Article

Smart Grid Theft Detection Based on Hybrid Multi-Time Scale Neural Network

Yuefei Sun, Xianbo Sun *, Tao Hu and Li Zhu

School of Intelligent Science and Engineering, Hubei Minzu University, Enshi 455000, China; 202030074@hbmzu.edu.cn (Y.S.)
* Correspondence: sunxianbo@whut.edu.cn

Abstract: Despite the widespread use of artificial intelligence-based methods in detecting electricity theft by smart grid customers, current methods suffer from two main flaws: a limited amount of data on electricity theft customers compared to that on normal customers and an imbalanced dataset that can significantly affect the accuracy of the detection method. Additionally, most existing methods for detecting electricity theft rely solely on one-dimensional electricity consumption data, which fails to capture the periodicity of consumption and overlooks the temporal correlation of customers’ electricity consumption based on their weekly, monthly, or other time scales. To address the mentioned issues, this paper proposes a novel approach that first employed a time series generative adversarial network to balance the dataset by generating synthetic data for electricity theft customers. Then, a hybrid multi-time-scale neural network-based model was utilized to extract customers’ features and a CatBoost classifier was applied to achieve classification. Experiments were conducted on a real-world smart meter dataset obtained from the State Grid Corporation of China. The results demonstrated that the proposed method could detect electricity theft by customers with a precision rate of 96.64%, a recall rate of 96.87%, and a significantly reduced false detection rate of 3.77%.

Keywords: smart grid; electricity theft detection; time GAN; deep learning; imbalance data

1. Introduction

Smart grids incur losses from both technical and non-technical sources in electricity distribution and transmission. The former stems from power dissipation in transmission and distribution lines, transformers, and other electrical equipment, which are inherent aspects of power systems. The latter, however, is primarily caused by electricity theft perpetrated by malicious customers [1]. Electricity theft results not only in significant financial losses for grid companies, but also in increased electricity demand, overloading, and other security concerns. Moreover, it poses a serious threat to public safety, including the risk of fires and electric shocks to customers [2]. As such, this study carries significant economic value and plays a critical role in addressing public safety issues.

In the past, the main means of checking electricity theft was by power grid inspectors checking the site and manually analyzing the electricity consumption records. However, this method was time-consuming and caused a great deal of wasted labor and material resources. Recently, the speedy growth of IoT technology and artificial intelligence has enabled the development of anti-theft technologies that can be divided into the following two types: hardware-based and data-driven [3]. Hardware-based methods rely primarily on the placement of sensors in relevant areas, which mainly change the design and architecture of smart meters, to better prevent illegal persons from stealing electricity; however, the high operating and maintenance costs of dedicated hardware have limited further development in this area [4–6]. The growing availability of smart meters provides a massive volume of high-precision, multi-dimensional, and fine-grained electricity consumption data, which provides us with the possibility of carrying out data-driven identification of electricity theft.
by electricity consumers [7]. Data-driven approaches are further classified into system state-based [8–10], game theory-based [11,12] and artificial intelligence-based methods, using models such as support vector machine (SVM), artificial neural network (ANN), convolutional neural network (CNN), and recurrent neural network (RNN).

SVM is a classical model frequently used in the detection of electricity theft. In the literature [13], the synthetic minority oversampling technique (SMOTE) was first used to balance the dataset, then the kernel function integrated with principal component analysis (KPCA) was used to extract features, and finally, SVM classification was used, which was tested to obtain an accuracy of 85% and an area under the ROC curve (ROC-AUC) of 0.89. In the literature [14], the raw data were first input into a decision tree (DT) to calculate the expected electricity consumption of users at a specific time, and then they were input to the SVM classifier along with other features, and the accuracy rate obtained after testing was 92.5% and the false alarm rate was 5.12%.

ANN is also used to detect electricity theft. In the literature [15], the time domain, frequency domain, and combinatorial domain features of electricity consumption data were obtained and used as input to a deep neural network (DNN) for categorization, and principal component analysis (PCA) with diminished subspace and a minimum redundancy maximum relevance (mRMR) scheme was performed to identify significant features, with an ROC-AUC of 0.92 obtained. In the literature [16], a hybrid deep neural network composed of an LSTM network and multilayer perceptron (MLP) was proposed to detect anomalous features in smart meters, and the tested ROC-AUC was 0.84. In the literature [17], a hybrid data resampler was proposed for dataset balancing using a simulated annealing algorithm, regularization method, and jump connection for optimizing ANN to improve the training and classification capability of the model, and the accuracy obtained after testing was 99.6%.

CNN is widely used in detecting electricity theft as deep learning advances. In the literature [18], a wide & deep convolutional neural network (wide & deep CNN) was proposed to study electricity theft in a smart grid, and the test results obtained an ROC-AUC of 0.7922. In the literature [19], a combination of graph convolutional network (GCN) and euclidean convolutional neural network (euclidean CNN) was tested and an ROC-AUC of 0.787 was obtained. In the literature [20], the SMOTE technique was first used to generate new data, and then a model combining CNN and LSTM architectures was used for feature extraction and classification, and the test results yielded an accuracy of 92% and ROC-AUC equal to 0.89. In the literature [21], an ADASYN algorithm for processing unbalanced datasets was proposed, after which the balanced data were transmitted to the VGG-16 module for feature extraction, and at last, the extracted features were delivered to the firefly algorithm-based extreme gradient boosting (FA-XGBoost) module for classification, and the test results obtained an accuracy of 93%.

