Blockchain and Fully Homomorphic Encryption for Secure Data Management in Smart Grids

Chu-Hui Li*, Zhong-Ming Dong,
Tian-Xiong Huang and Yi Dong

China Yangtze Power Co., Ltd. Wudongde Hydropower Plant, Kunming 651580, Yunnan, China
E-mail: Chuhui_Li1983@outlook.com
**Corresponding Author*

Received 25 February 2026; Accepted 30 March 2026

Abstract

The storage security and privacy protection of power plant ancillary service data face severe challenges, hindering power plant operation optimization and the efficient operation of the electricity market. This research aims to construct a secure and reliable data storage system for power plant ancillary services and establish a scientific and accurate performance evaluation method. To achieve this, a multi-layer technology fusion model based on blockchain, fully homomorphic encryption (FHE), and smart contracts is proposed. The architecture integrates blockchain for trusted data provenance, FHE for privacy-preserving computation, and smart contracts for automated business logic execution, forming a coherent and secure data management framework. Specifically, the study adopts a hybrid storage mode combining blockchain structure and private database. Secure interaction and homomorphic operations of encrypted data are achieved through smart contracts. An improved approximation-ideal solution sorting method is used, combined with fuzzy hierarchical analysis to determine indicator weights. The results

Journal of Cyber Security and Mobility, Vol. 15_2, 467–496.
doi: 10.13052/jcsm2245-1439.1528
© 2026 River Publishers

showed that in the ancillary business data test of a provincial power system in 2023, the proposed storage scheme achieved a data leakage rate of 1% for 10,000 pieces of data and a tampering detection success rate of 98.99%. This performance evaluation method was applied to six cross-regional power plants, effectively distinguishing the performance differences of ancillary services among different power plants. The relative similarity of the frequency regulation scenario in new energy power plants was 0.85, which was 12% higher than that in thermal power plants. This research provides a reliable and secure storage path for power plant ancillary service data, promoting the digital transformation of the power system and the standardized development of the electricity market. However, the proposed approach may face adaptability challenges in cross-regional deployment due to varying grid regulations and data standards, and the computational overhead of fully homomorphic encryption could impact real-time performance in large-scale applications. Future work will focus on optimizing algorithm efficiency, reducing computational costs, and validating the framework across diverse regional power systems to enhance its generalizability and practical deployment.

Keywords: Blockchain, fully homomorphic encryption, power plant ancillary services, secure data storage, performance evaluation.

1 Introduction

In the context of energy transformation and deepening of the power market, the secure storage and performance evaluation of power plant ancillary service data are crucial to grid stability and market fairness [1, 2]. This type of data is a high-value asset, and its storage reliability and scientific evaluation directly affect system operation efficiency and market regulation levels. Currently, data security storage mainly faces multiple risks such as privacy leakage, illegal tampering, and single point failure of centralized architecture [3]. The traditional centralized storage model has vulnerabilities exposed in centralized data sets. Although the pure blockchain certificate storage solution can ensure non-tamperability, it is difficult to effectively protect the privacy of sensitive data content itself. Therefore, the industry urgently needs to build a new storage solution that can combine tamper resistance, privacy protection and trusted sharing capabilities. Blockchain technology can provide a solid foundation for trustworthy certificates. However, its inherent full on-chain storage model can easily lead to data redundancy

and storage expansion, and it is difficult to directly support calculations and in-depth analysis of encrypted data. This limits its application in privacy-sensitive scenarios [4]. Meanwhile, ancillary service performance evaluation is the core link of data value conversion. Most of the existing methods are highly dependent on expert experience. There are common problems such as strong subjectivity in the evaluation process, failure of the indicator system to fully adapt to the characteristics of new energy, and arbitrary setting of indicator weights [5]. It is difficult to meet the urgent need for diversified and refined evaluation of ancillary service in power systems after a high proportion of new energy is connected.

Therefore, this research aims at the above two challenges and builds a secure storage architecture that deeply integrates blockchain and FHE technology to solve the contradiction between trustworthiness and privacy in data storage. At the same time, this research establishes a set of ancillary service performance evaluation methods based on fuzzy analytic hierarchy process (FAHP) and technique for order preference by similarity to ideal solution (TOPSIS) to improve the scientific nature of the evaluation process and the accuracy of the results. This research hopes to provide reliable technical support for the trustworthy management of power plant ancillary service data and the efficient operation of the power market through technological innovation in these two aspects.

2 Literature Review

Since the development of power system data security management, some of its theories and practical applications have become relatively mature. Scholars from many countries have conducted in-depth research on it and applied it in actual enterprise management. For example, Wang J et al. addressed the security challenges of data privacy leakage and tampering in the edge computing environment of the smart grid, proposing a data security enhancement scheme that integrates federated learning and blockchain. By constructing a distributed architecture of "local training – global aggregation – on-chain verification", they achieved protection of users' electricity privacy and integrity guarantee of the data transmission process without sharing the original data. Experimental results showed that the privacy leakage rate of the combined scheme of federated learning and blockchain was only 0.9%, much lower than 60.2% of the scheme without privacy protection [6]. Guo L et al. addressed the problems of data islands and data leakage in traditional power dispatching, proposing a collaborative operating

system for the metaverse power trading that integrates blockchain and privacy computing technology. This scheme integrates homomorphic encryption, zero-knowledge proof, and secure multi-party computation to achieve data security sharing under privacy protection, and uses the PBFT consensus mechanism to resist malicious nodes, combined with the MOPSO algorithm and smart contracts to optimize the scheduling decision. At the same time, through NFT and IPFS, a new data management scheme is constructed to provide a secure and efficient data storage and transmission environment for power transactions [7]. Jiyuan S et al. addressed the challenges of data privacy protection and verification efficiency in the blockchain, proposing a privacy computing scheme that integrates BGV homomorphic encryption and Pedersen secret sharing. While supporting secure computation of ciphertexts, it relies on blockchain to complete key splitting management and verification, constructing a trusted ciphertext computing environment and achieving the security goal of "data available but invisible" [8]. Altamimi E. et al. addressed the critical challenge of data scarcity in smart grid research due to the reluctance of operators to share proprietary information. They conducted a comprehensive review and categorization of over 50 publicly available datasets, systematically organizing them into three primary types: micro- and macro-consumption data, detailed in-home consumption data (including non-intrusive load monitoring and building data), and grid operation data. The study further identified key future research directions, such as synthetic data generation, data quality standardization, and enhanced big data management. This work aims to serve as a foundational reference for researchers, enabling them to systematically select appropriate public datasets for method validation and evaluation, thereby promoting more standardized and reproducible advancements in smart grid analytics [9]. Onukwulu E C et al. addressed the low efficiency and insufficient transparency problems of the traditional energy supply chain, proposing a decentralized energy supply chain solution based on blockchain and Internet of Things technology. This research ensures the non-tamperability and transparency of energy transaction records through blockchain technology, and combines IoT devices to achieve real-time monitoring of energy production, storage, and consumption, promoting point-to-point energy trading and microgrid development while effectively improving the operational efficiency, security, and sustainability of the energy system [10].

