Research Article

Ximing Chen, Yeping Gan, Min Ren, Aiqiong Ji, Jianshun Ding, and Kun Ma*

An anomaly analysis method for measurement data based on similarity metric and improved deep reinforcement learning under the power Internet of Things architecture

https://doi.org/10.1515/jisys-2024-0118
received March 01, 2024; accepted June 22, 2024

Abstract: A measurement data anomaly analysis method based on similarity metric and improved deep reinforcement learning under the power Internet of Things (PIoT) architecture is proposed. First, a data anomaly analysis architecture based on the PIoT is built, and high-quality data processing is achieved through cloud-edge collaboration. Then, on the edge side, a kernel function is used to optimize the fuzzy C clustering algorithm to obtain data feature curves and possible abnormal samples are screened out through similarity metric methods for further analysis. Finally, a deep Q network (DQN) combined with a long-short term memory network (LSTM) is deployed in the cloud center, and data anomaly analysis results are obtained through training and analysis of the LSTM-DQN network. Based on the selected data samples, experimental analysis is conducted on the proposed method, and the results show that its analysis accuracy, response time, and stability are 96.07%, 220 ms, and 0.02, respectively, which can quickly and accurately analyze abnormal measurement data.

Keywords: analysis of abnormal measurement data, power Internet of Things, similarity metric, LSTM-DQN network, kernel function optimization fuzzy C clustering algorithm

1 Introduction

With the construction and improvement of advanced measurement infrastructure and the power Internet of Things (PIoT), the informatization, digitization, interactivity, and intelligence of power systems are becoming increasingly high. Measurement data are growing exponentially, with a wide range of structural types and strong interactivity [1]. The electricity metering system contains data related to electricity consumption, such as current, voltage, and electricity consumption, reflecting changes in users' electricity consumption behavior. At present,

*** Corresponding author: Kun Ma**, Measurement and Quality Inspection Department, State Grid Anhui Marketing Service Center, Hefei, Anhui, 230088, China, e-mail: makun_one@163.com, mak6477@ah.sgcc.com.cn
Ximing Chen: State Grid Anhui Marketing Service Center, Hefei, Anhui, 230088, China, e-mail: 13605519004@139.com, chenxm0011@ah.sgcc.com.cn
Yeping Gan: State Grid Anhui Electric Power Co., LTD, Hefei, Anhui, 230022, China, e-mail: gwahjl@163.com, ganyp0070@ah.sgcc.com.cn
Min Ren: State Grid Anhui Marketing Service Center, Hefei, Anhui, 230088, China, e-mail: renmin_sgcc@163.com, renm0061@ah.sgcc.com.cn
Aiqiong Ji: Measurement and Quality Inspection Department, State Grid Anhui Marketing Service Center, Hefei, Anhui, 230088, China, e-mail: aiqiongji@163.com, jiaq202X@ah.sgcc.com.cn
Jianshun Ding: Measurement and Quality Inspection Department, State Grid Anhui Marketing Service Center, Hefei, Anhui, 230088, China, e-mail: ncepudjs@163.com, dingjs3812@ah.sgcc.com.cn

Open Access. © 2025 the author(s), published by De Gruyter. cc BY This work is licensed under the Creative Commons Attribution 4.0 International License.

with the continuous improvement of the requirements in the electricity market, higher requirements have been put forward for the abnormal energy metering and handling methods of electricity customers [2].

Abnormal electricity metering is usually caused by reasons such as electricity theft, instrument failures, and billing errors, while most abnormal situations are related to fraud and energy theft. The traditional method of stealing electricity mainly involves changing the internal wiring of the electricity meter or damaging the structure of the meter, which requires manual on-site regular inspection to determine whether there is electricity theft behavior [3,4]. With the rapid development of technology, the novelty and concealment of electricity theft methods are graduallyincreasing. If regular manual inspections are still used to detect electricity theft, not only the detection accuracy is not high, but real-time performance is difficult to ensure. At the same time, the lack of targeted inspections will also bring a lot of financial and human losses to the power grid company [5]. Therefore, how to quickly and accurately monitor abnormal electricity metering has become a key issue that cannot be underestimated by power supply enterprises at present.

At present, there are two main methods for anomaly detection in metrological data: manual detection and machine learning-based method detection. Manual detection not only wastes a large amount of manpower and resources but also fails to detect abnormal data such as electricity theft in a timely manner, resulting in low efficiency in antielectricity theft work [6]. The collection of massive power data in smart grids provides effective technical means for intelligent, efficient, and accurate data anomaly recognition using methods such as machine learning and artificial intelligence [7,8]. However, when using machine learning for data detection, the imbalance between classes can lead to the detection model being insensitive to minority classes, as the number of abnormal samples is much smaller than that of normal samples, thereby reducing the accuracy of anomaly detection. The existing machine learning methods still have certain shortcomings in accuracy, real-time performance, and other aspects. Therefore, a measurement data anomaly analysis method based on similarity metric and improved deep reinforcement learning under the PIoT architecture is proposed. The innovation points are summarized as follows:

(1) Due to the fact that most existing methods do not attach importance to the imbalance between normal and abnormal samples in the measurement data, the proposed method designs a similarity measurement method that integrates curve numerical and morphological features to minimize normal samples, ensure balance between samples, and improve data analysis efficiency.
(2) In response to the problems of poor time perception and lack of continuity in decision-making in deep Q-network (DQN), the proposed method combines the long-short term memory (LSTM) network and the fully connected network to build the agent of the DQN so as to improve the accuracy of data analysis.

2 Related research

At present, there has been some research on the detection of abnormal measurement data such as electricity theft, both domestically and internationally, and certain achievements have been made. It can be mainly divided into traditional detection methods and intelligent detection methods based on supervised learning. Among them, there are differences between supervised learning methods and whether big data are considered [9]. For example, Bohani et al. [10] compared several supervised learning methods based on decision trees, artificial neural networks, deep artificial neural networks, and AdaBoost in terms of prediction accuracy, recall rate, accuracy, etc. The results show that the supervised learning method can detect abnormal behaviors such as power theft, but the data quality is not high, and the detection accuracy needs to be further improved. Yan et al. [11] proposed a new method for electricity theft detection based on a user load shape dictionary, which optimizes the detection effect through corresponding threshold adjustable strategies. The effectiveness and applicability of this method were experimentally verified, but its detection performance is poor in the face of complex measurement data. However, this method is difficult to adapt to the detection of complex abnormal data. Kong et al. [12] proposed a theft detection method based on a similarity measure and decision tree, which combines a K-nearest neighbor and support vector machine. It comprehensively considers the numerical and morphological features in the similarity measurement process and effectively detects theft behavior. However, this method is time-consuming and cannot meet the real-time requirements. Santos et al. [13] proposed an efficient and scalable system combining XGBoost and an enhanced classification tree to predict electricity theft behavior, but the processing performance of this method is poor, making it difficult to analyze massive smart grid measurement data with high quality. Irfan et al. [14] proposed a method for detecting electric theft behavior that combines an adaptive Boosting classifier with a coronavirus population immune optimizer and a forensic investigation optimizer. The method solves the problem of data imbalance through Nearmiss undersampling technology, minimizes computational complexity, reduces training time and losses, and improves training accuracy. However, this method lacks strong learning algorithms to support it, so the detection accuracy needs to be improved. The above methods generally have the problem of simple algorithms and inability to balance real-time detection with accuracy.

