Electrical Engineering (2024) 106:5851–5867
https://doi.org/10.1007/s00202-024-02327-6

ORIGINAL PAPER

Anomaly detection in smart grid using a trace-based graph deep learning model

S. Ida Evangeline[1] · S. Darwin[2] · P. Peter Anandkumar[3] · M. Chithambara Thanu[4]

Received: 16 May 2023 / Accepted: 21 February 2024 / Published online: 22 March 2024

Abstract
Electricity plays a significant role in the everyday lives of people. Researchers have long been interested in the classification problem of electric power anomaly detection. Anomaly detection can stop little issues from snowballing into unmanageable issues. In addition, it helps cut down on energy waste. Existing anomaly detection models mostly ignore the spatial attribute of electricity consumption data. They would primarily emphasize the time series information contained within the energy consumption data. Furthermore, the trace has the ability to precisely reconstruct consumer pathways; the smart grid can thus use it to detect anomalies. To fill this research gap, we propose a trace-based graph deep learning model to detect anomalous consumers in the smart grid. An unsupervised encoder–decoder is used in the proposed model. First, our model combines traces using an efficient unified graph representation and provides quality scores. Then, the long short-term memory network extracts the temporal attributes, while the graph neural network extracts the spatial attributes. Finally, it computes the anomaly score by adding two hyper-parameters with two-part loss values. We conducted experiments on power consumption data that was gathered from an open-source dataset. The proposed model performs better than a range of standard anomaly detection models. The F1-score of our model is 94.60%, and the AUC is 98.90%. Experiments show that our model is stable even in extreme data imbalance.

Keywords Anomaly detection · Energy consumption · Spatio-temporal learning · Graph neural network

1 Introduction

Both technical and non-technical losses of electric energy occur at the transmission and distribution levels of the power grid [1, 2]. Estimating the technical loss is typically necessary for estimating the non-technical loss [3, 4]. Technical losses occur in the dielectrics and predominantly in conductors through Joule's effect [5]. They are naturally occurring losses resulting from unavoidable electric energy dissipation in the equipment that is required to implement transmission and distribution. Non-technical losses are non-natural losses, which are known as commercial losses in the literature. They are related to the quantity of unbilled and unpaid electric power. Either errors in billing or smart meter, or anomalous consumer behaviour, are the causes of unbilled electric power [6]. Anomalous behaviours, such as the unauthorized use of electric energy by the consumer, are non-legitimate activity, i.e., organized crime, corruption, and institutionalized theft [6]. And legitimate consumers pay the bills for non-technical losses.

In under-developing and developing countries, the public fund is used for providing electricity to economically disadvantaged demography or geography. For this service, additional funds are required. As a direct consequence of this, non-technical losses lead to increased costs for state government, legitimate consumers, and power corporations

✉ S. Ida Evangeline
ida.fragi@gmail.com

[1] Department of Electrical and Electronics Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi, Sivaganga District, Tamilnadu 630 003, India

[2] Department of Electronics and Communication Engineering, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, Thoothukudi District, Tamilnadu 628 215, India

[3] Department of Mechanical Engineering, VV College of Engineering, Tisaiyanvilai, Tirunelveli District, Tamilnadu 627 657, India

[4] Department of Mechanical Engineering, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, Thoothukudi District, Tamilnadu 628 215, India

[7]. Thus, the developing economies or economies in transition are in fragile environments and feel the negative impact of non-technical losses. The amount of electrical theft is stunning. For example, in India, annual electric power loss exceeds 1.2% of the gross domestic product [8]. Non-technical losses in Jamaica count for 18% of the fuel expenditure, totalling US $46 million annually [9]. Non-technical loss, in general, is prone to have a negative impact on the economy that is already unstable. Developed nations also face negative impact from non-technical loss. Hence, it is thought that the current non-technical losses require a practical cure. In the USA, electric power theft is estimated to cost $6 billion annually [10]. In the UK, it is £173 million annually [10]. In Europe, advanced meters are being deployed. In order to reap its benefits, it is essential to reduce non-technical losses [11].

Smart grid aims to optimize the entire electricity supply chain [12], enable intelligent integration [13], allow stable distributed generation [14], form strong engagement of consumers [15], and perform efficient transmission to promote sustainability-minded behaviour [16]. The smart meter is different from conventional meter because it has more advanced processing and communication capability, which enables them to collect high-resolution electric power consumption data to provide better consumer service in sectors, such as demand side management and automatic efficient control of appliances. The rapid implementation of smart meters in the smart grid increases the attack space on power grids and creates software-related vulnerabilities in meters. Cyber-attack has the capacity to compromise utility system's operation [17], disconnect consumer by remote action, deliver fraudulent readings to utilities, and manipulate meter software [18]. To develop effective methods to deal with non-technical losses, industry and academia pay more attention to the detection of non-technical losses. These methods may employ statistical analysis for making appropriate amendment to energy policies and capturing the primary drivers of fraudulent activity.

Other methods may employ intelligence algorithms to analyze consumption patterns and study the data collected from the smart meter that could reveal the presence of fraudulent behaviour. In order to detect and reduce non-technical losses, researchers have also proposed grid structures and equipment configurations. In this paper, a trace-based graph deep-learning model is proposed for anomaly detection in the smart grid. The following are some of the main features of our model. First, a trace quality graph is devised to integrate multiple anomaly factors and to represent consumer request. Second, a graph neural network is developed to capture the spatial attributes of traces. Third, an $LSTM$ is employed to extract the typical pattern of smart meter attributes (i.e., consumption behaviour, duration, consumer id, and spatial cluster number). The following are the main contributions of this paper:

- We propose a trace-based graph deep learning model, which encodes all smart meter attributes and traces them into the graph. In a unified style, the graph integrates the attributes of energy consumption and its environment.
- The proposed model extracts spatial and temporal attributes of the smart meter attributes using the unified graph representation. This improves the ability of anomaly detection in smart grid.
- We employ $LSTM$ to extract the temporal attributes of the trace and GNN to extract the spatial attributes of the trace. The encoder-decoder combines both $LSTM$ and GNN

The rest of this paper is structured as follows: Sect. 2 describes the research works related to anomaly detection in smart grid. Section 3 demonstrates the proposed trace-based graph deep learning model. Section 4 defines the dataset and its preprocessing. Section 5 details the experiment and declares the results. Section 6 draws the conclusion and discloses future research directions.

