İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2025; 25: 1-13

Enhanced Edge Data Security Scheme for Smart Grids Based on Federated Learning and Blockchain

Jie Wang[1], Jiangpei Xu[1], Jing Li[2], Chao Xu[3], Huihui Xie[3]

[1]State Grid Hubei Electric Power Research Institute, Wuhan, Hubei, China
[2]State Grid Hubei Electric Power Co., Ltd, Wuhan, Hubei, China
[3]State Grid Hubei Extra High Voltage Company, Wuhan, Hubei, China

Cite this article as: J. Wang, J. Xu, J. Li, C. Xu and H. Xie, "Enhanced edge data security scheme for smart grids based on federated learning and blockchain," *Electrica* 25, 0102, 2025. doi: 10.5152/electrica.2025.25102.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *In smart grid edge computing environments, traditional centralized data processing methods are vulnerable to cyber-attacks and struggle to protect user data privacy, with high risks of data leakage and tampering.*

WHAT THIS STUDY ADDS ON THIS TOPIC?

- *This study proposes a novel security architecture that innovatively integrates Federated Learning and Blockchain. It enables secure model training without sharing raw data, significantly reducing the privacy leakage rate to 0.9%, while maintaining high system performance and ensuring data integrity.*

Corresponding Author:
Jie Wang

E-mail:
JieWang332@126.com

Received: April 19, 2025
Revision Requested: May 26, 2025
Last Revision Received: June 19, 2025
Accepted: July 18, 2025
Publication Date: November 11, 2025

DOI: 10.5152/electrica.2025.25102

ABSTRACT

The authors propose a data security enhancement scheme for smart grids based on Federated Learning and Blockchain to address issues of data privacy leakage and tampering in edge computing environments within smart grids. In edge computing scenarios, traditional centralized model training is vulnerable to attacks and struggles to protect data privacy, with an attack success rate as high as 54.3%. By integrating Federated Learning and Blockchain technologies, the authors have constructed a secure architecture that enables the system to protect users' electricity consumption data privacy without sharing raw data, while ensuring the integrity and security of the data transmission process. Experimental results show that the privacy leakage rate of the Federated Learning + Blockchain scheme is only 0.9%, compared to 60.2% for schemes without privacy protection. Additionally, the Federated Learning + Blockchain approach outperforms traditional solutions in terms of data transmission, processing time, Central Processing Unit (CPU) and memory consumption, and security, achieving a balance between performance and security.

***Index Terms*—**Blockchain, data security, edge computing, federated learning, privacy protection, smart grid

I. INTRODUCTION

Smart grids, as a product of the deep integration of traditional power systems and information and communication technologies, achieve real-time monitoring and bidirectional interaction of power generation, transmission, and consumption by integrating sensors, smart meters, and data analysis tools. This significantly enhances energy efficiency and system reliability [1]. The importance of smart grids is increasingly prominent, as they are regarded as critical infrastructure for achieving energy transition and sustainable development (see Fig. 1). The introduction of edge computing further optimizes the responsiveness of smart grids by enabling distributed processing near the data source, reducing transmission latency, and alleviating the load on central servers (see Fig. 2). However, the widespread distribution of edge devices and the decentralized processing of data exacerbate security risks. Sensitive information such as user electricity consumption data and device status faces threats from cyberattacks, data tampering, and privacy breaches [2]. Existing centralized models rely on the sharing of raw data, making it difficult to balance privacy protection and computational efficiency in dynamic edge environments. There is an urgent need to explore innovative solutions that simultaneously address security, real-time performance, and scalability.

The smart grid and its data security have become a focal point of research in both academia and industry in recent years, particularly in the areas of data privacy and security (see Fig. 3). Many scholars have explored the critical challenges of data security in smart grids. Pasumponthevar and Jeyaraj proposed a false data intrusion detection framework based on Kalman reinforcement learning, which enhances system resilience by dynamically optimizing detection strategies. Theoretical validation shows a significant improvement in the detection accuracy of false data injection attacks. However, this scheme does not fully consider the computational constraints

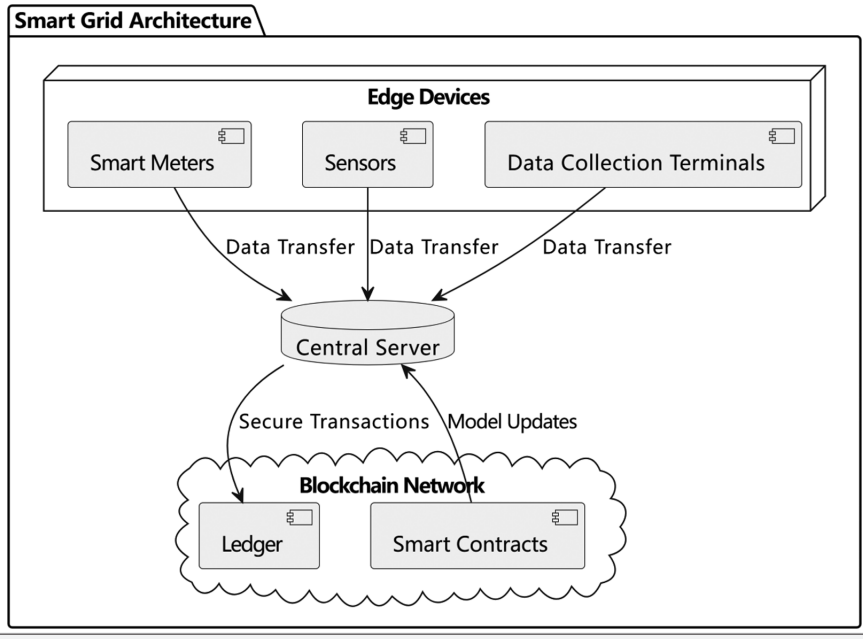


Fig. 1. Schematic diagram of smart grid architecture.

of edge devices, and the feasibility of deploying complex reinforcement learning models in resource-constrained scenarios remains questionable [3]. Yang et al. introduced the zero-trust architecture into the design of power system networks, reducing the risk of internal attacks through continuous identity verification and minimum privilege access. Their research provides new insights for

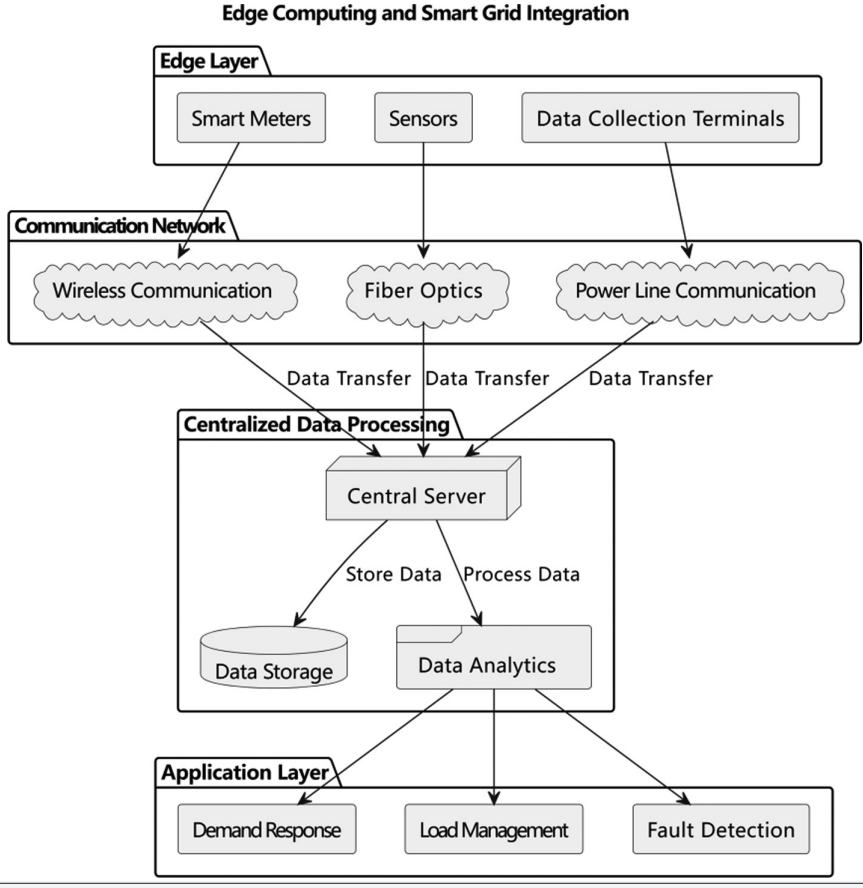


Fig. 2. Schematic diagram of edge computing integrated with smart grid.

