CIT. Journal of Computing and Information Technology, Vol. 33, No. 2, June 2025, 73–90
doi: 10.20532/cit.2025.1005947

A Hybrid CNN-LSTM Framework with Federated Learning for Enhanced Power Grid Intrusion Detection

Songyao Feng, Mingfei Zeng, Zhengyan Huang and Weigang Su

Information Center of Guangxi Power Grid Co., Ltd, Nanning, China

To address the issues of data silos, low detection accuracy, and insufficient generalization ability in traditional methods for power grid intrusion diagnosis, this study proposes the use of federated learning to construct a power grid intrusion diagnosis model and incorporates convolutional neural networks and long short-term memory network optimization models on this basis. The experiment outcomes indicate that in performance analysis, the accuracy of the raised model is 97.3%, the precision is 97.7%, the recall is 90.8%, the F1 value is 91.1%, the loss rate is 0.02, and the communication efficiency is 93.3%. In the case analysis, the error rate of the proposed model in dealing with Dos and Probe attacks does not exceed 1%, the storage value of abnormal intrusion information is 204 MB, the training time is 47.7 s, and the total expenditure required for the model in actual operation is the lowest. In summary, the raised model can substantially enhance the precision and timeliness of power grid intrusion diagnosis, and possesses significant practical utility, which can be widely applied in smart grid security systems.

ACM CCS (2012) Classification: Social and professional topics → Professional topics → Computing and business → Automation

Keywords: federated learning, convolutional neural network, long short-term memory network, power grid intrusion diagnosis, safety protection

1. Introduction

The power grid, as the cornerstone of modern energy supply, has immeasurable value for people's well-being, economic development, and even national security in terms of its safe and stable operation. It not only supports the daily electricity demand, but also drives the continuous operation of industrial production, and is an indispensable lifeline of modern society [1]. However, with the improvement of power grid scale and intelligence level, the challenges faced by the power grid are also constantly increasing. For example, with the widespread application of advanced technologies such as the Internet of Things, big data, and cloud computing in the power grid, the openness and interconnectivity of the power grid systems have significantly increased. Although this has improved the intelligence level and operational efficiency of power grids, it also provides more intrusion paths for potential attackers. Malicious hackers can launch targeted network attacks by infiltrating a power grid control system. At present, power grid intrusion incidents have become an important factor threatening power grid security. According to the "Crude Oil Security Sentinel" research project of S&P Global Platts, the number of cyber-attacks targeting the energy sector has surged globally since 2017. Among them, oil and gas infrastructure and power grids have become the "key areas" of cyber-attacks, accounting for over 50% of all cyber-attack incidents. In the past 5 years, the proportion of cyber-attacks targeting the power grid has been about 1/4. Power grid invasion, whether it is malicious attacks or unexpected failures, can cause large-scale power outages, equipment damage, and even the collapse of the entire power system, caus-

ing huge losses to the social economy and seriously affecting the normal lives of the people. Therefore, strengthening power grid intrusion detection and guaranteeing the secure and reliable functioning of the power grid is not only an urgent technical requirement, but also a crucial factor in preserving societal consistency and economic development [2]. However, with the expansion of the power grid scale and the diversification of intrusion methods, traditional power grid intrusion diagnosis models based on a single algorithm are difficult to effectively cope with complex and changing intrusion scenarios. Faced with massive power grid data, how to quickly and accurately identify intrusion behaviors and their characteristics from numerous sources of information monitoring has become the core issue of current research.

Based on this, a novel power grid intrusion diagnosis model is suggested by combining Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Federated Learning (FL). CNN can efficiently extract spatial features of power grid data, while LSTM can capture temporal dependencies of data. The combination of the two can notably improve the model's capability to identify complex intrusion behaviors. Meanwhile, the introduction of FL has achieved collaborative training of multiple power grid nodes while protecting data privacy, further improving the model's generalization ability and robustness. The innovation and the main contribution lies in the first combination of CNN, LSTM, and FL applied in the field of power grid intrusion diagnosis. This not only solves the problem of insufficient recognition ability of traditional models in complex and changing intrusion scenarios but also achieves the dual goals of data privacy protection and model performance improvement. In practice, the new model proposed in the research will provide more reliable support for power grid security monitoring, effectively reduce the occurrence of power grid intrusion events, and lower economic losses and social impacts. In theory, the research offers fresh perspectives and pathways for the progression of power grid intrusion detection technology and provides useful references and inspirations for research in related fields.

The goal of this study is to propose a new power grid intrusion diagnosis model to address the challenges posed by the expansion of power grid scale and the diversification of intrusion methods. It aims to solve the problem of insufficient recognition ability of traditional models in complex intrusion scenarios, thereby strengthening power grid intrusion detection and ensuring the safe and reliable operation of the power grid.

2. Literature Review

In recent times, numerous researchers have devised and introduced a variety of models and techniques aimed at enhancing the detection capabilities of power grid intrusion systems. Mhmood *et al.* proposed an innovative smart grid (SG) intrusion detection system that integrates game theory, swarm intelligence, and deep learning (DL) to resist complex network attacks [3]. The system was tested on the NSL-KDD dataset, and the results showed an accuracy of 99.82%, sensitivity of 99.69%, and accuracy of 99.76% in detecting attacks. Alsoufi *et al.* proposed a new anomaly-based Internet of Things intrusion detection system (AIDS) based on deep learning techniques, and combined it with sparse autoencoder (SAE) to reduce high dimensionality using CNN to create binary classification [4]. The experimental results show that the accuracy of the model on the Bot IoT dataset is 99.9%, the precision is 99.9%, and the recall rate is 100%. Huang *et al.* proposed a new FL-based method aimed at improving the accuracy of network intrusion detection, and combined CNNs with attention mechanisms [5]. Experimental results showed that compared with traditional methods, the research method can significantly improve detection accuracy. Priyadarshini proposed combining federated learning with split learning to cope with network intrusion attacks [6]. Experimental results show that compared with traditional deep learning models, this method can significantly improve the performance of the model.

In recent years, many scholars have been dedicated to exploring and introducing various algorithms to improve the detection performance of power grid intrusion diagnosis models. Although these studies have achieved certain

results in optimizing performance and improving model accuracy, most of them focus on algorithm level improvements and pay less attention to practical factors such as dynamic changes in power grid operation status. In actual power grid environments, the diagnostic process of power grid intrusion is much more complex than in laboratory environments. It is not only affected by algorithm accuracy but also constrained by multiple factors such as power grid load fluctuations, equipment status changes, and external environmental factors. Therefore, although existing research has made some progress in improving model performance, there are still many limitations. Especially in dealing with the complexity and diversity of power grid data, as well as ensuring the adaptability and practicality of the model in actual power grid environments, further exploration and optimization is still needed. This study aims to fill this gap by comprehensively considering the dynamic changes in the operation status of the power grid, combining advanced machine learning and deep learning techniques, and exploring the possibility of federated learning to improve model performance while protecting data privacy, in order to develop a more comprehensive, accurate, and practical power grid intrusion diagnosis model.

3. Research Methodology

3.1. Construction of Intrusion Detection Model for Power Grid Based on FL

Traditional power grid intrusion detection does not take into account the strong real-time nature of network traffic in power information, and the generated data is not evenly distributed. Therefore, with the deepening of informationization and intelligence of the power grid, traditional power grid intrusion detection models are becoming increasingly difficult to cope with. FL, as an emerging distributed machine learning paradigm, allows multiple participants to collaborate without data being shared locally, achieving the effect of "knowledge sharing without data sharing" [7, 8]. Therefore, based on this characteristic of FL, it can be effectively used to solve the above problems and achieve network security protection for the power grid system. The diagram in Figure 1 illustrates this particular configuration.

