ISSN 1840-4855
e-ISSN 2233-0046

Original Scientific Article
http://dx.doi.org/10.70102/afts.2025.1833.819

DATA SECURITY AND PRIVACY PROTECTION MECHANISM FOR POWER GRID SUPPLY CHAIN BASED ONDUAL-CONSORTIUM BLOCKCHAIN ARCHITECTURE AND IMPROVED BGN ALGORITHM

You Wen[1], Mingjun Tang[2], Yijun Yang[3*], Hong Luo[4]

[1]Guangdong Power Grid Corporation of India Limited, Guangzhou, Guangdong, China.
e-mail: wenyou@xxzx.gd.csg.cn, orcid: https://orcid.org/0009-0002-8656-9822
[2]Guangdong Power Grid Corporation of India Limited, Guangzhou, Guangdong, China.
e-mail: 13808841236@163.com, orcid: https://orcid.org/0009-0004-9706-6862
[3]Southern Power Grid Digital Platform Technology (Guangdong) Corporation of India Limited, Shenzhen, Guangdong, China. e-mail: yijuny06@gmail.com,*
orcid: https://orcid.org/0009-0001-3287-1674
[4]Southern Power Grid Digital Platform Technology (Guangdong) Corporation of India Limited, Shenzhen, Guangdong, China. e-mail: luohong@dptc.csg.cn,
orcid: https://orcid.org/0009-0003-4769-963X

Received: September 04, 2025; Revised: October 06, 2025; Accepted: November 24, 2025; Published: December 20, 2025

SUMMARY

In the process of multi-party collaborative data sharing, the power grid supply chain system often faces security risks such as data islands, privacy leakage and tampering risks. It is urgent to establish a security management mechanism that takes into account efficiency and credibility. To this end, this study proposes a power grid supply chain data security management model that integrates a dual alliance chain architecture and an improved Boneh-Goh-Nissim algorithm. This model uses the business chain and the chain of custody to separate transaction processing and audit supervision, and ensures the traceability and non-repudiation of data interaction through cross-chain communication; it also completes multi-party security calculation and privacy protection of aggregated data based on the improved Boneh-Goh-Nissim algorithm. Experimental results show that in a typical power grid supply chain scenario, the model's data integrity verification rate reaches 99.2%, the average transaction delay is 1.36 seconds, the encryption and decryption time is reduced by 27.4% compared with the traditional algorithm, and the system throughput is increased to 1,450 transactions per second. The research results have effectively improved the data security and operating efficiency of the power grid supply chain system under cross-domain sharing conditions, and provided a scalable technical path for supply chain collaboration and big data governance in the power industry.

Key words: *dual alliance chain, BGN algorithm, power grid supply chain, data security management, homomorphic encryption.*

BACKGROUND

With the swift advancement of technology and the deepening of digital transformation, traditional centralized data sharing methods can no longer fulfill the requirements of power grid supply chain systems (SCSs) for data confidentiality, integrity, traceability, and access control. As a decentralized, tamper proof, and traceable distributed ledger technology, blockchain has become an effective means of solving data sharing problems [1]. However, blockchain technology has a high demand for computing resources and storage space. In cases of frequent transactions or a large quantity of participating nodes, it is easy to encounter processing bottlenecks, which can affect system throughput and response speed [2]. Edge computing technology can effectively reduce network latency, reduce central server load and improve data processing efficiency by migrating data processing and analysis tasks to network edge nodes close to the data generation source [3]. Therefore, the data sharing method based on blockchain technology and edge computing technology has gradually become an important solution to realize data security management. For example, Zhong H C et al. put forward an Internet of Things access control model that leverages blockchain and edge computing. This model integrated smart contracts with attribute-based access control to tackle the issue of data security management among power Internet of Things edge nodes and numerous heterogeneous devices. The experimental findings demonstrated that the model could achieve dynamic permission management for edge nodes and terminal devices while ensuring data security and privacy protection [4]. However, when using blockchain protocol for edge computing, there is still a technology mismatch problem. To this end, Tulkinbekov K et al. proposed a new blockchain architecture, called Record chain, which could fully adapt to the edge computing environment. The experimental findings demonstrated that Record chain could independently locate actual data while providing security and scalability, thereby solving the storage utilization problem related to power big data [5]. In addition, to ensure the security of power grid data and intelligent computing offloading, Zhang S et al. proposed a secure cloud edge collaborative power IoT architecture based on blockchain and Lyapunov optimization methods [24]. The experimental findings demonstrated that this method had excellent performance in terms of total queuing delay and consistency delay [6].

The blockchain of the power grid SCS also involves a large amount of highly sensitive information such as data, transactions, and device access, which requires corresponding security measures to ensure data transmission security, transaction security, and device access security [7]. Homomorphic encryption algorithms have attracted much attention due to their ability to perform operations directly without decrypting data [8]. The Boneh-Goh-Nissim (BGN) algorithm is a semi-homomorphic encryption system constructed based on bilinear groups and pairing operations, which can perform any number of addition operations and only one multiplication operation in the encryption domain. This encryption structure supports aggregated computing and verification while ensuring data privacy, but its single multiplication limitation also leads to insufficient scalability in complex function operation scenarios [9] [10]. For example, Zhao et al. proposed a privacy protection billing method based on BGN algorithm and blockchain technology. The experimental findings demonstrated that this approach could ensure the privacy of smart meters (SMs), and guarantee the integrity and correctness of monthly and regular bills [11]. Zeng Z et al. proposed a data aggregation scheme based on BGN homomorphic encryption. This scheme ensured privacy protection while maintaining acceptable computational complexity and communication overhead, demonstrating strong practicality and promotional value [12]. In addition,

Xiao J Z et al. designed a key leakage elastic encryption data aggregation scheme suitable for fog assisted smart grids based on an improved BGN algorithm. The experimental findings demonstrated that even if the private key of the cloud server was leaked, it could not destroy user privacy, significantly improving the security resilience of the power system [13] [23]. Huang X et al. conducted a systematic review on the integration of "blockchain × edge computing" in the Internet of Things/power grid scenarios, presented the general architecture of IBEC, summarized the research progress in dimensions such as resource management, joint optimization, data management, computing offloading, and security mechanisms, and pointed out the bottlenecks of existing work in cross-domain collaboration and chain-edge coupling efficiency. It provides a systematic technical reference for the subsequent implementation of the design of "edge-level aggregation + on-chain trusted aggregation" in the power grid supply chain [14]. Zhang S et al. conducted a review on "Blockchain-Enabled Power Grid Security and Privacy Protection", compared the blockchain technology routes in key links such as privacy protection, identity authentication, data aggregation and electricity price settlement, and emphasized that scalability and interoperability need to be taken into account in actual deployment. The technical trade-offs summarized in this review (the synergy between homomorphic aggregation and smart contracts) are highly consistent with the path of "dual consortium chains + homomorphic encryption" in this article [15].