Blockchain is a comprehensive architecture that integrates distributed ledgers, smart contracts and cryptography technologies. By systematically integrating the advantages of different technology modules, it can build

collaborative solutions that go beyond a single technology and effectively respond to complex challenges such as trusted storage, privacy protection and multi-party collaboration faced in the digitalization process. Researchers from both domestic and foreign universities have studied it. For instance, to solve the data security and performance issues that chatbots encounter, Yu P et al. addressed the security risk that fine electricity consumption data in smart meters, although beneficial for grid management, could easily disclose users' behavioral privacy. They proposed an advanced verifiable privacy protection data aggregation scheme. This scheme designed a new HTVDA protocol, combining the Paillier cryptosystem with threshold decryption technology, effectively hiding the system private key, making it invisible to any participant except for the trusted third party, thereby simultaneously defending against user collusion and key leakage risks. Preliminary tests indicated that this scheme maintained high security while significantly reducing computational and communication costs, with the encryption speed approximately seven times faster than existing methods [11]. Mijwil M M et al. addressed the quantum computing threat and centralized architecture risks faced by the smart grid through a systematic review, pointing out the anti-quantum deficiencies of the existing blockchain federated learning model, and then proposed a scalable PQS-BFL framework integrating lightweight post-quantum cryptographic protocols. This framework enables decentralized, privacy-protected, and quantum-resistant secure collaboration among grid nodes, effectively enhancing data integrity and resisting quantum attacks and inference threats, providing a feasible security path for the next-generation intelligent energy system [12]. Zhang Z et al. addressed the challenges faced by the existing power grid, such as increasing power demand, increased system complexity, and the stability issues brought by the integration of renewable energy, proposing a new asynchronous renewable elastic energy grid architecture centered on communities. This research distinguished the concepts of grid resilience and reliability, proposed a system solution based on technical classifications such as natural source frequency, direct energy conversion/control, and fault protection, and demonstrated that the networked microgrid, when combined with distributed and centralized control algorithms, can effectively shorten power restoration time and enhance grid stability, providing a theoretical basis and technical path for the construction of future high-renewable energy grid [13]. Naiho et al. addressed the problem of reduced inertia in power systems due to large-scale renewable energy integration and the challenges to stability. They systematically expounded the key role of power electronic converters in the

grid connection of new energy generation. The study analyzed the technical requirements and control methods for the integration of wind power, photovoltaic, and energy storage systems, and proposed improving the current control of the converter and system-level coordinated operation to enhance the controllability and flexibility of the grid, indicating the technical path for the future power electronic development of high-renewable energy grids [14]. Ganesh P M J et al. addressed the key role of accurate load forecasting in optimizing energy management in smart grids and the lack of advanced prediction frameworks enabled by the Internet of Things in the grid system. They proposed a new intelligent deep optimization energy management framework. This framework uses a deep learning model based on stacked convolutional bidirectional gated attention networks to achieve precise prediction of energy load in the smart grid data set and introduces a hybrid dart-seagull optimizer for learning rate estimation to optimize the prediction process and reduce errors. Based on the evaluation results of several well-known datasets such as ISO-NE, SGSC, and IHEPC, the proposed framework can effectively reduce the prediction error rate to 0.3, providing an innovative technical solution for the efficient and reliable energy management of the Internet of Things-enabled smart grid [15]. Alzahrani A et al. proposed a verifiable data element circulation scheme combining BGV homomorphic encryption with blockchain, demonstrating improved privacy but lacking detailed analysis on deployment costs and scalability. A systematic review by Alzahrani and Alghazzawi specifically examined blockchain and homomorphic encryption for secure data sharing in smart grids, comparing various schemes in terms of encryption latency, throughput, and resistance to common attacks. Their analysis reveals that while FHE offers strong privacy guarantees, its integration with blockchain often results in high transaction latency and increased storage requirements due to the large ciphertext sizes. Moreover, most existing solutions are validated only in controlled laboratory settings, with limited evidence of successful deployment in real-world power grid environments [16]. This lack of empirical validation underscores the gap between theoretical advances and practical applicability, motivating the need for a solution that balances security, efficiency, and real-world deployability.

In conclusion, current research on power system data security management has produced some breakthroughs, but its storage solutions still have drawbacks such the possibility of a single point of failure, inadequate data privacy protection, and restricted ciphertext computing capabilities. The technical path of integrating blockchain and FHE can effectively make up for

these shortcomings through innovative solutions such as building a hybrid storage architecture and implementing ciphertext homomorphic operations. Therefore, this study proposes a comprehensive data security management solution for power plant ancillary service. This solution deeply integrates blockchain and FHE to build a secure storage and computing method. Moreover, it introduces the improved TOPSIS evaluation system to achieve scientific evaluation of ancillary service performance. This research hopes that it can improve the security, credibility and scientific evaluation of ancillary service data storage in the process of digitalization of the power system to meet the dual needs of new power systems for trusted data sharing and privacy protection.

3 Methods

3.1 Secure Storage of Power Plant Ancillary Service Data Integrating Blockchain and FHE

Building upon the literature review, this section elaborates the design logic and innovative points of the proposed blockchain-FHE fusion architecture for power plant ancillary service data management. Unlike existing approaches that treat blockchain and encryption as separate layers, this study integrates them through a tightly coupled mechanism addressing key management, smart contract invocation timing, and the connection between on-chain and off-chain computation. The architecture employs a hierarchical key management scheme where the FHE key pair is generated by a trusted authority, with public and evaluation keys distributed to participants and embedded into smart contracts, while the private key remains offline. Smart contract invocation is triggered by specific business events – such as data submission or settlement requests – automatically executing homomorphic operations on encrypted data. The connection between on-chain and off-chain computing is realized through a hybrid storage model: raw encrypted data resides in off-chain private databases, with only data hashes and computation results recorded on the blockchain, enabling verifiable integrity checks without exposing sensitive content. This design offers three key innovations: (1) separation of keys by function to minimize attack surface, (2) event-driven contract execution aligned with power ancillary service workflows, and (3) a verifiable link between on-chain hashes and off-chain data, transforming blockchain from a simple ledger into a privacy-preserving computation platform tailored for power system applications.

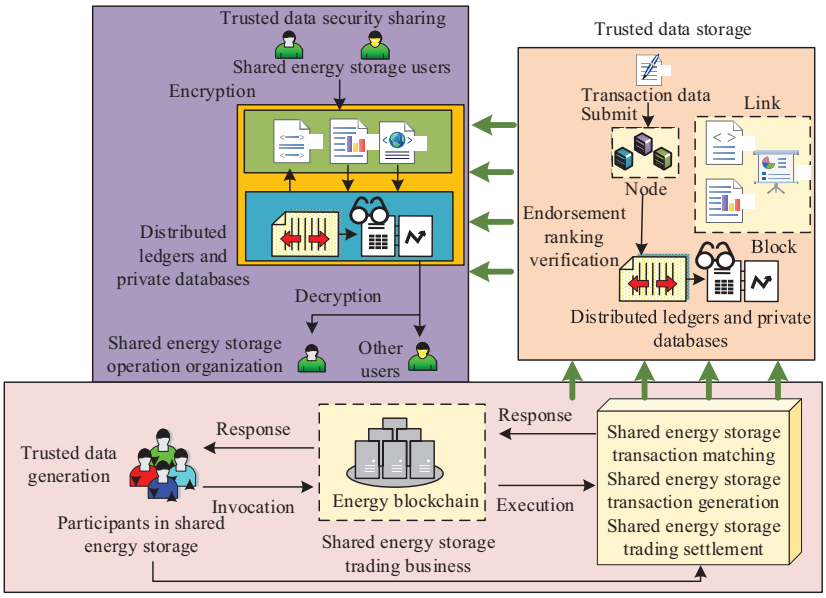

Figure 1 Data security storage mechanism of regional chain power plant ancillary service.