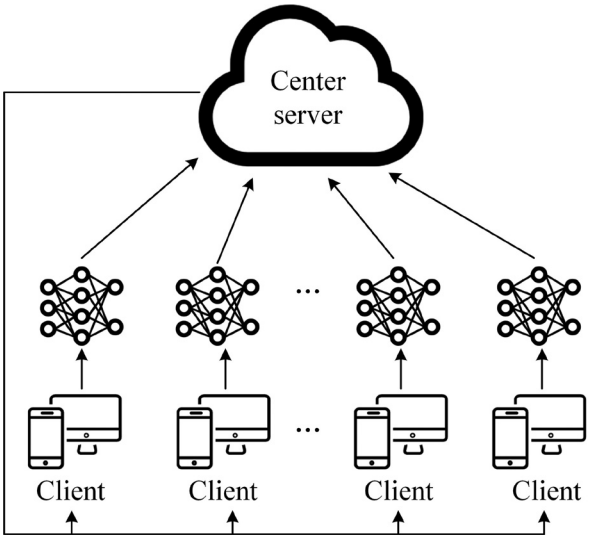
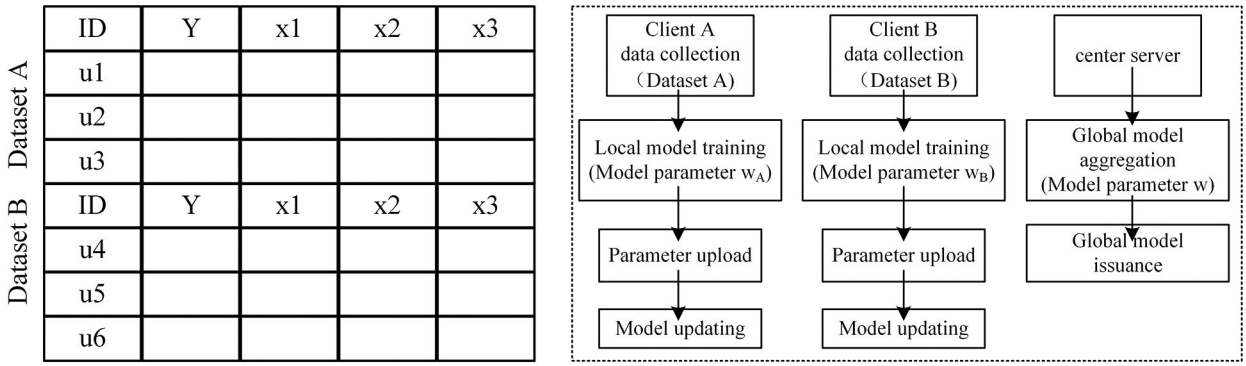


Figure 1. Structural illustration of the FL model framework.

Figure 1 is a structural illustration of the model flow for horizontal FL. From the figure, FL is based on the coordination of multiple client devices and a central server to jointly train a model. During this procedure, the client undertakes the task of utilizing local datasets for model training to produce a localized model, whereas the central server is accountable for amalgamating the locally trained models from each client with respective weights to construct the comprehensive global model [9,10]. It is worth noting that there are various types of FL [11]. Due to the fact that power grid systems typically cover a wide geographical area and multiple substations, and each substation may generate a large amount of network traffic data, although the geographical location and user groups of these data samples are different, they have significant overlap in data characteristics such as network protocols, packet formats, *etc.* Based on this, the study selected horizontal FL to construct a power grid intrusion detection model. The specifically proposed data architecture of horizontal FL can be seen in Figure 2.



（a）data architecture

（b）Detailed architecture diagram of data flow

```
def federated_averaging(parameters_list):
    """
    Federated Averaging Algorithm
    :param parameters_list: List of model parameters
uploaded by clients
    :return: Global model parameters
    """
    n = len(parameters_list)  # Number of clients
    global_weights = [0.0] * len(parameters_list[0])  #
Initialize global model parameters

    for client_params in parameters_list:
        for i in range(len(client_params)):
            global_weights[i] += client_params[i]

    for i in range(len(global_weights)):
        global_weights[i] /= n

    return global_weights

def local_model_training(dataset, global_weights):
    """
    Local Model Training
    :param dataset: Local dataset
    :param global_weights: Global model
parameters
    :return: Local model parameters
    """
    # Train the model using local data and global
model parameters
    # Here, you can use optimization algorithms like
gradient descent
    local_weights = global_weights  # Initialize local
model parameters
    # Assuming a simple gradient descent algorithm
for updates
    for epoch in range(num_epochs):
        for x, y in dataset:
            gradient = compute_gradient(x, y,
local_weights)
            local_weights -= learning_rate * gradient

                    return local_weights

def compute_gradient(x, y, weights):
    """
    Compute Gradient
    :param x: Input data
    :param y: Labels
    :param weights: Model parameters
    :return: Gradient
    """
    # Compute predictions
    predictions = model(x, weights)
    # Compute the gradient of the loss function
    gradient = compute_loss_gradient(predictions, y)
    return gradient


def compute_loss_gradient(predictions, y):
    """
    Compute the Gradient of the Loss Function
    :param predictions: Predictions
    :param y: Labels
    :return: Gradient
    """
    # Assuming mean squared error as the loss function
    loss = (predictions - y) ** 2
    gradient = 2 * (predictions - y) / len(y)
    return gradient
```

（c）Pseudo code for key algorithm of global model aggregation in horizontal federated learning

Figure 2. Pseudo code for key algorithm of global model aggregation in horizontal federated learning.

Figure 2 shows the internal data architecture of horizontal FL. From the figure, horizontal federated learning is characterized by the uniformity of dataset features X and label information Y across different clients, with the only variation being the unique sample IDs. It is precisely based on this characteristic that in model training, it is not necessary to transmit complete raw data, only the gradients or parameters of the model can be transmitted to achieve updates, thus greatly protecting data privacy [12, 13]. The power grid data often contains a lot of sensitive information, such as user behavior, device status, and so on. The characteristics of horizontal FL can be well addressed, and the calculation of this process can be seen in formula (1).

$$\begin{cases} \min\limits_{w \in R^d} f(w) = \dfrac{1}{n} \sum\limits_{i=1}^{n} f_i(w) \\ f_i(w) = L(x_i, y_i; w) \end{cases} \tag{1}$$

Here, w represents the given model parameters, $w \in R^d$. n is the total amount of training data, and L is the loss result. (x_i, y_i) represents a single data sample, where x_i is the feature attribute of the i-th training data point and y_i is the label category of the i-th training data point. Formula (1) can be used to enhance the horizontal federated training process and address communication instability issues in power grid intrusion detection [14, 15]. However, the intrusion detection model for power grids based on horizontal federation also needs to consider the number of clients and aggregation servers within the model. When each client has an independent dataset, the loss function on the dataset is given in formula (2).

$$\begin{cases} F_k(w^t) = \dfrac{1}{n_k} \sum\limits_{i=1}^{n_k} f_i(w^t) \\ n_k = \left| D_k \right| \end{cases} \tag{2}$$

Here, k represents the aggregated quantity of clients, and $k(k \in K)$. n_k represents the size of the dataset owned by the K-th client, D_k represents the dataset, and t represents the update round. According to formulas (1) and (2), the loss function for global iterative training can be calculated as represented in formula (3).

$$\begin{cases} f(w^t) = \sum\limits_{k=1}^{K} \dfrac{n_k}{n} F_k(w^t) \\ n = \sum_{k=1}^{K} n_k \end{cases} \tag{3}$$

Here, w^t is the current number of iterations, which is the global model parameter for round t, and n represents the total amount of data. Based on this, the loss function can be optimized using gradient descent to obtain the updated parameters of the local model, as shown in formula (4).

$$\begin{cases} w_k^{t+1} \leftarrow w^t - \eta g_k \\ g_k = \nabla F_k(w^t) \\ w_k^{t+1} = \arg\min\limits_{w^t \in R^d} F_k(w^t) \end{cases} \tag{4}$$

In formula (4), g_k represents the average gradient of the local dataset under the current model parameters, and $w_k{}^{t+1}$ represents the optimal parameters of the updated local model. The gradient and parameters are uploaded to the aggregation server, and model averaging is performed to complete the response to intrusion threats [16, 17]. Finally, based on horizontal FL, an intrusion detection model for the power grid can be constructed, as shown in Figure 3.