In summary, edge servers can share the computing and storage pressure of data centers, while blockchain can provide decentralized and tamper proof trusted ledgers. Despite the fact that homomorphic encryption technology offers a robust solution for ensuring data privacy protection and secure computing in cross-domain environments, the power grid SCS is plagued by a pervasive issue of information silos [25]. This phenomenon significantly hinders data exchange and sharing across different regions and hierarchical levels, thereby impeding the full circulation and utilization of power data resources. To address the above issues, a data security management method for power grid supply chains based on a dual consortium chain architecture and an improved BGN algorithm has been studied and constructed. In terms of research methods, a two-layer structure featuring the collaboration of the business chain and the regulatory chain was designed to achieve the functional separation of transaction processing and audit supervision, and to complete cross-chain communication and traceable data interaction in combination with smart contracts. At the algorithm layer, the improved BGN homomorphic encryption algorithm is introduced to conduct batch encryption and secure aggregation of power consumption data within the region. Meanwhile, the Proxy Re-Encryption (PRE) technology and the Shamir secret sharing mechanism are integrated to enhance key security and cross-domain data sharing capabilities. Through the above design, the research not only proposed a power grid supply chain data security management mechanism for multi-party participation scenarios, but also achieved an optimized balance among security, scalability and computing efficiency. The main contributions are reflected in: ① Forming a security management framework for the coordinated operation of the business chain and the regulatory chain; ② Build an aggregation and verification mechanism that supports multi-party secure computing; ③ Significantly enhance the efficiency of cross-domain data interaction and the level of privacy protection, providing a scalable technical path for big data governance and supply chain collaboration in the power industry.

METHODS

Data aggregation method for power grid SCS based on dual alliance chain

Data aggregation in the power grid SCS refers to the process of collecting, processing, and summarizing atomic data from multiple sources into a structured and analyzable dataset. Multiple rows of data are converted into single row summary information through aggregation functions, providing overall data insights for supply chain operations [16]. Among them, consortium blockchain is a type of blockchain jointly maintained by multiple specific institutions, allowing only consortium members to participate in consensus and access. Compared to public blockchain, consortium blockchain has advantages in efficiency and flexibility [17] [18]. Therefore, the study first proposes a data aggregation method for power grid SCS based on dual alliance chain. The overall network framework of the power grid SCS is shown in Figure 1.

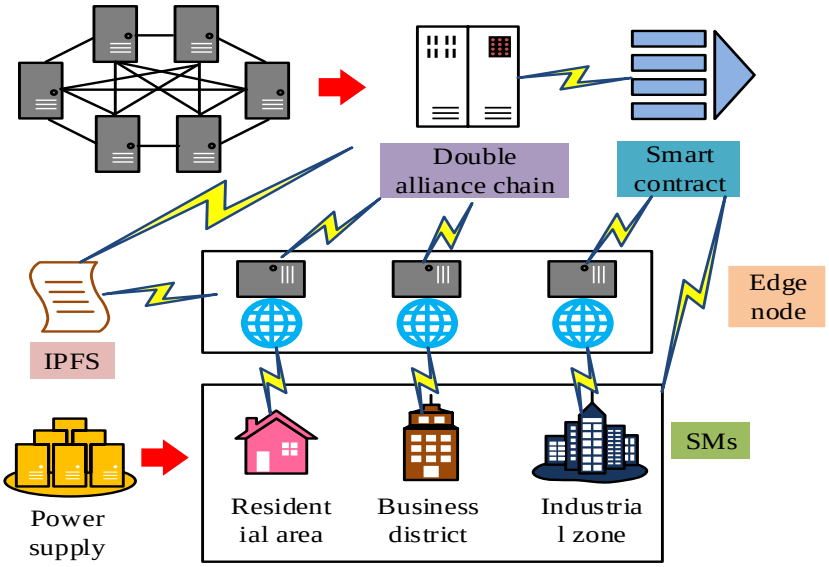

Figure 1. Network framework of power grid SCS

As shown in Figure 1, the overall network architecture of the power grid supply chain System consists of four core parts: SMs, edge nodes, Inter Planetary File System (IPFS), and dual consortium chains. SMs is deployed at residential, commercial and industrial power consumption terminals to collect real-time energy consumption data and report it to edge nodes. Edge nodes undertake data preprocessing, encryption and first-level aggregation computing functions, effectively reducing the computing and storage pressure on the central control node. The dual consortium chain structure divides the system functions into business chains and supervision chains: The business chain is responsible for handling aggregated transactions from edge nodes, ensuring the complete recording and verifiability of data; The chain of custody is responsible for cross-regional data auditing and consistency verification, achieving trusted supervision at the regulatory level. IPFS provides distributed storage and indexing support for large-scale power data, making historical data traceable and scalable. The overall architecture, through the collaborative design of edge computing and dual consortium chains, has achieved full-process trusted management from data collection, encrypted transmission to cross-chain auditing, laying a technical foundation for the secure sharing of the power grid supply chain system. The calculation formula for the encrypted first level aggregation result

C_{edge} is shown in equation (1).

$$C_{edge} = \sum_{i=1}^{n} E(d_i) \quad (1)$$

In equation (1), d_i represents the power consumption data of the ith user, n represents the total number of users under the edge node, and E represents the homomorphic encryption function. The secondary data aggregation framework is shown in Figure 2.

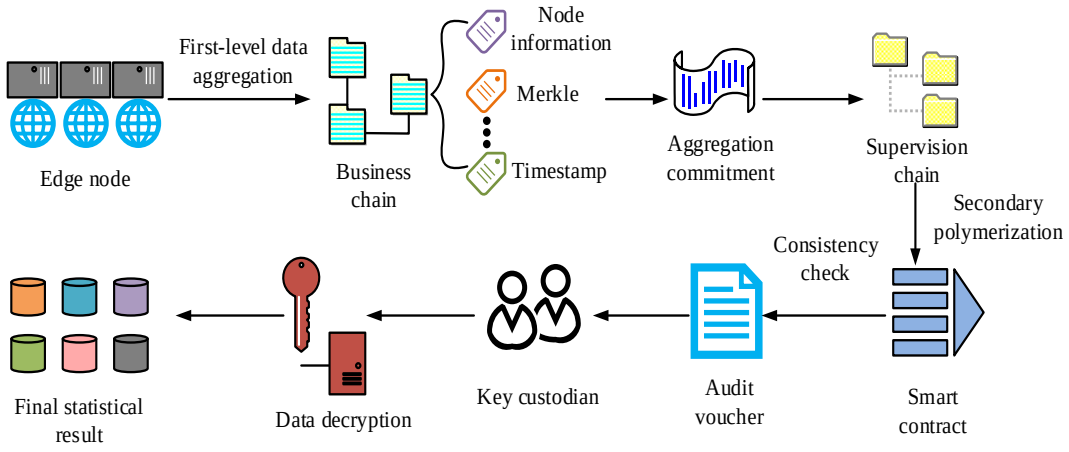

Figure 2. Secondary data aggregation framework

As shown in Figure 2, the secondary aggregation is mainly participated by both the business chain and the regulatory chain. Among them, the business chain is mainly responsible for processing the first level aggregation transactions uploaded by edge nodes, generating aggregation commitments for each transaction, recording participating node information, Merkle roots, timestamps, and related verification data to ensure the traceability and integrity of each aggregation transaction. The regulatory chain is responsible for performing secondary aggregation operations. Smart contracts receive aggregation commitments from the business chain, perform audit verification and consistency checks, and generate audit credentials to ensure the credibility and tamper proof of cross regional data aggregation. After the secondary aggregation is completed, the key custodian within the authorized domain decrypts the data and outputs the final statistical results. The formula for calculating aggregate commitment P_j is shown in equation (2).