As a high-value asset, the storage of power plant ancillary service data faces the dual challenges of privacy protection and trusted sharing. Traditional centralized solutions have single points of failure and tampering risks [17]. To this end, blockchain technology is introduced to build a decentralized storage solution, relying on its non-tamperable and traceable distributed ledger characteristics to provide a trustworthy evidence storage basis for data. It also combines smart contracts to achieve automation and transparency of business logic, fundamentally ensuring data integrity and transaction fairness [18]. The regional chain data security storage mechanism is shown in Figure 1.

As shown in Figure 1, the overall process of this mechanism is: energy storage users ENCRYPT original data and respond to business calls. The core link submits transaction data to the blockchain network, and is packaged into blocks after being endorsed, sorted, and verified by nodes. It also adopts a hybrid storage model of "distributed ledger and private database" to ensure data cannot be tampered with and privacy is secure. Finally, transaction matching, settlement, and other services are automatically completed through smart contracts on the chain. Moreover, the results are returned, forming a closed loop from data on-chain, safe storage to automatic execution. This

mechanism solves the problems of security, trust and efficiency in data sharing, and verifies the integrity of encrypted data in private libraries in the "trusted data storage" link [19]. This verification is done by comparing the hash value stored on the chain with the hash value recalculated from the off-chain data, as shown in Equation (1).

$$\text{Verify}(D) = \begin{cases} \text{True}, & \text{if} H(D_c) = H_{\text{chain}} \\ \text{False}, & \text{otherwise} \end{cases} \tag{1}$$

In Equation (1), $\text{Verify}(D)$ represents the data integrity verification function. D_c represents the encrypted data content obtained from the off-chain private database. H_{chain} represents the original hash value. In the "Shared Energy Storage (SES) Transaction Settlement" link, after the smart contract is called, the settlement amount of each participant is automatically calculated according to the preset rules, as shown in Equation (2).

$$P_i = \sum_{j=1}^{n} (Q_{ij} \times R_j) - C_i \tag{2}$$

In Equation (2), P_i represents the final income deserved by the ith user during the settlement cycle. n displays the total quantity of categories of ancillary service evaluation indicators. Q_{ij} represents the actual contribution or performance score of the ith user on the jth indicator. R_j represents the weight coefficient corresponding to the j indicator. C_i represents the system service fee borne by the ith user.

Although the blockchain can ensure that data cannot be tampered with, it cannot support direct calculation of ciphertext data. Decryption and calculation will destroy privacy. FHE enables encrypted data to be directly subjected to aggregation, statistical and other operations, and the decrypted calculation results are consistent with the results of the same calculation directly performed on plain text. This technology supports key businesses such as performance evaluation and revenue settlement without exposing original data. On the basis of blockchain's "certificate trustworthiness", "computing trustworthiness" and "process privacy" are achieved, and a closed loop of full-process privacy protection is built. Therefore, to achieve "available invisibility" in data sharing computing, this study introduces FHE technology. Figure 2 shows the core process of trustworthy computing of encrypted data based on FHE.

As shown in Figure 2, the FHE-based SES data security calculation process is as follows: The operating organization first generates a key system

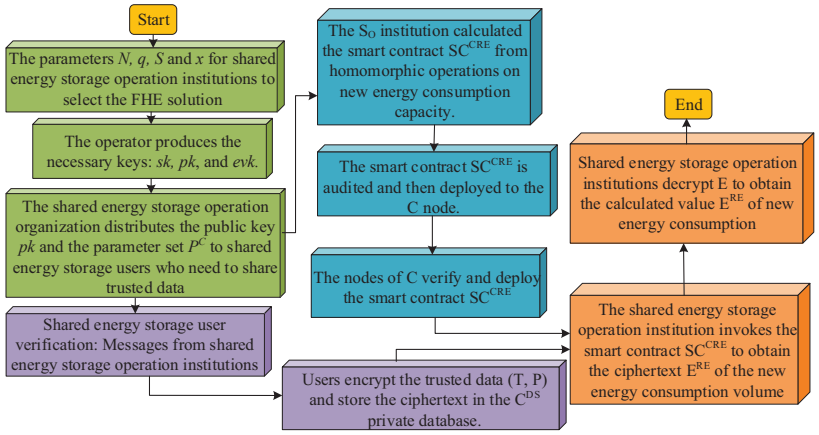

Figure 2 Core process of trusted computing of encrypted data based on FHE encryption scheme.

and distributes the public key. After the user is authenticated, the data is encrypted and stored in a private repository. Audited and verified smart contracts perform homomorphic operations directly on ciphertext. Finally, the operating organization calls the contract to obtain the encrypted calculation results, realizing trustworthy calculations with full-process encryption, taking into account both privacy protection and data value mining.

At the beginning of the process, the SES operating organization needs to initialize the cryptographic system [20], including selecting security parameters and generating keys: The private key is used for decryption, the public key is used for encryption, and the evaluation key is used for ciphertext calculation, as shown in Equation (3).

$$(pk, sk, evk) \leftarrow \mathrm{KeyGen}(1^{\lambda}, P^{c}) \tag{3}$$

In Equation (3), λ represents the safety parameter. P^c represents the common parameter set of the FHE system. KeyGen stands for key generation algorithm. pk represents the public key. sk stands for private key. evk stands for Evaluation Key. After SES users obtain the public key, they need to encrypt their sensitive data before they can be safely stored in the private database [21-22], as shown in Equation (4).

$$c := \mathrm{Enc}(pk, m) \tag{4}$$

In Equation (4), m represents the plaintext data to be encrypted. Enc stands for encryption algorithm. c represents the ciphertext obtained after

encryption. After the calculation is completed, the operating organization uses its private key to decrypt the final result, and the plaintext can be calculated as shown in Equation (5).

$$m_{\text{result}} := \text{Dec}(sk, \text{Eval}(evk, f, c_1, c_2, \ldots, c_n)) \tag{5}$$

In Equation (5), m_{result} represents the plaintext calculation result obtained after decryption. Dec represents the decryption algorithm. Eval stands for homomorphic assessment algorithm. f represents the calculation function that needs to be performed. $c_1, c_2, \ldots, c_n$ represents multiple ciphertext data input into the smart contract.

This study presents a hash function-based message authentication code technique to improve the FHE scheme's security in terms of data integrity verification and key derivation. This improvement aims to ensure that the ciphertext data can not only maintain content privacy during the homomorphic computing process, but also verify its integrity and authenticity to prevent data from being tampered with during transmission or processing. The hash function is shown in Figure 3.