With the continuous development of computer and communication technologies, the advantages of machine learning methods in intelligent detection have gradually become prominent. Yao et al. [15] proposed a hybrid method for electricity theft detection that combines the adaptive Boost algorithm and convolutional neural network (CNN). By training multiple CNN-based classifiers to extract different features and combining them into a powerful classifier using adaptive Boost, the feature information can be effectively classified and recognized. However, it is difficult to accurately obtain the time characteristics present in the measurement data, and the detection results need to be improved. However, this method lacks consideration for data imbalance, resulting in certain deviations in the detection results. Fei et al. [16] proposed a self-supervised detection method to detect fraudulent electricity theft in low-voltage networks by extracting the characteristic data of long-term consumption patterns, extracted global information by inputting one-dimensional CNN and gated recursive unit data from a smart meter and training a single-layer neural network classifier to achieve accurate detection of electricity theft. Ullah et al. [17] proposed a theft detection method based on the Internet of Things, which can effectively collect and analyze user electricity consumption data and detect theft behavior in a timely manner. However, it lacks powerful learning algorithms, and the detection results are not ideal. This method lacks the support of reliable algorithms and does not have universality. Ibrahem et al. [18] proposed a machine learning model to solve the problem of user privacy protection and power theft detection and realized data anomaly analysis by encrypting the reading of smart meters and calculating the inner product of encrypted reading. However, the application scope is small, and the universality is poor. This method focuses on privacy protection, but the analytical ability of the theft detection model is poor, resulting in low detection reliability. The above methods did not consider the temporal and imbalanced issues of the data, and the accuracy of the detection results needs further improvement. Li et al. [19] proposed an intelligent detection method for power grid data based on spatiotemporal transformer networks, in which a self-attention mechanism and graph convolutional layer are used to capture and establish global/local dependencies of the power grid, further improving detection accuracy. Fahmi et al. [20] identified data features based on an autoencoder and used its output latent layers to train a deep LSTM (DLSTM) model for data anomaly detection. Although the above methods can achieve reliable data detection, there is still room for improvement in detection efficiency.

3 Data analysis architecture based on the PIoT

3.1 Overall framework

By comprehensively utilizing modern technologies such as the IoT, big data, and cloud computing, the operation data of intelligent distribution equipment or traditional distribution equipment after intelligent upgrading and transformation in the distribution network can be integrated into the cloud management platform to improve the efficiency of operation and maintenance management of the distribution network. By analyzing big data of monitoring equipment, power supply equipment can achieve intelligent self-diagnosis, handle existing anomalies in a timely manner, and improve system operation stability. The architecture of the distribution network measurement data analysis system based on the IoT is shown in Figure 1.

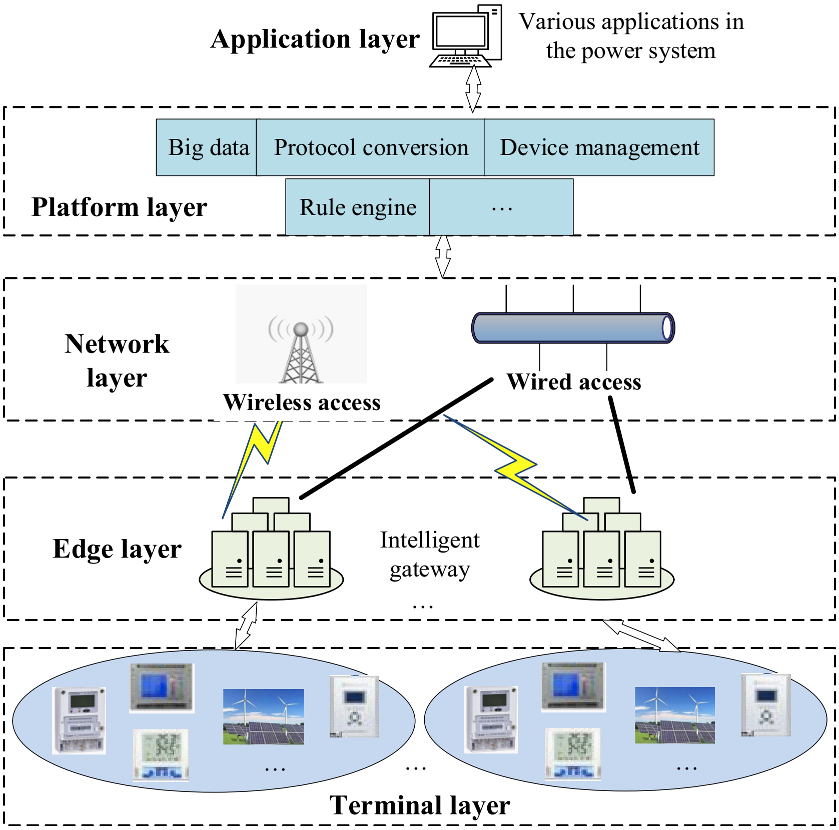


Figure 1: Overall framework of the proposed method. Source: Created by the authors.

The data analysis architecture based on the PIoT consists of the application layer, platform layer, network layer, edge layer, and terminal layer. Application layer: management systems for specific business applications, such as intelligent distribution network management systems and production monitoring centers. Network layer: the intelligent gateway supports wired fiber optic and wireless transmission methods. Terminal layer: includes various terminal devices, such as smart meters, sensors, and detection devices. The intelligent gateway supports rapid access to massive heterogeneous terminals.

Edge layer: an intelligent gateway distributed at various nodes of the distribution network, achieving local access to various types of sensors, device management, local intelligence, collaborative work with IoT platforms, and end-to-end cloud collaboration. Intelligent gateways focus on local rapid response to business needs while filtering and processing a large amount of invalid data. Specifically, in the edge layer of this architecture, similarity measures are used to obtain datasets that may have anomalies and then uploaded to the cloud center.

Platform layer: the PIoT platform provides functions such as terminal device management, connection management, and application enablement [21]. Specifically, the LSTM-DQN network is deployed on the platform, and further analysis is conducted on suspicious datasets to obtain accurate abnormal analysis results for measurement data.

3.2 Data preprocessing

3.2.1 Data feature clustering based on KFCM

The characteristics of measurement data are closely related to user electricity consumption behavior, and the correlation between various measurement data features is relatively large. The redundant information contained in the feature space leads to poor analysis results. The Kernel Fuzzy C Means (KFCM) clustering algorithm utilizes kernel functions to map the features of the original sample into high-dimensional space, highlighting the previously unseen features and improving the clustering performance of the algorithm [22]. During the clustering process, input the normal metering data curve and output the clustering center curve of the user's normal electricity consumption, which is the characteristic curve of the metering data.