Figure 3 shows a power grid intrusion detection model grounded on horizontal FL. From the figure, the specific architecture of the model is roughly categorized into four sections: data preparation layer, attribute retrieval layer, model training layer, and intrusion detection layer. The data preparation layer is mainly responsible for processing data from various components of the power grid [18,19]. The attribute retrieval layer is accountable for extracting key features from preprocessed data. The model training layer is accountable for using the extracted features for training. As FL is used, each power grid component or node will undergo model training locally. The intrusion detection layer mainly applies the trained model to detect abnormal behavior or intrusion events in the power grid.

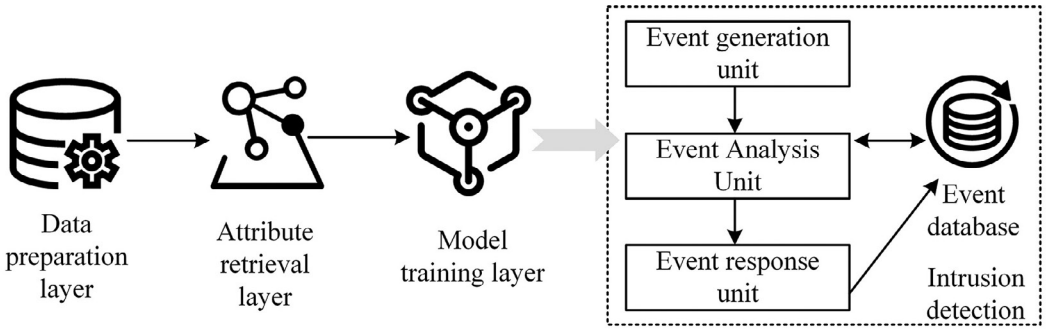


Figure 3. Grid intrusion detection model based on horizontal FL.

3.2. Improved Model for Power Grid Intrusion Detection Integrating CNN-LSTM Algorithm

The intrusion detection model based on FL can achieve indirect expansion of data, thereby improving data quality and enriching samples. However, in the FL environment, model updates often require frequent transmission between multiple users, which may increase the communication overhead of the power grid, especially in situations where network bandwidth is limited. Besides, if there are a significant quantity of users or frequent model updates, communication costs may further increase. To address this issue, the study proposes to combine CNN with LSTM to jointly raise the comprehensive efficacy of the power grid intrusion detection model. The core advantage of CNN lies in its powerful feature extraction capability. By stacking multiple convolutional and pooling layers, it can extract higher-level and more abstract feature representations, providing support for subsequent intrusion detection. The particular configuration is shown in Figure 4.

From Figure 4, CNN mainly consists of input, convolutional, pooling, and fully connected layers [20]. By increasing the number of convolutions composed of convolutional and pooling layers, the learning ability of the model can be improved. In addition, convolution also has dimensional differences. Considering that the power grid dataset is textual information, usually one data sample corresponds to one row of data, therefore, a one-dimensional CNN (1D-CNN) is selected in the study to extract spatial features of the data. The convolution calculation and activation function of 1D-CNN can be seen in formula (5).

$$\begin{cases} Convl = W * X + b \\ p(y = k \mid x) = Soft\max(w_k^T x) = \dfrac{\exp(w_k^T x)}{\sum_{k=1}^{K} \exp(w_k^T x)} \\ \mathrm{Re}\,LU = \max(0, x) \end{cases} \quad (5)$$

Here, W signifies the coefficient matrix of the convolutional filter, X is the feature matrix, and b is the bias term constant. y is the category label, $y \in \{1, 2, ..., K\}$. p represents category probability, and w_k represents category weight.

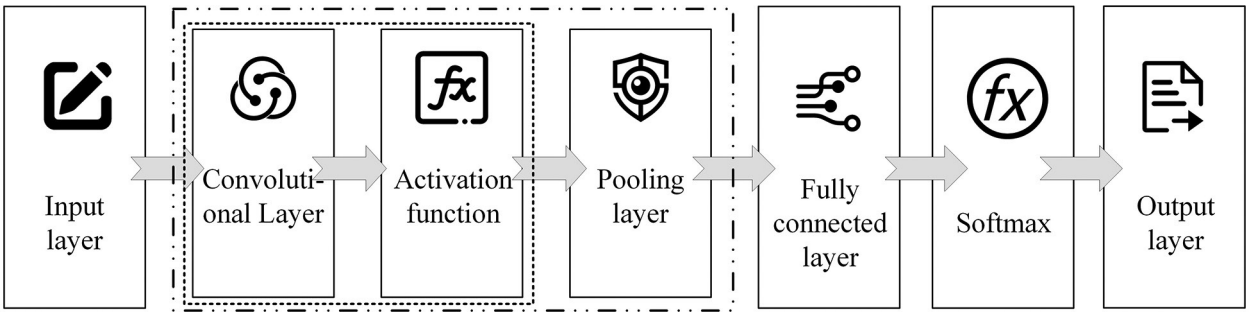


Figure 4. Configuration of the CNN structure.

To reduce changes in data distribution and improve the stability of model training, batch normalization (BN) on 1D-CNN is performed. The specific calculation of BN can be found in formula (6).

$$\begin{cases} \mu = \frac{1}{m}\sum_{i=1}^{m} X_i \\ \sigma^2 = \frac{1}{m}\sum_{i=1}^{m}(X_i - \mu)^2 \\ X_{normalized} = \frac{X_i - \mu}{sqrt(\sigma^2 + \varepsilon)} \end{cases} \tag{6}$$

Here, X represents the input set, and the input set contains m samples. μ is the mean of each feature across the whole dataset, and σ^2 is the variance of each feature across the whole dataset. ε is a very small number, mainly used to avoid situations where the variance is zero [21]. In addition, to avoid overfitting of the model, Dropout regularization operation is added, and the specific calculation can be seen in formula (7).

$$Output = \frac{x \cdot m}{1 - p} \tag{7}$$

Here, m is the random mask, x is the input vector, and p is the dropout probability. In addition, due to the use of 1D-CNN in the study, in order to complement the one-dimensional convolutional layer in the calculation of the pooling layer, one-dimensional max pooling (MaxPool 1D) was adopted. The specific calculation can be seen in formula (8).

$$L_{out} = \left\lfloor \frac{L_{in} + 2 \times padding - dilation \times (\ker nel_{size} - 1) - 1}{stride} + 1 \right\rfloor \tag{8}$$

Here, L_{out} represents the output length, L_{in} represents the input length, ker nel_{size} is the size of the pooling window, *stride* is the step size of the window movement, *dilatation* represents the parameter that controls the stride of elements in the window, and *padding* represents adding additional values around the boundaries of the input data. Based on the above optimization, a new CNN layer can be formed by combining them. However, CNN is more suitable for dealing with local feature extraction and is not good at processing sequential data, while power grid data usually has strong temporal characteristics, that is, there are dependencies between data at different time points. Therefore, considering this, the study incorporates LSTM to capture temporal dependencies in power grid data [22]. LSTM is very good at processing sequence data and can identify patterns, trends, and periodic changes in sequences. Its structure is given in Figure 5.