2 Relevant research

In recent years, researchers have been more interested in detecting anomaly in energy consumption data. For this detection, they have developed a wide range of detection models. These detection models can be distributed into three types: statistical models, machine learning models, and deep learning models. Researchers established a few statistical models for anomaly detection. Serrano-Guerrero et al. [19] presented a statistical method to evaluate changes in a facility consumption profile using patterns of electric power consumption that were taken from a historical database. However, the collection of historical data and the development of clusters require considerable effort. Serrano-Guerrero et al. [20] developed a method to handle time-series components, which significantly enhances the capability for obtaining patterns and detecting anomalies in electric power consumption profiles. This method has a drawback that the size of confidence intervals of the consumption patterns must be balanced. Because a narrow confidence interval may erroneously identify normal consumptions as abnormal, whereas a broader confidence interval may encounter difficulties in detecting abnormal consumption patterns. Kozitsin et al. [21] coded an auto-regression integrated moving average value method for solving anomaly detection problem and energy forecasting problem. Nevertheless, this algorithm exhibits variability and lacks robustness when confronted with the data. Wang and Ahn [22] constructed a framework for detecting anomalies in household electrical loads that combines a ruler-machine-based load anomaly detector with a one-step-ahead load predictor. The framework uses the k-nearest neighbors (kNN) to create a novel independent detection process. The experiments were carried out using data that was gathered from a rural region in East Africa. The power consumption patterns were relatively simple. This anomaly detection system was not applied in dense residential regions to test various power consumption patterns for a more general application. To enhance the anomaly detection performance of this system, it is imperative to employ more advanced approaches.

In addition to statistical models, researchers also widely used some machine learning models in energy consumption anomaly detection. Rashid and Singh [23] presented an approach known as Monitor. First, it identifies behaviour patterns present in previous consumption data. It then employs these patterns to detect abnormalities in residential energy consumption. The approach was validated using a dataset consisting of 16 weeks of smart meter data collected from real-world buildings. As only one case study was examined, this method cannot be generalized. Punmiya and Choe [24] focused on the features of engineering-based pre-processing to enhance detection performance while also reducing the time complexity. They detected energy theft with the help of a new gradient-boost theft detector. In this detection method, the classifier consists of LightGBM, CatBoost, and XGBoost. As a result, this method takes more time for computing the abnormal consumers. Amara Korba and Karabadji [25] detected energy fraud in advanced metering infrastructure using a machine learning-based method. Using a support vector machine (SVM), they used the predictability of the customer consumption profile to identify fraudulent activity. This method has high false positive rates and poor detection rates when there are more consumers in a dataset. Zhang et al. [26] built a new adaptive method to detect abnormal data from smart meters. The support vector machine with particle swarm optimization, clustering feature learning, linear discriminant analysis, and Gaussian mixture model are all used in this method. Nevertheless, there exists a degree of deviation in the power consumption behaviour analysis. Hence, it is imperative to make suitable modifications or enhancements for practical application. Cody et al. [27] presented an effective decision tree learning method for the detection of fraudulent activity from the profile of energy consumption behaviour. This method has low detection rates. Preprocessing techniques like feature extraction algorithm is required to better accurately detect future energy consumption values. Additionally, the method was not compared with other machine learning methods to assess its advantages and disadvantages. Kammerer et al. [28] described anomaly detections for manufacturing systems based on sensor data. They developed an isolation forest (IF) model to detect sensor data anomalies. Nevertheless, advanced strategies are still required to better deal with the production machines, sensors, and different settings. Atemkeng et al. [29] devised a label-assisted autoencoder in order to detect the anomalies of fuel consumption in power-generating plants. This method needs the feature importance analysis for the purpose of choosing the best reconstruction error. To address this issue, different autoencoder variants, such as memory-augmented autoencoders and long short-term memory autoencoders are needed. Touzani et al. [30] designed a gradient-boosting machine algorithm and introduced a machine-learning-based model to predict energy consumption in commercial buildings. Although the model may deliver better results, users might experience difficulties when using this unfamiliar model.

With the ongoing advancement of deep learning, researchers have presented several deep learning models for anomaly detection in energy consumption. Bontemps et al. [31] developed an anomaly detection system. This system is based on neural network learning. They explored temporal dynamic behaviours and analyzed time series data. However, differences in the number of inputs in an LSTM RNN may trigger different output responses. This reduces the classification accuracy of the model. da Silva et al. [32] constructed a negative selection technique based on a long short-term memory model, which provides useful information for energy efficiency and anticipates the anomalies occurrence in power consumption. The LSTM parameters were not fine-tuned to enhance the prediction of the consumption. Hence, the model does not perform well when there is a much lower or very high power consumption than expected. Wang et al. [33] created a Long Short-Term Memory model for anomaly detection and power consumption prediction. However, the accuracy of prediction and anomaly detection was suboptimal. Hollingsworth et al. [34] employed a recurrent neural network model to perform power anomaly detection. The model can remove trend and seasonality from data and produce residual value that can be compared to those from predictive analysis. The performance of the model on meters from a bigger region was not tested. Although the model delivers high accuracy, it is crucial to additionally identify more anomalies; as a result, the performance of the model is not good in terms of its true positive rate.

Fenza et al. [35] focused on the necessity to create anomaly detection methods that could deal with drift concept, such as a home becoming a second home or family structure changes. These authors adopted a long short-term memory network to forecast and analyze the behaviour of the consumer by examining his recent past consumptions. Nevertheless, there is a longer delay between the anomaly and its detection. It takes a few hours. It has an impact on the performance of the approach. Ali et al. [36] detected the outliers or anomalies from the data using the Cluster-Based Local Outlier Factor (CBLOF) algorithm. The experimental results indicated that the algorithm successfully detected the anomalies with the highest percentage. However, this algorithm requires a large number of execution steps for the large data sets. Kong et al. [37] developed a spatio-temporal learning-based anomaly detection (ADJST) model for building electricity consumption data. They demonstrated the performance of the method using a real-world dataset that contains three years of electricity consumption data from a Chinese university. However, it is imperative to enhance the model in order to improve its capability in detecting anomalous consumers. The existing models mostly concentrate on the temporal attributes of the energy consumption data. Yet, along with temporal attributes, spatial attributes can also play a significant role in anomaly detection from energy consumption data. In light of this, we propose a trace-based graph deep learning model for anomaly detection in the smart grid.