Assuming that the clustering center $\phi(u_k)$ on a high-dimensional space can find the original image u_k in the original space, and according to the Mercer kernel definition $l^2(\Theta_i, u_k) = \|\phi(\Theta_i) - \phi(u_k)\|^2$, the objective function of KFCM can be obtained as follows:

$$J = \sum_{k=1}^{c}\sum_{i=1}^{n}\vartheta_{ki}^{w}(K(\Theta_i, x_i) + K(u_k, u_k) - 2K(\Theta_i, u_k)), \tag{1}$$

where $K(,)$ is the Gaussian radial basis function, c is the number of clusters, w is the fuzzy index, ϑ_{ki} is the degree of membership, and Θ is a feature mapping.

Due to the inability of the Lagrangian number multiplication method to directly obtain the clustering center and membership matrix of the algorithm, using kernel mapping and multiplying by $\phi^T(x_j)$, one can obtain

$$K(\Theta_j, u_k) = \frac{\sum_{i=1}^{n}\vartheta_{ki}^{w}K(\Theta_j, \Theta_i)}{\sum_{i=1}^{n}\vartheta_{ki}^{w}}. \tag{2}$$

In the proposed method, if the kernel function is the Gaussian radial basis function ($K(x, x) = 1, \forall x \in X$), the objective function of the KFCM algorithm becomes

$$\begin{aligned} J &= \sum_{k=1}^{c}\sum_{i=1}^{n}\vartheta_{ki}^{w}(1 - K(\Theta_i, u_k)) \\ K(\Theta_i, u_k) &= \exp\{-\|\Theta_i - u_k\|^2/(2 \times \sigma^2)\}, \end{aligned} \tag{3}$$

where σ is the width parameter of the function, which controls the radial action range of the function.

At this point, the clustering center and membership matrix obtained by Lagrange number multiplication are

$$\vartheta_{ki} = \frac{(1 - K(\Theta_i, u_k))^{\frac{1}{1-w}}}{\sum_{k=1}^{c}(1 - K(\Theta_i, u_k))^{\frac{1}{1-w}}}, \quad u_k = \frac{\sum_{i=1}^{n}\vartheta_{ki}^{w}K(\Theta_i, u_k)\Theta_i}{\sum_{i=1}^{n}\vartheta_{ki}^{w}K(\Theta_i, u_k)}. \tag{4}$$

3.2.2 Measurement data preprocessing based on similarity metric

The characteristic curve of measurement data reflects the electricity consumption characteristics of users and the law of load changes over a period of time. The electricity consumption characteristic curve is obtained through the KFCM clustering algorithm, which reflects the normal electricity consumption characteristics of such users. Therefore, using a similarity method based on time series to measure the degree of matching between the test curve and measurement data characteristic curve, abnormal electricity users can be preliminarily screened [23].

The similarity of time series includes two parts: numerical and shape similarity; however, currently, most studies on time series similarity have not been able to balance them well. The normal electricity consumption characteristic curve $\Theta = (\Theta_1, \Theta_2,\ldots,\Theta_n)$ and the distribution network test curve $Z = (z_1, z_2,\ldots,z_n)$ were obtained from the input data through the KFCM algorithm. Using Euclidean distance to measure the difference in values between the characteristic curve Θ and the curve Z to be tested, the calculation is as follows:

$$D(\Theta, Z) = \sqrt{\sum_{i=1}^{n}(\Theta_i - z_i)^2}\,. \tag{5}$$

The use of Euclidean distance can reflect the numerical differences between curves and cannot characterize the morphological differences between curves. To accurately depict the morphological characteristics of curves in different time periods, such as rising, falling, and stationary, the slope of the straight line is used to represent the morphological characteristics of that time period. Therefore, the time series with a length of n is reduced to an $n - 1$ morphological sequence:

$$\Theta_i' = \frac{\Theta_{i+1} - \Theta_i}{\Delta t}, \quad i = 1, 2, \ldots, n - 1. \tag{6}$$

The sequences of Θ and Z morphological features are $\Theta' = (\Theta_1, \Theta_2, \ldots, \Theta_{n-1})$ and $Z' = (z_1, z_2, \ldots, z_{n-1})$, respectively. To align the two sequences, it is necessary to construct a distance matrix. Each element in the matrix is represented by an Euclidean distance:

$$D(i, j) = \|\Theta_i - z_j\|_2, \quad i, j = 1, 2, \ldots, n - 1. \tag{7}$$

A cumulative distance D' is constructed by the dynamic programming method. The cumulative distance $D'(i, j)$ is the sum of the distance $d(i, j)$ of the current grid point and the cumulative distance of the smallest adjacent element that can reach the point. The calculation is as follows:

$$D'(i, j) = d(i, j) + \min\{D'(i - 1, j - 1), \; D'(i - 1, j), D'(i, j - 1)\}. \tag{8}$$

The path with the smallest cumulative distance is the best path to reach that point.

Taking into account the numerical and morphological similarities of the curve time series, the calculation is as follows:

$$D_{\text{whole}}(\Theta, Z) = \sqrt{\alpha D(\Theta, Z) + \beta D'(\Theta', Z')}\,, \tag{9}$$

where α and β are the weights considering numerical and morphological factors, $\alpha + \beta = 1$.

In the process of similarity measurements, the normal measurement data characteristic curve is obtained from clustering, and the distribution network test curve is the input. First, the respective morphological sequences Θ' and Z' are calculated, and then the numerical and morphological similarity between the normal measurement data characteristic curve and the test curve are calculated. Finally, the matching degree between the characteristic curve and the test curve is the output. Based on the obtained matching degree and the set threshold, the possibility of anomalies is preliminarily determined. After multiple experiments, the final selected threshold $D_2 = 3.5$ and $D_1 = 0.8$ can ensure that there are fewer normal data in the threshold range that may be abnormal, while there are almost no abnormal users in the normal data [24]. By measuring similarity, the scope of secondary detection is reduced, and the balance between normal and abnormal samples during detection is reduced.

4 Anomaly analysis of econometric data based on improved deep reinforcement learning

4.1 Deep reinforcement learning

DQN is an important algorithm in the field of reinforcement learning, whose core idea is to enable agents to perceive the state of the environment, find the optimal policy function in the process of interacting with the environment, and maximize cumulative benefits. The policy function is defined as

$$\pi(a|s) = P(a_t = a|s_t = s). \tag{10}$$

In the decision-making process of the intelligent agent, the policy function obtains the state sample s_t and returns the action a_t (data anomaly) of that state based on a certain probability P. The cumulative return is defined as the return function G_t, which is

$$G_t = r_{t+1} + \gamma r_{t+1} + \cdots = \sum_{k=0}^{\infty} \gamma^k r_{t+k+1}, \tag{11}$$

where r_{t+k} is the reward value corresponding to the future state, and $\gamma \in (0, 1]$ is the discount factor; the larger the value of γ, the more consideration is given to future returns after discounts.