$$P_j = H \times C_{edge}^{j} \| N_j \| T_j \quad (2)$$

In equation (2), H represents the hash function, C_{edge}^{j} represents the aggregate ciphertext of the jth edge node, N_j represents the node identification information participating in the aggregation, and T_j represents the timestamp. The calculation formula of secondary aggregate ciphertext C_{reg} is shown in equation (3).

$$C_{reg} = \sum_{j=1}^{m} C_{edge}^{j} = E \sum_{j=1}^{m} \sum_{i=1}^{n_j} d_i^j \quad (3)$$

In equation (3), m represents the number of edge nodes under the service chain, n_j represents the number of users under the jth edge node, and d_i^j represents the power data of the ith user under the jth edge node. The calculation formula of secondary aggregation consistency verification result (Boolean value) is shown in equation (4).

$$V_{audit} = \sum_{j=1}^{m} Verify(P_j) \quad (4)$$

In equation (4), $Verify(\cdot)$represents the audit verification function of the smart contract for aggregate commitments. The final statistical data calculation formula is shown in equation (5).

$$D_{total} = D(C_{reg}) = \sum_{j=1}^{m} \sum_{i=1}^{n_j} d_i^j \quad (5)$$

In equation (5), $D(\cdot)$represents the homomorphic encryption and decryption function. To ensure that the aggregation results cannot be tampered with, the business chain builds a Merkle tree for the aggregation data submitted by the edge node, and the calculation formula of the root node R is shown in equation (6).

$$R = H \times H(C_{edge}^1) \| H(C_{edge}^2) \| \cdots \| H(C_{edge}^m) \quad (6)$$

In equation (6), the algebraic meaning remains the same as before. In the dual alliance chain architecture, smart contracts support regulatory transactions without third-party participation, and their execution process is shown in Figure 3.

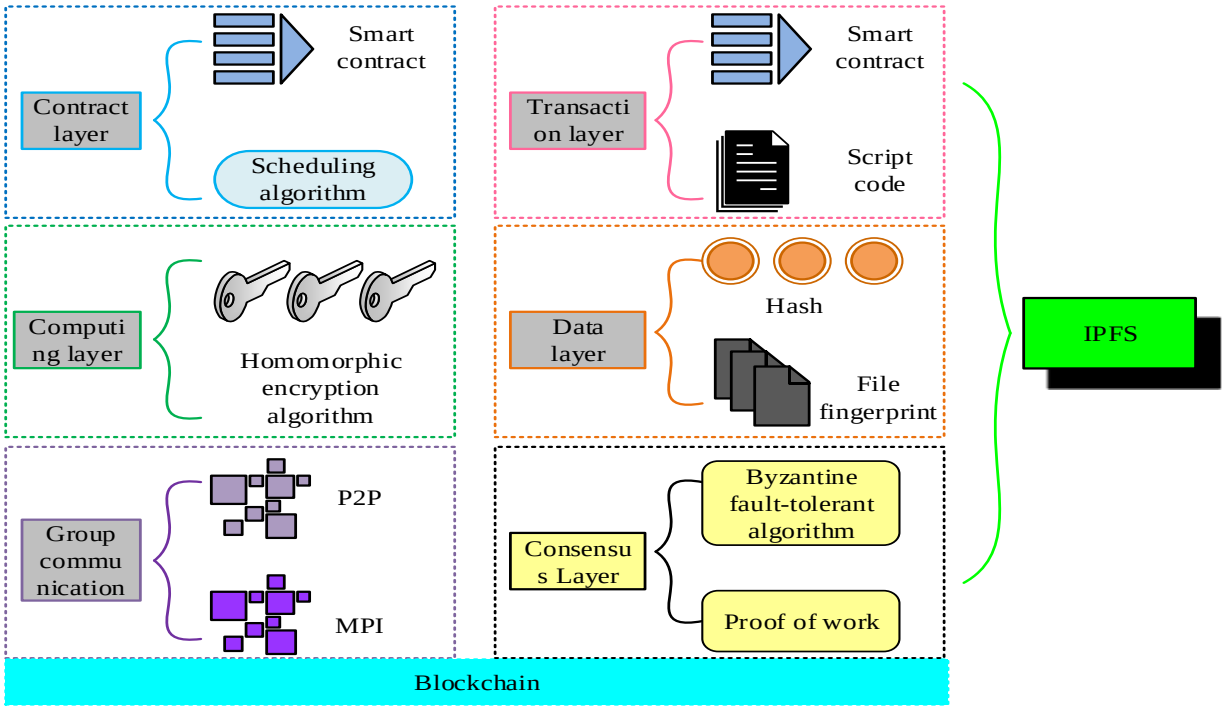

Figure 3. Smart contract execution process

As shown in Figure 3, firstly, secure communication and message passing between nodes are achieved through P2P protocol and MPI protocol, laying the foundation for cross node interaction. Secondly,

homomorphic encryption algorithms are introduced to encrypt sensitive data involved in contracts, thereby completing necessary logical operations without decryption, achieving a balance between privacy protection and data availability. At the data layer, transaction data is uniquely identified using hash algorithms and efficiently stored and retrieved through file indexing mechanisms. It is also integrated with IPFS to support distributed storage and retrieval of large-scale power data. At the consensus layer, the system adopts the improved PBFT as the main consensus mechanism and introduces the lightweight Proof of Work (PoV) module as an auxiliary means for evaluating the credibility of node behaviors, rather than the traditional high-energy-consuming Proof of Work (PoW). The design logic of this dual-mechanism lies in: PBFT ensures rapid consistency and low latency among the nodes of the consortium chain, while the PoV module generates reputation scores by recording the frequency of node submission, verification and execution, which are used to dynamically adjust the voting weights of nodes and select arbitration nodes, thereby achieving a balance among performance, energy consumption and security. This mechanism takes into account both the low energy consumption constraints and the high consistency requirements in the permissioning chain environment, avoids the high resource consumption problem of PoW, and simultaneously enhances the system's anti-malicious fault tolerance capability when the number of nodes is large. At the trading layer, the script code of the smart contract is triggered and executed, and the generated transaction records are stored on chain for automatic execution and status updates. At the contract layer, scheduling algorithms manage and invoke smart contracts based on predefined rules to ensure efficient operation of contract logic in different business scenarios. In the end, smart contracts achieved a complete closed-loop process from triggering, encrypted computation, storage invocation, consensus verification to result on chain.

Construction of aggregation data security management model based on improved BGN algorithm

The data aggregation method for power grid SCS based on dual alliance chain can not only achieve first level data aggregation of edge nodes and business chain aggregation commitment generation, but also ensure data integrity, privacy, and traceability through second level aggregation of regulatory chain, audit verification of smart contracts, and cross domain decryption. On this basis, to further improve the security and computational efficiency of the data aggregation process and solve the problem of data silos in the power grid SCS, the BGN algorithm and Shamir secret sharing mechanism were combined to construct an aggregated data security management model based on the improved BGN algorithm. Shamir secret sharing is a cryptographic technique based on polynomial interpolation principle [19] [26]. The core idea is to split a secret data into several shares, and only when the number of shares reaches a preset threshold can the original secret be reconstructed [20-21]. The study splits the key K into k shares, assuming the threshold is t, and the calculation formula of random polynomial $f(x)$ is shown in equation (7) [22].

$$f(x) = K + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{t-1} x^{t-1} \quad (7)$$

In equation (7), $\alpha_1 \sim \alpha_{t-1}$ represents random coefficient. The overall process framework of the aggregated data security management model is shown in Figure 4.