3 Graph neural network

This network is frequently employed in traffic prediction, fraud detection, and recommendation systems. It is a well-known deep-learning method for graph data. In addition, it produces promising solutions with various types of graph data. The graph neural networks are classified into three types, according to the survey [38]. They are spatial–temporal graph neural network, graph autoencoder-based recurrent graph neural network, and convolutional graph neural network. We employ the graph autoencoder in the proposed model to extract the attributes of power consumption [39]. The process of our model is explained in this section.

3.1 Overview

The process of the proposed model has several steps. The overview of the model is shown in Fig. 1. The workflow of the model is shown in Fig. 2. The entire electric power distribution network is considered as an undirected graph G [39]. In this graph, E denotes the relationships in the power distribution network, and V is the power distribution network.

The consumption pattern and trace smart meter attributes are transformed into a Trace Quality Graph (TQG) on the basis of the above assumption. Based on their timestamp, an attribute matrix and an adjacency matrix are processed, as shown in Fig. 3 [39].

The structural attributes of all traces are integrated into a one-dimensional vector vec in order to differentiate the types of consumer behaviours. The consumption behaviour i is accessed in the trace when the subscript value i in vec_i is 1. In other words, if there is an abnormal consumption, its value is1; otherwise, it is 0. For example, as Fig. 3 invocates different consumption patterns (SM^1, SM^2, SM^3, SM^N), the trace is encoded as shown in the adjacency matrix. When the model detects abnormal consumption, the corresponding cells are labeled as 1; otherwise, its value is 0. Then, the Euclidean distance is calculated between two vec to determine how structurally similar two traces are [39]. Based on k-means clustering results, all traces are classified into different categories. To detect electric power anomalies, all categories train the model. The consumption patterns not demanded in this trace type (isolated nodes) are eliminated from TQG in accordance with the attributes of each type, which could improve the stability and lower the computing complexity of the model [39]. The clustering DBSCAN [40] is employed to remove outliers while taking into account any potential noise in the training dataset. The unsupervised joint learning framework is used in our anomaly detection model. The modules that make up our model are the $LSTM$ autoencoder ($LSTM : AE$) [41] and the variational graph autoencoder ($VGAE$) [42]. Our model is able to detect both anomalies of trace consumption path as well as consumption time since it computes the anomaly score by combining the loss values of two modules.

3.2 Data integration and processing

Electric power consumption behaviour contains many data types that show how well the power distribution system is operating. We choose the smart meter attributes such as consumption, duration, customer id, and spatial cluster number for the consumptions and the trace data to create TQG, as shown in Fig. 3. The attribute matrix and the adjacency matrix are the components that make up the TQG. We create the TQG using the following three stages for the given trace.

Stage 1 Collect smart meter attributes

There could be hundreds or thousands of consumption behaviours in a power distribution system. Each consumption behaviour has a greater number of instances. We gather and keep the smart meter attributes in the temporal database for each instance.

Stage 2 Construct topology graph

We use the $spanid$ and its $parentid$ to create the adjacency matrix for all trace spans. In the attribute matrix, the invocation times are then entered for each span.

Stage 3 Connect traces and smart meter attributes

Based on the instance name and timestamp, the model explores the attributes of the consumption behaviours in the temporal database for all the spans of the trace. We can calculate the consumption times of the consumption behaviours as the average of all consumptions if it happens several times during a trace. In addition to providing operators with additional information about consumer behaviours, the unified graph representation uses the graph neural network to extract the topological attributes between electric power consumption behaviours. Considering that $x_i \in X$ represents the attribute matrix and $a_i \in A$ represents the adjacency matrix; we execute the sequence of trace $T_{\text{set}} = \{t_1, t_2, \ldots, t_n\}$ to