RNN is specifically designed for processing time series data, and because electricity consumption of electricity consumers varies over time, it is widely used for detecting electricity theft. In the literature [22], a deep RNN-based electricity theft technique was proposed using a gated recurrent unit (GRU) in the hidden layer, which could better learn the input time series energy consumption information, and the test results obtained an accuracy of 94.2% and false detection rate of 4.2%. In the literature [23], six types of electricity theft were first used to synthesize data to balance the dataset, then LSTM was used to extract the features, and finally GRU with dropout regularization and an added Adam optimizer was used for classification, and the test result obtained an ROC-AUC of 0.9168. In the literature [24], the SMOTE technique was combined with the under sampling technique Tomek Link, followed by feature extraction using KPCA and a bi-directional gated recurrent unit (Bi-GRU) for classification, and the test results yielded an accuracy rate of 80%. In the literature [25], the decomposition of electricity sequences into trend, seasonal, and residual information was input to the Bi-GRU model with the addition of multi-headed attention, which effectively converted the global and fine-grained features of the electricity consumption records, and the test results yielded an ROC-AUC of 0.965.
However, existing AI-based electricity theft detection models do not take the following factors into account. The first issue is data imbalance. In a real smart grid, normal electricity consumption data are relatively easy to obtain, but data from electricity theft consumers are rarely collected. Therefore, when training with classification algorithms to diagnose electricity theft, the framework features of a few classes are easily under-extracted, which negatively affects prediction results. Second, most current electricity theft detection approaches are based on one-dimensional electricity consumption data, which does not sufficiently take into account the time series properties of customers’ electricity consumption data to obtain the regularity of electricity consumption nor the time correlations of consumers’ electricity consumption based on time periods such as weeks and months, resulting in low accuracy and high false detection rates.

This paper proposes a new electricity theft detection method to solve the above problems. In the proposed method, a time series generative adversarial network (Time GAN) was used to balance the dataset by synthesizing data from a small number of electricity theft customers. Additionally, a hybrid multi-time scale neural network was designed for the extraction of features. At the daily time scale, bidirectional long short-term memory (Bi-LSTM) was used to iterate in reverse and extract the global features of customers by using the forward and backward information of the learning consumer sequences. At the weekly time scale, a residual network (ResNet) was used to solve the gradient disappearance problem in deep extraction of customer electricity data. Additionally, at the monthly time scale, the Alex network (AlexNet) was used to obtain the seasonal variation of the underlying monthly electricity consumption law of the electricity consumption data and enhance the learning effect. Finally, the proposed method deployed the CatBoost (categorical features gradient boosting) classifier in the model for final classification.

The main research contributions of this paper can be summarized as follows:

- To address the problem of imbalanced datasets in current AI-based power theft detection methods, this study proposes the use of a time generative adversarial network (Time GAN) to synthesize datasets, thus effectively solving the issue of insufficient power theft user data. The validity of this method is demonstrated through experiments.
- To address the issue of existing power theft detection methods only processing power consumption data in a singular manner, which does not fully consider the time series nature of consumption data, a hybrid multi-time scale neural network was designed to extract features, utilizing Bidirectional Long Short-Term Memory (Bi-LSTM), Residual Network (ResNet), and AlexNet to extract features at different time scales, thus improving detection accuracy and reducing the false positive rate.
- Using CatBoost for classification, the experimental results showed that this method could detect power theft with 96.64% accuracy and 96.87% recall rate while significantly reducing the false positive rate. This is a significant achievement of this study.

Therefore, the main contribution of this study is the proposal of a comprehensive power theft detection method that uses Time GAN for data synthesis, multi-time scale neural networks for feature extraction, and CatBoost for classification. The validity of this method is demonstrated through experiments.

2. Analysis of the Characteristics of Customers

To better identify electricity theft behavior, it is necessary to analyze the differences in annual, weekly, and daily electricity consumption characteristics between regular and electricity theft customers in order to provide a data foundation for the construction of electricity theft detection models. After analyzing the electricity consumption data of customers, the authors found significant differences in the annual, weekly, and daily electricity consumption characteristics between regular and electricity theft customers, which provided important information for subsequent models to accurately identify electricity theft behavior.
2.1. Characteristics of Customers

First, we arbitrarily selected one normal electricity consumer and one electricity theft consumer and drew their electricity consumption bar graphs for the whole year from 1 January 2015 to 31 December 2015, as shown in Figure 1. In this figure, we can see that both normal and electricity theft consumers had obvious seasonal characteristics during the year. As shown in Figure 1a, January to May was the low period of electricity consumption and June to October was the peak period of electricity consumption. In Figure 1b, there was a small peak in February, a peak in August, and troughs from March to May and from September to December. Customers’ electricity consumption was mainly affected by seasonal factors, such as hot weather in the summer when customers used air conditioners or other cooling measures, which resulted in a surge in electricity consumption. Electricity consumption was also affected by personal, work, rest, and economic conditions, resulting in differences in customers’ electricity consumption. Thus, it would be very difficult to judge whether customers were thieving electricity only from their daily electricity consumption for a year.

![Bar chart of yearly electricity consumption of normal customers and electricity theft customers. (a) Normal customer; (b) Electricity theft customer.](image)

Further, the annual electricity consumption of a normal customer and an electricity thief was plotted month by month, as mentioned above. Figure 2a shows the 12-month daily electricity load curve of a normal customer, while Figure 2b shows the 12-month daily electricity load curve of an electricity thief. It can be observed that in the monthly load curve of the normal customer, the electricity consumption curve of most months was relatively flat. However, in the monthly load curve of the electricity theft customer, the electricity load curve often fluctuated greatly during the peak period of electricity consumption, from May to October, which raised suspicion.