As shown in Figure 4, the constructed aggregated data security management model takes the improved BGN algorithm as the core, combines Shamir secret sharing and PRE technology, and forms a full-process security management system of "encryption - sharding - aggregation - reconstruction". The model first uses the BGN algorithm on the edge node side to perform batch homomorphic encryption

on the electricity consumption data of multiple users, achieving privacy protection before aggregation. Subsequently, the key is split into multiple shares through the Shamir secret sharing mechanism and distributed to different nodes to avoid single-point leakage; In the cross-domain sharing stage, PRE technology is introduced to generate re-encryption keys, ensuring that different consortium chains can securely access data without exposing the original keys.

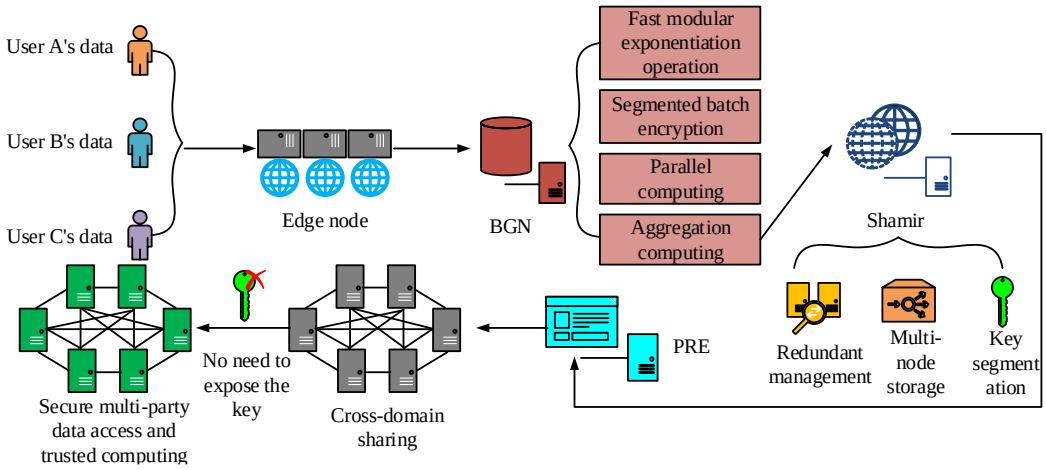

Figure 4. The overall process framework of the aggregated data security management model

Finally, the authorized node reorganizes the key and completes the data decryption and the output of the aggregation result. This process not only realizes the secure transmission and trusted computing of aggregated data in the power grid supply chain, but also takes into account the security, scalability and real-time performance of the system in a multi-node and multi-regional collaborative environment. Assuming that message b is encrypted, the homomorphic encryption calculation formula is shown in equation (8).

$$c = E(b) = g^b \cdot r^n \quad (8)$$

In equation (8), c represents ciphertext; g^b represents the message index; r stands for random number, which is used to ensure the uncertainty of encryption; r^n stands for random disturbance term. In the dual alliance chain architecture, the data sharing structure is shown in Figure 5.

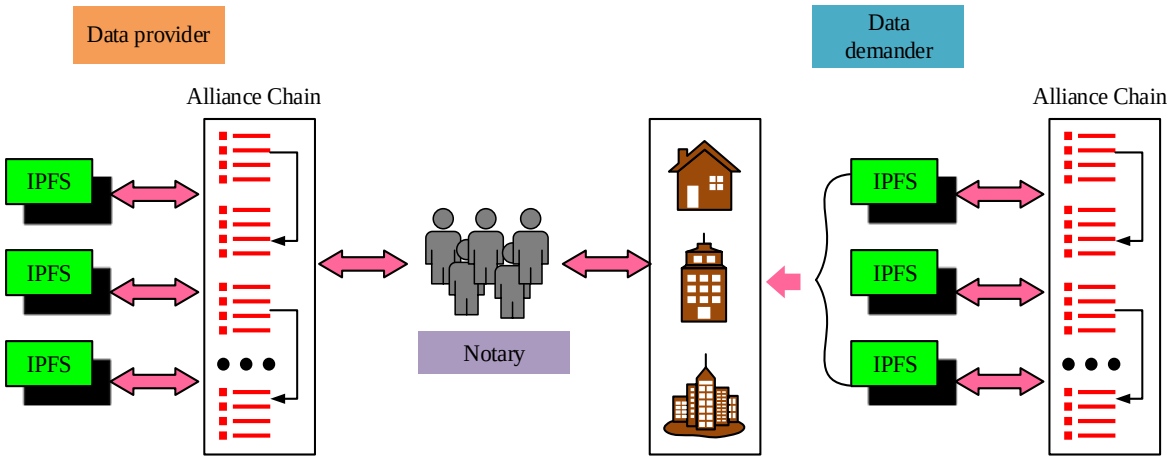

Figure 5. Data sharing structure

As shown in Figure 5, the data requester first initiates a data sharing request. After completing identity verification, the data provider encrypts the power data using BGN homomorphic encryption algorithm and Shamir secret sharing mechanism, and divides the encrypted data into multiple ciphertext segments and keys. Subsequently, key fragments are distributed. After receiving the power ciphertext, the result is transmitted to the data demander through an off chain secure channel. In the end, after collecting sufficient encrypted fragments, the data demander uses its own private key and the recombined key to complete decryption and reassembly, and outputs composite ciphertext. The schematic diagram of cross chain transmission is shown in Figure 6.