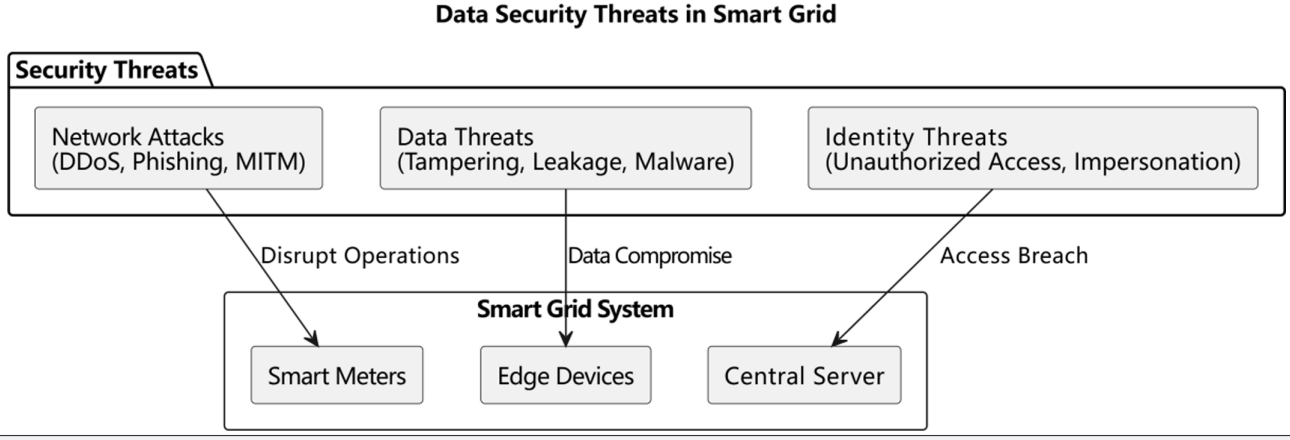


Fig. 3. Analysis of current data security threats.

fine-grained access control in distributed environments. However, the framework lacks sufficient support for real-time performance in high-frequency data interaction scenarios and is not deeply integrated with the characteristics of edge computing [4]. In the exploration of blockchain technology applications, Pillai and Deshmukh designed a service-centric blockchain security model for smart grids, utilizing smart contracts to achieve data traceability and access control. However, their design relies on a high-throughput consensus mechanism, which is difficult to adapt to the low-bandwidth characteristics of edge networks, leading to significantly increased transaction delays in practical scenarios [5]. Although existing research has made progress at the theoretical level, most solutions still face challenges such as insufficient computational resources in edge scenarios, weak protection during transmission, and a lack of comprehensive evaluation.

The existing shortcomings of the smart grid data security architecture can be analyzed from multiple dimensions. There is a significant contradiction between the limited computational resources of edge terminals and the complex security requirements. A typical manifestation is that privacy-preserving technologies such as homomorphic encryption, while effectively preventing data leakage, have a computationally intensive nature that severely conflicts with the lightweight characteristics of edge devices. This results in feasibility obstacles for security strategies in practical deployments [6, 7]. Current research excessively focuses on privacy protection during the model training phase but lacks effective mechanisms to address dynamic threats in the data transmission process. Although traditional static encryption methods can ensure the security of offline data, they struggle to adapt to the dynamic changes in edge network topology and the millisecond-level response requirements. Existing solutions reveal defects such as rigid defense strategies and delayed responses [8, 9]. Most security models lack systematic performance evaluation across scenarios and fail to fully consider the nonlinear impact of physical layer delay jitter and device heterogeneity on detection accuracy. This results in a significant deviation between theoretical performance and actual effectiveness. Current security frameworks generally lack collaborative protection designs among end users, edge nodes, and cloud systems. This fragmented security paradigm severely weakens the overall resilience of the system. Constructing a cross-layer collaborative and dynamically evolving defense system has become a critical challenge constraining the security upgrade of smart grids [10, 11].

Faced with the aforementioned issues, the primary objective of the author is to propose an efficient and secure data protection scheme aimed at addressing data privacy leakage and tampering in smart grids, particularly the challenges of real-time performance and efficiency in edge computing scenarios. Specific research questions include how to conduct effective model training without sharing raw data, as well as how to utilize blockchain to ensure data immutability and secure transmission [12, 13]. The author's contribution lies in the innovative integration of federated learning and blockchain technology, forming a novel security architecture. Compared to existing research, the author not only focuses on data privacy protection but also emphasizes efficiency in edge environments, providing a practical solution to meet the increasingly complex security demands of smart grids.

II. MODEL CONSTRUCTION

The system architecture proposed by the author aims to achieve efficient and secure data management in smart grids by leveraging the advantages of edge devices, central servers, and blockchain technology. The system primarily consists of three components: edge devices, central servers, and the blockchain network [14]. Edge devices include various smart sensors, smart meters, and data acquisition terminals responsible for the real-time collection of grid operation data (such as current, voltage, and power). Equipped with certain computational capabilities, they can perform preliminary data processing and analysis locally. This reduces data transmission latency, enhances the system's rapid response capability, and optimizes power management strategies. The central server is responsible for centralized processing of data from edge devices, conducting in-depth data analysis and model training. It also manages the federated learning process, sending the trained model parameters back to the edge devices. This ensures the privacy of user data while leveraging data from different devices to improve model accuracy (MA) [15, 16]. Blockchain technology is employed in this architecture to ensure the security and integrity of the data transmission process. All transmission records and data transactions are recorded on the blockchain, forming an immutable historical data chain. This not only enhances data transparency but also strengthens resistance to data tampering and malicious attacks [17]. Additionally, the introduction of smart contracts enables automated execution of data access control, ensuring that only

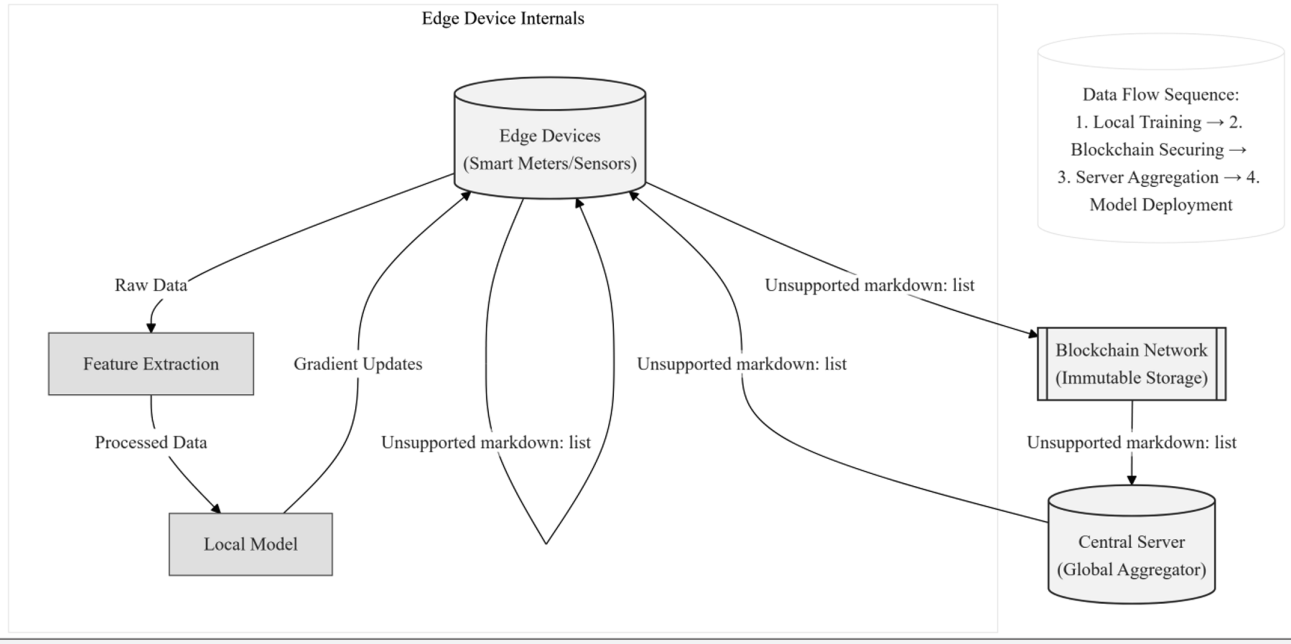


Fig. 4. System architecture diagram.

authorized users can access specific data. The specific architecture is illustrated in Fig. 4.

Through this interactive architecture, the various components can efficiently collaborate, ensuring the security and privacy of data during collection, transmission, and storage. Edge devices rapidly process and provide feedback on information, the central server conducts in-depth analysis, and the blockchain offers a secure and transparent environment for data sharing [18]. This design not only enhances the data security of smart grids but also meets the requirements for real-time performance and scalability, laying a solid foundation for further research and practical applications.