August, the peak month of electricity consumption, was chosen for the study, and daily electricity consumption load curves were plotted for normal and electricity theft customers to better observe their daily characteristics. As shown in Figure 3a, the daily electricity consumption curves in August for a normal customer, and Figure 3b, the daily electricity consumption curve in August for an electricity theft customer, it can be clearly observed from the graphs that the daily electricity consumption load of the normal customer in August was very flat most of the time, whereas the electricity consumption load of the electricity theft customer in August fluctuated drastically.
August, the peak month of electricity consumption, was chosen for the study, and daily electricity consumption load curves were plotted for normal and electricity theft customers to better observe their daily characteristics. As shown in Figure 3a, the daily electricity consumption curve in August for a normal customer, and Figure 3b, the daily electricity consumption curve in August for an electricity theft customer, it can be clearly observed from the graphs that the daily electricity consumption load of the normal customer in August was very flat most of the time, whereas the electricity consumption load of the electricity theft customer in August fluctuated drastically.

2.2. Correlation Analysis of Customer’s Characteristics

To analyze the robust correlation of electricity load more effectively amongst legitimate customers versus the feeble correlation amongst electricity theft customers, the study conducted a correlation analysis on electricity consumption data using the Pearson’s correlation coefficient (PCC). Figure 4 presents the correlation coefficient matrix heat map of the electricity consumption load data for a normal customer over 12 months in 2015, while Figure 5 displays the correlation coefficient matrix heat map of the electricity consumption load data for an electricity theft customer over the same period. Upon examination of the figures, it was evident that the majority of the PCC values for the normal customer exceeded 0.7, indicating a strong month-to-month correlation in their electricity consumption data.
Conversely, the PCC values for the electricity theft user were predominantly less than 0.3 or even negative, signifying very little correlation amongst their electricity consumption data.

Similarly, a correlation analysis was performed on electricity consumption data from both a regular customer and one engaged in electricity theft over a four-week period in August, utilizing the Pearson’s correlation coefficient (PCC). As depicted in Figure 6, the correlation coefficient matrix heat map for the electricity consumption load data of a regular customer over four weeks was examined, while Figure 7 displays the correlation coefficient matrix heat map for the electricity consumption load data of an electricity theft customer.
matrix heat map for the electricity consumption load data of an electricity theft customer over the same period. These maps revealed that there were distinct differences in the electricity consumption patterns between the two groups. The results showed that most of the PCC values of a normal customer were greater than 0.8, indicating that their electricity consumption data were highly correlated between different weeks. In contrast, most of the PCC values of an electricity theft customer were less than 0.3, indicating that their electricity consumption data had very low correlation with each other.

![Heat map of correlation coefficient matrix of weekly load data for a normal customer.](image)

**Figure 6.** Heat map of correlation coefficient matrix of weekly load data for a normal customer.

![Heat map of correlation coefficient matrix of weekly load data for an electricity theft customer.](image)

**Figure 7.** Heat map of correlation coefficient matrix of weekly load data for an electricity theft customer.

In summary, the statistical and correlation analyses conducted on the electricity consumption data of regular and electricity theft customers indicated that the consumption data of an electricity theft customer generally exhibited lower correlation than that of a regular customer. This observation was consistent with the findings of a previously published study [26], and similar trends were observed in other electricity consumption datasets from...
different regions and countries. Consequently, such data provided a more dependable foundation for the development of electricity theft detection models. Further examination of the data could reveal significant insight into electricity consumption patterns and inform the construction of more effective detection models.

3. Proposed Method

This section includes the following: the introduction of the dataset used in this paper, data pre-processing methods, data generation using Time GAN, feature extraction using the proposed model of a hybrid multi-time scale neural network, and classification using CatBoost classifier, as shown in Figure 8.

![Main content framework of this paper.](image)

**Figure 8.** Main content framework of this paper.

### 3.1. Introduction to the Dataset

This paper used a dataset that was publicly available online from the SGCC, which counted 1036 days of electricity consumption for a total of 42,372 customers during the period from 1 January 2014 to 31 October 2016, as shown in Table 1.

<table>
<thead>
<tr>
<th>SGCC Dataset</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Customers</td>
<td>38,757</td>
<td>91.5%</td>
</tr>
<tr>
<td>Electricity Theft Customers</td>
<td>3615</td>
<td>8.5%</td>
</tr>
<tr>
<td>Total Customers</td>
<td>42,372</td>
<td>100%</td>
</tr>
</tbody>
</table>

From Table 1, it can be observed that the percentage of normal customers was 91.5%, while electricity theft customers accounted for 8.5%. The difference between the proportion of electricity theft and normal customers was excessively large, which was also in line with common sense in real life. In deep learning, models trained using normal and abnormal samples with a large difference in the amount of data are less accurate for classifying data from abnormal samples. To solve this problem, this paper used Time GAN to generate new electricity theft samples from existing electricity theft data, so that the electricity theft sample data and the normal sample data could reach a relatively balanced state in order to better train the model.

### 3.2. Dataset Pre-Processing

The process of collecting data from smart meters may be affected by equipment collection errors, special events, and other complex factors, thus mixing the electricity consumption data with a large amount of noise and other irrelevant factors. Additionally, the neural network model is susceptible to changes in the data, so it is necessary to carry out appropriate pre-processing of the data [27]. The fundamental measures of pre-processing include missing value, abnormal value, and normalization processing.