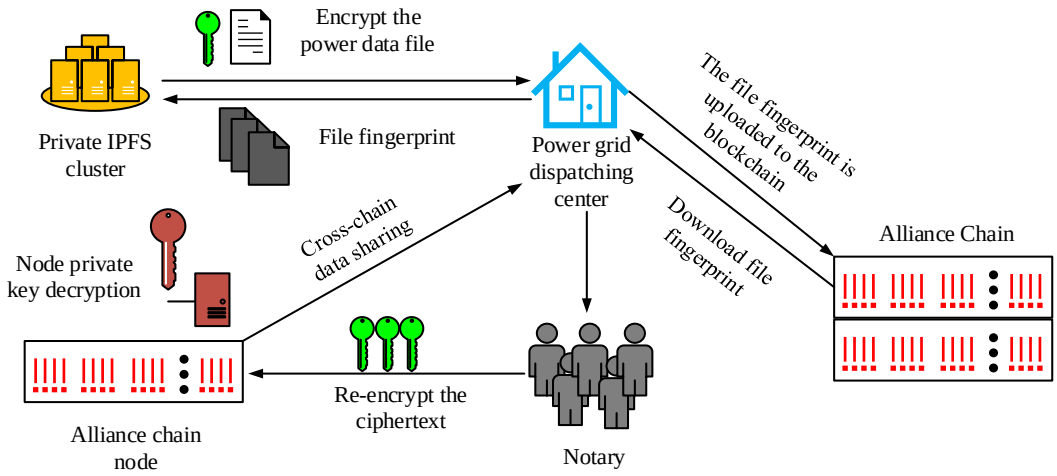

Figure 6. Cross-chain data sharing process

As shown in Figure 6, firstly, the encrypted power data file is uploaded to the private IPFS storage, and the fingerprint information of the file is recorded. After receiving the upload request, the power grid dispatch center requests the fingerprint information of the corresponding file from the dual alliance chain, downloads the file fingerprint, and generates are encryption key to support subsequent cross chain secure transmission. Subsequently, the power grid dispatch center sends the request to the nodes of the dual alliance chain, uses BGN homomorphic encryption algorithm and PRE technology to process the public key information required for cross chain sharing, and sends the re-encrypted ciphertext to the data demand side node through off chain transmission. After receiving the off chain re encrypted ciphertext, the data demand node uses the local node's private key to decrypt the ciphertext, achieving secure access to power data. Throughout the entire process, multi signature notaries provide ciphertext management and re-encryption key management services by requesting smart contracts, ensuring the integrity, traceability, and security of cross chain data sharing. The research collects the ciphertext fragment s_j by calling the gather function, and the calculation formula of s_j is shown in equation (9).

$$s_j = (\prod_{m=1,m\neq j}^{k} \frac{x-x_m}{x_j-x_m})\lambda_j \quad (9)$$

In equation (9), λ_j represents the Lagrange coefficient, and x_j and x_m represent the index of the j or mth node respectively. Recon function is used to reconstruct the ciphertext to obtain the ciphertext c of $k(k < (n-1)/2)$ multiple nodes. The calculation formula of multi node key reconstruction is shown in equation (10).

$$Re\,c\,on(\{(i, s_i), i \in n\}, k) \rightarrow c \quad (10)$$

RESULTS

Performance Testing of Aggregated Data Security Management Model

The hardware environment configuration of the experimental platform was determined through research, with Intel Xeon Gold 6330 2.0 GHz CPU, NVIDIA RTX 3090 GPU, and 128 GB DDR4 memory. The storage device was a 2 TB NVMe SSD. The operating system was Ubuntu 20.04 LTS, the underlying framework of the consortium chain was Hyperledger Fabric 2.5, the smart contract language was Go 1.19, and the encryption and multi-party secure computing modules were implemented in Python 3.10 environment, using CUDA 11.8 parallel acceleration computing. In the experiment, it is assumed that the average daily power load of each user node fluctuates within the range of 1.5-6.0kWh, and the sampling period is set to 15 minutes. The number of edge nodes is 200, each node manages 20 to 35 users, and the average size of data packets is approximately 2.5KB. The block generation interval of the consortium chain is set at 5 seconds, the upper limit of the block capacity is 2 MB, and the fault tolerance coefficient of the Byzantine Fault Tolerance (BFT) algorithm is taken as 1/3. The key length of the BGN encryption algorithm is set to 2048 bits, and the range of random perturbation parameters is [1, 1000]. The Shamir secret sharing threshold is set to (t, n) = (3,5), and the delay of public-private key conversion for proxy re-encryption is controlled within 10ms. The simulated network bandwidth value is 100Mbps, the average communication delay is 50ms, and the bit error rate is less than 10^{-4}. The experimental data mainly came from the energy consumption dataset of power users and the interaction log dataset of power equipment in the power grid supply chain of a certain province from January to December 2023. Among them, the energy consumption data set of power users included 1200000 records, including user ID, meter ID, timestamp, peak valley classification, and electricity price type. The interaction log data set of power equipment contained 300000 records, including device ID, operation type, operation time, status identification, etc. The study first conducted sensitivity tests on the consensus mechanism parameters and BGN encryption parameters in the dual consortium chain architecture, and the test results are shown in Figure 7.

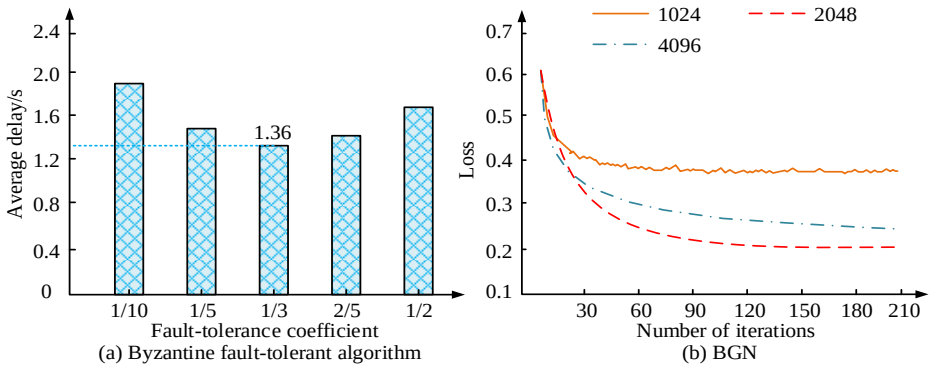

Figure 7. Sensitive test results

Figure 7 (a) shows the delay variation of Byzantine fault-tolerant algorithm under different fault tolerance coefficients, and Figure 7 (b) shows the performance variation of BGN algorithm under different key lengths. As shown in Figure 7 (a), a low fault tolerance coefficient could lead to insufficient system resistance to attacks, while a high fault tolerance coefficient could increase redundant computing overhead. When the fault tolerance coefficient was set to 1/3, the average transaction delay of the system was optimal at 1.36 seconds. As shown in Figure 7 (b), when the key length was set to 2048 bits, the

system could converge to 0.21 after 90 iterations and remain stable. When the key length was too small (1024 bits), although it converged quickly, its security was insufficient, while if it was too large (4096 bits), it would significantly increase the computational cost and prolong the convergence time. Taking into account both security and efficiency, the study ultimately selected a 2048 bit key and a 1/3 fault tolerance coefficient as the optimal parameter combination for the system. Subsequently, ablation experiments were conducted on the proposed model, and the test results are shown in Figure 8.