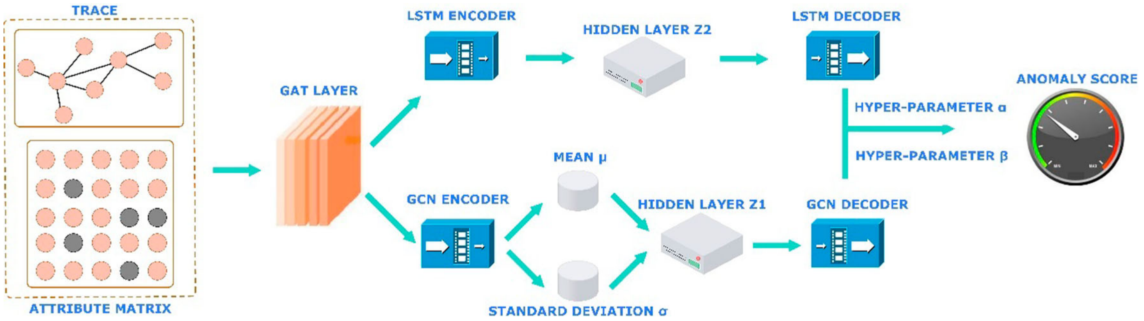


Fig. 1 Overview of proposed anomaly detection network structure

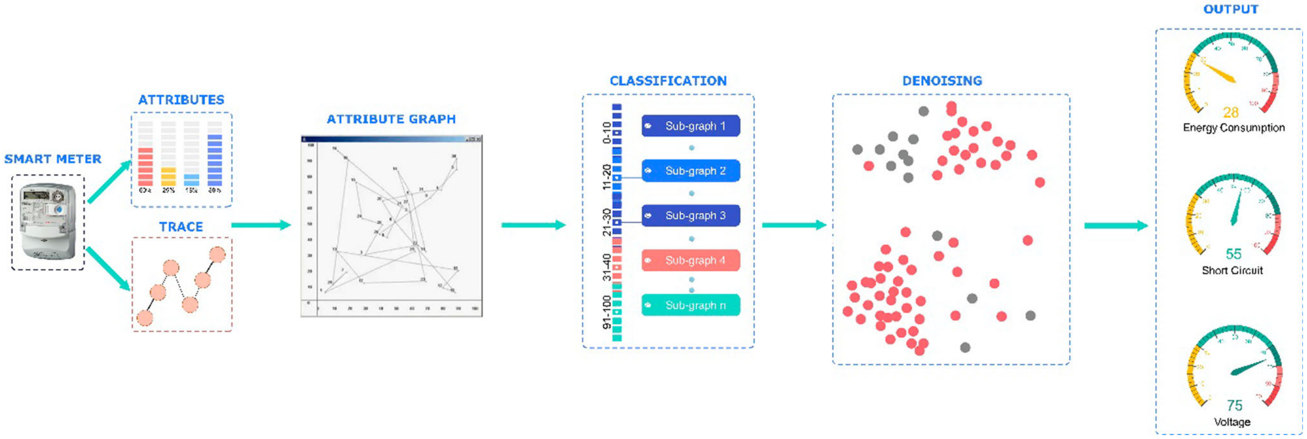


Fig. 2 Workflow of the proposed model

$A = \{a_1, a_2, \ldots, a_n\}$ and $X = \{x_1, x_2, \ldots, x_n\}$. To make sure that the graph convolutional network has the capability to integrate the node attributes, we augment the adjacency matrix with the identity matrix I. Finally, we normalize the adjacency matrix symmetrically in the following manner.

$$A = A + I, \tag{1}$$

$$\widetilde{A} = D^{-\frac{1}{2}} A D^{-\frac{1}{2}}, \tag{2}$$

In the above equations, $\widetilde{A}$ represents the normalized adjacency matrix, D represents the degree matrix A, and A represents the adjacency matrix. The min–max normalization is applied to the attribute matrix for each attribute.

3.3 VGAE module

To capture the spatial attributes of the TQG, our model uses $VGAE$ module. According to the Variational Auto-Encoder (VAE), the $VGAE$ draws the graph structure. The VAE has the encoder, which consists of h_1 and h_2 (two-layer GCN) [39]. It encodes the attribute and adjacency trace matrices into the hidden layer Z_1. This process is defined as follows:

$$h_1 = \widetilde{A} X W_1, \tag{3}$$

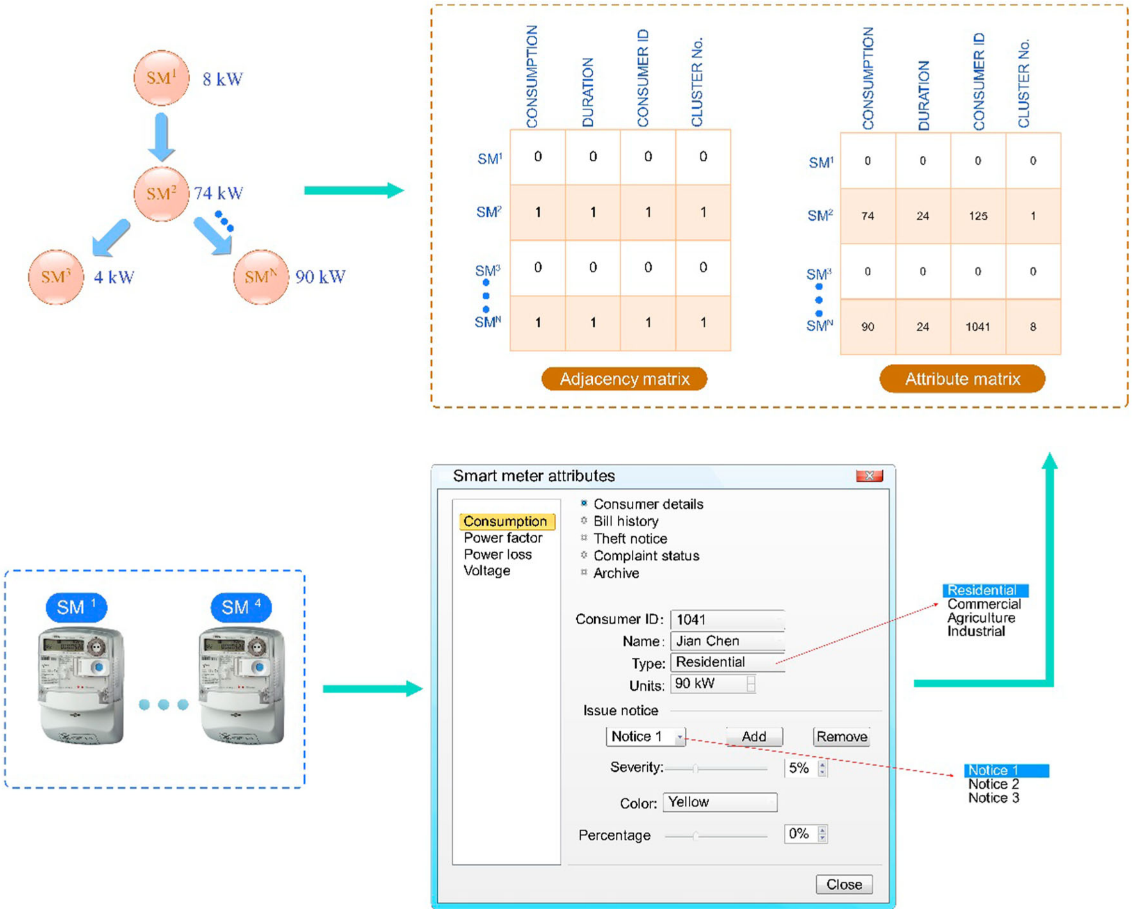
$$h_2 = \widetilde{A}\mathrm{ReLU}(h_1) W_2, \tag{4}$$

$$Z_1 = \mu_1 + \varepsilon * \sigma_1 \tag{5}$$

In the above equations, σ_1 represents the standard deviation of approximate posterior, μ_1 represents the mean of approximate posterior. Both are the outputs of h_2. ε is a normally distributed random number ranging between 0 and 1. W_1 and W_2 are the weight metrics. ReLU($\cdot$) is the activation function. Please note that the parameters of the hidden layer Z_1 are ε, σ_1, and μ_1. The decoder part reconstructs the original adjacency matrix $\widehat{A}$ using the inner product between latent variables. This adjacency matrix $\widehat{A}$ is defined as follows:

$$\widehat{A} = f\left(Z_1 Z_1^T\right), \tag{6}$$

In the above equation, $f(\cdot)$ is the sigmoid function. The incurred loss between the reconstructed and real adjacency