#### 3.2.1. Missing Value Processing

Given the problems of hardware failures and corrupted data transmission in smart meters, which result in missing data sampled at certain moments, missing value processing is required in the data processing process. In order to recover missing data, this paper...
used the nearest neighbor interpolation method, as shown in Equation (1), which estimates missing values based on the known data around the missing values and interpolates them by finding the nearest data point in the time series. This method is simple, effective, and can recover missing data well, thus maintaining the continuity of the time series.

\[
F(x_i) = \begin{cases} \frac{x_{i-1} + x_{i+1}}{2} & x_{i-1} \cap x_{i+1} \notin \text{NaN} \\ 0 & x_{i-1} \cup x_{i+1} \in \text{NaN} \end{cases}
\]  

where \( x_i \) represents the value in the electricity consumption data of a certain day and NaN is the vacancy value.

3.2.2. Abnormal Value Processing

Abnormal value handling is an important part of data pre-processing that reduces or eliminates errors and biases caused by the inclusion of outliers in the data. Outliers are usually discrete points that appear in the dataset that do not conform to the normal distribution or trend. In the data analysis and modeling process, outliers often have a negative impact on the results and therefore need to be handled accordingly. Common outlier processing methods include deletion, replacement, and interpolation techniques, among which deletion is the simplest and most direct method, although useful information may be lost. Replacement can retain data samples, but a suitable replacement strategy needs to be selected according to the specific situation. Interpolation estimates missing or abnormal values based on existing data points. In practical applications, it is necessary to consider what kind of abnormal value processing method is used in combination with various factors such as data distribution and feature analysis to ensure the accuracy and reliability of the data. In this paper, the abnormal values were processed according to Equation (2).

\[
F(x_i) = \begin{cases} \text{avg}(X) + 2 \cdot \text{std}(X) & x_i > \text{avg}(X) + 2 \cdot \text{std}(X) \\ x_i & \text{otherwise} \end{cases}
\]  

where \( X \) is the vector composed of \( x_i \), \( \text{avg}(X) \) is the mean of \( X \), and \( \text{std}(X) \) is the standard deviation of \( X \).

3.2.3. Normalization Processing

Normalization is a very important pre-processing step in deep learning models. Since different evaluation metrics have different units and ranges, the range of values of the data may also vary greatly. If normalization is not undertaken, the analysis results of the data may be biased. In addition, the neural network algorithm has very strict requirements on the range of input data. If the range of data is too large, convergence of the algorithm may be poor or fail, thus making the model fail to achieve the expected effect. Therefore, normalization can make the data have a fixed range of values, generally in the range of \([0,1]\), which can be convenient for subsequent deep learning model training. This paper used Equation (3) for normalization.

\[
F(x_i) = \frac{x_i - \text{Min}(X)}{\text{Max}(X) - \text{Min}(X)}
\]  

where \( \text{Min}(X) \) is the minimum value in \( X \) and \( \text{Max}(X) \) is the maximum value in \( X \).

3.3. Time GAN Generation of Data

From the analysis in Section 3.1, it was evident that the ratio of normal electricity consumers to electricity theft consumers in the SGCC dataset was close to 10:1. Thus, the model constructed from such a dataset may be biased toward normal electricity customers, which may easily result in a lower accuracy rate of electricity theft customers [28]. Methods commonly used to solve such problems include random under sampling (RUS) and random
over sampling (ROS) to reduce the quantitative differences between the two types of data [29]. The RUS technique randomly discards majority class data by random under sampling, which reduces the dimensionality of the dataset, but the random removal of data may discard potentially important information. The ROS technique increases the dataset size by replicating a few classes of data, and although this method does not discard any information, the developed model can suffer from overfitting problems because it is a simplistic replication of the data. In this paper, data were generated using the Time GAN algorithm, which is a generative adversarial network that can generate new samples from existing electricity theft data, thus expanding the scale of electricity theft data and making the ratio of electricity theft data and normal data relatively balanced. By increasing the samples of electricity theft data, it can improve the detection ability of the model for electricity theft users and improve the classification accuracy of the model. At the same time, the new samples generated by Time GAN also have high realism and can be used for training and testing of the model. This paper evaluated the effectiveness of Time GAN in addressing the data imbalance issue. To this end, different methods were compared in a series of experiments to determine the performance of the models. The results demonstrated the efficacy of Time GAN in solving the data imbalance problem.

3.3. Fundamentals of Time GAN

In December 2019, Yoon et al. introduced a novel Time GAN framework that captured not only the allocation of characteristics for each moment in a time series of a variable [30], but also the potentially complicated interplay of the variables over time. Time GAN is made up of four network components: the embedding network, the recovery network, the generator network, and the discriminator network. The embedding and recovery networks are members of the automatic encoding component, while the sequence generator and discriminator are members of the adversarial component. The adversarial and automatic encoding components are jointly trained so that Time GAN can learn encoding features, generate representations, and perform cross-time iterations all at the same time. Figure 9 depicts the Time GAN training structure framework.

![Figure 9. Training structure framework of Time GAN.](image)

In the figure, $\theta_e$, $\theta_r$, $\theta_g$, and $\theta_d$ denote the parameters of the embedding, recovery, generator, and discriminator networks, respectively. $L_R$ denotes the reconstruction loss function of the output results of the embedding and recovery networks, $L_U$ denotes the
unsupervised loss function of the output results of the generator and discriminator, and $L_S$ denotes the supervised loss of the output results of the embedding and generator networks.

$\theta_e$ and $\theta_r$ are trained based on the reconstructed loss function and supervised loss, as shown in Equation (4).

$$\min_{\theta_e, \theta_r}(\lambda L_S + L_R) \quad (4)$$

where $\lambda$ is the hyperparameter that balances the two loss functions of $L_R$ and $L_S$, and the embedding process is enabled by $L_S$ not only to lower the dimensionality of the adversarial learning space but to allow the generator network to learn time series features from real data.