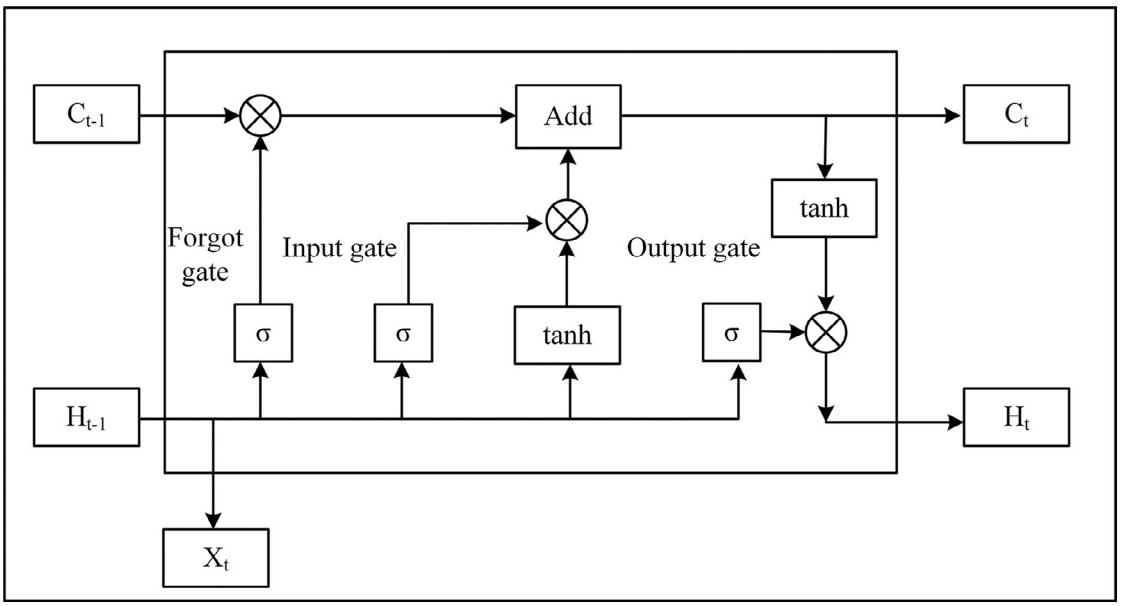


Figure 5. Schematic diagram of LSTM structure.

Figure 5 shows the inner configuration of LSTM. From the figure, the detailed procedure of LSTM is roughly divided into four stages, namely forget gate, input gate, update memory unit, and output gate [23]. The calculation of the forget and input gates can be seen in formula (9).

$$\begin{cases} f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f \\ i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \\ \tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C \end{cases} \tag{9}$$

Here, W_f is the weight matrix, b_f is the bias term, x_t is the input at time t, h_{t-1} is the output at time $t-1$, and $\tilde{C}_t$ represents the new candidate memory state. The calculation for the update memory unit and output gate is shown in formula (10).

$$\begin{cases} c_t = f_t * c_{t-1} + i_t * \tilde{C}_t \\ O_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \\ h_t = O_t * \tanh(C_t) \end{cases} \tag{10}$$

Here, f_t is the calculation result of the forget gate, i_t is the calculation result of the input gate, O_t is the result of the output gate, and h_t is the external information state. c_{t-1} is the memory state at time $t-1$, and c_t is the memory state at time t.

The output of LSTM is often multidimensional. In order to further expand the multidimensional output into one dimension and facilitate better feature extraction, Flatten and Dense layers were added after the LSTM layer. The specific calculation is given in formula (11).

$$\begin{cases} flatten(x) = x.reshape(-1) \\ y = Wx + b \end{cases} \tag{11}$$

Here, x represents a multidimensional array, and $reshape(-1)$ represents converting the multidimensional array into a one-dimensional array. y is the output, w is the weight matrix, x is the input matrix, and b is the bias vector. The improved CNN and LSTM ultimately form a structure as shown in Figure 6.

Figure 6 shows the optimized network structure fused with CNN-LSTM. From the figure, 1D-CNN is selected in the CNN layer, and BN layer, Dropout layer, and matching MaxPool 1D layer are added. After the LSTM layer, Flatten layer and Dense layer ensue. The former is used to flatten multidimensional input data, while the latter is used for further classification processing. The combination of the optimized CNN-LSTM network and the FL-based power grid intrusion detection model can achieve an overall improvement in the capability of the original model.

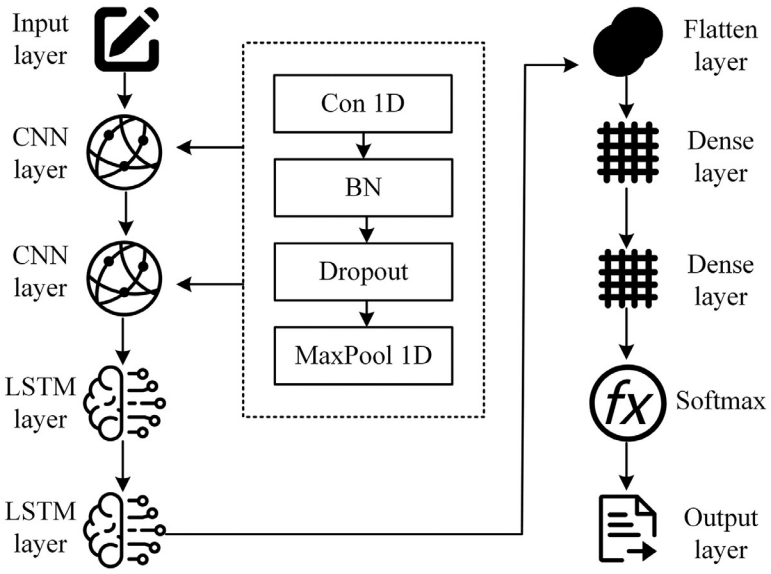


Figure 6. CNN-LSTM optimization network structure diagram.

4. Results and Discussion

4.1. Performance Analysis Based on Power Grid Intrusion Detection Model

The study selected the classic smart grid intrusion detection dataset KDD Cup 99 as the experimental research data. Before conducting formal testing, the original KDD Cup 99 dataset was cleaned, and various kinds of data in the dataset were appropriately manipulated and processed according to experimental needs. After processing, there were an overall 120,000 data samples in the training set and 21,000 data samples in the testing set. The laboratory setting used the Windows 10 operating system and Python 3.7 as the development language. The study used a comparative method to include intrusion detection models based solely on FL and CNN-LSTM as comparison models and named them FL model and CNN-LSTM model, respectively. The model proposed by the research institute is named FL-CNN-LSTM, and the main parameters, parameter values, and the role of parameter selection of the model are shown in Table 1.

Table 1. Parameter Settings of the Model.

Layer	Output Shape	Param	Function
Conv1D	1*122*48	192	Extract features from input data
Batch normalization	1*122*48	192	Accelerate the training process, improve model stability, and reduce dependence on initialization
Dropout	1*122*48	0	By randomly discarding some neurons in the network, overfitting can be prevented and the generalization ability of the model can be improved
MaxPooling1D	1*61*48	0	Reduce feature dimensionality, decrease computational complexity, while preserving the most important features
Conv1D	1*61*40	10656	Consistent with the previous statement
Batch normalization	1*61*40	160	Consistent with the previous statement
Dropout	1*61*40	0	Consistent with the previous statement
MaxPooling1D	1*30*40	0	Consistent with the previous statement
LSTM	1*30*40	15200	Process sequence data and capture long-term dependencies
	1*30*20	6240	
Flatten	1*600	0	Flatten multidimensional inputs into one dimension for input into fully connected layers
Dense	1*32	19200	Map features to output space
	1*10	330	Generate the final prediction result

Based on this, the complexity analysis results of the model are shown in Table 2.

Accuracy, precision, recall, and F1 value were selected as assessment metrics. The accuracy and precision results of the model are shown in Figure 7.