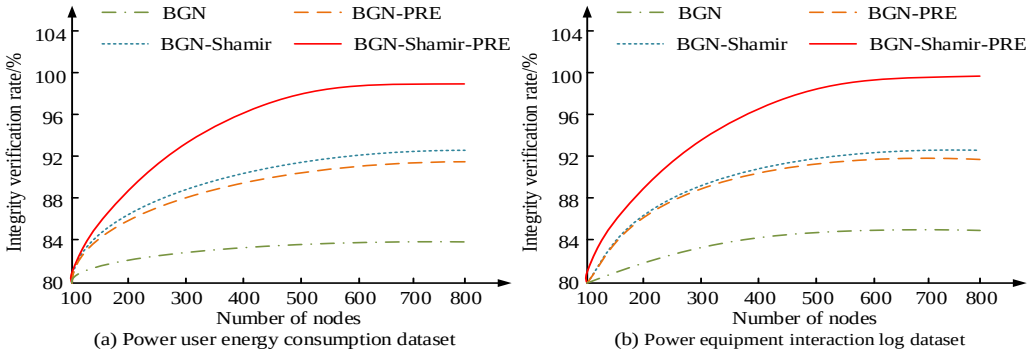

Figure 8. Results of the ablation experiment

Figures 8 (a) and 8 (b) show the data integrity verification rate test results of BGN, BGN Shamir, and BGN Shamir PRE models in the power user energy consumption dataset and power equipment interaction log dataset, respectively. As shown in Figure 8 (a), the data integrity verification rate gradually increased with the increase of the number of nodes and eventually reached stability. When only BGN was used, the data integrity verification rate was relatively low, at 82.1%. After introducing the Shamir secret sharing mechanism, the performance of the model was improved and ultimately stabilized at 90.3%, indicating that key sharding and redundancy management could effectively enhance data security. Further combining with PRE technology, the BGN Shamir PRE model showed the best performance, with a data integrity verification rate of 98.9%. From Figure 8 (b), on the power equipment interaction log dataset, the overall trend of each method was consistent with the power user energy consumption dataset, and the BGN Shamir PRE model achieved a data integrity verification rate of 99.2%. From this, the research model had high aggregation robustness and consistency in typical power grid supply chain scenarios. In addition, the study also introduced popular data security management methods, namely Paillier homomorphic encryption algorithm, Differential Privacy (DP) technology, and Fabric BGN model, for comparative testing. The test results are shown in Table 1.

Table 1. Index test results of different methods

Dataset	**Methods**	**Avg. encryption/decryption time (ms)**	**Throughput (TPS)**	**MAP**	**Safety level**	***p*-value**
Power user energy consumption dataset	Paillier	32.5	135	0.912	4	0.041
	DP	8.7	178	0.874	2	0.032
	Fabric-BGN	25.4	162	0.916	3	0.028
	Our model	21.3	185	0.978	5	0.003
Power equipment interaction log dataset	Paillier	34.1	130	0.905	4	0.047
	DP	9.2	175	0.869	2	0.031
	Fabric-BGN	26	160	0.912	3	0.024
	Our model	22.1	183	0.975	5	0.004

According to Table 1, the Paillier algorithm was relatively mature in terms of security, reaching level 4. However, its high complexity and communication overhead resulted in a longer average encryption/decryption time of 32.5ms, which was difficult to meet the real-time requirements of the power grid supply chain. DP performed well in encryption/decryption efficiency, but it had a significant impact on the Mean Average Precision (MAP) of data aggregation, with the highest MAP being only 0.842. Fabric BGN had a relatively balanced overall performance, with a maximum throughput of 162TPS and a MAP of 0.916. However, it had limitations in cross domain data sharing and privacy protection, with a security enhancement level of 3. The research model performed the best in both encryption/decryption and data aggregation accuracy, balancing security and efficiency. The average encryption/decryption time for aggregated data was only 21.3ms, and the security level was raised to 5, making it suitable for data management in power grid SCSs. In addition, the statistical test results compared with the research model are presented on the far right of Table 1: the differences in encryption/decryption time, throughput and MAP are all statistically significant (two-sample t-test, p<0.05; typical range p=0.003-0.047), indicating that the above performance improvements are statistically significant and robust.

Aggregation data security management model simulation testing

A simulation environment was constructed with 4900 user nodes, 200 edge nodes, and 10 alliance organization nodes. To verify the performance of the model under multi-node and multi-region collaboration, experiments were conducted to simulate the process of data upload, aggregation, and cross chain sharing in different power regions. The Cross chain Synchronization Success Rate (CSSR) and Concurrent Data Access (CDA) test results are shown in Figure 9.

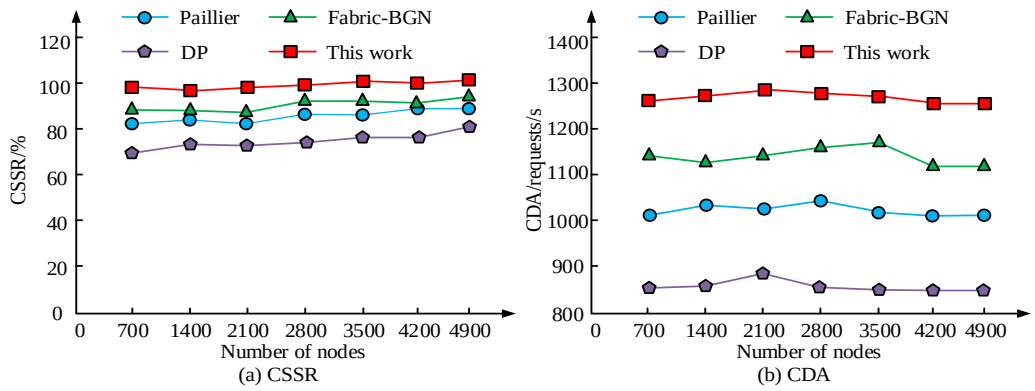

Figure 9. Test results of CSSR and CDA

Figure 9 (a) shows the CSSR test results of different methods in cross chain data synchronization of the power grid SCS, and Figure 9 (b) shows the CDA test results of each method in concurrent data access. As shown in Figure 9 (a), the Paillier algorithm had high cross chain data synchronization security, but there were still a few synchronization failures. When the number of nodes increased to 4900, the CSSR was 92.4%. The reliability of DP cross chain data synchronization was low, with a CSSR of only 87.9%. The Fabric BGN model performed moderately, with CSSR ultimately reaching 94.6%. The CSSR performance of the research model was the best, ultimately reaching 98.9%. According to Figure 9 (b), in the CDA test, the peak value of Paillier algorithm was 1035requests/s, and it eventually stabilized at 1002 requests/s. The DP peak was 890 requests/s and eventually stabilized at 865 requests/s, indicating that its ability to access concurrent data was affected by privacy noise. The peak value of the Fabric

BGN model was 1170 requests/s, and it eventually stabilized at 1135 requests/s. The peak value of CDA in the research model reached 1280 requests/s, and finally stabilized at 1255 requests/s, with high efficiency in cross domain concurrent data access. The resource utilization and efficiency performance of the model under large-scale concurrency conditions are shown in Figure 10.