	CONSUMPTION	DURATION	CONSUMER ID	CLUSTER No.
SM¹	0	0	0	0
SM²	1	1	1	1
SM³	0	0	0	0
SMᴺ	1	1	1	1

Adjacency matrix

	CONSUMPTION	DURATION	CONSUMER ID	CLUSTER No.
SM¹	0	0	0	0
SM²	74	24	125	1
SM³	0	0	0	0
SMᴺ	90	24	1041	8

Attribute matrix

Smart meter attributes

Consumption
Power factor
Power loss
Voltage

● Consumer details
○ Bill history
○ Theft notice
○ Complaint status
○ Archive

Consumer ID: 1041
Name: Jian Chen
Type: Residential
Units: 90 kW

Issue notice
Notice 1 Add Remove
Severity: 5%
Color: Yellow
Percentage 0%

Close

Residential
Commercial
Agriculture
Industrial

Notice 1
Notice 2
Notice 3

Fig. 3 Illustration of trace quality graph

matrices $\left(\widehat{A},\, A\right)$, is minimized for training the $VGAE$.

$$\text{Minimize} = \text{Loss}\left(\widehat{A},\, A\right) \tag{7}$$

The first GCN layer of $VGAE$ is changed with the GAT layer [43] because the consumption time in traces propagates the faults [44]. In the attributed graph, the relationships between the nodes can be defined. For each node i, the representation s_i are extracted as follows:

$$s_i = f\left(\sum_{j=1}^{K} \alpha_{ij} W v_j\right), \tag{8}$$

The attention coefficient α_{ij} is computed as follows:

$$\alpha_{ij} = \frac{\exp\left(\text{LeakyReLU}\left(\vec{a}^{T}\left[W v_i \| W v_j\right]\right)\right)}{\sum_{k=1}^{k} \exp\left(\text{LeakyReLU}\left(\vec{a}^{T}\left[W v_i \| W v_j\right]\right)\right)} \tag{9}$$

In this equation, K is the number of adjacent nodes, v_i is the node attributes, LeakyReLU$(\cdot)$ is the activation function, $\vec{a}\,\epsilon\mathbb{R}^{2F}$ and $W\epsilon\mathbb{R}^{F'\times F}$ are learnable parameters.

3.4 LSTM: AE module

$LSTM$ Network solves the shortage of short-term memory of the recurrent neural network (RNN). It is a well-known method in time series data. The memory cell is the special unit of $LSTM$ that contains the forget gate (f_t), input (i_t), and output (o_t) [39]. The memory cell uses the status (c_t) and output (r_t) to produce the information. The computation is formulated as follows:

$$f_t = \text{sigmoid}\left(W_f \cdot \left[r_{t-1},\, X_t\right] + b_f\right) \tag{10}$$

$$i_t = \text{sigmoid}\left(W_i \cdot \left[r_{t-1},\, X_t\right] + b_i\right) \tag{11}$$

$$o_t = \text{sigmoid}\left(W_o \cdot \left[r_{t-1},\, X_t\right] + b_o\right) \tag{12}$$

$$c_t = f_t * c_{t-1} + i_t * \left(\tanh\left(W_c \cdot \left[r_{t-1},\, X_t\right] + b_c\right)\right) \tag{13}$$

$$r_t = o_t * \tanh(c_t) \tag{14}$$

In the above equations, b_c, b_o, b_i, b_f are the biases of c_t, o_t, i_t, f_t, respectively. W_c, W_o, W_i, W_f are the weights of c_t, o_t, i_t, f_t, respectively. The smart meter attributes and electric power consumption behaviours are time-series data. We apply the GAT output as the $LSTM : AE$ module input because of the spatial dependence on the attributes between various nodes. Furthermore, the proposed model encodes the $MLPX_t$ output to the hidden layer Z_2 using the multi-layer $LSTM$ network. In addition, the proposed model reduces the consumption attribute dimensions using the multi-layer perception (MLP). The decoder relates Z_2 to reconstruct the attributes $\widehat{X}$ of consumption behaviours. This decoder is made up of a MLP and a single-layer $LSTM$.

3.5 Joint optimization

The variational lower bound $\mathcal{L}(\theta, \phi; x)$ is minimized to train the $VGAE$ module [39].

$$L_{\mathrm{VGAE}} = \mathcal{L}(\theta, \phi; x) = -D_{KL}\left(q_{\phi}(Z_1|X, A) \,\|\, p_{\theta}(Z_1)\right) + \mathbb{E}_{q\phi(Z_1|X,A)}\left[\log\left(p_{\theta}(A|Z_1)\right)\right], \quad (15)$$

The above equation has two parts. The first part computes the distance between two distributions. It is known as the Kullback–Leibler divergence. The second part represents the reconstruction probability of the input. The L_{VGAE} specifies the $VGAE$ loss function. Mean squared error (MSE) is the square of the difference between the reconstructed attribute matrix $\widehat{X}$ and the attribute matrix X. The MSE is introduced as the loss function in the $LSTM : AE$ module. We apply different weightages to the corresponding reconstructed losses to differentiate the relative importance of different attributes.

Compared to other smart meter attributes, the consumption time is severely penalized due to this differentiation. In the end, the final loss is obtained by linearly summing up the two-part loss. For this summation, two hyperparameters α and β are set.

$$L_{\mathrm{LSTM-AE}} = \|\widehat{X} - X\|^2 \quad (16)$$

$$L_{\mathrm{TraceGra}} = \alpha * L_{\mathrm{VGAE}} + \beta * L_{\mathrm{LSTM-AE}} \quad (17)$$

In the above equations, L_{TraceGra} represents the total loss function, and $L_{\mathrm{LSTM-AE}}$ represents the loss function of $LSTM : AE$ module.