In Figure 3, the hash function generation process begins with key filling and blocking. Then two layers of hashing calculations are performed: the inner layer of hashing XORs the processed key with the fixed constant ipad, and then splices it with the message and calculates it through a hash function. The outer hash XORs the same key with the constant opad, and then

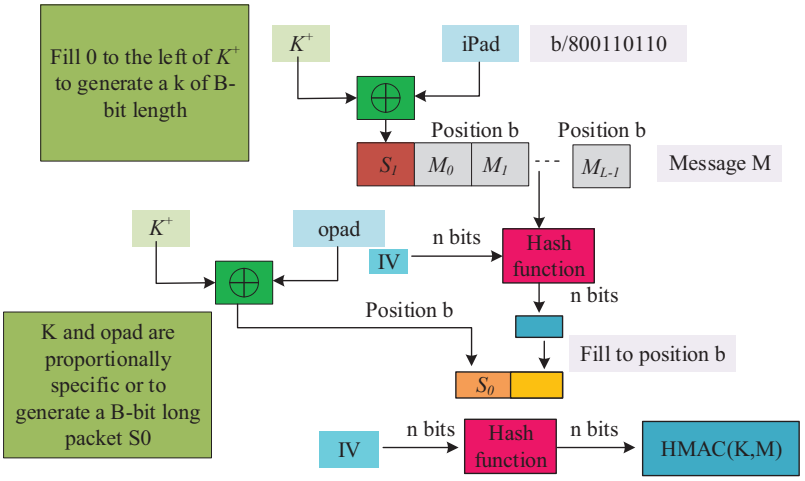

Figure 3 Hash function diagram.

concatenates it with the inner hash result for a second hash. Finally output the HMAC value of the specified length. Among them, the calculation process of the inner hash is displayed in Equation (6).

$$S_i = H((k \oplus \text{ipad}) \parallel M) \tag{6}$$

In Equation (6), S_i displays the calculated inner hash value. H represents the selected cryptographic hash function. ipad represents a fixed internal fill constant. M represents the original message that requires authentication. Then, the outer hash calculation is performed using the inner hash result and the key to obtain the final HMAC value, which is used as the authentication label of the message, as shown in Equation (7).

$$\text{HMAC}(K', M) = H((k \oplus \text{opad}) \parallel S_i) \tag{7}$$

In Equation (7), $\text{HMAC}(K', M)$ represents the final output message authentication code. opad represents a fixed external fill constant. The research proposes a safe storage method for power plant ancillary service data by integrating blockchain and FHE technology. Blockchain ensures that data cannot be tampered with, laying the foundation for trust. FHE realizes "available and invisible" secure calculation of data, and ultimately uses smart contracts to automate business execution and solve the problems of security, trust and efficiency in data sharing.

3.2 Power Plant Ancillary Service Performance Evaluation Based on Improved TOPSIS

The traditional TOPSIS method, while effective for multi-criteria decision-making, suffers from two major limitations when applied to power plant ancillary service performance evaluation: (1) it relies on subjectively assigned weights, which may introduce bias and reduce the credibility of evaluation results; (2) it lacks the capability to handle the inherent uncertainty and fuzziness in expert judgments and real-world operational data. To address these issues, this study proposes an improved TOPSIS method that integrates fuzzy set theory and FAHP-derived weights. The improvement consists of two key aspects: First, triangular fuzzy numbers are used to capture the vagueness of expert opinions during the weighting process, transforming qualitative comparisons into quantitative fuzzy judgments. Second, instead of using arbitrary or equal weights, the method incorporates the objective weights obtained from FAHP into the TOPSIS framework, ensuring that the distance to ideal solutions reflects the true importance of each criterion.

This FAHP-enhanced TOPSIS approach not only preserves the simplicity and intuitiveness of the original method but also significantly improves its robustness against subjective bias and data uncertainty.

The secure storage platform based on blockchain and FHE provides a trusted privacy computing basis for power plant ancillary service data, ensuring data integrity and privacy security, and supporting trusted transactions and settlements in the power market. Establishing a scientific multi-dimensional performance evaluation system is required to objectively quantify the performance differences of each power plant under scenarios like frequency regulation and peak regulation in order to effectively transform the value of data into dispatch decisions and market incentives. To this end, this study constructs a multi-dimensional, quantifiable power plant ancillary service evaluation index system (as shown in Table 1) to support accurate evaluation, power grid dispatching and market incentives, forming a benign closed loop of "trusted storage-accurate evaluation-efficient operation".

In Table 1, the evaluation system constructs a comprehensive evaluation framework from four dimensions: economic, technical, social, and sustainability. To scientifically evaluate the performance, the study uses triangular fuzzy numbers FAHP for index weighting to reduce subjectivity. To accomplish quantitative scoring and ranking of power plant performance, the TOPSIS model is then utilized to determine each scheme's relative proximity (RP) to the positive ideal solution (PIS) and negative ideal solutions (NIS) based on the collected weights. The combination of FAHP and TOPSIS forms a complete evaluation process from "subjective empowerment" to "objective ranking". The flow chart is shown in Figure 4.

As shown in Figure 4, the study uses FAHP and TOPSIS to comprehensively evaluate power plant ancillary service performance. This process first constructs the original evaluation matrix and eliminates the dimensional influence through standardization processing, and then uses FAHP to determine the index weight and construct a weighted standardized matrix. The ranking based on RP is then completed after determining the PIS and NIS, respectively, and calculating the weighted Euclidean distance (ED) between each solution and the ideal solution. The power plant's total performance improves with increasing proximity. The vector normalization method is a classic and effective standardization method in TOPSIS, as shown in Equation (8).

$$r_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{m} a_{ij}^2}} \tag{8}$$

Table 1 Assessment index system for ancillary services of power plants

Level	Main Criteria	Sub-criteria	Basic Indicator Layer
Overall objective	Development status (E_1)	Economic benefits (E_{11})	Unit capacity revenue (E_{11})
			Revenue quarter-on-quarter growth rate (E_{112})
			Dynamic investment payback period (E_{113})
		Low-carbon benefits (E_{12})	Proportion of new energy consumption (E_{121})
			New energy consumption per unit capacity (E_{122})
			CO_2 emission reduction (E_{123})
			Shared storage-to-renewable capacity ratio (E_{124})
	Market performance (I_2)	Market structure (E_21)	Seller market concentration (E_{211})
			Buyer market concentration (E_{212})
		Market participation (E_{22})	Supplier storage capacity participation (E_{221})
			Supplier market activity (E_{222})
			Demand-side market activity (E_{223})
		Market efficiency (E_{23})	Equivalent utilization rate of shared storage (E_{231})
			Proportion of market-traded electricity (E_{232})

In Equation (8), r_{ij} represents the standard value of the ith solution under the jth indicator after standardization. a_{ij} represents the original value of the ith solution (power station) under the jth evaluation index. The fundamental idea of the TOPSIS method is to rank each solution by comparing its closeness to PIS and NIS. After obtaining the weighted normalization matrix, two key reference benchmarks need to be determined: the PIS and the NIS, as shown in Equation (9).

$$V^+ = \{v_1^+, v_2^+, \ldots, v_n^+\} = \left\{ \left(\max_i v_{ij} | j \in J_1 \right), \left(\min_i v_{ij} | j \in J_2 \right) \right\} \quad (9)$$

In Equation (9), V^+ represents the ideal solution. J_1 represents a collection of benefit indicators. J_2 represents a collection of cost indicators.

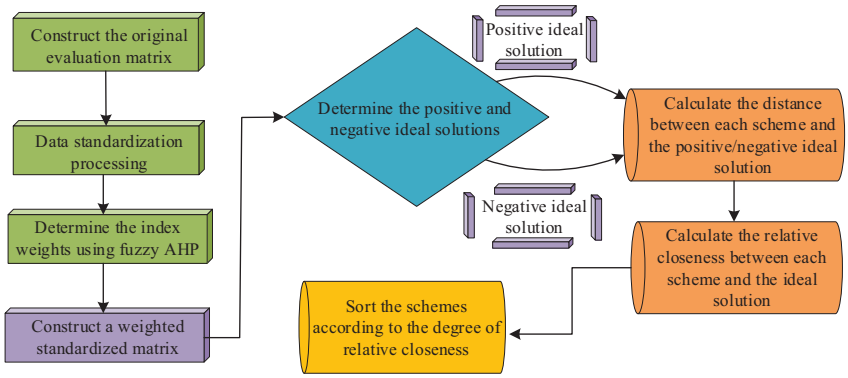

Figure 4 Flow chart of FAHP and TOPSIS evaluation.

