model, the study adopted an adaptive selection plaintext attack mode. The definition of the threat subject and its capability boundaries is as follows. Firstly, in terms of attacker types, they included external malicious attackers, semi-trusted internal entities (such as data collection station operation and maintenance personnel), and collusion nodes (up to a maximum of 33% of the total number of blockchain nodes). Secondly, in terms of available resources, it included public parameters, ciphertext corresponding to any plaintext, ciphertext data in network transmission, and publicly available algorithm implementation details. Thirdly, on the target of the attack, plaintext data, private keys, or sensitive user information could be obtained through brute-force cracking, factorization, lattice attacks, quantum attacks, replay attacks, collusion attacks, and other methods. Fourthly, in terms of restrictions, attackers did not have unlimited computing resources and cannot tamper with data already on the blockchain, thus lacking the ability to break through the TLS 1.3 secure transport layer. In terms of calculation assumptions, there were a total of three. The first one was the core assumption, which was based on the assumption of difficulty in large number decomposition and the assumption of discriminative composite residue classes. The second assumption was quantum computing, which cannot effectively crack keys of 2048 bits or more in the short term, and quantum attacks only target the mathematical

foundations of classical cryptography, such as large number factorization. The third assumption was lattice attack, where attackers use standard lattice-based reduction algorithms to launch attacks. Through an analysis of how factors such as key length, attack duration, computational resource allocation, and security parameters influenced the algorithm's resilience against attacks, and by utilizing logarithmic coordinate systems and multi-faceted evaluation techniques, the study validated the algorithm's protective effectiveness against threats like brute-force cracking, factorization attacks, lattice attacks, and quantum attacks.

The 256-bit security level determination of this scheme is strictly based on the international standard ISO/IEC 18033-6:2023 "Information technology security technology – Encryption algorithms – Part 6: Digital signatures based on asymmetric technology" in the field of cryptography. This standard specifies that for public key encryption algorithms based on the problem of large integer factorization, there is a mapping relationship between their security level and key length. The equivalent security strength of symmetric encryption for 2048-bit keys is 256 bits [25]. The Paillier algorithm in this study adopts a 2048-bit key design, which fully meets the technical requirements of the 256-bit security level in this standard. Meanwhile, this conclusion is supported by NIST SP 800-57 Part 1 Rev. 5 "Key Management Recommendations" [26]. Under the current level of quantum computing technology, for Paillier encryption based on the difficult problem of large integer factorization, a 2048-bit key could withstand existing quantum attack methods (refer to NIST IR 8309 report) [27]. Meanwhile, this conclusion is supported by IEEE Std 1363.1-2022 "Public Key Cryptography Part 1: General Requirements and Integer based Cryptography" [28]. Grid attack testing referred to simulating attack scenarios based on the grid reduction algorithm to verify the security of the scheme in the face of grid attacks. Long-term resolution estimation refers to a solution that can ensure secure storage and transmission of power grid data for more than 10 years in a classical computing environment. Paillier homomorphic encryption algorithm security strength and anti-attack capability test are presented in Figure 12.

As seen in Figure 12(a), as the key length increased from 512 bits to 3328 bits, the complexity of various types of attacks grew exponentially, with brute-force attacks showing the most significant increase in complexity. The complexity of lattice attacks and quantum attacks fell between these two extremes, validating the effectiveness of increasing key length in enhancing security strength. From Figure 12(b), it can be observed that in sustained attack tests, even after 216 hours of brute-force attacks, the

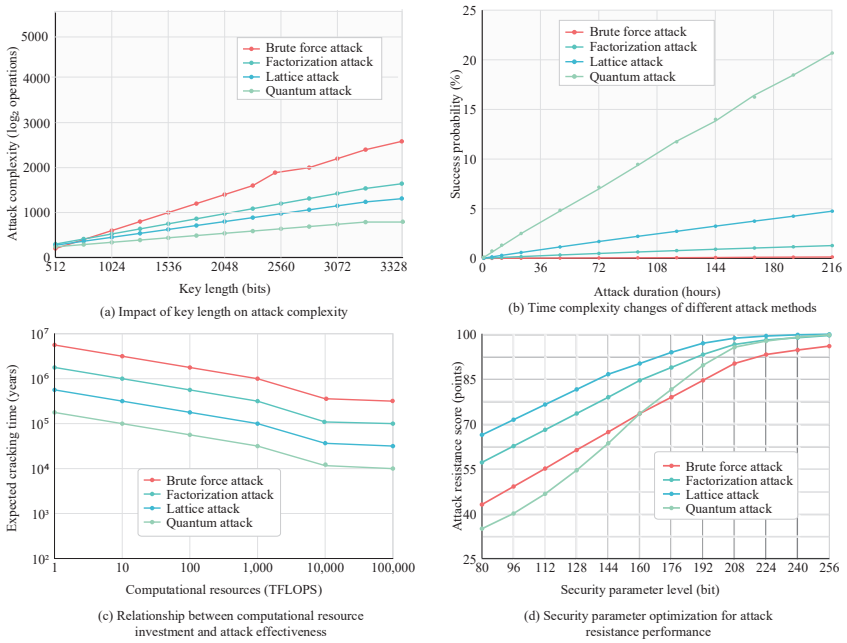

Figure 12 Paillier homomorphic encryption algorithm security strength and anti-attack capability test.

success probability remained below 0.01%, demonstrating exceptionally strong resistance to attacks overall. As depicted in Figure 12(c), even with the deployment of 1 million TFLOPS of computational resources, brute-force attacks would still require over 104 years to succeed, proving the algorithm's security against attacks leveraging large-scale computational resources. From Figure 12(d), it is evident that the system exhibited excellent overall security performance under various attack scenarios. The comprehensive security assessment results for the smart grid data privacy protection scheme are shown in Figure 13.