Figure 7 indicates the accuracy and precision performance of three models in smart grid intrusion detection. Figure 7 (a) shows the accuracy of the model. In comparison with the others, the FL-CNN-LSTM model had the highest accuracy, which was 97.3%. Next was the FL model, with the accuracy value of 90.1%. The accuracy of the CNN-LSTM model was the lowest, at 86.4%. Figure 7 (b) shows the precision of the three models. The results of precision and accuracy had similar performance. The order of model performance from poor to excellent was CNN-LSTM model, FL model, and FL-CNN-LSTM model. The specific values of precision were 82.3%, 89.5%, and 97.7%, respectively. From the scores of accuracy and precision, the FL-CNN-LSTM model performed better in smart grid intrusion detection. The specific results of recall rate and F1 value indicators are shown in Figure 8.

Table 2. Complexity Analysis of the Model.

Layer type	**Time complexity (big O notation)**	**Notes**
Conv1D	O(L×K×Cin×Cout)	L: Input sequence length, K: Convolutional kernel size, Cin: Number of input channels, Cout: Number of output channels
BN	O(L×Cout)	Batch normalization is usually the same as the output dimension of convolutional layers
Dropout	O(L×Cout)	Same output dimension as the convolutional layer
MaxPooling1D	O(L×Cout)	The output of the pooling layer is usually less than or equal to the output of the convolutional layer
Conv1D	O(L′×K′×Cout′×Cout″)	L′: The length of the pooled sequence, K′: The size of the new convolution kernel, Cout': Number of old output channels, Cout": Number of new output channels
BN	O(L′×Cout″)	Consistent with the previous statement
Dropout	O(L′×Cout″)	Consistent with the previous statement
MaxPooling1D	O(L″×Cout″)	L″: Final pooled sequence length
LSTM	O(L″×(Hin×Hout+Hout2))	Hin: Input the number of features, Hout: Number of hidden units in LSTM
Flatten	O(L‴×Hout)	L": LSTM output sequence length
Dense	O((L‴×Hout)×M)	M: Output the number of units (such as the number of categories in a classification task)
Federal Learning Communications	O(R×n×P)	R: Communication epochs, n: Number of clients, P: Number of model parameters

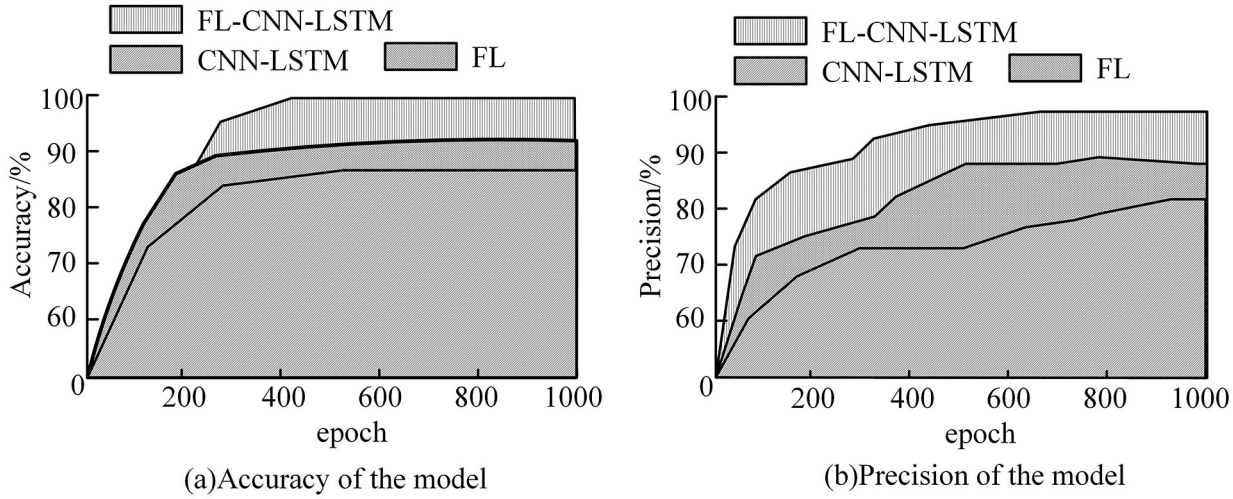


Figure 7. Accuracy and precision of each model.

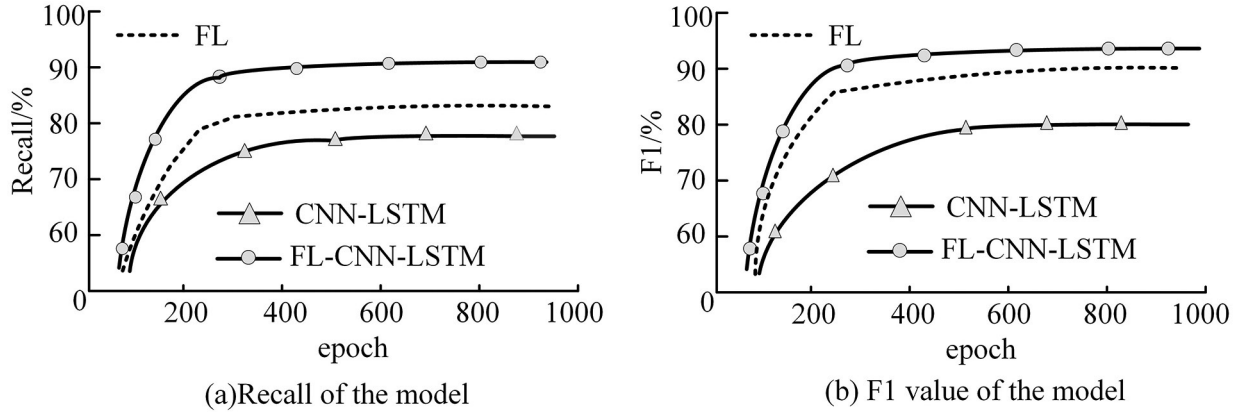


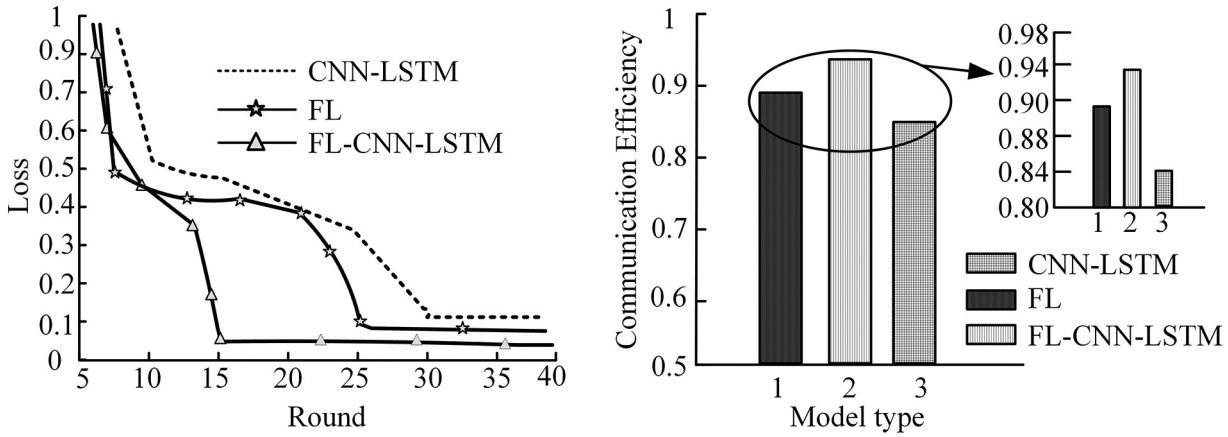
Figure 8. The recall and F1 value of the models.

Figure 8 indicates the recall and F1 value of three models in smart grid intrusion detection. Figure 8 (a) indicates the recall of the model. The recall of the CNN-LSTM model was 78.2%, the recall of the FL model was 82.7%, and the recall of the FL-CNN-LSTM model was 90.8%. Alternatively, the FL-CNN-LSTM model had the highest recall rate. Figure 8 (b) indicates the F1 value of the model. Consistent with the recall results of the model, the FL-CNN-LSTM model still had the highest F1 value compared to the other two models, specifically 91.1%. Next was the FL model, accounting for 88.1%, while the CNN-LSTM model had a relatively low score of 78.8%. Overall, the FL-CNN-LSTM model performed better in smart grid intrusion detection. In addition, the experiment further tested the loss rate and communication efficiency of each model, as shown in Figure 9.