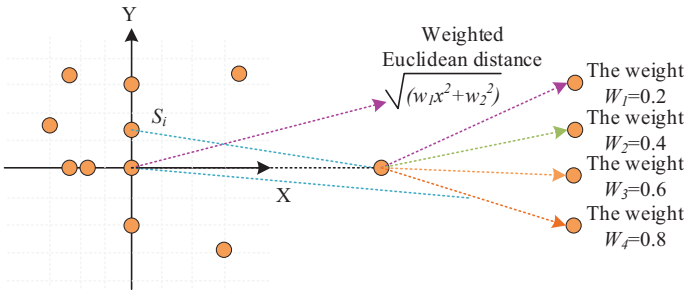

Figure 5 Weighted Euclidean distance.

$\max_i v_{ij}$ and $\min_i v_{ij}$ respectively represent finding the maximum and minimum values of the jth indicator in all schemes. The NIS is shown in Equation (10).

$$V^- = \{v_1^-, v_2^-, \ldots, v_n^-\} = \left\{ \left(\min_i v_{ij} | j \in J_1 \right), \left(\max_i v_{ij} | j \in J_2 \right) \right\} \tag{10}$$

In Equation (10), V^- represents the NIS. After determining the PIS and NIS, the TOPSIS model calculates the "distance" in the multi-dimensional space between each solution to be evaluated (power station) and the two ideal solutions. To reflect the importance of different indicators in distance measurement more scientifically, this study introduces weighted ED as a calculation method. The principle is shown in Figure 5.

As shown in Figure 5, the calculation logic of weighted ED is clarified through a two-dimensional example: the coordinates of the points are the

weighted standardized values of the indicators for each scheme, and the distance components of each dimension need to be multiplied by the corresponding weight. The greater the weight, the more significant the impact of this indicator on the total distance, allowing the evaluation results to focus more on key performance differences and ensuring the scientificity and accuracy of the ranking. Its general calculation formula is shown in Equation (11).

$$D(A,B) = \sqrt{\sum_{j=1}^{n} w_j \cdot (a_j - b_j)^2} \tag{11}$$

In Equation (11), $D(A,B)$ represents the weighted ED between point A and point B. n displays the total dimension of the space. a_j and b_j respectively display the coordinate values of point A and point B on the jth dimension (indicator). w_j represents the weight of the jth dimension (indicator). Equation (12) illustrates how the RP method is applied to solve this problem in order to fully take into account each solution's proximity to the ideal solution and its distance from the worst solution.

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{12}$$

In Equation (12), S_i^+ represents the weighted ED between the ith solution and the PIS, and the weighted ED between the S_i^-th i solution and the NIS. This study constructs a comprehensive evaluation system based on FAHP and TOPSIS. This method first determines the weight of each indicator through FAHP to reduce subjectivity. Then, the index weights obtained by FAHP are applied to the TOPSIS model to calculate the weighted ED between each candidate solution and the PIS and NIS. Finally, based on the RP, the comprehensive performance of the power station in terms of ancillary service is quantified and ranked, forming a complete evaluation closed loop from indicator construction to result output to ensure that the evaluation results are scientific and objective.

4 Results

4.1 Effectiveness Assessment of Power Plant Ancillary Service Data Security Storage Scheme

To verify the effectiveness of blockchain & FHE based ancillary service data security management and performance assessment system (B-FHE-AS), this

Table 2 System validation environment configuration

Category	Configuration Item	Technical Specification	Functional Description
Hardware platform	Server architecture	4-node Dell PowerEdge R740 Cluster	Building distributed storage network
	Computing resources	Intel Xeon Gold 5218 Processor	Supporting cryptographic operations and consensus mechanism
	Storage system	1TB NVMe SSD+10TB HDD Hybrid Array	Implementing on-chain/off-chain tiered storage
	Network environment	10 Gigabit Fiber Ethernet	Ensuring inter-node communication efficiency
Software environment	Underlying framework	Hyperledger Fabric 2.4	Providing blockchain foundation services
	Encryption module	Microsoft SEAL 3.7 FHE Library	Enabling homomorphic computation functionality
	Data management	MongoDB 5.0+IPFS Distributed Storage	Handling off-chain encrypted data storage
	Smart contracts	Go Language Chaincode	Executing business logic and access control
Test parameters	Data sample	Provincial Grid Ancillary Service Full Dataset	Covering scenarios like frequency regulation and reserves
	Performance baseline	Comparison with Traditional Centralized Storage	Evaluating system overhead and performance impact

study constructed a complete test environment. Its system evaluates its data security, system reliability and processing performance. The test is based on the ancillary service data of a provincial power grid in 2023, focusing on testing the performance of anti-leakage, anti-tampering and query efficiency. The main software and hardware configurations used in the test are detailed in Table 2.

Table 2 contains the computer hardware configuration used in the experiment, including key parameters such as processor model, memory size, and storage device type. This study analyzes B-FHE-AS with traditional centralized encryption method for ancillary services (TCE-AS) and blockchain-only attestation method for ancillary services (BA-AS, labeled as "blockchain only" in Figure 6) in data security, as shown in Figure 6.

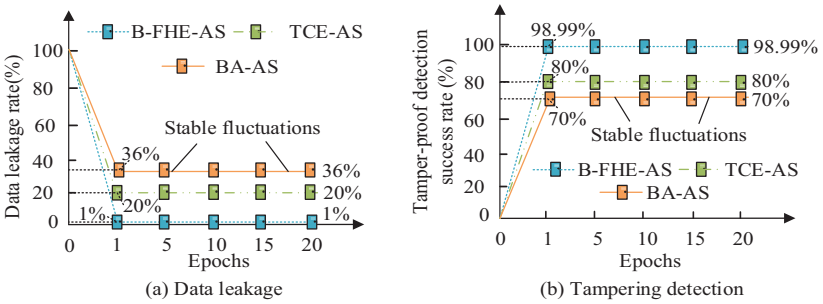

Figure 6 Data security analysis.

Data security performance comparison results in Figure 6(a) show that the B-FHE-AS solution proposed in the study always maintains an excellent level of 1% in data leakage rate, which is significantly lower than the 20% of TCE-AS and 36% of BA-AS. Specifically, compared to TCE-AS, B-FHE-AS reduces the data leakage rate by 95% (from 20% to 1%); compared to BA-AS, the reduction reaches 97.2% (from 36% to 1%). This dramatic improvement is attributed to the hybrid storage architecture combining blockchain and FHE: blockchain ensures data integrity through tamper-proof on-chain hashes, while FHE enables computation directly on ciphertext without exposing raw data, thereby eliminating the privacy leakage risks inherent in traditional centralized storage and plaintext blockchain solutions. The residual 1% leakage rate primarily stems from potential key management vulnerabilities and side-channel attacks during cryptographic operations, which remain within acceptable limits for power grid ancillary service applications according to industry standards.In Figure 6(b), in terms of data integrity, the tamper detection success rate of B-FHE-AS is as high as 98.99%, which is also significantly better than TCE-AS's 80% and BA-AS's 70%. This represents a 23.7% improvement over TCE-AS and a 41.4% improvement over BA-AS. The high detection rate is achieved through the on-chain/off-chain hash verification mechanism described in Equation (1), where each data block's hash is stored on the blockchain and periodically verified against recomputed hashes from the off-chain private database. Any tampering attempt would cause hash mismatch and be immediately detected. The results show that B-FHE-AS has significant advantages in data security and integrity protection.