A. Federated Learning Model

1) Local Model Structure:

The structure of the local model typically depends on the specific application scenario and data type. In this study, a deep learning model suitable for power load forecasting and network traffic anomaly detection was selected. The model includes the following main components:

a) Input layer: Receives power load or network traffic data from edge devices. Input features may include historical load data, timestamps, weather conditions, etc.

b) Hidden layer: Utilizes multiple fully connected layers (or convolutional layers) to extract features from the data. Each hidden layer employs an activation function (such as ReLU) to introduce non-linearity, thereby enhancing the model's expressive capability [19, 20].

c) Output layer: The structure of the output layer depends on the nature of the task. For power load forecasting, a linear regression output can be used; for network traffic anomaly detection, a binary classification output (normal or abnormal) can be employed.

The specific model structure can be expressed as (1):

$$y = f\left(x;\theta\right) \tag{1}$$

where y is the output of the model, x is the input feature, and θ is the model parameter.

2) Loss Function:

The loss function is used to measure the discrepancy between the model's predicted values and the true values. Selecting an appropriate loss function is crucial for the training of the model. In this study, the following loss function was adopted:

Mean squared error: Used for the power load forecasting task, defined as (2):

$$L\left(y,\check{y}\right)=\frac{1}{N}\sum_{i=1}^{N}\left(y_i-\check{y}_i\right)^2 \tag{2}$$

where y is the true value, $\check{y}_i$ is the predicted value, and N is the number of samples.

Cross-entropy loss: Used for the network traffic anomaly detection task, defined as (3):

$$L\left(y,\check{y}\right)=-\frac{1}{N}\sum_{i=1}^{N}\left[y_i\log\left(\check{y}_i\right)+\left(1-y_i\right)\log\left(1-\check{y}_i\right)\right] \tag{3}$$

3) Optimization Algorithm:

In order to effectively train the local model, a gradient descent-based optimization algorithm was adopted. Specifically, the Adam optimization algorithm was chosen due to its superior convergence performance when handling large-scale data. The update rules of the Adam optimization algorithm are as follows:

The calculation gradient is (4):

$$\nabla L\left(w_k^t,D_k\right) \tag{4}$$

The update mean and variance are given by (5) and (6):

$$m_t = \beta_1 m_{t-1} + (1-\beta_1)\nabla L\left(w_k^t, D_k\right) \tag{5}$$

$$v_t = \beta_2 v_{t-1} + (1-\beta_2)\left(\nabla L\left(w_k^t, D_k\right)\right)^2 \tag{6}$$

The updated model parameters are given by (7):

$$w_k^{t+1} = w_k^t - \eta \frac{m_t}{\sqrt{v_t + \epsilon}} \tag{7}$$

Here, β_1 and β_2 are momentum decay parameters, η is the learning rate, and $\in$ is a smoothing term to prevent division by zero.

4) Local Model Training Process:
Under the framework of federated learning, each edge device performs local training based on the aforementioned model structure and algorithm. The specific process is as follows:

- Model initialization: Initialize using the global model parameters.
- Local training: Perform multiple rounds of training on the local dataset D_k, calculate and update the model parameters [21, 22].
- Model parameter upload: After completing the training, upload the updated model parameters to the central server instead of the raw data.

In this way, federated learning models effectively leverage the computational capabilities of edge devices while protecting user privacy, enhancing the security and efficiency of smart grid data processing. The settings of hyperparameters for help outlinefederated learning was shown in Table 1.

B. Integration of Blockchain and Federated Learning
In this study, edge devices upload the trained local model parameters to the blockchain instead of directly sending them to the central server. This process ensures the privacy of the uploaded model parameters by adding noise [23, 24]. The formula for uploading the model parameters can be expressed as:

Let w_k^t be the model parameters of the edge device at the ith iteration. The model parameters uploaded to the blockchain can be expressed as (8):

$$w_k^{t+1} = w_k^t + N\left(0, \sigma^2\right) \tag{8}$$

Here, $N(0,\sigma^2)$ represents the Gaussian noise added to the model parameters, ensuring the privacy of the uploaded data.

TABLE I. SETTINGS OF HYPERPARAMETERS FOR FEDERATED LEARNING

Parameter	Value
Number of local training rounds	5
Global aggregation rounds	100
Batch size	32
Learning rate (η)	0.001
Momentum attenuation (β 1/β α)	0.9/0.999

Blockchain technology provides the characteristic of data immutability, enabling each model parameter update to be recorded and verified [25]. This mechanism ensures that each update is secure and reliable. Each time the model parameters are updated, the blockchain will record the following information as (9):

$$\text{Record=Hash}\left(w_k^{t+1}, \text{timestamp}, \text{device\_id}\right) \tag{9}$$

Here, Hash()performs a hash operation on the uploaded model parameters to ensure the secure storage of the data on the blockchain.

Through the blockchain, the central server or designated edge devices can obtain the model parameters from all participating devices and update the global model using an aggregation algorithm. The update of the global model can be expressed as (10):

$$w^{t+1} = \frac{1}{K}\sum_{k=1}^{K} w_k^{t+1} \tag{10}$$

Here, K represents the number of participating edge devices. This formula generates a new global model by performing a weighted average of all valid model parameters.

By leveraging smart contract technology, the automation of model updates and data access control can be achieved. For instance, smart contracts can define certain conditions, and when these conditions are met, data access or model updates are automatically executed [26, 27]. The execution conditions of smart contracts can be expressed as (11):

$$\text{if}\left(w_k^{t+1}\text{is valid}\right) \rightarrow \text{update global model} \tag{11}$$

This ensures that only valid model parameters can update the global model, thereby further enhancing the security and efficiency of the entire system.

Smart contract implements the logic to verify the validity of model parameters, digital signature, and device certificate.

Trigger conditions: When $\left|w_k^{t+1} - w_k^t\right| < \epsilon$ prevents abnormal updates,

Automatically aggregate: call the Aggregate()function to calculate the global model

Solidity example of a contract code snippet:

```
function verify Update(bytes32 hash, uint timestamp, address device ID) public {

require(registered Devices [device ID], "Unauthorized device");

require(block.timestamp - timestamp < THRESHOLD, "Expired update");

emit Update Verified(hash);
```

C. Data Privacy Protection Mechanism

1) Differential Privacy:
As shown in Fig. 5, differential privacy (DP) is a method of protecting user data privacy by adding noise to query results. In federated learning, DP can be achieved by adding noise before uploading

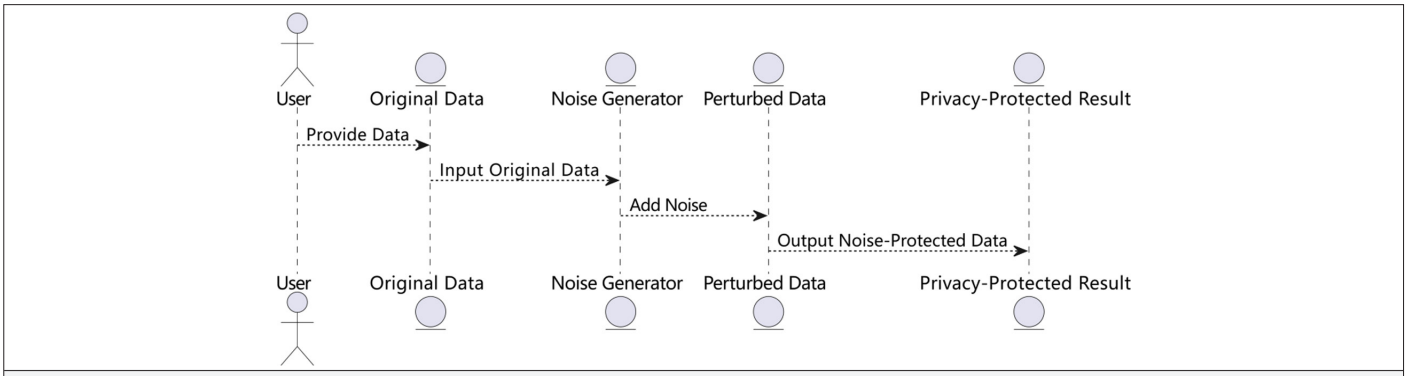


Fig. 5. Schematic diagram of differential privacy.

model parameters. This ensures that even if someone obtains the model parameters, they still cannot reverse-engineer the true data of any individual user [28, 29].

In order to achieve differential privacy, noise was added to the model parameters uploaded by each edge device. Specifically, it can be expressed as (12):

$$w_k^{t+1} = w_k^t + N\left(0, \sigma^2\right) \tag{12}$$

Here, $N(0,\sigma^2)$ is noise that follows a Gaussian distribution, and its standard deviation σ can be set based on the privacy budget ε. The privacy budget controls the degree of noise added, thereby influencing the model's usability and the effectiveness of user privacy protection.