3.6 Model training

Based on the k-means results, we split the training data into several classes. All classes are used to train the model. There is a similar sequence in the workflow process of power consumption behaviours in the power distribution network [45]. The model receives the online data as input. Based on the Euclidean distance calculation, the model performs anomaly detection. The structure of the proposed model has two modules. In each epoch, we optimize the model parameters using the Adam optimizer. In multi-task learning, the multi-loss optimization problem has different magnitude levels [46]. Similarly, the two modules of the model produce losses which have different magnitude levels. This gave us the idea to balance the loss gap between the two modules by establishing two hyper-parameters α and β. Hence, the training gradients for the two modules are roughly equivalent. Furthermore, we assign the threshold γ as $\mu + 3\sigma$, in which σ is the standard deviation, and μ is the mean of historical residuals. For each trace, we calculate the anomaly score after computing the final loss value. The label' anomaly' will be applied to a trace if its anomaly score is greater than γ. In the training set, we compute the standard deviation and mean of the loss after setting the time window. The threshold is dynamically updated as the training dataset is updated.

3.7 Dataset preparation

Figure 4 shows a sample network topology, which consists of three main components: the smart meters, data aggregator, and data management system [47]. The network provides remote control of smart meter, two-way data communication, and gathers information about electricity consumption from the consumer's home [48]. The data that has been gathered will thereafter be transmitted to the data aggregator specific to that region via the utilization of a network area network (NAN) [49]. Lastly, the data reaches the data management system using WAN technology. The data aggregator serves as an intermediary between the data management system and smart meters [50]. The dataset used in this study was derived from real-world applications. The State Grid Corporation of China (SGCC) [51] provides this dataset (http://www.sgcc.com.cn/). The dataset comprises 42372 rows, which means that 42372 individual consumers are considered. This dataset is partitioned into ten clusters using k-means clustering, each cluster representing a distinct spatial region. Smart meters collect electricity consumption data. Hence, there are 42,372 smart meters used for data collection. In the dataset, rows reflect the electric power consumption of a consumer from 01.01.2014 to 31.10.2016. It is a period of 34 months, which is exactly 1035 days. The dataset is structured as time-series data, which are collected every 24 h. Hence, there are, in total 43,855,020 events. Each consumer has a unique household ID. The consumption volume of each consumer is recorded against their household ID, along with the date. Consumptions are labeled as '1' for abnormal consumptions

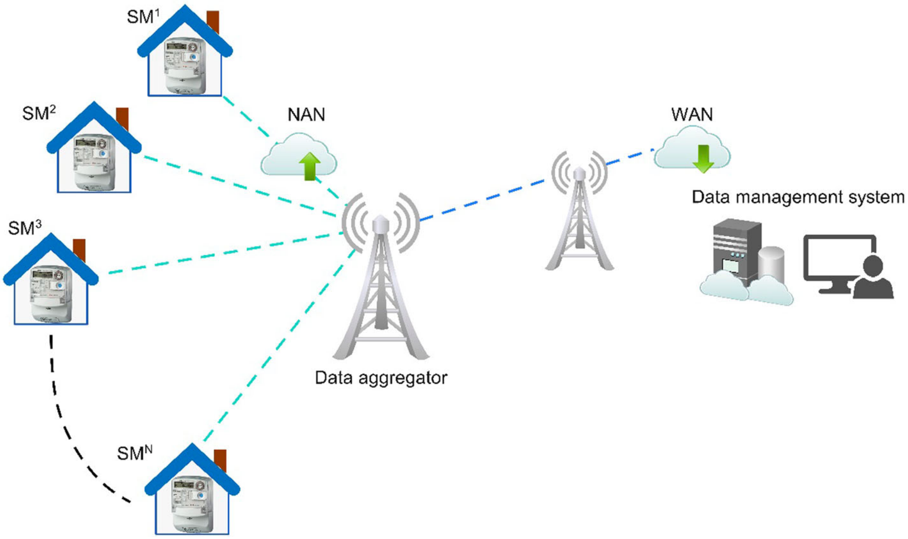


Fig. 4 Smart meter network topology

(for example, short circuit, overload, electricity theft) and a ‘0’ for normal consumptions [37].

3.8 Missing value imputation

The smart meter, or data transmission server, may fail to store a few data, and therefore, the electricity consumption statistics may contain missing data. How to fill out the missing data is, therefore, an important issue. Traditional methods such as linear filling and mean filling are generally used for missing value imputation in the dataset. They require little calculation and are simple to apply [37]. When we apply these filling methods, the model may become underfit during the training process. Hence, we cannot achieve the expected detection effect. Thus, we do not use them in this paper. Instead, to deal with missing data, we therefore use the short interval selection method [52]. There are two types of intervals, namely, long interval and short interval. The concept behind this method is that when compared to long intervals, the short interval produces more accurate missing data estimation. We, therefore, prefer short interval-based missing value imputation compared to long interval-based one. The short interval method is expressed by using the Bayes theorem [52], which states that

$$p(y|x_1, \ldots, x_n) = \frac{p(y)p(x_1|y)p(x_2|y)p(x_n|y)}{p(x_1)p(x_2)\cdots p(x_n)} \tag{18}$$

We could rewrite it as follows

$$p(y|x_1, \cdots x_n) = \frac{p(y)\prod_{i=1}^{n} p(x_i|y)}{p(x_1)p(x_2)\cdots p(x_n)} \tag{19}$$

Table 1 Notations for missing value imputation

Notation	Description
Q^{imputed}	Imputed value
P^{true}	True value
p	Probability
X	short interval length
Y	long interval length
T	correct imputation case
F	incorrect imputation case

We can remove the denominator term when it is constant for a particular input.

$$p(y|x_1, \cdots x_n) \propto p(y)\prod_{i=1}^{n} p(x_i|y) \tag{20}$$

The imputed value $\left(Q^{\text{imputed}}\right)$ replaces the missing value. We have the true value (P^{true}) for the missing value, which determines the accuracy of the imputed value (Q^{imputed}). In order to compare the effectiveness of the missing value, which has to be imputed to the true value, the effectiveness of (Q^{imputed}) is examined. The short (X) and long (Y) intervals are used to accomplish the performance analysis. The notations used for missing value imputation are described in Table 1.