To further demonstrate the competitive advantages of the proposed B-FHE-AS scheme, we introduce two additional baseline methods representing mainstream "blockchain+privacy computing" fusion paradigms:

Table 3 Performance comparison of different "blockchain+privacy computing" fusion schemes

Performance Metric	B-FHE-AS (Proposed)	B-SMPC-AS	B-ZKP-AS
Data leakage rate	1%	3%	2%
Tamper detection success rate	98.99%	97.50%	98.10%
Average computational latency (ms/transaction)	245	1,280	890
Storage overhead (MB/10,000 records)	156	312	234

(1) blockchain-based secure multi-party computation for ancillary services (B-SMPC-AS), which enables multiple parties to jointly compute a function without revealing their private inputs; and (2) blockchain-based zero-knowledge proof for ancillary services (B-ZKP-AS), which allows data owners to prove the validity of certain statements without disclosing the underlying data. These methods were implemented in the same test environment described in , and their performance metrics are compared with B-FHE-AS in terms of data leakage rate, tamper detection success rate, computational latency, and storage overhead, as summarized in Table 3.

As shown in Table 3, B-FHE-AS achieved the lowest data leakage rate (1% compared to 3% and 2%), the highest tampering detection success rate (98.99% compared to 97.50% and 98.10%), the lowest computational delay (245 milliseconds per transaction compared to 1,280 milliseconds and 890 milliseconds), and the lowest storage overhead (156 MB per 10,000 records compared to 312 MB and 234 MB). These advantages stem from FHE's direct ciphertext computation without intermediate decryption, continuous on-chain/off-chain hash verification, and hybrid storage model. Although B-SMPC-AS and B-ZKP-AS provide alternative privacy protection paths, their higher latency and storage requirements make them less suitable for large-scale, real-time power assistance service scenarios.

The study compares the long-term performance and load conditions of each scheme in the provincial and municipal power grid data environments, as shown in Figure 7.

Figures 7(a) and 7(b) show the performance and load comparison of the three methods B-FHE-AS, TCE-AS, and BA-AS in long-term operation throughout the year (January to December) under the provincial power grid environment in 2023. The results show that the execution time and amount of stored data of B-FHE-AS are significantly lower than those of TCE-AS and BA-AS in each month. Figures 7(c) and 7(d) further show the comparison

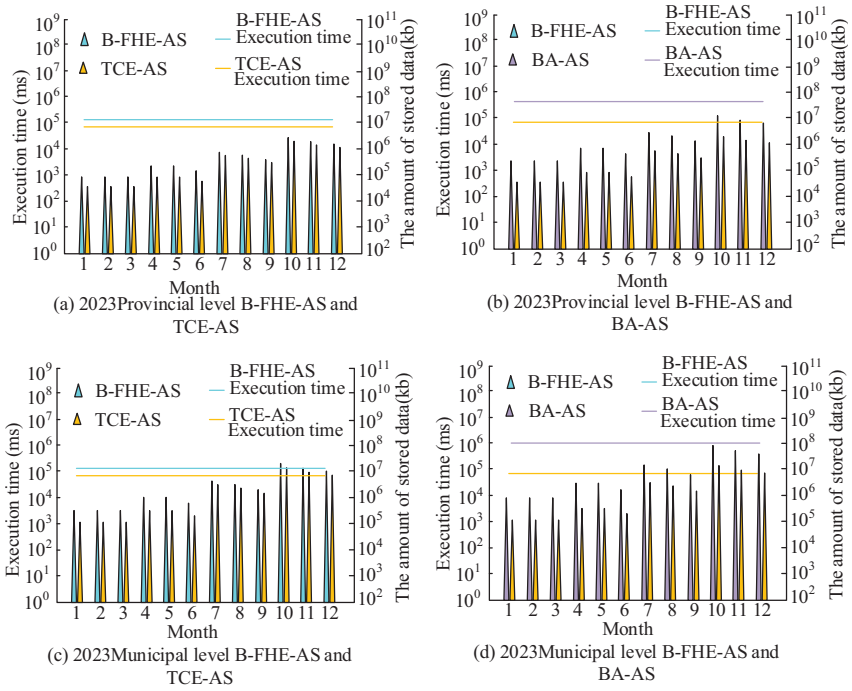

Figure 7 Long-term performance and load conditions.

in the municipal power grid environment in the same year. B-FHE-AS also maintains the lowest execution time and stored data volume over 12 months of operation. In summary, the B-FHE-AS solution can effectively reduce time overhead and optimize storage efficiency in high load and long-term operation scenarios. This result verifies that the system has excellent performance stability and scalability in continuous large-scale data processing. This provides solid technical support for large-scale secure storage and trustworthy and efficient processing of power plant ancillary service data.

4.2 Application and Result Analysis of Power Plant Ancillary Service Performance Evaluation Methods

To systematically evaluate the practical application effect of the proposed performance evaluation method, FAHP is first introduced to scientifically weight the evaluation index system constructed in Table 1. By integrating the judgments of multiple experts in the field and processing fuzzy evaluation information, the comprehensive weight of each indicator is calculated, thus

effectively reducing subjective arbitrariness. Table 3 displays the weight distribution for each level of the indicator system.

To systematically evaluate the practical application effect of the proposed performance evaluation method, FAHP is first introduced to scientifically weight the evaluation index system constructed in Table 1. The weighting process involved the following steps: First, a panel of 10 experts from power grid companies, power plants, and research institutions was invited to conduct pairwise comparisons of the indicators at each level using a fuzzy semantic scale (equally important, slightly more important, etc.). Second, triangular fuzzy numbers were used to construct fuzzy judgment matrices, and the fuzzy weights of each criterion and sub-criterion were calculated. Third, a consistency check was performed to ensure the reliability of expert judgments (consistency ratio < 0.1). Finally, the global weights of the basic indicators were obtained by multiplying the local weights along the hierarchy. This FAHP-based approach effectively integrates expert domain knowledge while reducing subjective arbitrariness through fuzzy set theory. The resulting weight distribution for each level of the indicator system is presented in Table 4.

Table 4 (Power station ancillary service performance evaluation indicator weight distribution) systematically presents the relative importance of each evaluation indicator from three levels: criterion level, local weight and

Table 4 Distribution of weights for performance evaluation indicators of power plant ancillary services

Criteria Layer	Weight	Indicator Layer	Local Weight	Global Weight
E1	0.420	E_{111}	0.360	0.151
		E_{112}	0.240	0.101
		E_{113}	0.190	0.080
		E_{121}	0.600	0.252
		E_{122}	0.220	0.092
		E_{123}	0.100	0.042
		E_{124}	0.080	0.034
E2	0.580	E_{211}	0.310	0.180
		E_{212}	0.260	0.151
		E_{221}	0.380	0.220
		E_{222}	0.340	0.197
		E_{223}	0.260	0.151
		E_{231}	0.100	0.058
		E_{232}	0.070	0.041

Table 5 Scenario-based performance evaluation results of cross-regional power plants in ancillary services

Plant id	Plant Type	Frequency Regulation Scenario Relative Closeness	Peak Shaving Scenario Relative Closeness	Reserve Scenario Relative Closeness
PP-03	New energy	0.85	0.78	0.82
PP-01	New energy	0.83	0.76	0.80
PP-06	New energy	0.82	0.75	0.78
PP-02	Thermal	0.73	0.82	0.75
PP-04	Thermal	0.71	0.80	0.73
PP-05	Thermal	0.69	0.78	0.70

global weight. In the criterion layer, market performance (E2, 0.580) has a higher weight than development status (E1, 0.420). In the indicator layer, the proportion of new energy consumption (E121) has the highest local weight (0.600). Its global weight is also the most prominent (0.252). In the market performance dimension, supplier energy storage capacity participation (E221) has the highest local weight (0.380). This table completely displays the top-down weight distribution structure of the evaluation system. Note: Criterion weights represent the relative importance of the two main dimensions (development status and market performance) obtained from the FAHP expert evaluation. Local weights indicate the importance of each indicator within its own criterion group, and global weights reflect the overall contribution of each basic indicator to the total objective.