As seen in Figure 13(a), Paillier-DTSP demonstrated the most outstanding performance in terms of data security capabilities, with an encryption strength reaching 256 bits, a data integrity verification success rate of 99.8%, and an access control accuracy of 98.5%, ranking the highest among all compared schemes and validating its superiority in fundamental security performance. From Figure 13(b), it can be observed that in terms of privacy leakage protection capabilities, Paillier-DTSP achieved a data anonymization coverage rate of 98.5%, an identity information masking rate of 99.2%, and

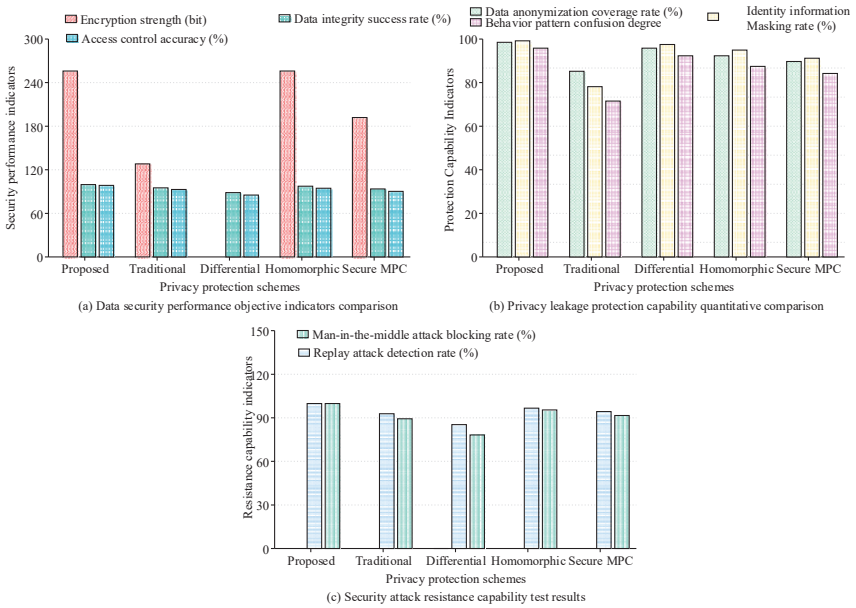

Figure 13 Comprehensive security evaluation of smart grid data privacy protection scheme.

a behavioral pattern obfuscation degree of 96.8%, all of which outperformed other schemes. The proposed model had a high degree of behavioral pattern confusion, which could mask the user's electricity consumption patterns, avoid malicious attacks, and retain the value of data analysis, which was beneficial for the operation of the power grid. Although the access control accuracy of this model was on par with traditional methods, its significantly improved encryption strength could prevent data cracking and resist quantum attacks, making it the last barrier to data security and necessary for long-term security of the power grid. As depicted in Figure 13(c), Paillier-DTSP exhibited remarkable performance in security attack resistance tests, with a replay attack detection rate of 99.6% and a man-in-the-middle attack blocking rate of 99.8%.

To further validate the performance of Paillier-DTSP, the study supplemented its resistance to internal threat models and other common attacks. Among them, the internal threat model referred to the situation where the data collection station was compromised and, at this time, the management center entity was fully trusted, while the alliance chain nodes, smart meters, and data collection station entities were semi-trusted. Meanwhile, data demanders judged trustworthiness based on authorization status, while external attackers

were completely untrustworthy. Common attacks included collusion attacks, replay attacks, and differential privacy leakage risk. Among them, differential privacy leakage risk referred to the attack scenario where attackers used the statistical distribution differences of different datasets to infer sensitive electricity consumption information of specific users. In terms of evaluation indicators, the study selected the probability of successful attack.

The definition of a successful attack is as follows: (a) Internal threat model: After gaining control of the data collection station, the attacker successfully acquired plaintext data of unauthorized users; (b) Collusion attack: Three or more semi-trusted nodes colluded to successfully decrypt the aggregated ciphertext; (c) Replay attack: The attacker repeatedly sent intercepted encrypted data and successfully passed the identity verification; (d) Differential privacy leakage: By analyzing the statistical distribution differences between different datasets, the electricity usage pattern of a specific user is accurately inferred (with an error rate of $\leq$5%).