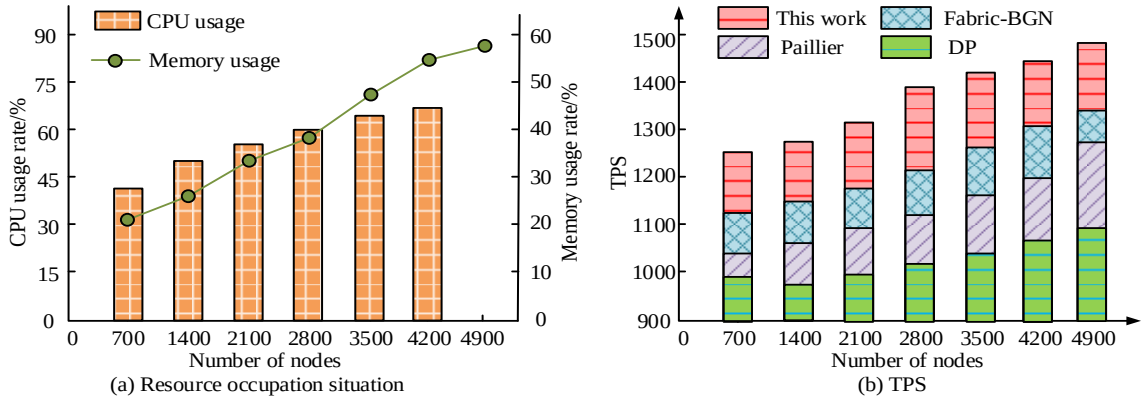

Figure 10. Resource occupancy and efficiency performance

Figures 10 (a) and 10 (b) show the resource utilization and efficiency results of the model under large-scale concurrency conditions, respectively. As shown in Figure 10 (a), the CPU usage of the research model gradually increased with the increase of the number of nodes under large-scale concurrency conditions. When the number of nodes was 1400, the CPU usage was about 48% and the memory usage was about 36%;As the number of nodes increased to 3500, the CPU usage rate rose to 62% and the memory usage rate reached 49%;In the case of 4900 nodes, the CPU utilization rate ultimately stabilized at 71% and the memory utilization rate was 58%, indicating that the model could still maintain a reasonable level of resource utilization in high concurrency scenarios. As shown in Figure 10 (b), the research model exhibited excellent processing efficiency under large-scale concurrency conditions. When the number of nodes was 1400, it could process approximately 1280 transactions per second (TPS). As the number of nodes increased to 3500, TPS rose to 1395;At node 4900, TPS ultimately stabilized at 1450 transactions per second. From this, the research model achieved a good balance between resource utilization and processing efficiency. Finally, to verify the security and robustness of the model in the face of abnormal or malicious nodes, a certain proportion (5%~20%) of nodes were set up to submit abnormal data, and evaluated through abnormal detection rate (ADR), false positive rate (FPR), and abnormal recovery time (ART) indicators. The outcomes are presented in Table 2.

Table 2. Security robustness test results under abnormal/malicious nodes

Node anomaly ratio	Methods	ADR (%)	FPR (%)	ART (s)	*p*-value
5%	Paillier	91.2	6.8	3.2	0.038
	DP	85.7	10.5	4.8	0.029
	Fabric-BGN	93.5	5.2	2.9	0.021
	Our model	97.8	3.1	1.7	0.004
10%	Paillier	88.6	7.5	3.8	0.035
	DP	82.3	11.2	5.1	0.026
	Fabric-BGN	90.9	6.0	3.4	0.018
	Our model	96.5	3.5	2.0	0.003
20%	Paillier	81.7	9.0	5.0	0.041
	DP	74.5	13.8	6.2	0.032
	Fabric-BGN	85.3	7.5	4.5	0.020
	Our model	93.8	4.6	2.7	0.005

According to Table 2, as the proportion of abnormal nodes increased, the ADR values of all methods showed a downward trend, while the FPR and ART values increased accordingly, indicating an increase in the safety pressure faced by the system. The research model maintained a high ADR between 93.8% and 97.8% under various abnormal ratios, a low FPR between 3.1% and 4.6%, and a short ART between 1.7s and 2.7s, indicating its strong security robustness and fast response capability in multi-node, multi-region, and high concurrency environments. Even in the face of 20% abnormal nodes, it could effectively identify anomalies and quickly restore normal system operation, reflecting the high reliability and practical value of the model in cross domain data security management of power grid SCSs. Meanwhile, the above differences were statistically significant when compared with Paillier, DP and Fabric-BGN under each abnormal proportion (univariate ANOVA supplemented by Tukey post test, $p<0.05$;) The typical range is $p=0.003$-0.041. Under the condition of 20% abnormal nodes, the relative increase/decrease of ADR, FPR and ART all reached significant levels, further confirming the robustness of the results.

It should be pointed out that although the improved BGN algorithm demonstrated excellent encryption performance and security robustness in experiments, its semi-homomorphic characteristics still retained the limit on the number of multiplication operations. Therefore, the current model mainly relies on the phased operation mode of additive blocking and proxy re-encryption when dealing with multi-layer nonlinear aggregation tasks, and has not achieved fully homomorphic computing. Future work can introduce polynomial homomorphism or lattice-based encryption extension mechanisms while maintaining computational efficiency, in order to further enhance the expressive power and scalability of encrypted data analysis.

To further verify the defense effect of the improved BGN algorithm in different attack scenarios and provide formal support for the aforementioned "Security Level 5" conclusion, the study constructed a security test model for typical threat scenarios based on the robustness analysis in Table 2. The test assumptions include four types of threats: passive monitoring, active tampering, key leakage and replay attacks, and define the corresponding security goals: ① Ensure the confidentiality and integrity of encrypted data during transmission and aggregation processes; ② Prevent aggregation forgery caused by the leakage of node private keys; ③ Ensure the non-repudiation of identity and the verifiability of results in cross-chain communication. The attack simulations of each model are all based on the same network and computing environment And the Attack Success Rate (ASR), Key Inference Probability (KIP), and Defense Overhead (DO) are taken as the main indicators. The test results are shown in Table 3.

Table 3. Threat model and security evaluation results

Attack Type	Security Objective	Compared Methods	ASR (%)	KIP ($\times 10^{-5}$)	DO (ms)	Evaluation
Passive eavesdropping	Data confidentiality	Paillier / DP / Fabric-BGN / Our model	5.8/7.2/4.3/0.9	4.2/5.6/3.1/0.5	2.6/1.8/2.1/2.9	Excellent
Active tampering	Data integrity	Paillier / DP / Fabric-BGN / Our model	6.5/9.4/5.2/1.3	5.0/7.8/3.9/0.7	3.5/2.4/2.8/3.2	Excellent
Key exposure	Key privacy & re-encryption resilience	Paillier / DP / Fabric-BGN / Our model	8.9/11.3/6.7/1.1	8.5/9.8/5.4/0.8	4.2/3.5/3.6/4.1	Excellent
Replay attack	Non-repudiation & verifiability	Paillier / DP / Fabric-BGN / Our model	4.7/8.5/5.0/0.7	3.9/6.2/2.8/0.4	2.8/2.0/2.3/3.0	Excellent

As can be seen from Table 3, the improved BGN model demonstrates significant advantages in all four types of threat scenarios. For passive eavesdropping and active tampering attacks, its attack success rate (ASR) dropped to 0.9% and 1.3% respectively, which was approximately 80% and 75% lower than that of the Paillier and Fabric-BGN models respectively, indicating that the confidentiality and integrity during the transmission link and aggregation process were effectively guaranteed. In the scenario of key leakage, after combining Shamir's secret sharing and proxy re-encryption mechanisms, the minimum key inference probability (KIP) is only 0.8×10^{-5}, which proves that this mechanism can resist the risks of single-node leakage and key replay. The defense time cost (DO) is within the range of 2.9 to 4.1 ms, which is approximately 30% higher than that of the traditional Paillier algorithm, indicating that the security enhancement has a limited impact on system latency. Overall, the improved BGN algorithm takes into account both high defense strength and computational feasibility under provable security assumptions. It achieves an "Excellent" assessment level in all attack scenarios, thereby providing a quantitative basis for the definition of comprehensive security Level 5.