In the next step, the generator and discriminator networks are trained adversarially, as shown in Equation (5).

$$\min_{\theta_g}(\eta L_S + \max_{\theta_d} L_U) \quad (5)$$

where $\eta$ is the hyperparameter that balances the two losses of $L_U$ and $L_S$, and the above equation minimizes the supervised loss of the generator in addition to the unsupervised game in classification accuracy. In summary, it is through this combined training approach that Time GAN achieves encoding, generation, and iteration.

3.3.2. Generated Data Evaluation

To ensure the synthetic samples accurately reflect the original data distribution, the effectiveness of the Time GAN model’s data generation method was compared against traditional methods (ROS and RUS) and improved methods (SMOTE and ADASYN). To visually assess the degree of similarity between the generated and real data, we utilized PCA and t-SNE to map the two datasets onto two dimensions. This approach provided a qualitative evaluation of the quality of the generated samples relative to the real data distribution.

The visualization results of data samples generated on the 2D plane using four different methods, namely ROS, RUS, SMOTE, and ADASYN, as well as the Time GAN method, are shown in Figures 10–14. In these figures, blue dots represent real samples, while red dots represent synthetic samples. From the visualization, it was apparent that our Time GAN model method generated synthetic samples that closely aligned with the distribution of the original data, indicating high diversity and fidelity. There were some extremely special points where the generated samples deviated from the real ones, but these were few and far between.

![Figure 10](image_url)

**Figure 10.** The ROS method utilizes PCA and t-SNE in the two-dimensional plane to visualize the results. (a) PCA; (b) t-SNE.
Figure 10. The ROS method utilizes PCA and t-SNE in the two-dimensional plane to visualize the results. (a) PCA; (b) t-SNE.

Figure 11. The RUS method utilizes PCA and t-SNE in the two-dimensional plane to visualize the results. (a) PCA; (b) t-SNE.

Figure 12. The SMOTE method utilizes PCA and t-SNE in the two-dimensional plane to visualize the results. (a) PCA; (b) t-SNE.

Figure 13. The ADASYN method utilizes PCA and t-SNE in the two-dimensional plane to visualize the results. (a) PCA; (b) t-SNE.

3.4. Feature Extraction
In this section, the hybrid multi-time scale neural network model that was used in this study to extract the characteristics of electricity consumption data is thoroughly described. The model's framework is depicted in Figure 15.
3.4. Feature Extraction

In this section, the hybrid multi-time scale neural network model that was used in this study to extract the characteristics of electricity consumption data is thoroughly described. The model’s framework is depicted in Figure 15.

LSTM, as a variant structure of RNN, can capture the hidden features inside the time series when processing electricity consumption data with temporal properties, and it can overcome the gradient disappearance problem of RNN [31]. For electricity consumption data with day as the time scale, inspired by previous research in the literature [18], Bi-LSTM was used to extract the global features of consumers’ electricity consumption. Bi-LSTM is

![Figure 15. Model structure framework of hybrid multi-time scale neural network.](image-url)
iterated in opposite directions to boost the whole learning of the sequence using forward and backward information, respectively. In this model, the input size was 1035, the hidden size was 128, and the number of layers was 2.

Second, for electricity consumption data with week as the time scale, ResNet was used to extract the users’ electricity consumption features. ResNet preserves the completeness of the input information by bypassing it directly to the output, where the whole network only requires learning the input, the part of the output difference, thus simplifying the learning objective and difficulty [32]. In this model, the input size was $7 \times 148$, the number of layers was 3, the numbers of filters were 16, 8, and 4, respectively, the kernel size was 3, the move step stride was 1, and the activation was ‘relu’.

Finally, for the electricity consumption data with month as the time scale, AlexNet was employed to extract the electricity consumption features of consumers. AlexNet has been widely used in the field of image recognition, and with increasing computational power, AlexNet has also gradually been used to extract time series data for feature extraction [33]. AlexNet has an 8-layer structure; the front 5 layers are convolutional layers, and the last 3 layers are fully connected layers. In this model, the input size was $30 \times 34$, the numbers of filters were 8, 16, 32, 32, and 16, respectively, the kernel size was 3, the move step stride was 1, and the activation was ‘relu’.

After several rounds of training, the size of each batch of data was finally selected as a batch size of 20, the learning rate was 1, and the loss function was binary cross-entropy.

### 3.5. Classifier

This section focuses on the CatBoost classifier, an open-source machine learning library developed by the Russian search giant Yandex in 2017. CatBoost is specifically designed to effectively handle categorical features in decision tree-based based learners. To address issues such as gradient bias and prediction shift, which can lead to overfitting and reduce the accuracy and generalizability of the algorithm, CatBoost implements a symmetric boosting approach [34]. Previous research has shown that hybrid multi-time scale neural network models can be effective in feature extraction for electricity consumption data [35]. Therefore, the study used a hybrid neural network model in combination with CatBoost to extract high-level features from the data. Our implementation set the maximum number of tree iterations to 100, the learning rate to 0.005, and the tree depth to 2. Other parameters were set to their default values.

### 4. Experimental Analyses

To support the proposed hybrid multi-time scale neural network-based model for electricity theft detection, the experiments were implemented on a real dataset from the SGCC. The experimental conditions in this paper included: CPU was Intel Core i7-11700K 3.6 GHz, GPU was NVIDIA GeForce RTX 3090 (24 GB), memory was 32 GB, the deep learning framework was TensorFlow 2.4, and Python 3.7 was used for model implementation.