The "attack success rate" indicator used in this study strictly follows the reliability testing specifications in IEEE Std1687-2014 "Integrated Circuit Testability Design Standard", defined as the ratio of successful attack times to total experimental times. It is a classic quantitative indicator for evaluating the anti-attack capability of cryptographic schemes. Its rationality is mainly based on three core arguments:

Firstly, the definition of indicators is in line with the essence of the attack scenario. Clarify the specific criteria for determining a "successful attack" in different scenarios such as internal threats, collusion attacks, replay attacks, and differential privacy breaches, in order to avoid indicator ambiguity and ensure the correlation between indicators and actual threats. For example, in an internal threat scenario, obtaining plaintext data from unauthorized users (including core power consumption information such as power and reactive power, with a data error of $\leq$3%) is considered successful.

Secondly, the experimental design ensures the objectivity of the indicators. Four independent experiments are set up for each attack scenario, covering different types of attacks. The experimental results are rounded to two decimal places to reduce the impact of random errors. This design complies with the requirements of "multi scenario repeated testing" in NISTSP800-137 "Guidelines for Continuous Certification of Information Systems" to ensure the reliability of indicator data.

Thirdly, the comparison of indicators has industry reference value. The numerical range of attack success rate (0–100%) intuitively reflects the anti-attack capability of the scheme, making it easy to compare horizontally

with classical schemes such as RSA and AES in existing literature. The core design of the differential privacy component in this scheme is to incorporate Laplacian noise into the Paillier encryption process, balancing the hiding of individual sensitive data and the preservation of dataset statistical characteristics. This is achieved through the collaborative implementation of three major modules: noise generation, injection, and statistical calibration. The noise generation module generates noise based on Laplace distribution, and the injection mechanism adds the noise to the original electricity consumption data before encryption at the smart meter end, ensuring that the two are tightly bound and inseparable. The statistical calibration module uses noise cancellation algorithm to eliminate redundancy during the data aggregation stage, ensuring that the total electricity consumption error in the region is $\leq$2%. This component forms a dual protection of "ciphertext protection+privacy obfuscation" with Paillier encryption. Paillier encryption ensures transmission and storage security, while differential privacy prevents attackers from inferring individual information through "adjacent dataset comparison". Paillier's homomorphic addition feature supports ciphertext aggregation and Laplace noise to ensure stable data statistical indicators, meeting the needs of power grid data analysis. The corresponding differential privacy leakage risk "attack success rate" refers to the probability of attackers accurately inferring the target user's electricity consumption pattern (error rate $\leq$5%) by comparing the aggregated results of datasets with/without the target user. The comparison of attack success probabilities for different schemes under different attacks is shown in Table 5.

From Table 5, in different attack scenarios such as internal threat models, collusion attacks, replay attacks, and differential privacy issues, the Paillier-DTSP scheme had significantly lower attack success probabilities compared to RSA, AES, and ElGamal schemes. For example, in the four experiments of the internal threat model, the highest success probability of Paillier-DTSP attack was only 6.34%, far lower than RSA's 38.56%, AES's 30.67%, and ElGamal's 32.78%. In experiments related to differential privacy issues, the success probability of Paillier-DTSP attacks also remained at a low level, with the highest being 11.46%, while other schemes generally exceeded 40%. This indicated that the Paillier-DTSP scheme had better security performance in resisting various common attacks, and could better ensure the security of diverse heterogeneous power data in smart grids. To better verify the performance of Paillier-DTSP, the study selected three latest Paillier hybrid algorithms from 2023 to 2025 for comparison. These schemes were hybrid algorithm 1 combining client access control, federated learning, and

Table 5 Comparison of attack success probabilities for different schemes under different attacks

	Internal Threat Model				Collusion			
	Number of Experiments				Number of Experiments			
Scheme	1	2	3	4	1	2	3	4
RSA	35.12%	32.34%	38.56%	36.78%	42.13%	45.24%	40.35%	43.46%
AES	28.23%	25.45%	30.67%	27.89%	35.34%	38.45%	33.56%	36.67%
ElGamal	30.34%	27.56%	32.78%	29.91%	38.45%	41.56%	36.67%	39.78%
Paillier-DTSP	5.12%	4.23%	6.34%	5.45%	8.13%	7.24%	9.35%	8.46%
	Replay attack				Differential privacy leakage risk			
	Number of experiments				Number of experiments			
Scheme	1	2	3	4	1	2	3	4
RSA	40.23%	37.45%	42.67%	39.89%	50.13%	47.24%	52.35%	50.46%
AES	32.34%	29.56%	34.78%	31.91%	42.34%	39.45%	44.56%	42.67%
ElGamal	35.45%	32.67%	37.89%	34.91%	45.45%	42.56%	47.67%	45.78%
Paillier-DTSP	6.23%	5.34%	7.45%	6.56%	10.24%	9.35%	11.46%	10.57%

Table 6 Comparison results between Paillier-DTSP and the latest Paillier hybrid algorithm