To evaluate the return value of a certain state under a given strategy π, a state value function ψ_π is introduced. The definition of $\psi_\pi(s)$ at state s is as follows:

$$\psi_\pi(s) = E_\pi(G_t | S_t = s). \tag{12}$$

For convenience, the Q function is introduced in reinforcement learning. When the input is a state action pair, and the output is a reward value, the state action value function $Q_\pi(s, a)$ of strategy π is

$$Q_\pi(s, a) = E_\pi[G_t | S_t = s, A_t = a] = E_\pi\left[\sum_{k=0}^{\infty} \gamma^k R_{t+k+1} | S_t = s, A_t = a\right]. \tag{13}$$

Among all possible state value functions, there must be an optimal state value function. Therefore, iterative updating of DQN is required, as shown in Figure 2.

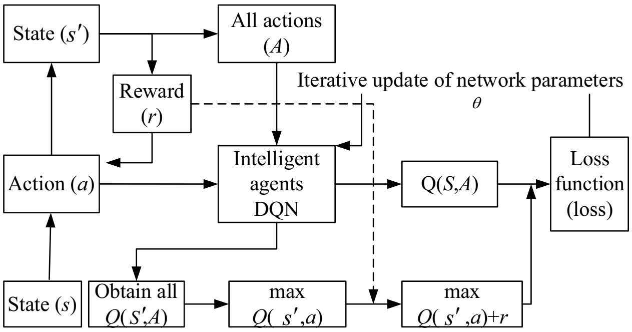


Figure 2: Iterative updating process of DQN networks. Source: Created by the authors.

To minimize the loss function $L(\theta)$, the network parameters θ are constantly updated in the process of network training. $L(\theta)$ is calculated as follows:

$$\begin{aligned} L(\theta) &= E_{(s,a,r,s')}[y^{\mathrm{DQN}} - Q(s, a;\theta)]^2 \\ y^{\mathrm{DQN}} &= r + \gamma \max_a Q(s', a;\theta^-). \end{aligned} \tag{14}$$

4.2 LSTM-DQN network

To enhance the perception ability of intelligent agents from state variables and ensure a certain degree of coherence in decision-making actions, LSTM units are introduced as the basic neurons of the hidden layer, and the input layer of the network is improved to obtain an LSTM-DQN network, which can better extract the temporal characteristics of data [25].

The basic unit of LSTM is a structure that contains multiple sets of neurons. f, i, and o are forgetting gates, input gates, and output gates, respectively [26]. By setting the parameters of the three control gates reasonably, the memory function of LSTM can be achieved. The core calculation formula is as follows:

$$\begin{cases} f_t = \sigma(\varpi_f \cdot [h_{t-1}, x_t] + b_f) \\ i_t = \sigma(\varpi_i \cdot [h_{t-1}, x_t] + b_i) \\ \tilde{c}_t = \tanh(\varpi_c \cdot [h_{t-1}, x_t] + b_c) \\ c_t = f_t \cdot c_{t-1} + i_t \cdot \tilde{c}_t \\ o_t = \sigma(\varpi_0 \cdot [h_{t-1}, x_t] + b_0) \\ h_t = o_t \cdot \tanh(c_t), \end{cases} \tag{15}$$

where f, σ, i, t, o, h, c, ϖ, and b represent forgetting, sigmoid activation function, input, time step, output layer, hidden layer, unit state, weight matrix, and deviation, respectively.

The LSTM-DQN network structure is shown in Figure 3.

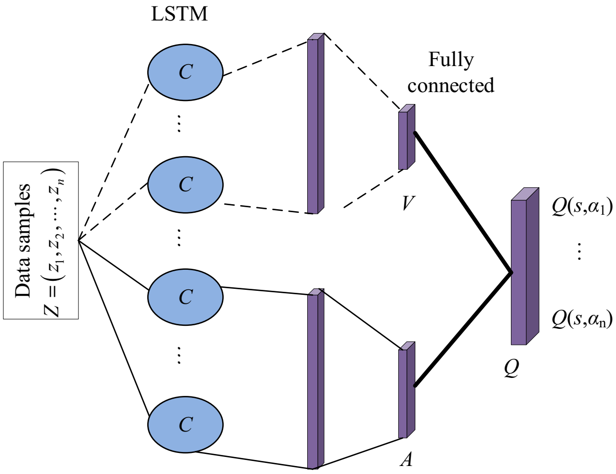


Figure 3: Structure of the LSTM-DQN value network. Source: Created by the authors.

In the LSTM-DQN network, the input layer is the state variable of the agent at each moment. At time t, the input of the network is the metric data $Z = (z_1, z_2,...,z_n)$ by similarity metric. When the LSTM network is used as the basic unit, an environmental state transition model is used for sampling, and its output is the input into the DQN network through the fully connected layer. After iterative learning of the DQN network, the final analysis result is the output.

4.3 Measurement data anomaly analysis process based on LSTM-DQN

Due to the significant impact of the environment on measurement data, the ability of DQN to perceive environmental states through intelligent agents and interact with the environment to obtain real-time decisions, and the ability of LSTM to extract the temporal characteristics of the data, LSTM-DQN is used for anomaly analysis of measurement data. Under the architecture of the PIoT, similarity metrics are first used at the edge layer to obtain datasets that may have anomalies and then uploaded to the cloud center. Based on the deployed LSTM-DQN network, suspicious datasets are further analyzed to obtain accurate abnormal analysis results for measurement data [27,28]. The specific analysis process of the proposed method is shown in Figure 4.

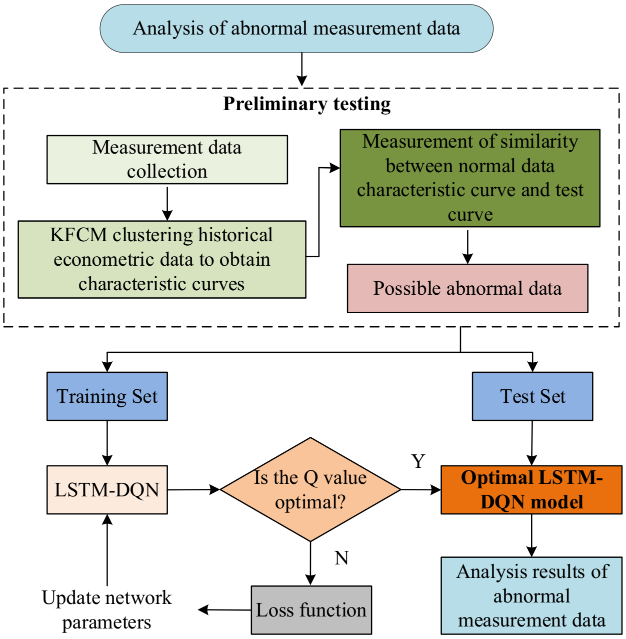

Analysis of abnormal measurement data
Preliminary testing
Measurement data collection
KFCM clustering historical econometric data to obtain characteristic curves
Measurement of similarity between normal data characteristic curve and test curve
Possible abnormal data
Training Set
Test Set
LSTM-DQN
Is the Q value optimal?
Y
N
Optimal LSTM-DQN model
Update network parameters
Loss function
Analysis results of abnormal measurement data

Figure 4: Process of abnormal analysis of measurement data. Source: Created by the authors.