2) Homomorphic Encryption:
As shown in Fig. 6, homomorphic encryption is a technology that allows computations to be performed on encrypted data without the need to decrypt it. This enables effective model training while ensuring data privacy.

In the context of federated learning, edge devices can use homomorphic encryption to encrypt model parameters, denoted as $E\left(w_k^t\right)$, where $E()$ represents the operation of encrypting the model parameters. Subsequently, the central server or aggregation node can perform computations on the encrypted parameters without needing to know the original data [30].

After receiving the encrypted model parameters, the central server can perform operations such as weighted averaging to obtain the encrypted global model parameters as (13):

$$E\left(w^{t+1}\right) = Aggregate\left(E\left(w_1^t\right), E\left(w_2^t\right), \ldots, E\left(w_K^t\right)\right) \tag{13}$$

3) Application Scenarios and Connections:
In the context of smart grids, users' electricity consumption data is highly sensitive and involves user privacy. Therefore, employing DP or homomorphic encryption can facilitate model training and updates while ensuring data privacy. Specifically:

Differential privacy and user data: By adding noise to the model updates of each edge device, it ensures that even if the model parameters are obtained by malicious users, individual users' electricity consumption data cannot be identified. This is crucial for data privacy in smart grids [31, 32].

Homomorphic encryption and secure computation: Homomorphic encryption permits the aggregation of model parameters without exposing user data. This way, even if the central server processes encrypted data, it can still efficiently update the global model, thereby enhancing the security of the entire system.

Federated learning enables edge devices to train models locally without uploading raw data. To enhance the privacy protection of

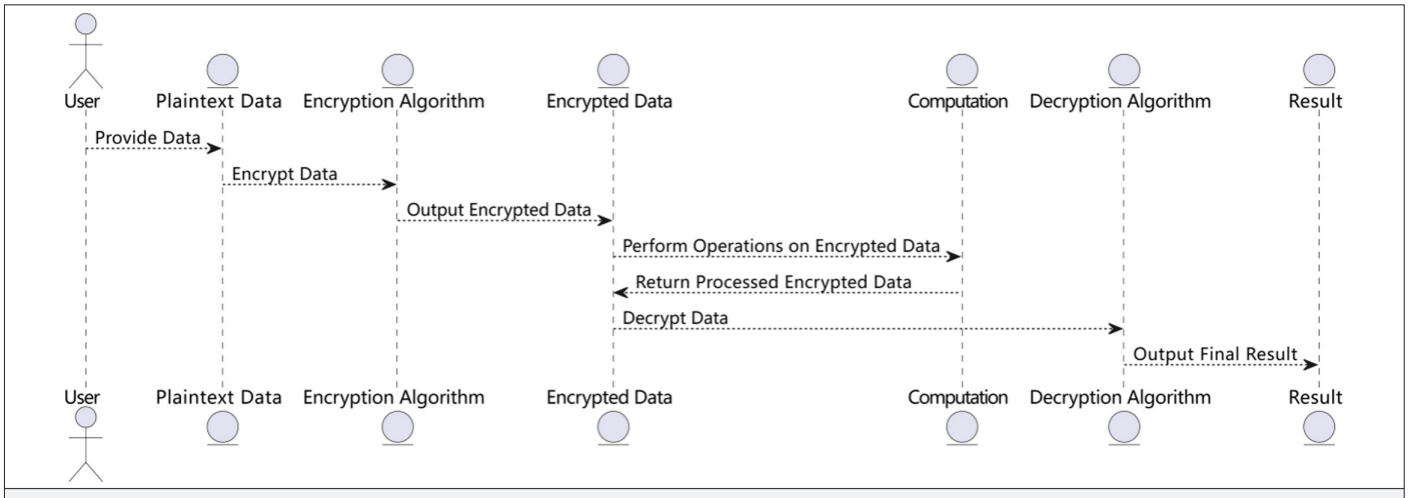


Fig. 6. Schematic diagram of homomorphic encryption.

the models, the data update process can be integrated with blockchain. Edge devices upload their local model parameters to the blockchain instead of a central server. This ensures that even if someone accesses the blockchain, what they obtain is only the encrypted model parameters.

III. EXPERIMENTAL RESULTS

A. Experimental Setup

The power load data are from the 2022 version of the IEEPES (Post-evaluation system for smart energy economy) Power Open Database, which contains 100 000 records with a time span from January 2021 to June 2023. The feature dimension is 23, including environmental variables such as temperature and humidity. The preprocessing adopts MinMax normalization, and abnormal values are eliminated through the 3σ principle.

The experiments were conducted in a virtual machine-based environment to simulate real-world smart grid scenarios. The experimental setup included multiple edge devices and a central server, all interconnected via a secure local area network, forming an integrated network architecture. The central server was responsible for aggregating the model parameters uploaded from each edge device and updating the global model [33]. In order to ensure the reproducibility and accuracy of the experiments, all devices were configured with identical hardware and software environments.

The detailed configuration of the experimental environment is as follows: Edge Devices: Five edge devices were used, each equipped with an 8-core CPU, 16GB of RAM, and a 256GB SSD. All devices ran the same version of the operating system (e.g., Ubuntu 20.04) and were installed with the necessary machine learning libraries (e.g., PyTorch) and federated learning frameworks (e.g., Flower). Central Server: The central server was configured with a 32-core CPU, 64GB of RAM, and a 1TB SSD. It ran the same operating system as the edge devices and was installed with deep learning frameworks for data aggregation and model training. A blockchain node was also configured on the server to support smart contract functionality. Network Environment: The local area network bandwidth was set to 1 Gbps to ensure efficient data transmission. Network simulation tools (e.g., NetEm) were used to emulate different network latencies (10 ms, 50 ms, and 100 ms) to evaluate the model's performance under varying network conditions.

This experiment employed multiple datasets to thoroughly assess the performance of the proposed solution across various scenarios. The primary datasets consist of the power load dataset and the network traffic dataset. The power load dataset includes a variety of feature information, such as timestamps, user identities, weather conditions (temperature, humidity, etc.), load categories (residential electricity, industrial electricity, etc.), and specific parameters like current, voltage, and power. The dataset is characterized by its large volume and diverse dimensions, offering a comprehensive scenario for load forecasting and analysis. The goal is to utilize this dataset for load forecasting, evaluating the accuracy and robustness of the model in predicting power loads. To achieve this, the raw data underwent cleaning and normalization processes and was then divided into a training set (70%), a validation set (15%), and a test set (15%). The network traffic dataset simulates both normal and abnormal traffic in a real-world network environment, including traffic characteristics during normal operations and traffic data during network attacks (e.g., DDoS attacks). The objective is to assess the performance of anomaly detection algorithms, particularly their responsiveness under high load and attack conditions. Each data point in the dataset is labeled as either normal or abnormal to facilitate supervised learning [34].

The design of the test scenarios aims to evaluate the performance of the proposed solution under different conditions, primarily focusing on two scenarios. Scenario 1: This scenario tests the model's prediction accuracy under normal load conditions. The power load dataset is used to train the model, and its prediction accuracy is observed across different time periods (e.g., peak hours and off-peak hours). The model's performance is assessed by calculating the root mean square error and mean absolute percentage error. Scenario 2: This scenario evaluates the system's security under high load and abnormal conditions. The network traffic dataset is employed to test the system's anomaly detection capabilities [35]. In simulated network attack situations, the system's detection time and accuracy are recorded, and the false positive rate and false negative rate are calculated to assess the system's responsiveness.

B. Performance Evaluation

The success rate of using the privacy leakage rate (PLR) model to reconstruct the original data with an attack tool such as DeepLeak is defined as

$$PLR = NleakedNtotal \times 100\% PLR = \frac{N_{leaked}}{N_{total}} \times 100\% PLR = NtotalNleaked \times 100\% \cdot$$

Attack success rate (ASR) is based on the white-box attack to obtain the data tampering success rate under the model parameters.

1) Effectiveness of Data Privacy Protection:

In order to evaluate the effectiveness of the proposed edge data security enhancement scheme for smart grids based on federated learning and blockchain in terms of data privacy protection, the experiments primarily analyzed and compared aspects such as data leakage risk, confidentiality of model parameters, and robustness of data privacy. By conducting experiments across different test scenarios and with various algorithms, the privacy protection capabilities of the proposed scheme were compared with those of traditional approaches.