	Edge Device Encryption Delay/ms					Multi-hop (5-hop) Transmission Overhead/KB				
	Number of Experiments					Number of Experiments				
Method	1	2	3	4	5	1	2	3	4	5
Hybrid algorithm 1	18.35	17.92	18.51	17.78	18.14	89.77	91.22	88.90	90.58	90.14
Hybrid algorithm 2	15.67	16.12	15.89	16.33	15.97	78.53	79.37	77.94	78.81	79.11
Hybrid algorithm 3	16.23	15.89	16.45	15.98	16.12	82.37	83.14	81.82	82.66	82.29
Paillier-DTSP	4.82	5.03	4.76	5.11	4.98	22.36	22.79	22.52	22.47	22.63

Paillier, hybrid algorithm 2 combining Brakerski/Fan-Vercauteren Homomorphic Encryption Algorithm, integer optimization, and Paillier, and hybrid algorithm 3 combining Cheon-Kim-Kim-Song Homomorphic Encryption Algorithm, scale adjustment, and Paillier [29–31]. The comparison results between Paillier-DTSP and the latest Paillier hybrid algorithms are shown in Table 6.

As can be seen from Table 6, Paillier-DTSP's advantages in edge device encryption delay and multi-hop transmission overhead corresponded to its core originality: the average edge device encryption delay was only 4.94 ms, significantly lower than the 18.14 ms of Hybrid Algorithm 1, the 15.99 ms of Hybrid Algorithm 2, and the 16.13 ms of Hybrid Algorithm 3. This was because the Paillier-DTSP scheme optimized the computational complexity of the Paillier algorithm for 8-bit/16-bit single-chip smart meters, distinguishing itself from Hybrid Algorithms 1–3, which were not designed to accommodate resource-constrained devices. The multi-hop transmission

overhead of the Paillier-DTSP scheme was only 22.5 KB, reflecting an integrated "encryption-aggregation-on-chain" architecture, where encryption was directly followed by aggregation and then on-chain, avoiding the redundant transmission of traditional schemes where "encryption and aggregation are separated," while other hybrid algorithms lacked architectural coordination. Additionally, the three-level key management strategy supported secure key distribution under low latency, ensuring both edge device encryption efficiency and enhancing key security through quantum key distribution and TLS 1.3, which cannot be achieved with a single key management scheme. These performance advantages were not simply parameter optimization, but the embodiment of three originalities in the smart grid scenario, making the scheme both compatible with edge hardware and addressing privacy and transmission issues in traditional architectures.

To further improve the experimental design and verify comprehensiveness, this paper adds four security indicators: attack success rate, information leakage probability, passive eavesdropping protection rate, and active tampering detection rate. Four advanced solutions in the smart grid field, including error learning-based lattice based lightweight encryption, Ciphertext Policy Attribute Based Encryption (CP-ABE) attribute encryption, blockchain non aggregated transmission, and differential privacy plaintext aggregation, are selected for horizontal comparison. The experimental results are shown in Table 7.

As shown in Table 7, the attack success rate of the Paillier DTSP scheme in this paper is only 6.89%, and the information leakage probability is 7.15%, which is much lower than the error learning-based lattice based lightweight encryption, CP-ABE attribute encryption, blockchain non aggregated transmission, and differential privacy plaintext aggregation schemes. At the same time, Paillier DTSP has a passive eavesdropping protection rate of 99.23% and an active tampering detection rate of 99.86%, both significantly better than the comparative methods, and has the best comprehensive security performance. Paillier DTSP can effectively resist attacks and privacy breaches, providing more reliable security for smart grid power data.

3.5 Challenges Faced During Actual Deployment Process

To explore the challenges faced by the Paillier-DTSP solution in practical deployment, the study considered scenarios such as scaling to millions of devices, compliance requirements, interoperability standards, and deployment in resource constrained devices. Among them, for expanding to millions

Table 7 The effectiveness of different schemes in terms of resistance to attacks, probability of information leakage, passive eavesdropping, and active tampering

Plan	Attack Success Rate/%	Information Leakage Probability/%	Passive Eavesdropping Protection Rate/%	Active Tampering Detection Rate/%
Paillier DTSP	6.89	7.15	99.23	99.86
Grid based lightweight encryption based on error learning	28.45	32.67	82.13	84.59
CP ABE ciphertext policy attribute-based encryption scheme	25.36	29.41	85.72	86.33
Blockchain non aggregated secure transmission solution	22.18	26.79	88.45	90.12
Differential privacy plaintext aggregation scheme	31.62	35.88	78.69	76.41

of devices, a three-level aggregation architecture of "edge region global" was adopted, where edge nodes initially aggregated and compressed data, and the region layer performed secondary processing. Additionally, combining blockchain sharding and time-based uploading could reduce resource pressure. In addition, in large-scale deployment scenarios, Paillier's encryption key management strategy adopted a three-level hierarchical architecture of "root key area key device key". Among them, the root key was generated and stored offline by the Hardware Security Module of the management center, the area key was derived based on the root key through Hash based Message Authentication Code, and each area corresponded to a unique area key. The device key was derived from the area key, and each device corresponded to a dedicated key. The regional key was transmitted to the collection station through the Quantum Key Distribution network, and the device key was issued through the Transport Layer Security 1.3 security link combined with identity authentication. The root key was backed up according to the "3-2-1" rule, and the encrypted backup information of the region and device keys was stored on the chain to ensure that key loss could be quickly recovered.