Step 1: Input the measurement data to be tested according to the generalized Kirchhoff law, the submeter reading + network loss = total meter reading. If the network loss is too large, it is considered that there is a possibility of power theft, and the data may be abnormal.

Step 2: Carry out unsupervised learning tests on the measurement data. First, the KFCM clustering algorithm is used to classify the data and obtain the characteristic curves of various types of data. Then, taking into account the numerical value and shape of the curve, the similarity between the feature curve and the curve to be tested is measured using methods such as Euclidean distance. Finally, determine normal data, abnormal data, and possible abnormal data based on the set threshold curve. This step ensures the maximum possible abnormal data and the minimum normal data for secondary detection, balancing the number of normal and abnormal samples during detection.

Step 3: Based on the obtained measurement data, extract the temporal characteristics of the data using LSTM and use it as the input layer of the DQN network. The DQN network agent starts from the state s_t and adopts the ε-greedy strategy to select the action a_t' corresponding to the maximum value and passes a'_t to the environment to determine the correctness of the classification and obtain the corresponding reward. If the classification is correct, the reward is +1, and if the classification is incorrect, the reward is −1. Store the results of each interaction with the environment in the form of tuples in the precreated experience pool Memory D. When the data in the experience pool reaches the set threshold, randomly collect batch_size samples from it each time and input them into LSTM-DQN to calculate the loss and update the network parameters. When the training reaches a fixed training cycle, the optimal network parameters are obtained and used for data analysis of the test set to obtain the classification of possible abnormal data in step 2 [29].

Step 4: Output the detection results. Obtain the analysis results of metrological data through the LSTM-DQN network and evaluate the model by calculating accuracy, false detection rate, and other indicators based on the analysis results while updating the model parameters in real-time.

5 Experiment and analysis

In the experiment, choose an SP-DPP cloud platform with a good throughput and acceleration ratio. The hardware configuration of the cloud server host is as follows: Intel Xeone3-1220v53.0 GHz quad core, memory: 8GB DDR4, hard disk: 1 * Intel Enterprise SSD, 1 * SATA1T, network card: 2 * Gigabit Ethernet port. The hardware configuration of the working machine node is CPU model Intel Xeone3-1220v53.0 GHz, with 8 GB of memory. The hard disk capacity is 1 TB. The experiment uses a Keras deep learning platform based on TensorFlow 2.1, using Sklearn and imbearn libraries, with a Python version of 3.7. In the experiment, these nodes are connected to each other through a gigabit switch in the local area network. Then, more than 100,000 pieces of abnormal electrical energy measurement data are collected in the cloud database and divided into training and testing sets according to 5:1. These data are normalized to improve calculation accuracy.

At the same time, the methods in previous studies [11,13,15] are selected for comparison in the experiment. The three methods represent traditional detection, supervised learning detection, and deep learning detection, respectively, and the comparison results with the proposed methods are more convincing. The network parameters are set as follows: dropout is 0.5; the learning rate is 0.001; using Adam optimizer; the number of iterations is 100.

5.1 Performance index

In order to effectively evaluate the analysis effect of the proposed method, the confusion matrix shown in Table 1 is usually used. The actual classification of data is analyzed and classified through model detection, dividing all metric data into TP, FP, FN, and TN.

Table 1: Confusion matrix for data anomaly analysis

Data category	Analyze normal data	Analyze abnormal data
Actual abnormal data	FN	TP
Actual normal data	TN	FP

Select accuracy (ζ_{AC}) and false detection rate (ζ_{PO}) as the evaluation indicators for the proposed method, which are defined as follows:

$$\begin{cases} \zeta_{\mathrm{PO}} = \dfrac{N_{\mathrm{FP}}}{N_{\mathrm{FP}} + N_{\mathrm{TN}}} \\ \zeta_{\mathrm{AC}} = \dfrac{N_{\mathrm{TP}}}{N_{\mathrm{TP}} + N_{\mathrm{FN}}}, \end{cases} \tag{16}$$

where N_{FP} is the number of false-positive samples detected, N_{FN} is the number of false-negative samples detected, N_{TP} is the number of true-positive samples detected, and N_{TN} is the number of true-negative samples detected.

5.2 Electricity theft detection based on similarity measurements

The objective function value in the KFCM clustering algorithm reflects the sum of distances from various sample points to the cluster center. The smaller the objective function, the tighter the clustering effect within the class and the separation between classes. The performance comparison between KFCM and FCM is shown in Figure 5.

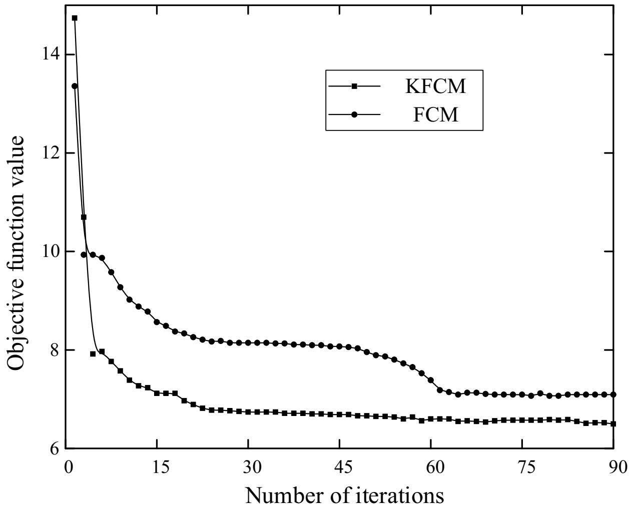


Figure 5: Performance comparison between KFCM and FCM. Source: Created by the authors.

From Figure 5, it can be observed that KFCM has a faster convergence speed and smaller objective function value compared to those of FCM. The convergence is achieved after about 30 iterations, and the objective function value is reduced by about 0.7. This demonstrates that the KFCM clustering algorithm has higher accuracy, better clustering performance, and faster convergence characteristics.

The common application for abnormal analysis of measurement data is electricity theft detection. Currently, the main methods of electricity theft include the undercurrent method, undervoltage method, spread difference method, phase shift method, and high-tech means. Based on the characteristic curve of the metric data obtained by the clustering algorithm, the similarity between the tested curve and its time series is measured, with the weights of morphology and numerical values set to $\alpha = \beta = 0.5$. The results of data anomaly analysis of unsupervised learning for eight groups of data are shown in Table 2.

Table 2: Measurement of time-series similarity

Characteristic curve and test curve	Measured value
Data group 1	1.533
Data group 2	0.734
Data group 3	2.409
Data group 4	2.681
Data group 5	1.257
Data group 6	0.898
Data group 7	3.326
Data group 8	3.815

From Table 2, it can be seen that according to the set thresholds of 3.5 and 0.8, data groups 2 and 8 can be detected. However, for data groups 1 and 3–7, it is not possible to distinguish whether there are abnormalities, so a secondary detection is required. By similarity metric, the amount of data can be reduced and the efficiency of analysis can be improved.