Fig. 7 illustrates the privacy protection effectiveness of different algorithms. In terms of PLR, the No Privacy Protection Scheme (NPPS) exhibits the highest leakage rate at 60.2%, while the Federated Learning + Blockchain integrated scheme (FL+BC) demonstrates the best privacy protection, with a leakage rate of only 0.9%, significantly lower than other schemes, highlighting its substantial advantage in privacy safeguarding. Regarding MA, NPPS achieves the highest accuracy of 95.6% due to the absence of additional protection measures. In contrast, FL+BC maintains a high accuracy of 91.5%, slightly lower than NPPS but superior to other privacy protection schemes, showcasing its balanced approach in ensuring model performance. CPU Usage (CPUU) and Bandwidth Consumption (BC) are critical metrics for evaluating computational overhead. Homomorphic Encryption (HE) incurs the highest consumption, with CPU usage reaching 50.3% and bandwidth consumption at 11.3 MB/s, due to its computationally intensive encryption and decryption processes. In contrast, the Federated Learning + Blockchain (FL+BC) scheme achieves higher computational efficiency while maintaining privacy, with CPU usage at 23.3% and bandwidth consumption at 5.5 MB/s, significantly lower than HE. In terms of Resistance to Inference Attack Rate (RIAR), FL+BC once again demonstrates the best protective

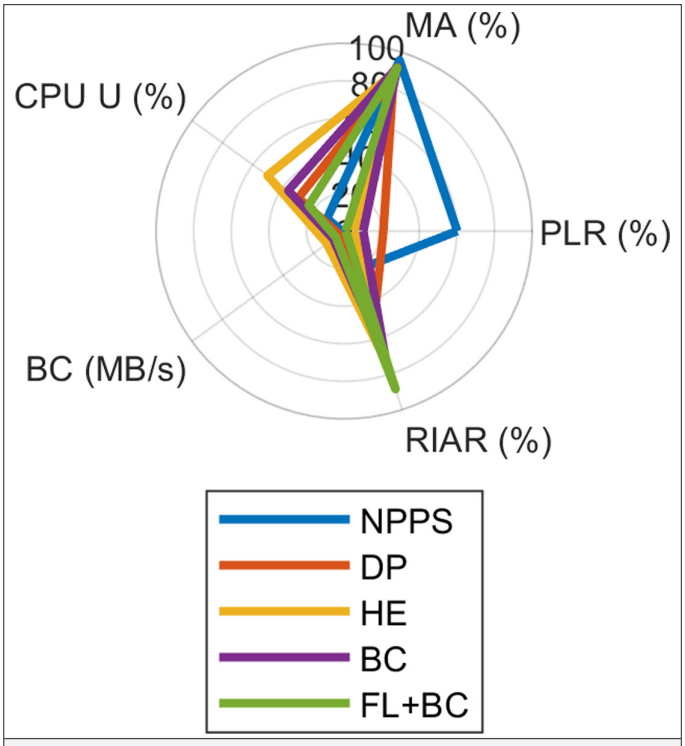


Fig. 7. Privacy protection effectiveness of different algorithms.

performance, achieving 88.5%, far surpassing traditional DP at 51.2% and NPPS at 21.9%. This indicates that FL+BC can effectively resist malicious attacks and ensure data security.

In summary, although the NPPS offers the lowest computational overhead and the highest MA, it provides almost no protection in terms of privacy and security. On the other hand, the Federated Learning + Blockchain (FL+BC) scheme demonstrates a balanced performance across all metrics, significantly reducing the PLR while maintaining high MA and low computational resource consumption. This highlights the advantages of FL+BC as an efficient and secure privacy protection solution.

2) System Performance Metrics:

From Fig. 8, it can be observed that in terms of system latency comparison, the Non-Privacy Preserving Edge Computing (NPPS) exhibits the lowest latency, averaging 68.5 ms, but lacks privacy protection. Centralized model training, on the other hand, has the highest latency, averaging 222.7 ms, which is significantly affected by high data transmission volumes and computational pressure. Its latency performance is notably poor across various scenarios. For instance, during peak electricity usage and in cases of data loss or delay, the latency reaches 248.8 ms and 309.3 ms, respectively. The Federated Learning + Blockchain (FL+BC) integration scheme, on the other hand, achieves an average latency of 86.4 ms, demonstrating a good balance between performance and privacy protection. In scenarios of normal electricity load and network attacks, the latency of FL+BC is 75.8 ms and 91.4 ms, respectively, which is significantly lower than that of centralized model training. Even in the most extreme scenario of data loss or delay, the latency of FL+BC is 128.5 ms, which, although higher than that of NPPS, is still far superior to centralized model training. This indicates that FL+BC can maintain low latency while ensuring privacy protection, making it

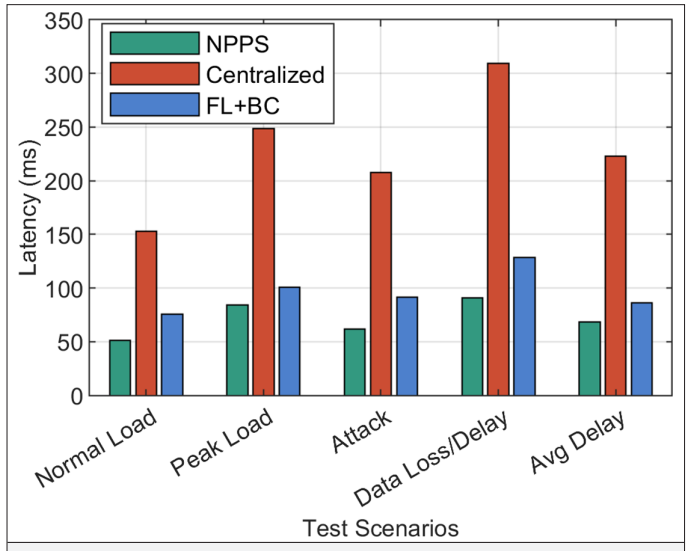


Fig. 8. System latency comparison chart.

an optimized solution that balances performance and security. It is well-suited for scenarios where both privacy and system performance are highly demanded.

As shown in Fig. 9, in terms of bandwidth consumption comparison, Non-Privacy Preserving Edge Computing (NPPS) exhibits the lowest bandwidth consumption across all scenarios, averaging only 0.725 MB/s, as there is no additional communication or privacy protection overhead. Under normal electricity load and peak electricity usage scenarios, its bandwidth consumption is 0.5 MB/s and 0.8 MB/s,

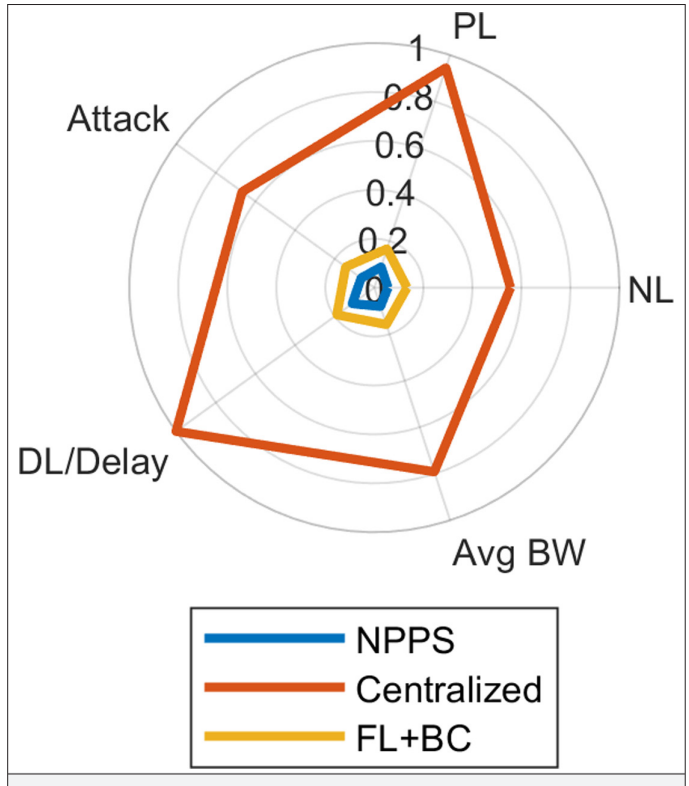


Fig. 9. Bandwidth consumption comparison.

respectively, demonstrating minimal data transmission requirements. In contrast, centralized model training exhibits significantly higher bandwidth consumption, averaging 7.125 MB/s, with the highest bandwidth usage reaching 9 MB/s in scenarios of data loss or delay. This is due to the centralized model training requiring substantial data to be uploaded to the central server, resulting in high bandwidth demands. The Federated Learning + Blockchain (FL+BC) integration scheme effectively reduces bandwidth consumption while ensuring privacy, averaging 1.425 MB/s. In peak electricity usage and network attack scenarios, its bandwidth consumption is 1.5 MB/s and 1.3 MB/s, respectively, significantly lower than that of centralized model training. Overall, FL+BC achieves an efficient balance in bandwidth consumption. While it introduces some additional communication overhead compared to NPPS, it substantially reduces bandwidth usage compared to centralized solutions, making it a more suitable approach for efficient and secure communication.