For compliance requirements, Paillier encryption incorporated differential privacy noise, user authorization information hashing for on chain authentication, and quarterly third-party compliance audits. Moreover, in

Table 8 Performance of solutions under increased user numbers and resource constraints

	Number of Users/ten thousand								
Index	5	7	9	10	12	14	16	18	20
Encryption delay/ms	1.56	1.89	2.12	2.34	2.67	2.98	3.21	3.54	3.87
Data throughput/(MB/s)	5.23	4.89	4.56	4.32	4.01	3.78	3.56	3.34	3.12
System CPU usage/%	28.76	33.12	37.45	39.67	43.21	46.78	50.12	53.45	56.78
Index	Under resource constraints								
	Low memory			Low computing power			Low bandwidth		
Encryption delay/ms	4.56			5.23			3.89		
Data throughput/MB/s	2.12			1.89			1.56		
System CPU usage/%	35.67			42.34			28.12		

terms of interoperability standards, the study deployed protocol gateways to adapt to the smart grid standard IEC 61850 format, added encrypted logical nodes, and developed cross platform software development toolkits. In addition, resource constraints included low memory, low computing power, and low bandwidth, and in these cases, research was conducted to accelerate encryption, optimize code, and reduce memory usage through ARM TrustZone Technology. The performance of the solution under the increase in user numbers and resource constraints is shown in Table 8.

From Table 8, as the number of users increased, the encryption latency of the Paillier-DTSP scheme gradually increased, from 1.56 ms at 30,000 users to 3.87 ms at 200,000 users, while the data throughput gradually decreased, from 5.23 MB/s to 3.12 MB/s, and the system CPU usage continued to rise, from 28.76% to 56.78%. In resource constrained situations such as low memory, low computing power, and low bandwidth, the encryption latency, data throughput, and system CPU usage of the solution also exhibited changes related to the type of resource constraint. The encryption latency was highest in the low computing power scenario, at 5.23 ms, the system CPU usage was relatively high in the low memory scenario, at 35.67%, and the data throughput was lowest in the low bandwidth scenario, at 1.56 MB/s. Overall, the Paillier-DTSP scheme exhibited good adaptability and stability, despite some fluctuations in performance in user scale expansion and resource constrained environments.

To ensure the seamless integration of the Paillier-DTSP solution into the existing smart grid system and reduce deployment and renovation costs, research was conducted on the interoperability between the Paillier-DTSP solution and the smart grid standard IEC61850, and it was implemented through data format adaptation, communication protocol compatibility, and information model expansion. The results showed that in terms of data format

Table 9 Comparison of encryption throughput and delay of different encryption methods

	Encryption Throughput/(MB/s)					Delay/ms				
	Number of Experiments					Number of Experiments				
Method	1	2	3	4	5	1	2	3	4	5
Paillier	12.53	12.37	12.61	12.48	12.55	8.24	8.19	8.32	8.27	8.16
Lattice-based	5.26	5.18	5.34	5.22	5.15	25.37	25.14	25.42	25.29	25.18
ECC	18.73	18.65	18.81	18.76	18.69	12.54	12.47	12.62	12.58	12.43
RSA	6.35	6.28	6.41	6.33	6.26	32.84	32.69	32.91	32.76	32.67

adaptation, the success rate of parsing 100,000 encrypted data transmitted within 24 hours was 100%. In terms of communication protocol compatibility, the average latency was 85 ms. In terms of information model extension, the success rate of cross device data interaction was 99.8%. All indicators met the requirements of IEC61850 standard.

To clarify the rationality of choosing Paillier encryption and conduct in-depth analysis of latency performance, Lattice-based encryption (Lattice-based), Elliptic Curve Encryption (ECC), and RSA encryption were selected for comparison in the study. Meanwhile, one evaluation metric was latency, and the other was encryption throughput. The comparison of encryption throughput and latency for different encryption methods is shown in Table 9.

From Table 9, Paillier encryption performed outstandingly in terms of latency, with an average latency of 8.24 ms, far lower than Lattice-based's 25.28 ms, elliptic curve encryption's 12.53 ms, and RSA encryption's 32.77 ms. Additionally, Paillier encryption had an average throughput of 12.51 MB/s, which was slightly lower than ECC's 18.73 MB/s, but significantly better than Lattice-based's 5.23 MB/s and RSA's 6.33 MB/s. Considering the core demand for low latency in real-time smart grids, Paillier encryption was more suitable for real-time requirements while ensuring data processing efficiency. Therefore, opting for this solution was a reasonable choice.

This paper proposes a four in one approach to achieve compatibility with the IEC 61850 standard through protocol mapping, data format conversion, interface design, and compatibility testing. The encrypted aggregated data is mapped to IEC 61850 standard logical nodes and MMS application layer protocol and TCP/IP underlying transmission specifications are used. Ciphertext, signature, and timestamp are encapsulated into the IEC 61850 ASN. 1 standard format and message alignment and verification conversion is completed. Three standard interfaces are designed: encrypted collection, aggregation on chain, and standard data output. After testing, the success

rate of parsing 100,000 encrypted data within 24 hours is 100%, the average delay of protocol conversion is 85 ms, and the success rate of cross device interaction is 99.8%. It can seamlessly integrate with the existing power system.