CONCLUSION

The study proposed a data security management method for the power grid supply chain based on a dual-consortium blockchain architecture and an improved BGN algorithm. Within the dual-consortium blockchain framework, edge nodes were responsible for the preliminary processing, encryption, and primary aggregation of local data. The aggregated results were then uploaded to the business chain for transaction processing and summarization. Subsequently, audit supervision and secondary aggregation were performed through the supervisory chain, ensuring traceability and non-repudiation of data interactions under cross-chain communication. The improved BGN algorithm protected sensitive information by processing data in an encrypted form, thereby restricting service providers to accessing only encrypted data. The experimental findings indicated that the CDA peak of the proposed method reached 1,280 requests/s and eventually stabilized at 1,255 requests/s, demonstrating high efficiency in cross-domain concurrent data access. Even when faced with 20% abnormal nodes, the ADR value still achieved 97.8%. Moreover, compared with the Paillier, DP, and Fabric-BGN methods, the proposed method exhibited superior performance in terms of security, encryption efficiency, and cross-domain data sharing capabilities, with an average encryption/decryption time of only 21.3 ms and a security level of 5, fully meeting the comprehensive requirements for efficiency, security, and privacy protection in the power grid SCS. However, cross chain data sharing relies on the coordination of multiple signature notary nodes, and if the nodes fail or are delayed, it may affect the system's response speed. In the future, intelligent anomaly detection and adaptive strategies can be explored to improve the model's self recovery ability in multiple regions and types of anomaly nodes.

REFERENCES

[1] Wang L, Wang Y. Supply chain financial service management system based on block chain IoT data sharing and edge computing. Alexandria engineering journal. 2022 Jan 1;61(1):147-58. https://doi.org/10.1016/j.aej.2021.04.079

[2] Ting L, Khan M, Sharma A, Ansari MD. A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing. Journal of Intelligent Systems. 2022 Feb 2;31(1):221-36. https://doi.org/10.1515/jisys-2022-0012

[3] Pragadeswaran S, Subha N, Varunika S, Moulishwar P, Sanjay R, Karthikeyan P, Aakash R, Vaasavathathaii E. Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. Archives for Technical Sciences. 2024 Oct;31(2):148-58. https://doi.org/10.70102/afts.2024.1631.148

[4] Li KC, Shi RH, Guo WP, Wang PB, Shao BS. Dynamic range query privacy-preserving scheme for blockchain-enhanced smart grid based on lattice. IEEE Transactions on Dependable and Secure Computing. 2023 Jun 21;21(4):1652-64. https://doi.org/10.1109/TDSC.2023.3288228

[5] Sharma A, Pandey A. Design and Implementation of a Secure Cloud-Based Storage System. International Academic Journal of Science and Engineering. 2024;11(4):22-6. https://doi.org/10.71086/IAJSE/V11I4/IAJSE1166

[6] Zhonghua C, Goyal SB, Rajawat AS. Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. The Journal of Supercomputing. 2024 Jan;80(2):1396-425.

[7] Aravind B, Harikrishnan S, Santhosh G, Vijay JE, Saran Suaji T. An efficient privacy-aware authentication framework for mobile cloud computing. International Academic Journal of Innovative Research. 2023;10(1):1-7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[8] Tulkinbekov K, Kim DH. Blockchain-enabled approach for big data processing in edge computing. IEEE Internet of Things Journal. 2022 Mar 21;9(19):18473-86.

[9] Prabu K, Sudhakar P. An automated intrusion detection and prevention model for enhanced network security and threat assessment. International Journal of Computer Networks and Applications. 2023 Aug;10(4):621. https://doi.org/10.22247/ijcna/2023/223316

[10] Zhang S, Wang Z, Zhou Z, Wang Y, Zhang H, Zhang G, Ding H, Mumtaz S, Guizani M. Blockchain and federated deep reinforcement learning based secure cloud-edge-end collaboration in power IoT. IEEE Wireless Communications. 2022 Apr;29(2):84-91.

[11] Lee HS, Lim S, Yie I, Yun A. On insecure uses of BGN for privacy preserving data aggregation protocols. Fundamenta Informaticae. 2023 Mar 15;188(2):91-101. https://doi.org/10.3233/FI-222143

[12] Hu C, Liu Z, Li R, Hu P, Xiang T, Han M. Smart contract assisted privacy-preserving data aggregation and management scheme for smart grid. IEEE Transactions on Dependable and Secure Computing. 2023 Aug 1;21(4):2145-61. https://doi.org/10.1109/TDSC.2023.3300749

[13] Zhang QY, Wang K. Parallel Speech Encryption Method Based on BGN Homomorphic Encryption in Cloud Computing. International Journal of Network Security. 2024 Nov 1;26(6):943-56. https://doi.org/10.6633/IJNS.202411 26(6).04

[14] Benamara O, Merazka F. A new distribution version of Boneh-Goh-Nissim cryptosystem: Security and performance analysis. Journal of Discrete Mathematical Sciences and Cryptography. 2022 Aug 18;25(6):1633-47. https://doi.org/10.1080/09720529.2020.1782570

[15] Zhao M, Ding Y, Tang S, Liang H, Wang H. A blockchain-based framework for privacy-preserving and verifiable billing in smart grid. Peer-to-Peer Networking and Applications. 2023 Jan;16(1):142-55.

[16] Zeng Z, Liu Y, Chang L. A robust and optional privacy data aggregation scheme for fog-enhanced IoT network. IEEE Systems Journal. 2022 Jun 3;17(1):1110-20. https://doi.org/10.1109/JSYST.2022.3177418

[17] Zhang X, Huang C, Xu C, Zhang Y, Zhang J, Wang H. Key-leakage resilient encrypted data aggregation with lightweight verification in fog-assisted smart grids. IEEE Internet of Things Journal. 2020 Dec 29;8(10):8234-45.

[18] Huang X, Wu Y, Liang C, Chen Q, Zhang J. Distance-aware hierarchical federated learning in blockchain-enabled edge computing network. IEEE Internet of Things Journal. 2023 Jun 28;10(21):19163-76. https://doi.org/10.1109/JIOT.2020.3047958

[19] Zhang S, Zhang Y, Wang B. Antiquantum privacy protection scheme in advanced metering infrastructure of smart grid based on consortium blockchain and RLWE[J]. IEEE Systems Journal, 2023, 17(2): 3036-3046. DOI: 10.1109/JSYST.2023.3244630.

[20] Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems. 2023 Aug;9(4):3759-86.

[21] Tomar A, Tripathi S. Blockchain-assisted authentication and key agreement scheme for fog-based smart grid. Cluster Computing. 2022 Feb;25(1):451-68.

[22] Vangala A, Das AK, Chamola V, Korotaev V, Rodrigues JJ. Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. Cluster Computing. 2023 Apr;26(2):879-902.

[23] Almasabi S, Shaf A, Ali T, Zafar M, Irfan M, Alsuwian T. Securing smart grid data with blockchain and wireless sensor networks: A collaborative approach. IEEE Access. 2024 Feb 2;12:19181-98. https://doi.org/10.1109/ACCESS.2024.3361752

[24] Li D, Gong Y. The design of power grid data management system based on blockchain technology and construction of system security evaluation model. Energy Reports. 2022 Oct 1;8:466-79. https://doi.org/10.1016/j.egyr.2022.05.277

[25] Yu P, Huang W, Li Z. A Secure, lightweight, and verifiable data aggregation scheme for smart grids. Peer-to-Peer Networking and Applications. 2025 Jun;18(3):1-1.

[26] Mahato GK, Chakraborty SK. Securing edge computing using cryptographic schemes: a review. Multimedia Tools and Applications. 2024 Apr;83(12):34825-48.