5.3 Data analysis results

The training process of the LSTM-DQN network model was set up to 50 rounds, with 64 steps set for each round of training. Randomly select 2,000 samples from a total of 10,000 samples as inputs and train the LSTM-DQN network according to the reward value update method and network iteration process. Treat the five reward values as a set and calculate the average as one data point. The change in reward value is shown in Figure 6.

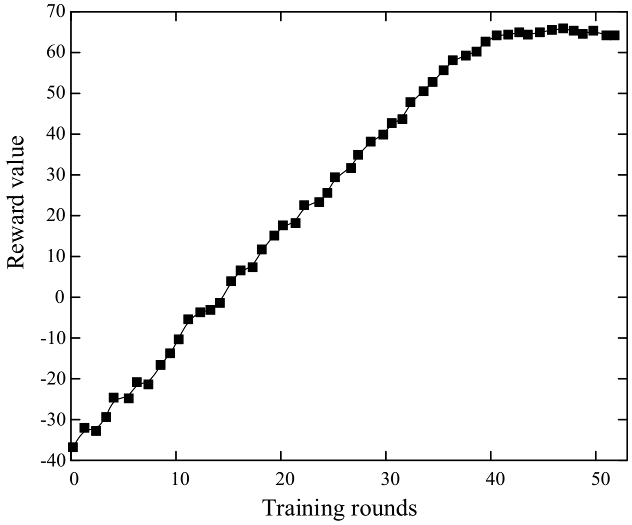
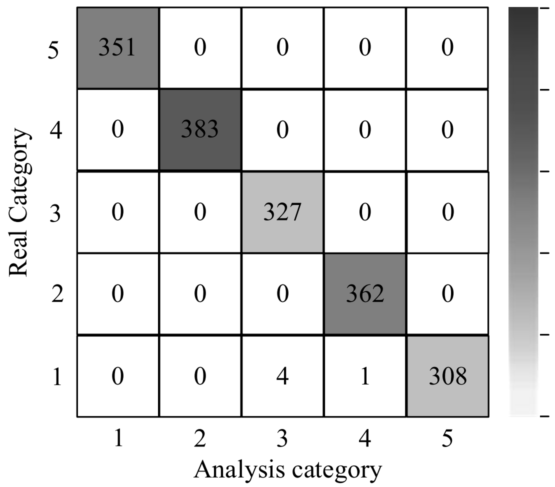


Figure 6: Performance comparison between KFCM and FCM. Source: Created by the authors.

As shown in Figure 6, as the number of learning rounds increases, the reward value gradually increases and tends to around 65. This indicates that the LSTM-DQN network model obtained through training has a high accuracy.

To test the accuracy of the LSTM-DQN network model, electricity theft sample data are used as the test set. The types of electricity theft include the undervoltage method, undercurrent method, spread difference method, phase shift method, and high-tech methods, which are classified as categories 1–5. The confusion matrix of LSTM-DQN model diagnosis results is shown in Figure 7.



Real Category	1	2	3	4	5
5	351	0	0	0	0
4	0	383	0	0	0
3	0	0	327	0	0
2	0	0	0	362	0
1	0	0	4	1	308

Figure 7: Confusion matrix. Source: Created by the authors.

From Figure 7, categories 1–4 were randomly selected with 351, 383, 327, and 362 samples, all of which were analyzed correctly, while category 5 bearings were selected with a total of 308 samples, of which 4 samples were mistakenly classified as category 3 and 1 sample was mistakenly classified as category 4. This is because high-tech methods have caused hidden data on electricity theft, which is difficult to analyze and prone to false detection. Based on the five types of electricity theft, the proposed analysis has good results and good accuracy.

5.4 Performance comparison

5.4.1 Accuracy comparison

The six groups of data after similarity metric analysis are taken as test samples, and the proposed method is used for repeated analysis. The accuracy rate and missed detection rate of anomaly analysis are shown in Table 3.

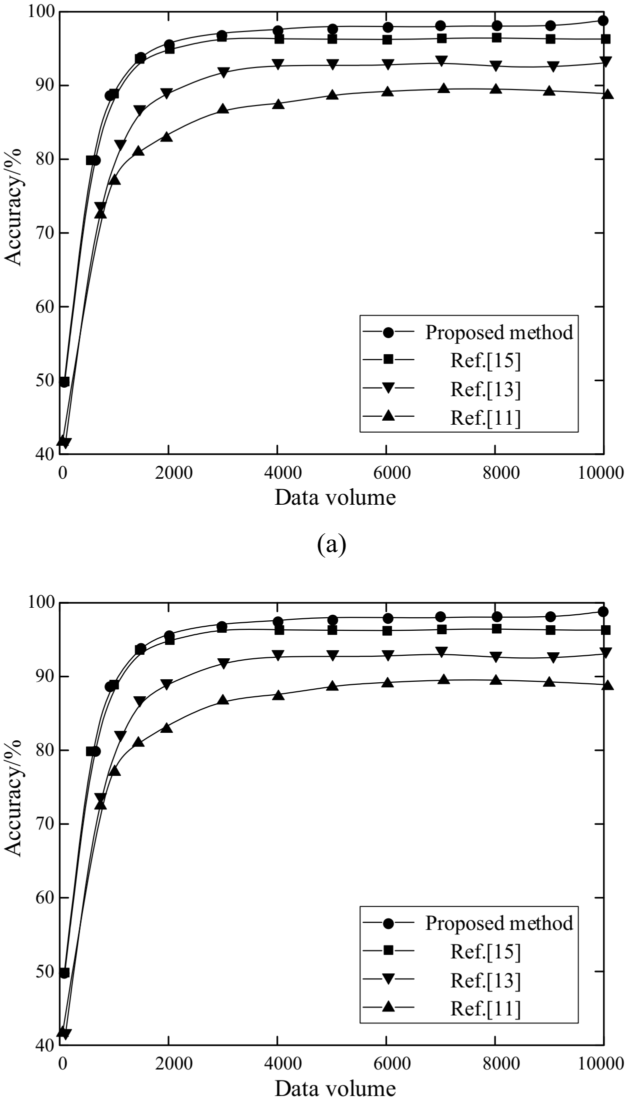
Table 3: Data anomaly analysis results

Data group	Accuracy (%)	False detection rate (%)
1	99.59	0.41
3	98.63	1.37
4	95.71	4.29
5	93.05	6.95
6	97.98	2.02
7	91.46	8.54
Mean value	96.07	3.93

As shown in Table 3, the proposed method has a high accuracy for most arrays, exceeding 95%, especially for Array 1, with an accuracy of up to 99.59%. The analysis error detection rate of array 7 is relatively high, reaching 8.54%, which may be due to the complexity and similarity of the data in the array, such as the use of high-tech methods to steal electricity, which are not easily detected. However, on the whole, the analysis accuracy of the proposed method reached 96.07%, which is ideal. This also proves that the proposed method can reduce the problem of error accumulation, and the combination of similarity measurement and the LSTM-DQN network can ensure the analysis accuracy of abnormal data.

To further validate the effectiveness of the proposed method, it was compared with previous studies [11,13,15]. The analysis accuracy and response time under different data volumes are shown in Figure 8.