The study selects six cross-regional power plants for empirical analysis. The scenario-based evaluation results of its ancillary service performance are shown in Table 4.

Table 5 shows that new energy power plants perform well in frequency regulation scenarios (RP are both >0.82). Among them, PP-03 reaches 0.85, and thermal power plants have more advantages in peak load-shaving scenarios (RP are both >0.78). This shows that the evaluation system can effectively distinguish the technical characteristics of different power plants. The average frequency modulation closeness of new energy power plants reaches 0.85, which is 12% higher than that of thermal power plants (0.71). This is mainly due to its advantages in response speed (+56.3%) and adjustment accuracy (+8.2%). The results verify the effectiveness of the method in distinguishing power plant ancillary service performance, and can provide a reference for power grid dispatching and market compensation.

To verify the feasibility and effectiveness of the power plant ancillary service performance comprehensive evaluation system built for system

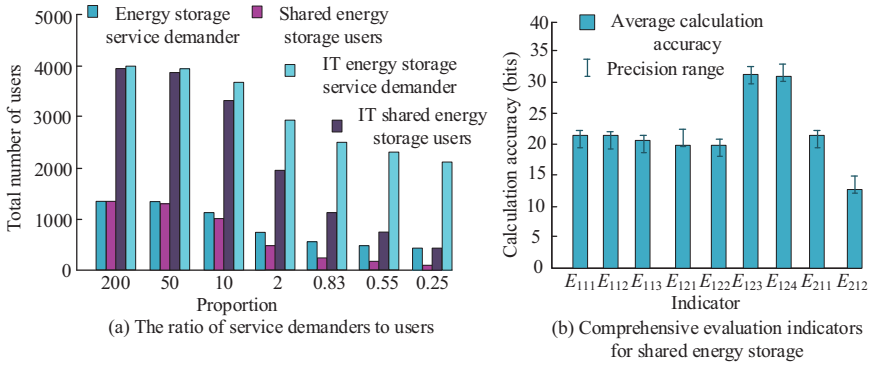

Figure 8 Extensibility of calculation method and accuracy of evaluation results.

verification in actual deployment and operation, this study carries out experimental analysis from two key dimensions: the scalability of the calculation method and the accuracy of the evaluation results, as shown in Figure 8.

As shown in Figure 8(a), the power plant ancillary service performance comprehensive evaluation system shows clear scale flexibility and robust carrying capacity. When the ratio of energy storage service demanders to SES users changes from 400 to 0.25, the system can support user scales of 446∼1380 and 2121∼4008 respectively in different server environments. This shows that it can dynamically adapt to resource requirements and processing loads in different business scenarios. As shown in Figure 8(b), the calculation accuracy of indicators E123 and E124 is close to the theoretical optimal value, which provides a reliable and accurate indicator quantification basis for the comprehensive evaluation system of power plant ancillary service performance. This strongly supports the objectivity and fairness of the evaluation results.

To verify the power plant ancillary service performance evaluation based on improved TOPSIS, the dynamic response and discrimination capabilities of development targets at different time scales are compared. Figure 9 displays the outcomes.

In Figures 9(a) and 9(b), the results of the comprehensive evaluation based on the FAHP determination of index weights and the TOPSIS model show that the RP of the long-term target is 0.99 (less than 1), because the actual optimal values of some indicators exceed the target set value. This shows that the system recognizes excellence. In terms of time, typical month 1 is closest to the long-term goal, and typical month 5 has the largest gap. Moreover, the closeness of typical month 1 under the short-term target

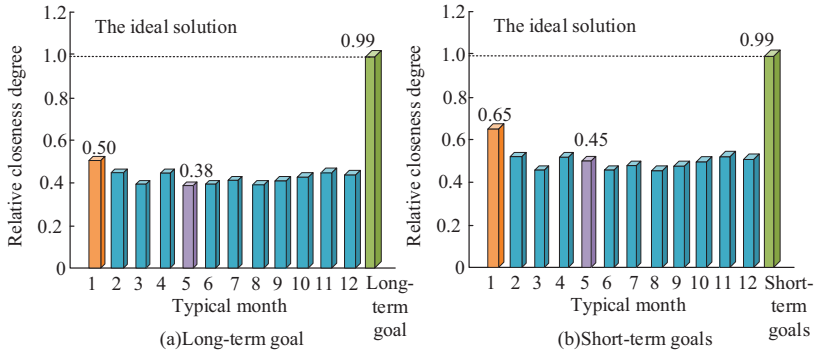

Figure 9 Comparison of RP of typical months under different development goals based on FAHP-TOPSIS.

increases from 0.50 to 0.65, indicating that its status is closer to the short-term target. The results verify that the evaluation system can effectively distinguish states in different time periods and is sensitive to targets at different time scales. This provides a highly adaptable and clearly oriented quantitative tool for policy and performance evaluation.

5 Conclusion

Aiming at the security privacy and evaluation accuracy issues of power plant ancillary service data, this study proposed a B-FHE-AS secure storage architecture that integrates blockchain and FHE. It used FAHP to determine the index weight, and combined it with the improved TOPSIS evaluation method to achieve secure calculation under data ciphertext and scientific evaluation of power station performance. Experimental verification revealed that the proposed B-FHE-AS scheme was significantly better than traditional centralized encryption and BA-AS in terms of data security and integrity. In the actual data environment of the provincial power grid, the data leakage rate of this solution was only 1%, and the tamper detection success rate reached 98.99%. In performance evaluation applications, empirical analysis of six cross-regional power plants showed that the average closeness of new energy power plants (such as PP-03) in frequency regulation scenarios reached 0.85, which was approximately 19.7% higher than the 0.71 of thermal power plants (such as PP-05). This was mainly due to its advantages in response speed (an average increase of 56.3%) and adjustment accuracy (an average increase of 8.2%). Under the guidance of short-term goals, the comprehensive evaluation

closeness in a typical month could be improved from the baseline of 0.50 to 0.65, proving the sensitivity of its policy orientation. In summary, the data security storage and performance evaluation system constructed in this study has strong engineering applicability and can provide technical support for the trusted management of power plant ancillary service data and the efficient operation of the power market. Although the proposed system has excellent performance in terms of safety and performance, the study has not subdivided and optimized it for power stations in different regions and sizes, and there is still room for further improvement in its versatility. In the future, the system architecture and evaluation model will be further optimized in a multi-region and multi-type power station environment to continue to improve its applicability and comprehensive performance.

Funding

This research was funded by the Luquan Wudongde Hydropower Plant of the Three Gorges Jinsha River Yunchuan Hydropower Development Co., Ltd., Research Project No.: 5225020003.