#### 4.1. Evaluation Metrics

Due to the imbalance between the normal and theft customer numbers, accuracy was not a well-evaluated metric to assess the goodness of a model [36]. Therefore, the study only used precision, recall, false positive rate (FPR), area under the precision–recall curve (PR-AUC), and area under the ROC curve (ROC-AUC) to evaluate our model.

1. **Precision**: the proportion of those who are correctly identified as electricity thieves to all electricity thieves, which can be calculated by Formula (6).

   $$\text{Precision} = \frac{TP}{TP + FP}$$

2. **Recall**, also the positive detection rate (true positive rate, TPR): the proportion of those who are correctly identified as electricity thieves to the proportion of those detected as electricity thieves, which can be calculated by the Formula (7).
Recall = \frac{TP}{TP + FN} \quad (7)

3. False Positive Rate (FPR): the proportion of those who are incorrectly identified as electricity thieves to those who are detected as normal customers, which can be calculated by Formula (8).

Recall = \frac{TP}{TP + FN} \quad (8)

In the above three equations: TP denotes those who are correctly classified as electricity theft customers; TN denotes those who are correctly classified as normal customers; FP denotes those who are incorrectly classified as electricity theft customers; and FN denotes those who are incorrectly classified as normal customers.

4. PR-AUC: The corresponding precision and recall are calculated by selecting thresholds in the range of [0,1], and all points are connected to form the area surrounded by the PR curve and the coordinate axis.

5. ROC-AUC: The corresponding positive and false detection rates are calculated by selecting thresholds in the range of [0,1], and all points are connected to form the area surrounded by the ROC curve and the coordinate axis.

4.2. Performance Comparison before and after Dataset Enhancement

To test the effectiveness of the method proposed in this paper to balance the dataset using Time GAN-generated data, we selected commonly used methods such as ROS, RUS, SMOTE, and ADASYN, as well as the pre-processed raw data for comparison. Additionally, to predict the presence of electricity theft by electricity consumers, a hybrid multi-time scale neural network model was trained with the same parameters. At the end of the experiment, we plotted PR and ROC curves based on the experimental results, as shown in Figure 16, to evaluate the performance of the model. This helped us to determine whether the Time GAN method significantly improved the balance of the dataset and thus improved the prediction accuracy of the model. The experiment followed the following steps.

1. Collect and pre-process the data of electricity consumers, including the original data and the data processed by ROS, RUS, SMOTE, ADASYN, and Time GAN.
2. Design hybrid multi-time scale neural network models and train each dataset using the same parameters.
3. Evaluate the performance of each model separately and plot PR and ROC curves to determine whether the Time GAN approach could improve the balance of the dataset.

(a)

Figure 16. Cont.
1. Collect and pre-process the data of electricity consumers, including the original data with a PR-AUC value of 0.9469 and ROC-AUC value of 0.9684, because it not only used the raw data to gradually supervise the loss, but also let the model capture the distribution in the time series data.

2. Design hybrid multi-time scale neural network models and train each dataset using the same parameters.

3. Evaluate the performance of each model separately and plot PR and ROC curves to determine whether the Time GAN approach could improve the balance of the dataset.

Table 2 displays the detailed results.

With this experimental design, we could more accurately evaluate the effectiveness of the Time GAN method and determine whether it was a viable data-balancing method.

In Figure 16, it was observed that the PR-AUC value of the raw data was only 0.5338 and the ROC-AUC value was only 0.5795, indicating inadequate performance in distinguishing normal and electricity theft customers. The RUS and ROS techniques improved the impact of data imbalance to some extent, but the test results were still relatively poor. The SMOTE technique achieved a PR-AUC value of 0.7915 and ROC-AUC value of 0.8527, but it could not overcome the problem of easy distribution marginalization, resulting in poorer results. ADASYN, with a PR-AUC value of 0.7832 and ROC-AUC value of 0.9358, achieved further improvements but was susceptible to outlier effects, which affected the balance of the sample. In addition, Time GAN achieved a great improvement, with a PR-AUC value of 0.9469 and ROC-AUC value of 0.9684, because it not only used the raw data to gradually supervise the loss, but also let the model capture the distribution in the time series data. Table 2 displays the detailed results.

Table 2. Comparison of data balancing performance.

<table>
<thead>
<tr>
<th>Models</th>
<th>Precision</th>
<th>Recall</th>
<th>FPR</th>
<th>PR-AUC</th>
<th>ROC-AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw data</td>
<td>57.11%</td>
<td>43.12%</td>
<td>42.36%</td>
<td>0.5338</td>
<td>0.5795</td>
</tr>
<tr>
<td>RUS</td>
<td>71.47%</td>
<td>71.39%</td>
<td>35.29%</td>
<td>0.6439</td>
<td>0.7058</td>
</tr>
<tr>
<td>ROS</td>
<td>82.07%</td>
<td>81.72%</td>
<td>24.46%</td>
<td>0.7490</td>
<td>0.8156</td>
</tr>
<tr>
<td>SMOTE</td>
<td>86.21%</td>
<td>85.34%</td>
<td>18.26%</td>
<td>0.7915</td>
<td>0.8527</td>
</tr>
<tr>
<td>ADASYN</td>
<td>93.47%</td>
<td>92.08%</td>
<td>9.37%</td>
<td>0.7832</td>
<td>0.9358</td>
</tr>
<tr>
<td>Time GAN</td>
<td>96.64%</td>
<td>96.87%</td>
<td>3.77%</td>
<td>0.9469</td>
<td>0.9684</td>
</tr>
</tbody>
</table>
From Table 2, it was observed that the method of generating electricity theft customer data to balance the dataset by Time GAN improved our test results by 39.53% over the original data in precision, 53.75% in recall, 38.59% in FPR reduction, 0.4131 in PR-AUC, and 0.3889 in ROC-AUC, which greatly improved the detection accuracy and reduced the false detection rate. These results qualitatively illustrated the effectiveness of the Time GAN-generated data utilized in this study and confirmed the proposed model's ability to accurately detect electricity theft customers.