Figure 9 shows the iteration rounds and communication efficacy of three models in smart grid intrusion detection. Figure 9 (a) indicates the loss rate of the model. The CNN-LSTM model took nearly 30 rounds to converge, and the loss value during convergence was about 0.13. The FL model needed nearly 25 rounds to reach convergence, and the loss value during convergence was about 0.08. By comparison, the FL-CNN-LSTM model achieved convergence in the least number of epochs, only requiring about 15 epochs, and had the lowest

loss value during convergence, approximately 0.02. Figure 9 (b) indicates the communication efficiency of the model. The communication efficiency of the CNN-LSTM model was about 84.6%, which was lower than 89.3% of the FL model. In comparison with the others, the FL-CNN-LSTM model had the highest communication efficiency of 93.9%. In order to further highlight the performance of the model, other models of different types were used for performance comparison, and the results are shown in Table 3.

Table 3 shows the performance of other comparative models that are not very similar to the research model. Based on the comprehensive performance of the above research models, the performance of the proposed model is still the best compared to these four models. Considering that ablation experiments can be used to demonstrate the contributions of various components in the research model, further ablation experiments were conducted, and the results are shown in Table 4.



(a) Comparison of model loss values (b)The communication efficacy of the model

Figure 9. Loss rate and communication efficacy of the model.

Table 3. Performance comparison of the models.

Medel	F1	Recall	Accuracy
CNN-BiLSTM	82.5%	88.3%	89.7%
PSO-BiLSTM	82.7%	88.7%	90.1%
fl-AMI	82.4%	88.1%	89.4%
RFECV-VAE	82.8%	87.9%	89.3%
DNSAE-RF	83.1%	88.6%	89.1%

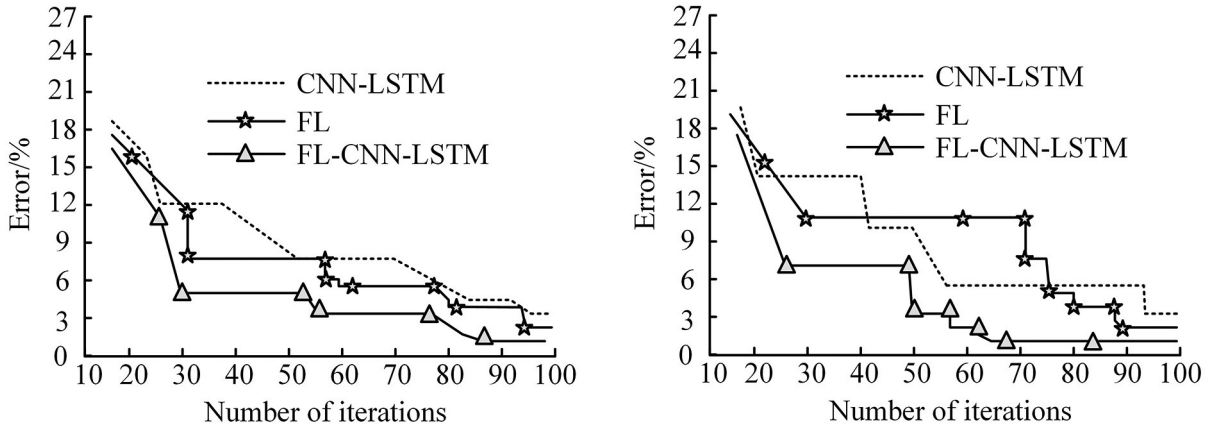
Table 4. Results of the ablation experiment.

Model configuration	ROC-AUC (%)	MAE	MSE	Training Time (min)
LSTM	85	0.23	0.11	113
CNN	87	0.22	0.13	110
CNN-LSTM	90	0.18	0.08	120
FL-CNN-LSTM	96	0.12	0.04	150

Table 4 shows the results of the ablation experiment. From the table, it can be seen that there is not much difference in performance between the LSTM model and the CNN model alone, but the overall performance of the model quickly improved after combining CNN with LSTM. After adding FL to the CNN-LSTM component, the performance of the model continued to improve. Overall, the capability of the smart grid intrusion detection model based on FL-CNN-LSTM was better.

4.2. Case Analysis Based on Power Grid Intrusion Detection Model

The above experiment only tested the comprehensive capabilities of the model. To gain a deeper understanding of the raised model's capability in real-world intrusion detection, case validation was carried out. The dataset obtained based on KDD Cup 99 cleaning contains two classic attack types, Dos and Probe. The experiment evaluated the intrusion detection errors of the three models separately, and the results are shown in Figure 10.



(a)Intrusion detection error during Dos attack (b)Intrusion detection error during Probe attack

Figure 10. Intrusion detection errors of various models in response to different types of attacks.

Figure 10 shows the intrusion detection error performance of three models in response to Dos and Probe attacks, respectively. Figure 10 (a) shows the intrusion detection error of the model in response to Dos attacks. According to observation, the initial error of the CNN-LSTM model was the highest, about 18.2%, before the start of iteration, and its intrusion detection error rate was about 3.2% in the later stage of iteration. Next was the FL model, which had an error rate of about 17.4% at the beginning of iterations. As the iterations progressed, its intrusion detection error rate dropped to around 2.8%. In contrast, the FL-CNN-LSTM model had lower intrusion detection errors than the other two models in both the early and late stages of iterations, with an intrusion detection error rate of 12.3% in the early stages and 0.7% in the late stages. Figure 10 (b) shows the intrusion detection error of the model in response to Probe attacks. Similar to Dos attacks, in the early stages of iterations, the error rate of the FL-CNN-LSTM model was still the lowest among the three models, about 11.8%. As the iteration progresses, the error rate began to decrease, dropping to 0.6%. These results indicate that the FL-CNN-LSTM model has significant advantages in detecting the classic Dos and Probe attacks. Its low initial error rate and fast error reduction speed not only demonstrate the effectiveness of the model in handling imbalanced data and improving detection performance but also demonstrate the potential of federated learning in enhancing model generalization ability and adaptability. In addition, the fast convergence characteristics of the FL-CNN-LSTM model mean that it can achieve high performance levels in fewer iterations, which is an important advantage for real-time power grid intrusion diagnosis systems. Furthermore, the experiment also examined the proportion of abnormal intrusion information in the power grid storage environment and the training duration of the model, as shown in Figure 11.

Figure 11 shows the storage values and training duration of abnormal intrusion information for the three models. Among them, Figure 11 (a) shows the numerical performance of the abnormal intrusion information storage of the model, which can reflect the detection and processing ability of the power grid host to intrusion parameters. The smaller the value, the stronger the detection and processing ability of the model to intrusion parameters. From the graph, the highest storage capacity of the CNN-LSTM model was 395 MB, and the lowest storage capacity was approximately 321 MB. The maximum storage capacity of the FL model was 348 MB, and the minimum storage capacity was approximately 304 MB. Compared to others, the FL-CNN-LSTM model had the lowest storage capacity, with the highest storage capacity of only 204 MB. Figure 11 (b) shows the training duration of the models. Among the three models, the CNN-LSTM model had the longest training duration, about 95.8 seconds, followed by