As shown in Fig. 10, Non-Privacy Preserving Edge Computing (NPPS) demonstrates the lowest processing time across all tested scenarios, averaging only 2.95 seconds. In normal electricity load and network attack scenarios, the processing times are 2.5 seconds and 2.8 seconds, respectively. Centralized model training exhibits significantly higher processing times, averaging 11.25 seconds, with a peak of 15 seconds in data loss or delay scenarios, highlighting the computational bottlenecks of centralized processing under high load or abnormal conditions. The Federated Learning + Blockchain (FL+BC) integration scheme strikes a balance in processing time efficiency, averaging 3.95 seconds. While this is slightly higher than NPPS, it is significantly superior to centralized model training. In peak electricity usage scenarios, FL+BC processing time is 4 seconds, compared to the centralized model training's 12 seconds. Overall, FL+BC maintains a relatively low processing time, demonstrating a balanced advantage in ensuring both privacy and system performance. Compared to NPPS, FL+BC slightly increases processing time but remains within a reasonable range. In contrast to centralized model training, FL+BC significantly reduces processing overhead, making it an efficient and secure processing solution.

As shown in Fig. 11, in terms of CPU resource consumption, Non-Privacy Preserving Edge Computing (NPPS) exhibits the lowest CPU usage across all scenarios, indicating relatively lower computational overhead in the absence of privacy protection measures. In contrast, centralized model training shows the highest CPU consumption, especially under high load or abnormal conditions, as data needs to be processed centrally, leading to a significant increase in CPU resource usage. On the other hand, Federated Learning + Blockchain (FL+BC) strikes a balance between privacy protection and computational efficiency, with CPU consumption falling between that of NPPS and centralized model training. In practical applications, FL+BC can ensure data privacy while achieving high computational performance, making it a more balanced solution, particularly suitable for scenarios where resource usage and privacy protection need to be carefully weighed.

As shown in Fig. 12, in terms of memory resource consumption, Non-Privacy Preserving Edge Computing (NPPS) exhibits the lowest memory usage, indicating that it can maintain lower resource occupancy without adopting privacy protection measures. In contrast, centralized model training, which requires centralized data processing, shows significantly higher memory usage compared to other solutions, especially under high load and abnormal data scenarios, where memory consumption is particularly pronounced. On the other hand, Federated Learning + Blockchain (FL+BC) demonstrates more balanced memory consumption, maintaining moderate memory usage while ensuring privacy protection. FL+BC is able to sustain lower resource consumption under high load and abnormal scenarios, making it a superior choice for applications that require a balance between performance and memory usage.

3) Security Evaluation:

The security evaluation is shown in Fig. 13. Non-Privacy Preserving Edge Computing (NPPS) performs the worst, with an ASR as high as 54.3%, indicating that attacks are more likely to succeed without any protection. Its threat detection rate (TDR) is only 28.5%, and its data

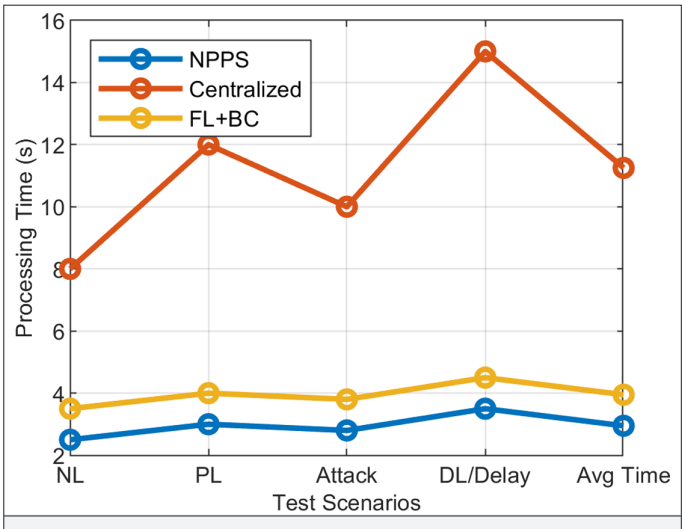


Fig. 10. Processing time comparison.

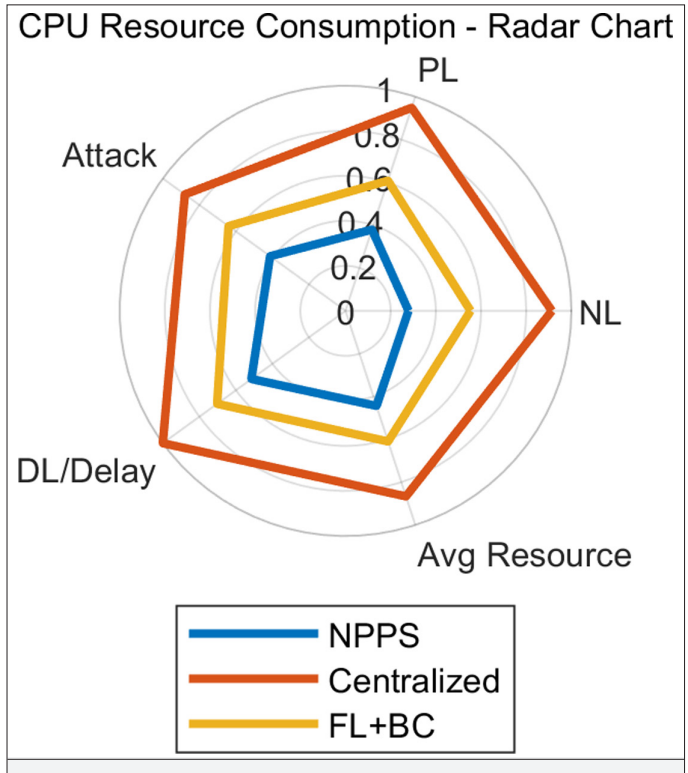


Fig. 11. CPU resource consumption comparison.

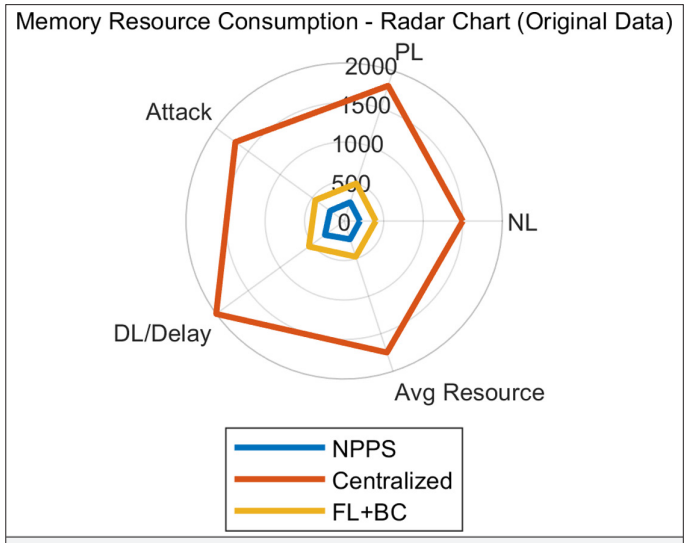


Fig. 12. Memory resource consumption comparison.

integrity resistance (DIR) is merely 8.5%. In contrast, the centralized model training reduces the ASR to 42.3%, but the TDR and DIR are only 53.5% and 27.3%, respectively, showing some improvement but still posing significant security risks. Traditional DP further reduces the ASR to 18.2%, while its TDR increases to 66.5%, and its DIR reaches 39.6%, demonstrating strong security protection effectiveness.

However, the Federated Learning + Blockchain integration scheme (FL+BC) excels in all security metrics. Its ASR is only 1.3%, significantly lower than other schemes, greatly reducing the likelihood of successful attacks. The TDR reaches 87.6%, indicating an exceptionally high capability to detect potential threats. Additionally, its DIR is 91.5%, demonstrating the strongest resilience against data tampering. Therefore, the FL+BC scheme significantly outperforms other schemes in overall security, making it the optimal choice for protecting data security.

Simulate the attacker adjusting the strategy every two hours (such as model inversion, member inference attacks), and record the

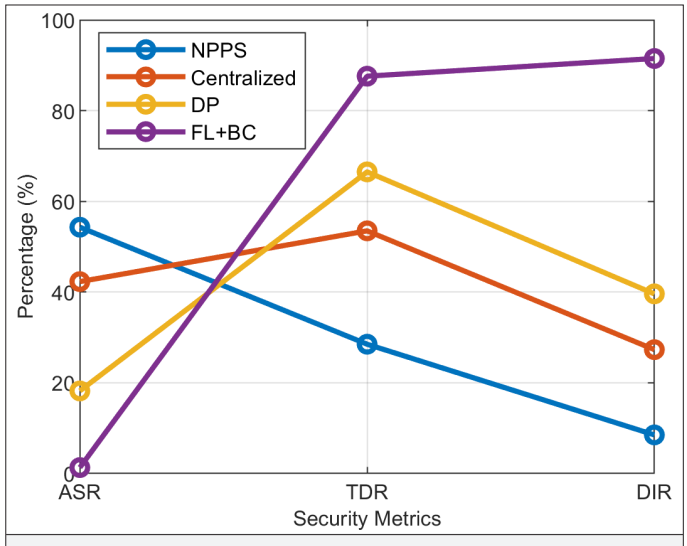


Fig. 13. Security evaluation comparison.