In the incorrect imputation case, the imputed values are outside of the acceptable range. That is, with a higher error degree. T/F indicates that the imputed value is inside the permitted range, even though it does not exactly match the true value. For example, one downward ($P^{\text{true}} - 1$) or one upward ($P^{\text{true}} + 1$) values. F/T indicates that the imputed values are closer to either the lower or upper bound of the range, and it is obvious that they are outside the permitted

Table 2 Different possible results for missing value imputation

F	T	F/T	T/F
$(X-9)/X$	$1/X$	$4/X$	$4/X$

Table 3 Calculated values based on the Naive Bayes theorem

Accepted	Rejected
$9/X$	$(X-9)/X$

range. This case represents the imputation with a medium error degree. Please note that we can use the characteristic of specific data to adjust the above-mentioned acceptable range. In this paper, we consider the acceptable ranges as follows: $P^{\text{true}}-1$, $P^{\text{true}}-2$, P^{true}, $P^{\text{true}}+1$, $P^{\text{true}}+2$. The T probability is $1/X$, when Q^{imputed} is similar to the true value (P^{true}). Moreover, T/F probability is $4/X$. The possibility of deviating from the true value is $P^{\text{true}}+2$, or $P^{\text{true}}-2$. As stated in Table 2 [52], the F/T probability is $4/X$ and the F probability is $(X-9)/X$.

The conditions F/T, T/F, T are satisfied when an imputed value is inside the permitted range ($P^{\text{observed}}+2$, $P^{true}-2$). Else, condition F is satisfied. This denotes that compared to the short interval; the long interval has more potential to satisfy the F condition. The probability of selecting Q^{imputed} is decreasing as the imputation value range is increased and vice versa. Compared to the long interval, the short interval has more potential to impute the value in a permitted range or impute the exact true value. The probability of the rejected or accepted imputed value is shown in Table 3 [52].

Based on short or long intervals, the probability for obtaining the correct imputed values inside the permitted range can be calculated using the following formula.

$$P(\text{imputedvalue} \in \text{acceptablerange}) = p^{T} + p^{TF} + p^{FT} \tag{21}$$

The following equation can be derived from Eq. (21),

$$P(\text{imputedvalue} \in \text{acceptablerange}) \propto 9/X \tag{22}$$

From the aforementioned equation, it is inferred that the imputed values range is indirectly proportional to the probability of obtaining the correct imputed value [52]. In other words, the probability will be more when the denominator has a smaller value. Obtaining the imputed probability value inside the permitted range is decreased when a Y length (long interval) replaces a X length (short interval), as indicated in Eq. (22).

$$P(\text{imputedvalue} \in \text{acceptablerange}) \propto 9/Y \tag{23}$$

Figure 5 shows power consumption graphs of the consumer id 41675 before and after the missing value imputation.