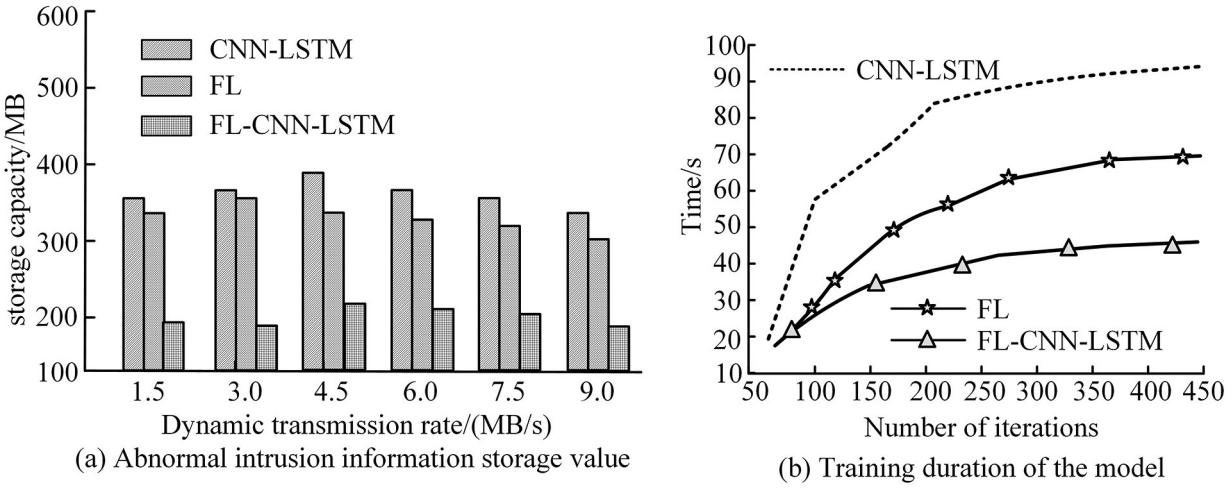


Figure 11. Storage values and training duration of abnormal intrusion information in the model.

Table 5. Cost situation of each model.

Model	Operation and maintenance costs		Other costs	
	Inspection fees	Maintenance cost	Electricity and network costs	Labor cost
CNN-LSTM	24,000 RMB	16,900 RMB	13,800 RMB	12,000 RMB
FL	16,600 RMB	9,800 RMB	9,250 RMB	8,900 RMB
FL-CNN-LSTM	9,900 RMB	7,600 RMB	6,900 RMB	6,300 RMB

the FL model with a training duration of about 68.5 seconds, and the FL-CNN-LSTM model had the shortest training duration, about 47.7 seconds. In addition, the experiment further examined the cost situation of three models in intrusion detection of smart grids, as represented in Table 5.

Table 5 shows the actual operating costs of three power grid intrusion detection models. From Table 5, the study divided expenses into two major categories, namely operation and maintenance costs and other costs. There were two sub-costs under the operation and maintenance cost, namely inspection cost and maintenance cost. From the table, the FL-CNN-LSTM model had the lowest inspection cost, at 9,900 yuan, which was 6,700 yuan lower than the FL model and 14,100 yuan lower than the CNN-LSTM model. The maintenance cost was also the lowest, at 7,600 yuan, which was 2,200 yuan lower than the FL model and 9,300 yuan lower than the CNN-LSTM model. Among other expenses, the FL-CNN-LSTM model only required 6,900 yuan for power and network costs, and 6,300 yuan for labor costs, which was much lower than the other two intrusion detection models. Overall, the FL-CNN-LSTM model could be effectively used for intrusion detection in smart grids.

4.3. Discussion

The FL-CNN-LSTM model proposed in the study demonstrated excellent performance in smart grid intrusion detection. On the basis of FL, by introducing CNN and LSTM, the model achieved efficient detection performance while handling imbalanced data. Compared with the FL model and traditional CNN-LSTM model, FL-CNN-LSTM significantly improved accuracy, precision, recall, and F1 value. Especially during the initial and final phases of iteration, the error rate of FL-CNN-LSTM model in detecting Dos and Probe attacks was much lower than other models, with a minimum of 0.7%, demonstrating its high efficiency in practical applications. In terms of performance optimization, the inference speed of the research model significantly improved while maintaining a high accuracy. In addition, the model proposed by the research achieved a communication efficiency of 93.9%, far higher than models in other studies. In cost-benefit analysis, the FL-CNN-LSTM model had the lowest total cost expenditure, which is in contrast with the research results of Song et al [24]. Namely, the CNN-based model proposed by Song *et al.*, although more accurate, was not as cost-effective as the FL-CNN-LSTM model. Compared with Durairaj *et al.*'s use of deep belief networks and rule-based detection techniques, the FL-CNN-LSTM model performed better in terms of false positive rate, with an accuracy of over 92% and a false positive rate of less than 1% [25]. This indicates that, although deep belief networks and rule-based detection techniques are effective in some respects, the FL-CNN-LSTM model exhibits superior overall capabilities. In summary, the FL-CNN-LSTM model not only provided a new perspective in theory but also demon-

strated excellent performance and cost-effectiveness in practical applications. The research provides an effective technical solution for the security protection of smart grids. Although this study has achieved certain results, there are also some limitations. Firstly, the performance of the model on small sample data has not been fully validated, which may affect its generalization ability in practical applications. Secondly, the model's ability to recognize abnormal behavior may be affected by data quality and feature selection, which requires further research to optimize. In addition, federated learning may encounter challenges in data privacy and security during actual deployment, which requires more work to ensure the security and reliability of the model. Future research can be conducted in the following directions: firstly, exploring more advanced feature extraction methods and model architectures to further improve the performance and generalization ability of the model. Secondly, research on how to improve the learning ability of models in distributed environments while maintaining communication efficiency. In addition, research on how to better protect data privacy and how to effectively handle non independent and identically distributed data in federated learning environments. In actual deployment, the FL-CNN-LSTM model may face some challenges. For example, how to ensure the stability and reliability of the model in different devices and network environments, as well as how to handle heterogeneity and communication delays between devices. In addition, how to balance the computational and communication costs of the model, and how to reduce the demand for computing resources while ensuring model performance, are also issues that need to be considered. The scalability analysis of the FL-CNN-LSTM model shows that it has good scalability potential. As the amount of data increases, the model can improve its processing power by adding more CNN and LSTM layers. Meanwhile, federated learning frameworks allow models to be trained without centralized data, providing convenience for handling large-scale distributed data. However, as the model size expands, it is also necessary to consider the computational complexity and storage requirements of the model, as well as how to optimize the resource utilization efficiency of the model while ensuring its performance. In summary, the FL-CNN-LSTM model proposed in this study performs well in power grid intrusion detection, but there is still room for improvement and optimization. Future research needs to further explore the limitations of the model, address challenges in practical deployment, and improve the scalability of the model to achieve wider applications.

5. Conclusion

In order to address the imbalanced data in the smart grid and improve detection performance, the study proposed to use the FL algorithm and improve it by introducing CNN and LSTM to capture spatial characteristics in the grid and process sequential data, respectively. The FL-CNN-LSTM smart grid intrusion detection model was constructed. The experiment outcomes indicated that the overall ability of the raised model was substantially improved, with an accuracy rate of 97.3%, an accuracy rate of 97.7%, a recall rate of 90.8%, and an F1 value of 91.1%. Compared with other models, it performed the best. Moreover, in comparison with the others, the loss rate of the proposed model had the lowest score and the highest communication efficiency. In the case analysis, the research model could effectively deal with both Dos and Probe attacks, with an intrusion detection error rate of only 0.7%. In addition, the abnormal intrusion information storage value and training time of the research model were the lowest, and the total operating cost in actual power grid intrusion detection was also the lowest. Overall, the proposed model can be effectively applied for intrusion detection in smart grids. However, although the model uses FL to ensure data security, with the development of technology, it is still not ruled out that attackers can infer the original data through some kind of reverse engineering. Therefore, in the future, further exploration of more sophisticated encryption methodologies and privacy safeguarding mechanisms should be conducted to guarantee the security of the model's updated information.

Declaration of Competing Interests

There is no conflict of interest in this paper.

Acknowledgment

This paper has no supporting funded projects.

Data availability

The data used in this study is proprietary and not suitable for sharing.