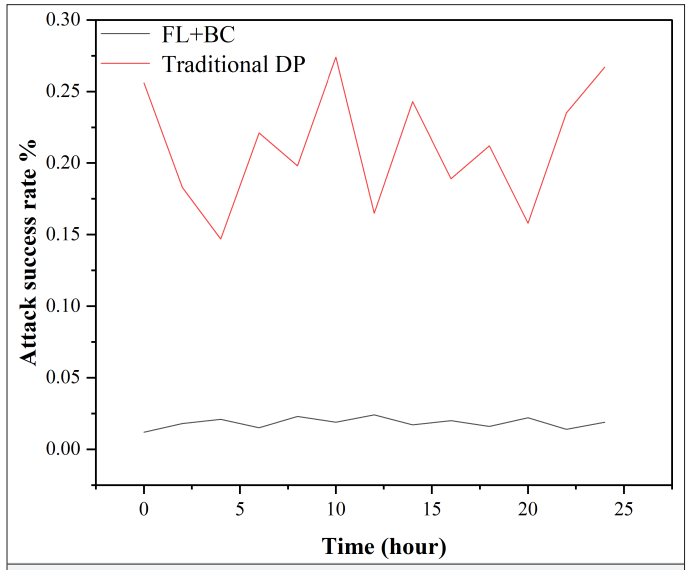


Fig. 14. Attack success rate under 24-hour dynamic attacks.

changes in ASR. As shown in Fig. 14, the ASR of the FL+BC scheme is stably lower than 2.5% under dynamic attacks, while the ASR of the traditional DP scheme fluctuates by 12%-28%.

Analyze the impact of noise intensity σ on MA and PLR:

When σ = 0.5, MA = 93.2%, PLR = 8.7%,

When σ = 2.0, MA = 85.1%, PLR = 0.2%,

As shown in Fig. 15, when σ = 1.0 (MA = 91.5%, PLR = 0.9%) is the optimal equilibrium point.

C. Comparison Experiment With the Frontier Scheme

In the same experimental environment, the performance of the SMPC blockchain solution was compared with the deployment of

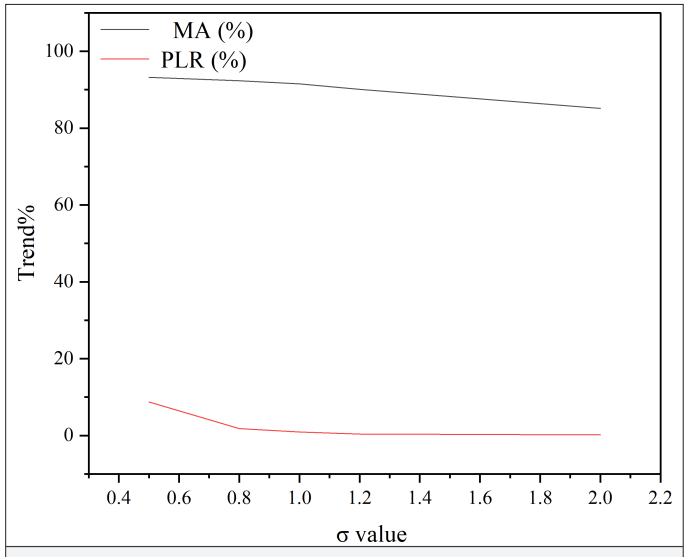


Fig. 15. Impact of noise intensity (σ) on model accuracy (MA) and privacy leakage rate (PLR).

SMPC using the SPDZ (Secure Computation Protocol for Dishonest Majority Zero-Knowledge) protocol and the blockchain integration scheme. The test results showed that the average computing delay of the Super-Mobile Personal Computer (SMPCBC) solution was 1426 ms, which is 65% higher than the 864 ms of Flathead Lutheran Bible Camp (FLBC). The communication overhead was 82 MBs, 475% higher than the 1425 MBs of FLBC. Due to the encryption computation and multi-party verification mechanisms of SMPC, its computing and communication costs are significantly higher than those of the FLBC solution, confirming the high efficiency of this solution in edge scenarios.

To verify the feasibility of resource-constrained devices, the Raspberry Pi 4B (4-core ARM Cortex-A72, 4GB RAM) test was supplemented:

FL local training time: average 8.2 seconds/round (3.7 times slower than the virtual machine),

CPU peak occupancy: 89% (reduced to 72% through model lightweight),

It indicates that this scheme needs to optimize the model structure for low-end equipment (such as using MobileNet), but the basic framework is still applicable.

IV. CONCLUSION

The experimental results demonstrate that the combination of Federated Learning and Blockchain (FL+BC) exhibits significant advantages in the edge computing environment of smart grids. In terms of system latency, FL+BC reduces latency by more than 60% compared to centralized model training and maintains low latency even under high load or abnormal conditions. Although FL+BC slightly increases processing time and resource consumption, these increments remain within acceptable limits compared to the Non-Privacy Preserving Scheme (NPPS), while significantly reducing the risk of data leakage. In terms of CPU utilization, FL+BC averages 56.6%, significantly lower than the 80.4% of the centralized model training. In the security evaluation, FL+BC achieves an ASR of only 1.3%, a TDR of 87.6%, and a DIR of 91.5%, outperforming all other schemes and fully demonstrating its ability to effectively resist attacks and ensure data integrity and security. Overall, the FL+BC scheme not only significantly surpasses other schemes in privacy protection and security but also performs well in computational efficiency and system performance, providing a comprehensive and efficient solution for smart grid data security. It is suitable for smart grid application scenarios with high demands for privacy and performance.

The heterogeneity of edge devices should be considered in the actual deployment. For devices with less than an 8-core CPU, such as Advanced RISC Machine-based (ARM) terminals, model quantization, such as FP16 precision, can reduce the computing load. In the hybrid communication protocol environment, it is recommended to use the gRPC framework to implement the protocol conversion layer.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – J.W.; Design – J.X.; Supervision – J.X.; Resources – J.L.; Materials – H.X.; Data Collection and/or Processing – Jie Wang; Analysis and/or Interpretation – H.X.; Literature Search – J.L.; Writing – J.W.; Critical Review – C.X.

Declaration of Interests: The authors have no conflicts of interest to declare.

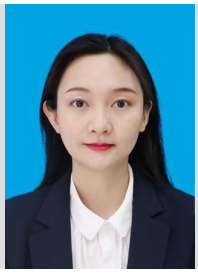
Funding: The research work was conducted with the financial supports by 2022 science and technology project of State Grid Hubei Electric Power Co., Ltd, "research and demonstrational application of key technologies of industrial control security proactive defense architecture for novel power systems" (No.52153222001D).