4.3. Performance Comparison with Other Models

To validate the effectiveness of the proposed model, experiments were conducted and compared with six other models, including SVM, RF, DT, Wide & Deep CNN [18], LSTM & MLP [16], SOSTLink & Bi-GRU [24], Bi-RNN [36], CNN & LSTM [20], and LSTM & GRU [23] models. To comprehensively evaluate the performance of the models, the study utilized both PR and ROC curves as evaluation metrics. By using the same dataset and evaluation methods across all experiments, the PR and ROC curves were generated based on the probability values generated by each model. The resulting curves are illustrated in Figure 17 and serve as valuable tools for assessing the effectiveness of the models.

![Figure 17. PR and ROC curves compared with other models. (a) PR curves; (b) ROC curves.](image-url)
In Figure 17, it was evident from the PR-AUC of only 0.3743 and ROC-AUC value of only 0.6144, that the SVM model could not classify well when the sample of electricity consumption data in this paper was too large. The PR-AUC value of 0.4703 and ROC-AUC value of 0.7053 for the RF model indicated a poor result for processing our 1D electricity consumption data. The PR-AUC value was 0.5824 and ROC-AUC value was 0.7444 for the DT model, which did not consider the temporal characteristics of electricity consumption data well, resulting in poor results. The PR-AUC value was 0.5724 and the ROC-AUC value was 0.8123 for the Wide & Deep CNN model, which did not extract user periodicity features well and had relatively singular features, which limited the performance improvement. The PR-AUC value was 0.6719 and the ROC-AUC value was 0.8123 for the LSTM & MLP model, indicating that the network structure was too simple and did not extract the deep features of customers’ electricity consumption data well. The PR-AUC value was 0.7795 and the ROC-AUC value was 0.9332 for the SOSTLink & BiGRU model, which did not extract user periodicity features well and had relatively singular features, which limited the performance improvement. The PR-AUC value of Bi-RNN was 0.7799 and the ROC-AUC value was 0.8488. The PR-AUC value of CNN & LSTM was 0.8146 and the ROC-AUC value was 0.8733. The PR-AUC value of LSTM & GRU was 0.6656 and the ROC-AUC value was 0.7328. Table 3 displays the detailed results.

Table 3. Comparison of the performances of the proposed models.

<table>
<thead>
<tr>
<th>Models</th>
<th>Precision</th>
<th>Recall</th>
<th>FPR</th>
<th>PR-AUC</th>
<th>ROC-AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>61.07%</td>
<td>69.42%</td>
<td>17.75%</td>
<td>0.3743</td>
<td>0.6144</td>
</tr>
<tr>
<td>RF</td>
<td>71.58%</td>
<td>71.77%</td>
<td>16.67%</td>
<td>0.4703</td>
<td>0.7053</td>
</tr>
<tr>
<td>DT</td>
<td>74.06%</td>
<td>73.81%</td>
<td>15.97%</td>
<td>0.5824</td>
<td>0.7444</td>
</tr>
<tr>
<td>Wide &amp; Deep CNN</td>
<td>80.79%</td>
<td>81.13%</td>
<td>13.15%</td>
<td>0.5724</td>
<td>0.8123</td>
</tr>
<tr>
<td>LSTM &amp; MLP</td>
<td>87.41%</td>
<td>87.36%</td>
<td>15.63%</td>
<td>0.6719</td>
<td>0.8789</td>
</tr>
<tr>
<td>SOSTLink &amp; BiGRU</td>
<td>93.42%</td>
<td>93.14%</td>
<td>10.34%</td>
<td>0.7795</td>
<td>0.9332</td>
</tr>
<tr>
<td>Bi-RNN</td>
<td>85.38%</td>
<td>85.47%</td>
<td>21.24%</td>
<td>0.7799</td>
<td>0.8488</td>
</tr>
<tr>
<td>CNN &amp; LSTM</td>
<td>88.02%</td>
<td>87.11%</td>
<td>17.56%</td>
<td>0.8146</td>
<td>0.8733</td>
</tr>
<tr>
<td>LSTM &amp; GRU</td>
<td>74.98%</td>
<td>73.24%</td>
<td>32.18%</td>
<td>0.6656</td>
<td>0.7328</td>
</tr>
<tr>
<td>Proposed models</td>
<td>96.64%</td>
<td>96.87%</td>
<td>3.77%</td>
<td>0.9469</td>
<td>0.9684</td>
</tr>
</tbody>
</table>

From Table 3, it was clear that the proposed model obtained the best results, with precision reaching 96.64%, recall reaching 96.87%, the FPR was as low as 3.77%, the PR-AUC value improved to 0.9469, and the ROC-AUC value improved to 0.9684. These results further illustrated that use of the hybrid multi-time scale neural network-based model effectively extracted user features, considering not only the temporal characteristics of user electricity data but also the periodic characteristics and deep features of user electricity consumption. Additionally, using the CatBoost classifier achieved user classification with a high accuracy rate and low false detection rate.