From Figure 8, it can be seen that when the data volume is less than 3,000, the response times of the four methods are not significantly different. However, the analysis accuracy of the proposed method and that of Yao et al. [15] is about 96 and 94%, respectively, higher than that of previous studies [11,13]. It can be seen that the performance of the method using deep learning networks is better than that of traditional detection methods. However, as the amount of data increases, due to the long response time of deep learning networks, the combination of adaptive Boost algorithm and CNN for analysis in the study of Yao et al. [15] took over 300 ms. The proposed method uses similarity measurement to reduce a certain amount of data, resulting in a shorter response time of approximately 220 ms. Yan et al. [11] and Santos et al. [13], respectively, used the user load shape dictionary method and the enhanced classification tree method for data anomaly detection. The method was simple and the response time was short, but the analysis accuracy of both methods decreased, especially in the study of Yan et al. [11], which was less than 90%. Therefore, considering the accuracy, false detection rate, response time, and other aspects of data anomaly detection, the proposed method has a relatively ideal effect in practical applications.



(a)

(b)

Figure 8: Comparison of data anomaly analysis results using different methods: (a) accuracy and (b) response time. Source: Created by the authors.

In addition, to increase the credibility of the experimental results, the proposed method is compared with two deep learning models [15,19]. When the data volume is 10,000, the accuracy and response time of the three methods are shown in Table 4.

Table 4: Abnormal analysis results of different methods

Method	Accuracy (%)	Response time (ms)
Ref. [15]	95.73	300
Ref. [19]	97.12	415
Proposed method	98.54	220

According to Table 4, Li et al. [19] used a spatiotemporal transformer network for data anomaly analysis. Due to its improved performance compared to CNN, the accuracy reaches 97.12%. However, due to the complexity of the model, the response time is relatively long, at 415 ms. The proposed method combines similarity measurement and LSTM-DQN network to ensure the reliability of data analysis results, thus achieving the best overall performance.

5.4.2 Stability comparison

The stability of a method is also an important evaluation criterion. Stability refers to the stability state of a model under the influence of external interference information and different measurement states, which can reflect the constant degree of measurement characteristics over time. The calculation of stability τ is as follows:

$$\tau(\%) = \frac{V_{\max} - V_{\min}}{\bar{V}} \times 100\%, \tag{17}$$

where $V_{\max}$, $V_{\min}$, and $\bar{V}$ are the maximum, minimum, and mean values of the measured values, respectively.

For the convenience of measurement, 6 days of measurement data were selected for analysis. The comparison curves of the four methods (the proposed method with previous studies [11,13,15]) are shown in Figure 9. The smaller the stability value, the better the model stability; on the contrary, the larger the value, the poorer the stability.

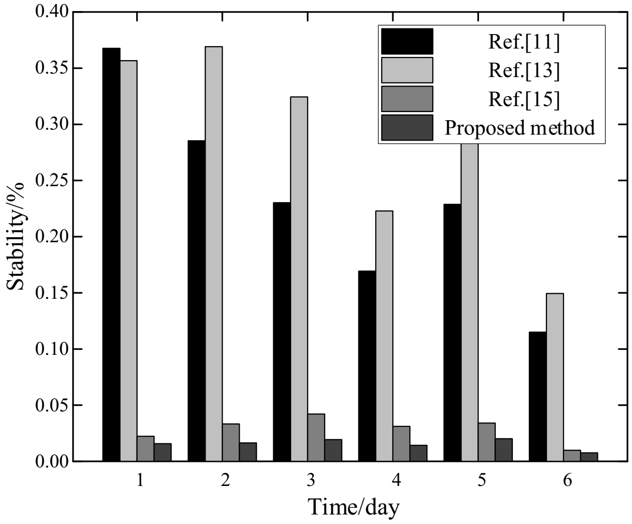


Figure 9: Stability comparison results of different methods. Source: Created by the authors.

From Figure 9, based on the 6-day data situation, the proposed method has the best stability performance, with stability of about 0.02 and no significant fluctuations. Due to the introduction of the LSTM network in the DQN network of the proposed method, which has good time characteristics, it maintains good analytical stability. Yao et al. [15] combined the adaptive Boost algorithm with CNN to achieve anomaly detection and ensured the stability of the model through the adaptive Boost algorithm, which does not exceed 0.05. However, Yan et al. [11] and Santos et al. [13] used traditional detection methods for anomaly analysis, which cannot obtain the temporal characteristics of the data. Therefore, their stability is relatively high, about ten times that of the proposed method, so their stability is poor.

6 Conclusion

To achieve higher quality data anomaly identification, a measurement data anomaly analysis method based on similarity measurement and improved deep reinforcement learning in the power IoT architecture is proposed. Based on the PIoT architecture, the KFCM algorithm is used to obtain data feature curves on the edge side and similarity metric methods are used to screen out possible abnormal samples. Simultaneously, the LSTM-DQN network is deployed in the cloud center, and data anomaly analysis results are obtained through updated training. The experimental results based on selecting data samples indicate the following:

(1) The similarity metric method can reduce data samples and screen out potentially abnormal samples by setting thresholds $D_2 = 3.5$ and $D_1 = 0.8$, thereby improving analysis efficiency.

(2) The LSTM-DQN network can quickly and accurately analyze abnormal measurement data, with analysis accuracy, response time, and stability of 96.07%, 220 ms, and 0.02, respectively, which has strong practicality.

Deep reinforcement learning networks have good performance in analyzing abnormal data, but their complex structure and numerous parameters limit their practical application and promotion to a certain extent. Therefore, in future work, we will attempt to apply a new deep-learning model for data anomaly analysis to improve detection performance. In addition, only the abnormal data analysis of electricity theft detection was considered in the experiment, and no discussion was made on abnormal situations such as equipment failures. Therefore, future research will enrich the application scenarios to improve the universality of the proposed method.

Funding information: Authors state no funding involved.

Author contributions: Ximing Chen and Yeping Gan are responsible for method design. Min Ren and Aiqiong Ji are responsible for data analysis. Jianshun Ding and Kun Ma are responsible for writing.

Conflict of interest: The authors declare no conflicts of interest.

Data availability statement: The original data can be obtained by contacting the author.

References

[1] Takiddin A, Ismail M, Zafar U, Serpedin E. Robust electricity theft detection against data poisoning attacks in smart grids. IEEE Trans Smart Grid. 2021;12(3):2675–84. doi: 10.1109/TSG.2020.3047864.

[2] Javaid N, Jan N, Javed MU. An adaptive synthesis to handle imbalanced big data with deep siamese network for electricity theft detection in smart grids – ScienceDirect. J Parallel Distrib Comput. 2021;153:44–52. doi: 10.1016/j.jpdc.2021.03.002.

[3] Hussain S, Mustafa MW, Jumani TA, Baloch SK, Alotaibi H, Khan I, et al. A novel feature engineered-CatBoost-based supervised machine learning framework for electricity theft detection. Energy Rep. 2021;7(12):4425–36. doi: 10.1016/j.egyr.2021.07.008.