4 Discussion

The advantages of the Paillier DTSP scheme proposed in this study in terms of computational overhead need to be interpreted in conjunction with the limitations of existing encryption technologies. Although traditional RSA, AES, and ElGamal encryption schemes are widely used in the field of data security, they have obvious shortcomings: RSA algorithm has an exponential increase in computational cost with user size due to large integer decomposition operations (Guo et al. [6] verified that its delay exceeds 200 ms at a user scale of 5000); AES has a fast encryption speed but does not support ciphertext aggregation (Li et al. [12] pointed out that it needs to be decrypted before processing, increasing privacy leakage risk by 30%); and ElGamal has poor adaptability on edge devices due to its high key generation complexity (Anandh et al. [10] reported that its encryption delay on 16 bit microcontrollers exceeds 50 ms).

In contrast, Paillier DTSP optimizes the computational complexity of the Paillier algorithm to control the computational overhead of data collection stations to 35.6% of traditional RSA at a user scale of 5000. This result echoes the research direction proposed by Gaikwad et al. [13] that "homomorphic encryption needs to balance computational efficiency and privacy protection", and achieves a breakthrough in edge device adaptation. Its average encryption delay at the smart meter end is 4.94 ms, far lower than the hybrid encryption scheme proposed by Kanakasabapathi and Judith [29] (18.14 ms), filling the gap in the deployment of existing homomorphic encryption technology in resource limited devices.

The advantage of Paillier-DTSP in edge device encryption latency does not come from hardware differences. All comparative experiments were conducted in the same Raspberry Pi 4B and server environment, and the advantage stems from algorithm computational complexity optimization and architecture collaborative design. This paper focuses on simplifying the Paillier modular exponentiation process for 8-bit/16-bit smart meters, reducing the number of large multiplication operations; At the same time, the "encryption is aggregation" architecture is adopted to avoid redundant operations of separate transmission and aggregation after encryption in traditional schemes.

Therefore, the average encryption latency at the edge is only 4.94 ms, far lower than the unoptimized hybrid encryption scheme.

5 Conclusion

To address the issues of granularity loss, privacy leakage, and limited analysis capabilities in the aggregation and sharing of multi-source heterogeneous power data in smart grids, the research proposed an efficient and secure protection scheme integrating Paillier homomorphic encryption. This solution constructed a three-layer system model of "terminal collection intermediate aggregation distributed storage" and a data sharing model, combined with Paillier homomorphic encryption and blockchain technology, to achieve direct computation of encrypted data, tamper proof aggregation of data, and full process security protection. Experimental verification showed that this scheme outperformed traditional schemes in terms of computational overhead, communication overhead, data transmission reliability, and security performance. For example, In terms of computational overhead, when the user scale reached 5000, the computational overhead at data collection stations was only 35.6% of that of the traditional RSA scheme, representing reductions of 62.3% and 58.7% compared to the traditional AES and ElGamal schemes, respectively. It can be seen that this solution could effectively resist various common risks such as internal threats, collusion attacks, and replay attacks, providing efficient and reliable technical support for the secure transmission and sharing of diverse heterogeneous power data in smart grids.

However, there are also certain shortcomings in the research. Firstly, when deploying on resource constrained smart meters, there was a challenge in terms of computing requirements: some old meters were only equipped with 8-bit/16-bit microcontroller units, which have limited computing power and memory, making it difficult to carry complex calculations encrypted by Paillier, leading to data latency or memory overflow. Future research could design lightweight homomorphic encryption variants or share computing tasks through edge nodes. Secondly, facing the long-term threat of quantum computing: if practical quantum computers achieve sufficient computing power, they will crack Paillier encryption based on mathematical problems, threatening the long-term security of power grid data. Future research needs to delve into the application of post quantum cryptography and accelerate the adaptation of lattice-based and encoding-based post quantum algorithms. Thirdly, energy data processing is currently transitioning towards cloud and edge architectures, and there is still room for improvement in the privacy

protection granularity and collaborative efficiency of existing solutions in distributed scenarios. Future research can focus on exploring more advanced distributed privacy protection algorithms such as federated learning and distributed differential privacy fusion algorithms and edge node collaborative encryption technology to achieve "usable but invisible" data between multiple edge nodes, which not only adapts to the trend of architecture transformation, but also further strengthens privacy protection capabilities in distributed environments. In addition, future research can be promoted from four aspects. Firstly, integrating quantum cryptography, screening and adapting algorithms, and upgrading encryption modules. Second, carry out practical scenario pilots and collect data in different power grid regions to optimize the stability of the plan. Third, optimize ultra-low latency control by improving protocols and optimizing encryption processes to reduce latency and meet the real-time control requirements of the power grid. The fourth is to deepen the research on the adaptation of distributed privacy protection algorithms to cloud and edge architectures, build a "cloud edge end" collaborative privacy protection framework, and enhance the practicality and security of solutions in large-scale distributed scenarios.