REFERENCES

1. Q. Li et al., "Deep reinforcement learning based resource allocation for fault detection with cloud edge collaboration in smart grid," *CSEE J. Power Energy Syst.*, vol. 10, no. 3, pp. 1220–1230, 2024.
2. K. Fan et al., "MSIAP: A dynamic searchable encryption for privacy-protection on smart grid with cloud-edge-end," *IEEE Trans. Cloud Comput.*, vol. 11, no. 2, p. 1170–1181, 2023. [CrossRef]
3. M. K. Pasumponthevar, and P. R. Jeyaraj, "Kalman reinforcement learning-based provably secured smart grid false data intrusion detection and resilience enhancement," *Electr. Eng.*, vol. 107, no. 3, pp. 2883–2901, 2025.
4. C. Yang et al., "Research on the application of zero trust framework in the design of power system network architecture," *Proc. SPIE*, vol. 13073, p. 6, 2024.
5. A. G. Pillai, and S. M. Deshmukh, "Efficient service centric blockchain data security for smartgrid systems," in E3S Web Conf., Vol. 540, 2024, p. 9.
6. A. Wang, J. Li, and H. Nan, "Achieving light-weighted secure scheme for communication in a smart grid," *IEEE Access*, vol. 11, p. 14951–14960, 2023. [CrossRef]
7. J. B. Shriram, and P. Anbalagan, "Hybrid chaotic ABC-CSO and GK-LIP techniques for smart grid competence and security," *Electr. Eng.*, vol. 107, no. 2, pp. 1463–1482, 2025. [CrossRef]
8. W. Zhikang, W. Wendi, and Z. F. Baochuan, "Microgrid trading mechanism enhancement for smart contract considering reputation values," *Cybern. Phys. Syst.*, vol. 10, no. 1/4, pp. 214–230, 2024.
9. E. S. Kolawole et al., "Optimization of stealthwatch network security system for the detection and mitigation of distributed denial of service (DDoS) attack: Application to smart grid system," *Commun. Netw.*, vol. 16, no. 3, pp. 108–134, 2024. [CrossRef]
10. R. Pirta-Dreimane et al., "Enhancing smart grid resilience: An educational approach to smart grid cybersecurity skill gap mitigation," *Energies*, vol. 17, no. 8, 2024. [CrossRef]
11. M. Z. Gunduz, and R. Das, "Smart grid security: An effective hybrid CNN-based approach for detecting energy theft using consumption patterns," *Sensors (Basel)*, vol. 24, no. 4, p. 1148, 2024. [CrossRef]
12. R. R. Ramya, and J. Banumathi, "An optimized approach with 128-bit key management for IoT-enabled smart grid: Enhancing efficiency, security, and sustainability," *Electr. Eng.*, vol. 107, no. 2, pp. 2207–2225, 2025. [CrossRef]
13. A. Gehlot, M. A. Normurodovich, D. R. Primmia, G. Saritha, A. Alawady, and S. Singh Dari, "Decentralized blockchain solutions for smart grid data management and security," in E3S Web of Conf., vol. 540, p. 8, 2024. [CrossRef]
14. C. E. Ogbogu, J. Thornburg, and S. O. Okozi, "Smart grid fault mitigation and cybersecurity with wide-area measurement systems: A review," *Energies*, vol. 18, no. 4, p. 994, 2025. [CrossRef]
15. M. A. Hasnat, "Enhancing smart grid security and reliability through graph signal processing and energy data analytics," *Eng. Petrol.*, vol. 1, no. 1, p212, 2023.
16. K. Sarieddine et al., "A real-time cosimulation testbed for electric vehicle charging and smart grid security," *IEEE Secur. Priv.*, vol. 21, no. 4, p. 10, 2023.
17. E. Vignesh, and P. A. Jeyanthy, "Efficient and secure integration of renewable energy sources in smart grids using hybrid fuzzy neural network and improved Diffie-Hellman key management," *Comput. Electr. Eng.*, vol. 123, p. 110206, 2025. [CrossRef]
18. S. Selvarajan, H. Manoharan, T. Al-Shehari, H. Alsalman, and T. Alfakih, "Smart grid security framework for data transmissions with adaptive practices using machine learning algorithm," *Comput. Mater. Contin.*, vol. 82, no. 3, pp. 4339–4369, 2025. [CrossRef]

19. A. A. Elshazly, I. Elgarhy, M. Mahmoud, M. I. Ibrahem, and M. Alsabaan, "A privacy-preserving RL-based secure charging coordinator using efficient FL for smart grid home batteries," *Energies*, vol. 18, no. 4, p. 961, 2025. [CrossRef]
20. S. Binyamin, and S. B. Slama, "IntelliGrid AI: A blockchain and deep-learning framework for optimized home energy management with V2H and H2V integration," *AI*, Vol. 6, no. 2, 2025, p. 34.
21. R. Li, J. Zhang, and F. Deng, "Accident factors importance ranking for intelligent energy systems based on a novel data mining strategy," *Energies*, vol. 18, no. 3, p. 716, 2025. [CrossRef]
22. S. N. Vodapally, and M. H. Ali, "A novel ConvXGBoost method for detection and identification of cyberattacks on grid-connected photovoltaic (PV) inverter system," *Computation*, vol. 13, no. 2, p. 33, 2025. [CrossRef]
23. N. Sifakis, K. Armyras, and F. Kanellos, "Real-time power management of plug-in electric vehicles and renewable energy sources in virtual prosumer networks with integrated physical and network security using blockchain," *Energies*, vol. 18, no. 3, p. 613, 2025. [CrossRef]
24. M. Natkaniec, and P. Kępowicz, "StegoEDCA: An efficient covert channel for smart grids based on IEEE 802.11e standard," *Energies*, vol. 18, no. 2, p. 330, 2025. [CrossRef]
25. G. Johncy, R. S. Shaji, T. M. Angelin Monisha Sharean, and U. Hubert, "Enhancing smart grid security using BLS privacy blockchain with Siamese Bi-LSTM for electricity theft detection," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 1, p. e70033, 2025. [CrossRef]
26. J. Xiong, L. Shen, Y. Liu, and X. Fang, "Enhancing IoT security in smart grids with quantum-resistant hybrid encryption," *Sci. Rep.*, vol. 15, no. 1, p. 3, 2025. [CrossRef]
27. M. A. Alomari et al., "Security of smart grid: Cybersecurity issues, potential cyberattacks, major incidents, and future directions," *Energies*, vol. 18, no. 1, p. 141, 2025. [CrossRef]
28. B. N. Palety, C. Mahalakshmi, and P. N. Reddy, "Anomaly detection in residential electricity consumption with GAN-CNN for enabling smart grid security and efficiency monitoring," *J. Adv. Inf. Technol.*, vol. 16, no. 2, pp. 156–169, 2025. [CrossRef]
29. A. R. Singh, R. S. Kumar, K. R. Madhavi, F. Alsaif, M. Bajaj, and I. Zaitsev, "Optimizing demand response and load balancing in smart EV charging networks using AI integrated blockchain framework," *Sci. Rep.*, vol. 14, no. 1, p. 31768, 2024. [CrossRef]
30. A. A. Abdellatif, K. Shaban, and A. Massoud, "Blockchain-enabled distributed learning for enhanced smart grid security and efficiency," *Comput. Electr. Eng.*, vol. 123, p. 110012, 2025. [CrossRef]
31. Z. Afzal, M. Ekstedt, N. Müller, and P. Mukherjee, "Security challenges in energy flexibility markets: A threat modelling-based cyber-security analysis," *Electronics*, vol. 13, no. 22, p. 4522, 2024. [CrossRef]
32. H. Wen, X. Liu, B. Lei, M. Yang, X. Cheng, and Z. Chen, "A privacy-preserving heterogeneous federated learning framework with class imbalance learning for electricity theft detection," *Appl. Energy*, vol. 378, p. 124789, 2025. [CrossRef]
33. S. Deng, L. Zhang, and D. Yue, "Data-driven and privacy-preserving risk assessment method based on federated learning for smart grids," *Commun. Eng.*, vol. 3, no. 1, p. 154, 2024. [CrossRef]
34. E. C. Piesciorovsky, G. Hahn, R. Borges Hink, and A. Werth, "Total power factor smart contract with cyber grid guard using distributed ledger technology for electrical utility grid with customer-owned wind farm," *Electronics*, vol. 13, no. 20, p. 4055, 2024. [CrossRef]
35. A. Bondok et al., "Accurate power consumption predictor and one-class electricity theft detector for smart grid 'Change-and-Transmit' advanced metering infrastructure," *Appl. Sci.*, vol. 14, no. 20, p. 9308, 2024. [CrossRef]

Jie Wang was born in Huanggang City, Hubei Province in 1984. He obtained a PhD in Computer Application Technology from Huazhong University of Science and Technology in November 2014. Since November 2014, he has been working as the special supervisor of information security technology at the Energy Internet Technology Center of Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd. His research interests include cybersecurity, industrial control security, data security, etc.



Jiangpei Xu was born in Huanggang City, Hubei Province in 1990. She obtained a master's degree in the field of integrated circuits from Tsinghua University in June 2014. Since July 2014, she has been working as the special supervisor of information and communication technology at the Energy Internet Technology Center of Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd. Her research interests include power information communication and cybersecurity.

Jing Li was born in Wuhan, Hubei Province in 1984. He obtained a PhD in Information Security from Wuhan University in August 2012. Since 2016, he has been engaged in network security management and currently serves as the Director of the Network Security Division of the Digitalization Department of State Grid Hubei Electric Power Co., Ltd. His research interests include information security, cybersecurity, data security, and information operations management.

Chao Xu was born in Enshi City, Hubei Province, China in 1976. He obtained a bachelor's degree in computer software from the Department of Computer Science at Central South University for Nationalities in 1998. Since 1998, he has been serving as the head of the information class of the Information and Communication Center of State Grid Hubei Ultra High Voltage Company. His research interests include power information network operation and maintenance, and information security protection.

Huihui Xie was born in Hanchuan City, Hubei Province in 1994. He obtained a master's degree from Beijing Institute of Technology in 2019. Since 2019, he has been serving as a network security monitoring duty officer at the Information and Communication Center of State Grid Hubei Ultra High Voltage Company. His research interests include cybersecurity and artificial intelligence.