[4] Yan Z, Wen H. Electricity theft detection base on extreme gradient boosting in AMI. IEEE Trans Instrum Meas. 2021;70(8):2504909.1–9. doi: 10.1109/I2MTC43012.2020.9128712.

[5] Razmi P, Buygi MO, Esmalifalak M. A machine learning approach for collusion detection in electricity markets based on nash equilibrium theory. J Mod Power Syst Clean Energy. 2021;9(1):170–80. doi: 10.1002/2050-7038.13046.

[6] Pereira J, Saraiva F. Convolutional neural network applied to detect electricity theft: A comparative study on unbalanced data handling techniques. Int J Electr Power Energy Syst. 2021;131(10):107085.1–7. doi: 10.1016/j.ijepes.2021.107085.

[7] Shen Y, Shao P, Chen G, Gu X, Wen T, Zang L, et al. An identification method of anti-electricity theft load based on long and short-term memory network. Procedia Comput Sci. 2021;183(8):440–7. doi: 10.1016/j.procs.2021.02.082.

[8] Qu Z, Liu H, Wang Z, Xu J, Zhang P, Zeng H. A combined genetic optimization with AdaBoost ensemble model for anomaly detection in buildings electricity consumption. Energy Build. 2021;248(10):111193.1–11. doi: 10.1016/j.enbuild.2021.111193.

[9] Firoozi H, Mashhadi HR. Non-technical loss detection in limited-data low-voltage distribution feeders. Int J Electr Power Energy Syst. 2022;135(3):107523.1–18. doi: 10.1016/j.ijepes.2021.107523.

[10] Bohani FA, Suliman A, Saripuddin M, Sameon SS, Md Salleh NS, Nazeri S. A comprehensive analysis of supervised learning techniques for electricity theft detection. J Electr Comput Eng. 2021;2021(1):9136206.1–10. doi: 10.1155/2021/9136206.

[11] Yan C, Ma F, Nie W, Han X, Hai X, Xu Y, et al. Adaptive electricity theft detection method based on load shape dictionary of customers. Glob Energy Internet: Engl Version. 2022;5(1):1–10. doi: 10.1016/j.gloei.2022.04.009.

[12] Kong X, Zhao X, Liu C, Li Q, Dong D, Li Y. Electricity theft detection in low-voltage stations based on similarity measure and DT-KSVM. Int J Electr Power Energy Syst. 2021;125(3):106544.1–11. doi: 10.1016/j.ijepes.2020.106544.

[13] Santos RN, Yamouni S, Albiero B, Vicente R, Silva J, Souza T, et al. Gradient boosting and Shapley additive explanations for fraud detection in electricity distribution grids. Int Trans Electr Energy Syst. 2021;31(9):e13046.1–13. doi: 10.1002/2050-7038.13046.

[14] Irfan M, Ayub N, Althobiani F, Ali Z, Idrees M, Ullah S, et al. Energy theft identification using adaboost ensembler in the smart grids. Comput Mater Cont (Engl). 2022;1(72):2141–58. doi: 10.32604/cmc.2022.025466.

[15] Yao Y, Hui H, Liang Z, Feng X, Guo W. AdaBoost-CNN: A hybrid method for electricity theft detection. 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE). 2021. p. 2021. doi: 10.1109/ACPEE51499.2021.9436837.

[16] Fei K, Li Q, Zhu C, Dong M, Li Y. Electricity frauds detection in low-voltage networks with contrastive predictive coding. Int J Electr Power Energy Syst. 2022;137(5):107715.1–8. doi: 10.1016/j.ijepes.2021.107715.

[17] Ullah F, Salam A, Amin F, Ahmad Khan I, Ahmed J, Alam Zaib S, et al. Deep trust: A novel framework for dynamic trust and reputation management in the internet of things (IoT)-based networks. IEEE Access. 2024;12:13. doi: 10.1109/ACCESS.2024.3409273.

[18] Ibrahem MI, Nabil M, Fouda MM, Mahmoud MMEA, Alasmary W, Alsolami F. Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks. Inst Electr Electron Eng (IEEE). 2021;8(2):1243–58. doi: 10.1109/JIOT.2020.3026692.

[19] Li X, Hu L, Lu Z. Detection of false data injection attack in power grid based on spatial-temporal transformer network. Expert Syst Appl. 2024;238:121706. doi: 10.1016/j.eswa.2023.121706.

[20] Fahmi AT, Kashyzadeh KR, Ghorbani S. Fault detection in the gas turbine of the Kirkuk power plant: An anomaly detection approach using DLSTM-Autoencoder. Eng Fail Anal. 2024;160:108213. doi: 10.1016/j.engfailanal.2024.108213.

[21] Alharbi A, Dong H, Yi X, Tari Z, Khalil I. Social media identity deception detection: a survey. ACM Comput Surv. 2022;54(3):69.1–35. doi: 10.1145/3446372.

[22] Bian J, Wang L, Scherer R, Wozniak M, Zhang P, Wei W. Abnormal detection of electricity consumption of user based on particle swarm optimization and long short term memory with the attention mechanism. IEEE Access. 2021;9:47252–65. doi: 10.1109/ACCESS.2021.3062675.

[23] Zhao Q, Chang Z, Min G. Anomaly detection and classification of household electricity data: a time window and multilayer hierarchical network approach. IEEE Internet Things J. 2022;9(5):3704–16. doi: 10.1109/JIOT.2021.3098735.

[24] Hussain S, Mustafa MW, Ateyeh Al-Shqeerat KH, Saleh Al-rimy BA, Saeed F. Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel-Tree boosting classifier-A novel sequentially executed supervised machine learning approach. IET Gener Transm Distrib. 2022;16(6):1257–75. doi: 10.1049/gtd2.12386.

[25] Cheng G, Zhang Z, Li Q, Li Y, Jin W. Energy theft detection in an edge data center using deep learning. Math Probl Eng. 2021;2021(1):1–12. doi: 10.1155/2021/9938475.

[26] Farmonov N, Amankulova K, Szatmari J, Sharifi A, Abbasi-Moghadam D, Mirhoseini Nejad SM, et al. Crop type classification by DESIS hyperspectral imagery and machine learning algorithms. IEEE J Sel Top Appl Earth Obs Remote Sens. 2023;16:1576–88. doi: 10.1109/JSTARS.2022.3220042.

[27] Vaithyasubramanian S, Saravanan D, Kirubhashankar CK. Communal fraud detection algorithm for establishing identity thefts in online shopping. Int J E-Collab. 2021;17(3):75–84. doi: 10.4018/IJeC.2021070105.

[28] Hiruta T, Maki K, Kato T, Umeda Y. Unsupervised learning based diagnosis model for anomaly detection of motor bearing with current data. Procedia CIRP. 2021;98(2):336–41. doi: 10.1016/j.procir.2021.01.113.

[29] Deng C, Wu K, Wang B. Residential appliance detection using attention-based deep convolutional neural network. CSEE J Power Energy Syst. 2022;8(2):621–33. doi: 10.17775/CSEEJPES.2020.03450.