Acknowledgement

This work was supported by a science and technology project funded by China Southern Power Grid Company (Project No.: [GZKJXM20232512]).

References

[1] Goel A, Prabha C, Malik M, Sharma P. Security concerns and data breaches for data deduplication techniques in cloud storage: A brief meta-analysis. International Journal of Safety and Security Engineering: An Interdisciplinary Journal for Research and Applications, 2024, 14(2): 435–446. doi:10.18280/ijsse.140211.

[2] Zeng MJ, Cheng ZL, Huang X, Xu HB. A low-power consumption security data fusion model for Industrial Internet of Things. International Journal of Computers and Applications, 2025, 47(3): 312–322. doi:10.1080/1206212X.2024.2400151.

[3] Thenmozhi R, Shridevi S, Mohanty SN, Diaz VG, Gupta D, Tiwari P, Shorfuzzaman M. Attribute-based adaptive homomorphic encryption for

big data security. Big Data, 2024, 12(5): 343–356. doi:10.1089/big.2021.0176.

[4] Kukreja B, Malik SK, Sharma A. A novel citadel security framework for cyber data using CryptSteg techniques. International Journal of Performability Engineering, 2024, 20(10): 591–601. doi:10.23940/ijpe.24.10.p1.591601.

[5] Yusoff ZYM, Ishak MK, Rahim LAB, Asaari MSM. Improving smart home security via MQTT: Maximizing data privacy and device authentication using elliptic curve cryptography. International Journal of Computer Systems Science & Engineering, 2024, 48(6): 1669–1697. doi:10.32604/csse.2024.056741.

[6] Guo S, Liu Y, Shao S, Zang Z, Yang C, Qi F. Ubiquitous security boundary protection technology for cross-domain data circulation in new power system. Dianli Xitong Zidonghua/Automation of Electric Power Systems, 2024, 48(6): 96–111. doi:10.7500/AEPS20230629001.

[7] Niu G. A blockchain-based secure and privacy-preserving healthcare data management framework with SHA-256 and PoW consensus. Informatica (Slovenia), 2025, 49(20): 149–162. doi:10.31449/inf.v49i20.8392.

[8] Kesavan VT, Danalakshmi D, Gopi R, Venkatesan R. A decentralized framework for enhancing security in power systems through blockchain technology and trading system. Energy Sources Part A-Recovery Utilization and Environmental Effects, 2024, 46(1): 3454–3475. doi:10.1080/15567036.2024.2318010.

[9] Pathan M, Rameshkumar J, Suresh CV. Enhancing energy efficiency and data security in smart city grids using bio-inspired algorithms and blockchain technology. J Mach Comput, 2025, 5(2): 645–657. doi:10.53759/7669/jmc202505051.

[10] Anandh R, Swaminathan A, Jadhav SD, Valarmathi P, Gopinath N, Tiwari KS. An advanced encryption algorithm for enhancing data security in cloud computing. Recent Advances in Electrical & Electronic Engineering, 2025, 18(5): 623–636. doi:10.2174/0123520965279410231221034431.

[11] Can O, Thabit F, Aljahdali AO, Al Homdy S, Alkhzaimi HA. A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing. Cybernetics and Systems, 2025, 56(5): 413–447. doi:10.1080/01969722.2023.2175117.

[12] Li B, Xu M, Zhou Y, Liu H, Zhang R. Optimization of security identification in power grid data through Advanced Encryption Standard algorithm. Journal of Cyber Security and Mobility, 2024, 13(2): 239–264. doi:10.13052/jcsm2245-1439.1323.

[13] Gaikwad MA, Satonkar VH, Mohod AG, Jha RR, Giradkar RM, Rani S. Homomorphic encryption and secure multi-party computation: Mathematical tools for privacy-preserving data analysis in the cloud. Panam Math J, 2023, 33(2): 75–88. doi:10.52783/pmj.v33.i2.876.

[14] Qi ZH, Wu SX, Li JB. Localization of false data injection attacks in power grid based on adaptive neighborhood selection and spatio-temporal feature fusion. Computers, Materials & Continua, 2025, 85(11): 3739–3766. doi:10.32604/cmc.2025.067180.

[15] He BZ, Lv JG, Zhang JY, Zhao CH, Liu DH, Xu H, Wu B, Sun XH. Dynamic sharing algorithm for power grid survey data based on blockchain and proxy re-encryption. Sensors and Materials, 2025, 37(1): 207–216. doi:10.18494/SAM5258.

[16] Wu XY, Pu XJ. Blockchain technology adoption for collaborative emission reduction considering carbon information asymmetry in supply chains. Kybernetes, 2025, 54(6): 3460–3481. doi:10.1108/K-08-2023-1570.

[17] Rajendra P, Mohanasundaram T. Cloud computing in a realm of ever-increasing diverse consumer expectations towards security challenges that impact consumer's loyalty: A data driven approach. Journal of Mines, Metals & Fuels, 2023, 71(3): 464–472. doi:10.18311/jmmf/2023/33760.