References

[1] Lakshmi T S, Jayamangala H. MFSA: Migration flamingo search algorithm based trust aware multi-party data sharing in blockchain using hierarchical homomorphic encryption[J]. Intelligent Decision Technologies, 2025, 19(3): 1380–1399. DOI:10.3233/IDT-240268.

[2] Sudha S, Manikandasaran S S. Cloud Data Security Using Cryptoga and Blockchain Recovery[J]. Journal of Theoretical and Applied Information Technology, 2023, 101(16): 6286–6300. DOI:10.5281/zenodo.10025012.

[3] Avwioroko A, Ibegbulam C, Afriyie I, & Fesomade A T. Smart grid integration of solar and biomass energy sources[J]. European Journal of Computer Science and Information Technology, 2024, 12(3): 1–14. DOI:10.37745/ejcsit.2013/vol12n3114.

[4] Zhang J, Cheng X, Yang L, Hu J, Liu X, & Chen K. Sok: Fully homomorphic encryption accelerators[J]. ACM Computing Surveys, 2024, 56(12): 1–32. DOI:10.1145/3676955.

[5] Mandinyenya G, Malele V. Post-Quantum Cryptographic Techniques For Future-Proofing-Blockchain-Based Personal Data Sharing[J]. Iraqi

Journal For Computers And Informatics, 2025, 51(2): 109–125. DOI:10 .25195/ijci.v51i2.623.

[6] Wang J, Xu J, Li J, & Xie, H. Enhanced Edge Data Security Scheme for Smart Grids Based on Federated Learning and Blockchain[J]. ELECTRICA, 2025, 25(1): 1–13. DOI: 10.5152/electrica.2025.25102.

[7] Guo L, Wang H, Liu J, Wang L, He C, & Li X. Blockchain-powered secure trading framework for power dispatch in metaverse[C]//IET Conference Proceedings CP921. Stevenage, UK: The Institution of Engineering and Technology, 2025, 2025(13): 44–50. DOI:10.1049/icp. 2025.2434.

[8] Jiyuan S, Hongmin G, Keke Y, Yushi S, Zhaofeng M, & Chengzhi F. A privacy protection scheme for verifiable data element circulation based on fully homomorphic encryption[J]. China Communications, 2025, 22(4): 223–235. DOI: 10.23919/JCC.fa.2024-0345.202504.

[9] Altamimi E, Al-Ali A, Malluhi Q M, & Al-Ali A K. Smart grid public datasets: Characteristics and associated applications[J]. IET Smart Grid, 2024, 7(5): 503–530. DOI:10.1049/stg2.12161.

[10] Onukwulu E C, Agho M O, Eyo-Udo N L. Decentralized energy supply chain networks using blockchain and IoT[J]. International Journal of Scholarly Research in Multidisciplinary Studies, 2023, 2(2): 066–085. DOI:10.56781/ijsrms.2023.2.2.0055.

[11] Yu P, Huang W, Li Z. A Secure, lightweight, and verifiable data aggregation scheme for smart grids[J]. Peer-to-Peer Networking and Applications, 2025, 18(3): 1–11. DOI:10.1007/s12083-025-01960-7.

[12] Mijwil M M, Ali G, Peter K S, Dhoska K, & Adamopoulos I. Post-Quantum Secure Blockchain-Based Federated Learning Framework for Enhancing Smart Grid Security[J]. Iraqi Journal for Computers and Informatics, 2025, 51(2): 156–223. DOI:10.25195/ijci.v51i2.637.

[13] Zhang Z, Liu M, Sun M, Deng R, Cheng P, Niyato D. Vulnerability of machine learning approaches applied in iot-based smart grid: A review[J]. IEEE Internet of Things Journal, 2024, 11(11): 18951–18975. DOI:10.1109/JIOT.2024.3364031.

[14] Naiho H N N, Layode O, Adeleke G S. Addressing cybersecurity challenges in smart grid technologies: Implications for sustainable energy infrastructure[J]. Engineering Science & Technology Journal, 2024, 5(6): 1995–2015. DOI:10.51594/estj.v5i6.1218.

[15] Ganesh P M J, Sundaram B M, Balachandran P K. IntDEM: an intelligent deep optimized energy management system for IoT-enabled smart

grid applications[J]. Electrical Engineering, 2025, 107(2): 1925–1947. DOI:10.1007/s00202-024-02586-3.

[16] Alzahrani A, Alghazzawi D. Blockchain and Homomorphic Encryption for Secure Data Sharing in Smart Grids: A Systematic Review[J]. Sensors, 2024, 24(4): 1234. DOI: 10.3390/s24041234.

[17] George A S, Baskar T, Srikaanth P B. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors[J]. Partners Universal International Innovation Journal, 2024, 2(1): 51–75. DOI:10.5281/zenodo.10639463

[18] Abdi N, Albaseer A, Abdallah M. The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: A survey[J]. IEEE Internet of Things Journal, 2024, 11(9): 16398–16421. DOI:10.1109/JIOT.2024.3364030.

[19] Arcas G I, Cioara T, Anghel I, et al. Edge offloading in smart grid[J]. Smart Cities, 2024, 7(1): 680–711. DOI:10.3390/smartcities7010028.

[20] Zafar A, Che Y, Faheem M, Abubakar M. Ali S. Machine learning autoencoder-based parameters prediction for solar power generation systems in smart grid[J]. IET Smart Grid, 2024, 7(3): 328–350. DOI:10.1049/stg2.12153.

[21] Muthubalaji S, Muniyaraj N K, Rao S P V S, Thandapani K, Mohan P R, Somasundaram T. An intelligent big data security framework based on aefs-kenn algorithms for the detection of cyber-attacks from smart grid systems[J]. Big Data Mining and Analytics, 2024, 7(2): 399–418. DOI:10.26599/BDMA.2023.9020022.

[22] Udo W S, Kwakye J M, Ekechukwu D E, & Ogundipe O B. Smart grid innovation: machine learning for real-time energy management and load balancing[J]. International Journal of Smart Grid Applications, 2024, 22(4): 405–423. DOI:10.51594/estj.v4i6.1395.

Biographies

Chu-Hui Li (December 1983–), male, graduated from the School of Hydropower and Digital Engineering at Huazhong University of Science and Technology, majoring in Hydraulic and Hydropower Engineering, and obtained a master's degree. After graduation, I worked as a senior engineer at the Wudongde Hydropower Plant of China Yangtze Power Co., Ltd. My current research direction is engaged in hydropower automation and intelligence.

Zhong-Ming Dong (December 1975–), male, graduated from the College of Water Resources and Hydropower Engineering at Sichuan University with a major in Hydropower Engineering, and obtained a bachelor's degree. After graduation, I worked as a senior engineer at the Wudongde Hydropower Plant of China Yangtze Power Co., Ltd. My current research direction is engaged in the management of power station machinery and hydraulic engineering technology.

Tian-Xiong Huang (April 1990-), male, graduated from the School of Hydropower and Digital Engineering at Huazhong University of Science and Technology with a major in Hydraulic and Hydropower Engineering, and obtained a bachelor's degree. After graduation, I worked as an engineer at the Wudongde Hydropower Plant of China Yangtze Power Co., Ltd. Currently, my research focus is on hydropower automation and intelligence.

Yi Dong (December 1991 –), male, graduated from Wuhan University with a major in Energy and Power Systems and Automation, and obtained a bachelor's degree. After graduation, I worked as an engineer at the Wudongde Hydropower Plant of China Yangtze Power Co., Ltd. My current research direction is engaged in hydropower automation work.