References

[1] H. Li *et al.*, "Optimizing Intelligent Edge Computing Resource Scheduling Based on Federated Learning", *Journal of Knowledge Learning and Science Technology*, vol. 3, no. 3, pp. 235–260, 2024. http://dx.doi.org/10.60087/jklst.vol3.n3.p.235-260

[2] M. S. Mastoi *et al.*, "Large-scale Wind Power Grid Integration Challenges and Their Solution: A Detailed Review", *Environmental Science and Pollution Research*, vol. 30, no. 47, pp. 103424–103462, 2023. http://dx.doi.org/10.1007/s11356-023-29653-9

[3] A. A. Mhmood *et al.*, "Detection of Cyber-attacks on Smart Grids Using Improved VGG19 Deep Neural Network Architecture and Aquila Optimizer Algorithm", *Signal, Image and Video Processing*, vol. 18, no. 2, pp. 1477–1491, 2024. http://dx.doi.org/10.1007/s11760-023-02813-7

[4] M. A. Alsoufi *et al.*, "Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks", *Computer Modeling in Engineering & Sciences*, vol. 141, no. 1, pp. 823–845, 2024. http://dx.doi.org/10.32604/cmes.2024.052112

[5] J. Huang *et al.*, "Improved Intrusion Detection Based on Hybrid Deep Learning Models and Federated Learning", *Sensors*, vol. 24, no. 12, p. 4002, 2024. http://dx.doi.org/10.3390/s24124002

[6] I. Priyadarshini, "Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning", *Big Data and Cognitive Computing*, vol. 8, no. 3, p. 21, 2024. http://dx.doi.org/10.3390/bdcc8030021

[7] M. Ye *et al.*, "Heterogeneous Federated Learning: State-of-the-art and Research Challenges" *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–44, 2023. http://dx.doi.org/10.1145/3625558

[8] K. He *et al.*, "Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey", *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 538–566, 2023. http://dx.doi.org/10.1109/COMST.2022.3233793

[9] J. Wen *et al.*, "A Survey on Federated Learning: Challenges and Applications", *International Journal of Machine Learning and Cybernetics*, vol. 14, no. 2, pp. 513–535, 2023. http://dx.doi.org/10.1007/s13042-022-01647-y

[10] A. Oroojlooyjadid *et al.*, "A Deep Q-network for the Beer Game: Deep Reinforcement Learning for Inventory Optimization", *Manufacturing & Service Operations Management*, vol. 24, no. 1, pp. 285–304. http://dx.doi.org/10.1287/msom.2020.0939

[11] J. Chen *et al.*, "When Federated Learning Meets Privacy-preserving Computation", *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–36, 2024.

[12] A. W. Salehi *et al.*, "A Study of CNN and Transfer Learning in Medical Imaging: Advantages, Challenges, Future Scope", *Sustainability*, vol. 15, no. 7, p. 5930, 2023. http://dx.doi.org/10.1145/3679013

[13] M. Khaleel *et al.*, "Artificial Intelligent Techniques for Identifying the Cause of Disturbances in the Power Grid", *Brilliance: Research of Artificial Intelligence*, vol. 3, no. 1, pp. 19–31. http://dx.doi.org/10.47709/brilliance.v3i1.2165

[14] Z. Alshingiti *et al.*, "A Deep Learning-based Phishing Detection System Using CNN, LSTM, and LSTM-CNN", *Electronics*, vol. 12, no. 1, p. 232. http://dx.doi.org/10.3390/electronics12010232

[15] F. Calero *et al.*, "A Review of Modeling and Applications of Energy Storage Systems in Power Grids", in *Proceedings of the IEEE*, vol. 111, no. 7, 2022, pp. 806–831.

[16] D. Javeed *et al.*, "An Intelligent Intrusion Detection System for Smart Consumer Electronics Network", *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 906–913, 2023.

[17] J. Xin *et al.*, "A Signal Recovery Method for Bridge Monitoring System Using TVFEMD and Encoder-decoder Aided LSTM", *Measurement*, vol. 214, http://dx.doi.org/10.1016/j.measurement.2023.112797

[18] A. Hechifa *et al.*, "Improved Intelligent Methods for Power Transformer Fault Diagnosis Based on Tree Ensemble Learning and Multiple Feature Vector Analysis", *Electrical Engineering*, vol. 106, no. 3, pp. 2575–2594. http://dx.doi.org/10.1007/s00202-023-02084-y

[19] Y. Chen *et al.*, "Traffic Signal Optimization Control Method Based on Adaptive Weighted Averaged Double Deep Q Network", *Applied Intelligence*, vol. 53, no. 15, pp. 18333–18354. http://dx.doi.org/10.1007/s10489-023-04469-9

[20] T. Wang *et al.*, "Fault Detection for Motor Drive Control System of Industrial Robots Using CNN-LSTM-based Observers", *CES Transactions on Electrical Machines and Systems*, vol. 7, no. 2, pp. 144–152. http://dx.doi.org/10.30941/CESTEMS.2023.00014

[21] G. Singh and N. Khare, "A Survey of Intrusion Detection from the Perspective of Intrusion Datasets and Machine Learning Techniques", *International Journal of Computers and Applications*, vol. 44, no. 7, pp. 659–669, 2022. http://dx.doi.org/10.1080/1206212X.2021.1885150

[22] N. K. Singh *et al.*, "Forecasting Intrusion in Critical Power Systems Infrastructure Using Advanced Autoregressive Moving Average (AARMA) Based Intrusion Detection for Efficacious Alert System", *Scientia Iranica*, vol. 31, no. 17, pp. 1490–1503, 2024. http://dx.doi.org/10.24200/sci.2023.58059.5550

[23] O. A. Wahab, "Intrusion Detection in the Iot Under Data and Concept Drifts: Online Deep Learning Approach", *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19706–19716, 2022.

[24] D. Song *et al.*, "Intrusion Detection Model Using Gene Expression Programming to Optimize Parameters of Convolutional Neural Network for Energy Internet", Applied Soft Computing, vol. 134, no. 1, pp. 109960–109961. http://dx.doi.org/10.1016/j.asoc.2022.109960

[25] D. Durairaj *et al.*, "Intrusion Detection and Mitigation of Attacks in Microgrid Using Enhanced Deep Belief Network", *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol. 46, no. 1, pp. 1519–1541. http://dx.doi.org/10.1080/15567036.2021.2023237

Received: December 2024
Revised: January 2025
Accepted: January 2025

Contact addresses:
Songyao Feng
Information Center of Guangxi Power Grid Co., Ltd
Nanning
China
e-mail: fsy199608@sina.com

Mingfei Zeng*
Information Center of Guangxi Power Grid Co., Ltd
Nanning
China
e-mail: zengmf0405@yeah.net
*Corresponding author

Zhengyan Huang
Information Center of Guangxi Power Grid Co., Ltd
Nanning
China
e-mail: hzy900529@163.com

Weigang Su
Information Center of Guangxi Power Grid Co., Ltd
Nanning
China
e-mail: swgang86@yeah.net

Songyao Feng received his BSc degree in information security from Sichuan University in 2019. He is currently an engineer at the Information Center of Guangxi Power Grid Co., Ltd, Nanning, China. His research interest is network security.

Mingfei Zeng received his PhD in communication and information systems from Sun Yat-sen University in 2013. He is currently a senior engineer at the Information Center of Guangxi Power Grid Co., Ltd, Nanning, China. His research interest is network security.

Zhengyan Huang received her MSc degree in computer technology from the Communication University of China in 2018. She is currently an engineer at the Information Center of Guangxi Power Grid Co., Ltd, Nanning, China. Her research interest is network security.

Weigang Su received his MSc degree in electrical engineering from Guangxi University in 2018. He is currently an engineer at the Information Center of Guangxi Power Grid Co., Ltd, Nanning, China. His research interest is communication engineering.