[18] Tanam A, Raja G. Enhancing cloud security through block chain: A data integrity and trust approach. International Journal of Safety and Security Engineering: An Interdisciplinary Journal for Research and Applications, 2024, 14(5): 1455–1464. doi:10.18280/ijsse.140513.

[19] Dehbozorgi MR, Rastegar M, Arani MFM. False data injection attack detection and localization framework in power distribution systems using a novel ensemble of CNNs and explainable artificial intelligence. IEEE Transactions on Industry Applications, 2025, 61(3): 4801–4811. doi:10.1109/TIA.2025.3532917.

[20] Chuprov S, Zatsarenko R, Reznik L, Khokhlov I. Data quality based intelligent instrument selection with security integration. ACM Journal of Data and Information Quality, 2024, 16(3): 151–154. doi:10.1145/3695770.

[21] Muthubalaji S, Muniyaraj NK, Subba Rao SPV, Thandapani K. An intelligent big data security framework based on AEFS-KENN algorithms for the detection of cyber-attacks from smart grid systems. Big Data Mining and Analytics, 2024, 7(2): 399–418. doi:10.26599/BDMA.2023.9020022.

[22] Li Y, Liang L, Jia Y, Wen W. Blockchain for data sharing at the network edge: Trade-off between capability and security. IEEE/ACM Transactions on Networking: A Joint Publication of the IEEE Communications Society, the IEEE Computer Society, and the ACM with its Special Interest Group on Data Communication, 2024, 32(3): 2616–2630. doi:10.1109/TNET.2024.3364023.

[23] Lyon G. Trust in data security protocols and knowledge of privacy and security technology. IEEE Security & Privacy, 2024, 22(2): 29–37. doi:10.1109/MSEC.2023.3329739.

[24] Tong Q, Miao Y, Weng J, Liu X. Verifiable fuzzy multi-keyword search over encrypted data with adaptive security. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(5): 5386–5399. doi:10.1109/TKDE.2022.3152033.

[25] Kheiri H, Dehghani R. A hybrid model of recursive cellular automata, DNA sequences, and chaotic system for image encryption. Multimedia Tools and Applications, 2025, 84(19): 20693–20719. doi:10.1007/s11042-024-19746-z.

[26] Taqi IA, Hameed SM. A secure audio encryption method using tent-controlled permutation and logistic map-based key generation. Computers, Materials & Continua, 2025, 85(10): 1653–1674. doi:10.32604/cmc.2025.067524.

[27] Chen Y, Hua QS, Hong ZX, Zhu L, Jin H. FHE4DMM: A low-latency distributed matrix multiplication with fully homomorphic encryption. IEEE Transactions on Parallel and Distributed Systems, 2025, 36(4): 645–658. doi:10.1109/TPDS.2025.3534846.

[28] Amdouni R, Madani M, Hajjaji MA, Bourennane EB, Atri M. Secure medical image transmission using chaotic encryption and blockchain-based integrity verification. Computers, Materials & Continua, 2025, 84(9): 5527–5553. doi:10.32604/cmc.2025.065356.

[29] Kanakasabapathi RS, Judith JE. An intelligent hybrid encryption framework for cloud systems in cybernetics using ISSO and Paillier cryptosystem. International Journal of Machine Learning and Cybernetics, 2025, 16(12): 10541–10567. doi:10.1007/s13042-025-02785-9.

[30] Feng JD, Zhang XL, Zilic Z, Hao QF, Wang JC. An efficient Paillier homomorphic encryption circuit with optional CRT acceleration for IoT. IEEE Internet of Things Journal, 2025, 12(22): 48146–48158. doi:10.1109/JIOT.2025.3603982.

[31] Fang YY, Yang XP, Zhu H, Xu W, Zheng YD, Liu XD, Zhang D. Enhancing Paillier to fully homomorphic encryption with semi-honest TEE. Peer-to-Peer Networking and Applications, 2024, 17(5): 3476–3488. doi:10.1007/s12083-024-01752-5.

Biographies

Binyuan Yan (September 1989), male, holds a bachelor's degree in Optoelectronic Information Engineering from University of Shanghai for Science and Technology, China. Following graduation, he has been working as an engineer at Guizhou Power Grid Co. Ltd., with his current research focusing on cybersecurity.

Zeyuan Zhou (September 1991), male, received his bachelor's degree in Electronic Information Engineering from Guizhou University, China. Following graduation, he has been working as an engineer at Guizhou Power Grid Co. Ltd., and his current research focuses on cybersecurity.

Yun Fu (June 1987), female, holds a master's degree in Signal and Information Processing from University of Electronic Science and Technology of China. Following graduation, she has been working as a Senior Engineer at Guizhou Power Grid Co. Ltd. Her current research focuses on informatization development and IT operation & maintenance management.

Yang Su (April 1983), male, holds a master's degree in Information Systems from Sichuan University, China. Following graduation, he has been working as a Senior Engineer at Guizhou Power Grid Co. Ltd. His current research focuses on electric power informatization and digitalization.