4.4. Ablation Experiments of the Model

To further validate the effectiveness of the model, the study performed the following ablation experiments: (1) use only Bi-LSTM networks to extract data features on a daily time scale, and then feed them into the CatBoost classifier, denoted as Test 1; (2) use only ResNet to extract data features on a weekly time scale, and then feed them into the CatBoost classifier, denoted as Test 2; (3) use only AlexNet to extract data features on a monthly time scale, and then feed them into the CatBoost classifier, denoted as Test 3. The above models were trained separately, and the test data were fed into the models to draw PR and ROC curves, as shown in Figure 18.
Figure 18. PR and ROC curves of the model ablation tests. (a) PR curves; (b) ROC curves.

In Figure 18, it was clear that using only the Bi-LSTM network to extract data features on a daily time scale yielded a PR-AUC value of 0.7765 and ROC-AUC value of 0.8434. Using only ResNet to extract data features on a weekly time scale yielded a PR-AUC value of 0.7974 and ROC-AUC value of 0.8631. Using only AlexNet to extract data features on a monthly time scale yielded a PR-AUC value of 0.8988 and ROC-AUC value of 0.9363. Although each model achieved a certain feature extraction effect, it was notable that fusing three-time scales of customer electricity consumption features could more comprehensively reflect the patterns of customer electricity consumption and achieve a better classification effect. Table 4 displays the detailed results.
Table 4. Comparison of results of model ablation experiments.

<table>
<thead>
<tr>
<th>Models</th>
<th>Precision</th>
<th>Recall</th>
<th>FPR</th>
<th>PR-AUC</th>
<th>ROC-AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td>84.26%</td>
<td>85.12%</td>
<td>21.93%</td>
<td>0.7765</td>
<td>0.8434</td>
</tr>
<tr>
<td>Test 2</td>
<td>86.53%</td>
<td>87.06%</td>
<td>19.76%</td>
<td>0.7974</td>
<td>0.8631</td>
</tr>
<tr>
<td>Test 3</td>
<td>94.25%</td>
<td>94.64%</td>
<td>9.21%</td>
<td>0.8988</td>
<td>0.9363</td>
</tr>
<tr>
<td>Proposed model</td>
<td>96.64%</td>
<td>96.87%</td>
<td>3.77%</td>
<td>0.9469</td>
<td>0.9684</td>
</tr>
</tbody>
</table>

From Table 4, it was clear after testing that the model fusing three-time scales was more comprehensive than a single time scale model in responding to the features of normal and electricity theft customers. In terms of the accuracy rate, the model in this paper improved the accuracy by 12.38% compared to Test 1, 10.11% compared to Test 2, and 2.39% compared to Test 3. In terms of the false detection rate, the model in this paper reduced the false detection rate by 18.16% compared to Test 1, 15.99% compared to Test 2, and 5.44% compared to Test 3. By comparison, it was striking that using AlexNet to extract data features on a monthly time scale was the best, using ResNet to extract data features on a weekly time scale was the second best, and using Bi-LSTM to extract data features on a daily time scale was the worst.

5. Conclusions

In this paper, an innovative method for detecting electricity theft among consumers in a smart grid is presented. Firstly, to address the issue of imbalanced datasets, Time GAN was employed to synthesize data from a limited number of customers engaged in electricity theft, thereby increasing the precision of the detection method. Secondly, a hybrid neural network model was introduced that captured customers’ daily, weekly, and monthly energy consumption patterns using Bi-LSTM, ResNet, and AlexNet networks. This approach addressed the limitations of existing methods, which cannot adequately capture the periodicity of electricity consumption or consider the temporal correlations of customers’ energy usage based on weeks and months. Finally, the CatBoost classifier was employed to classify customers and achieve both high accuracy and low false detection rates. Comparative and ablation experiments conducted on real electricity consumption data provided by the SGCC demonstrated the efficacy of the proposed method. Notably, the Time GAN method utilized exhibited a 39.53% improvement in accuracy rate, a 53.75% improvement in recall rate, and a 38.59% reduction in false detection rate compared to the original dataset. Similarly, the proposed hybrid multi-time scale neural network model achieved an accuracy rate of 96.64%, a recall rate of 96.87%, and a 3.77% false detection rate, underscoring the effectiveness of the approach.

The current method may have some limitations, and consideration will be given in future research to the following aspects to address these limitations:

Data collection issue: The method relies on the energy consumption patterns of customers to detect electricity theft, which requires a large amount of customer electricity data to train the model. If the data collection is insufficient or the data quality is poor, the model may not be able to accurately detect electricity theft. Therefore, further research will be conducted on data pre-processing and augmentation techniques to improve the accuracy and robustness of electricity theft detection.

Accuracy issue: Although the model uses multiple networks to capture energy consumption patterns at different time scales, its accuracy is still influenced by many factors, such as model parameter settings and network structure. Therefore, more optimization and improvement will be carried out to improve the accuracy of the model.

Model complexity: The method combines multiple neural network models, making the model complex. This may lead to long training times, high computation costs, and difficulty in explaining the model’s decision-making process. Therefore, exploration will be conducted on new model structures to improve the model’s performance and generalization ability while maintaining model simplicity in future research.
Privacy issue: The method requires access to customer electricity data, which may raise privacy and data security concerns. Therefore, practical applications will require the consideration of privacy protection and data security measures.

Author Contributions: Writing—original draft preparation, Y.S.; writing—review and editing, X.S.; supervision, T.H.; funding acquisition, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (grant number 61961017).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References


10. Lepolesa, L.J.; Achari, S.; Cheng, L. Electricity Theft Detection in Smart Grids Based on Deep Neural Network. IEEE Access 2022, 10, 39638–39655. [CrossRef]


22. Nabil, M.; Mahmoud, M.; Ismail, M.; Serpedin, E. Deep Recurrent Electricity Theft Detection in AMI Networks with Evolutionary Hyper-Parameter Tuning. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1002–1008. [CrossRef]


Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.