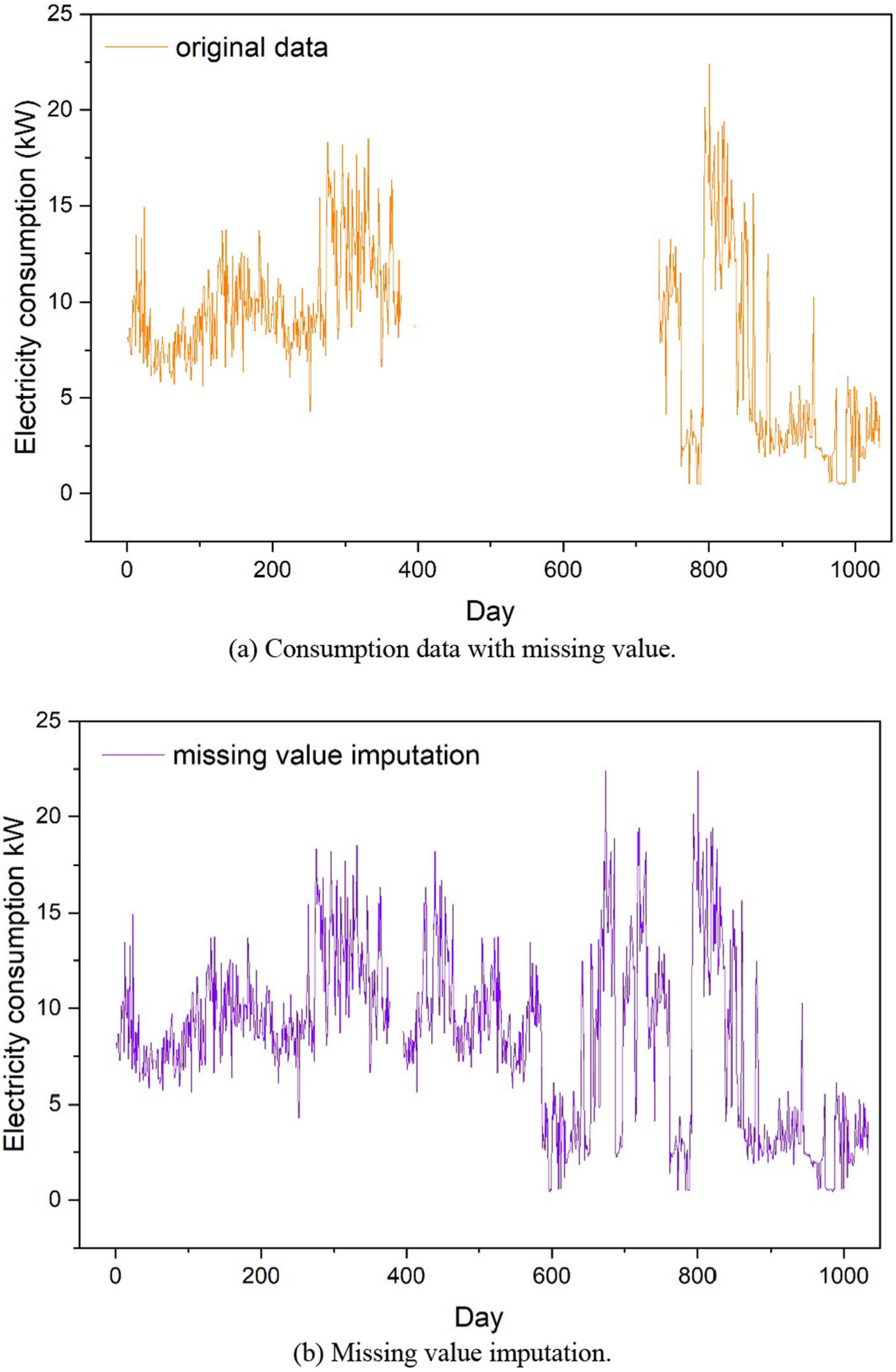
3.9 Oversample method

An abnormal consumer will be identified if there is one occurrence of abnormal power consumption. There were 3615 abnormal consumers and 38757 normal consumers, among the total 42372 consumers. That is, 8.53% of consumers are abnormal. There are more than ten times as many normal consumers as abnormal ones, as can be seen. As a result, we must deal with the class imbalance issue when thinking about solutions to the problem of electricity anomaly detection. Extreme data imbalance is a challenge in anomaly detection. The model is unable to capture discriminative attributes due to the scarcity of abnormal data. In this paper, we use the convex hull-based synthetic minority oversample technique (CHSMOTE) method [53] to tackle the unbalanced class issue in the electric power consumption dataset. To increase the abnormal samples, this method oversamples the abnormal consumption data in the original sample set. There are three steps in the CHSMOTE method. Initial minority sample selection is the first step [37]. Sample synthesis area identification is the second step, and oversampling is the third step [53].

Step 1 Initial minority sample selection.

In this first step, the method randomly selects initial minority samples. The classifier precisely divides the minority and majority classes using the decision boundary (line 1 of Algorithm 1). When boundary samples in various classes are nearby to each other around the decision boundary, they are more likely to be misclassified [54, 55]. Thus, the classifier should pay them more attention [56]. Furthermore, samples located distant from the decision boundary contribute relatively insignificantly to classification because they may provide less effective information (lines 2 to 5 of Algorithm 1). The method concentrates on the boundary samples as a result of the above fact [53]. In other words, this method only selects the boundary minority data as initial data for oversampling. To be more specific, it divides the imbalanced dataset into two datasets: data from minority class are collected to form a minority dataset T_{min} and data from the majority class are collected to form the majority dataset T_{maj}. For each minority sample (x_i), the method obtains the k nearest neighbour from T_{maj}. Without duplication, the boundary majority dataset T_{bmaj} is added with the k nearest majority neighbours (lines 6 to 10 of Algorithm 1). For your kind information, when two or more minority data belong to the k nearest majority neighbours, the method extracts them only

Fig. 5 Consumption data before and after missing value imputation



(a) Consumption data with missing value.

(b) Missing value imputation.

once. The data in T_{bmaj} could have a negative impact on the minority data as they are viewed as a potential critical majority data. Furthermore, for each data in T_{bmaj}, the method obtains the k nearest minority neighbours. Without duplication, the boundary minority dataset T_{bmin} is included them. Finally, the method generates synthetic data by selecting the data from T_{bmin} as the initial minority data [57]. Algorithm 1 details the process of selecting T_{bmin} [53].

Step 2: Identification of sample synthesis area.

CHSMOTE does not consider the spatial distribution of the sample. It considers the line segment between two samples and creates synthetic data (lines 1 to 3 of Algorithm 2). Constructing the convex hulls is an ideal solution (line 4 of Algorithm 2). It considers different nearest minority samples and reflects the local spatial distribution (lines 5 to 8 of Algorithm 2). From line segments, it extends the synthetic sample generation range to spatial geometric areas [58] (lines 10 to

12 of Algorithm 2). Algorithm 2 explains the identification of sample synthesis area [53].

Step 3 Oversampling of minority samples.

The method explores the sample synthesis area, and it creates a new minority sample. By using the constructed convex hull $CH(x_i, x_i^1, x_i^2)$, it determines the new minority sample X_{new} as follows.

$$X_{\text{new}} = \lambda_1 X_i + \lambda_2 X_i^1 + \lambda_3 X_i^2 \tag{24}$$

In the above equation, λ_1, λ_2, λ_3 are normally distributed random numbers ranging from $[0, 1]$. However, they must satisfy the condition $\sum_{i=1}^{3} \lambda_i = 1$ (line 2 of Algorithm 3). In the sample synthesis area, the method explores each of the convex hulls and capture at least $q = \left\lfloor \frac{|T_{\text{maj}}||T_{\text{min}}|}{N} \right\rfloor$ points (lines 3 to 5 of Algorithm 3). To balance the dataset, it becomes the new synthetic minority sample [59] (lines 6 to 8 of Algorithm 3). Here, N represents the number of convex hulls; $|T_{\text{maj}}|$ represents the total number of majority samples. Algorithm 3 details the oversampling process of CHSMOTE [53]. The process uses Eq. (24) and generates the new minority sample when the method does not achieve balanced class distribution. Until the balance is obtained, this process fills in the difference [60].

3.10 Normalization

When the data are not evenly distributed or when the attribute exhibits large variance, detection performance can be significantly reduced for the given dataset. Hence, we are normalizing the electric power consumption data with missing values to alleviate the dimension influence between different attributes. We can express the normalization process as follows:

$$Nx_j^i = \frac{x_j^i - x_{\text{min}}^i}{x_{\text{max}}^i - x_{\text{min}}^i} \tag{25}$$

In this equation, Nx_j^i is the normalized data of the i^{th} user, x_j^i is the original data of the i^{th} user. x_{min}^i is the minimum power consumption data of the i^{th} user, x_{max}^i is the maximum power consumption data of the i^{th} user.

4 Result and discussion

4.1 Performance metrics

We comprehensively assess the performance of the model using different performance metrics. We use the precision, recall, true positive rate (TPR), false positive rate (FPR), F_1 score, and area under the curve (AUC) to evaluate the model. In energy consumption, when the actual data is not abnormal, and the detection is not abnormal; it is the true negative (TN). When the actual data is abnormal, and the detection is normal, this particular type is the false negative (FN). When actual data is normal, but the detection is abnormal, this particular type is the false positive (FP). When the actual data is abnormal, and the detection is abnormal, it is the true positive (TP). With the help of TN, FN, FP, and TP, we can calculate the precision and recall rates using the following equations [37].

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{26}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{27}$$

The precision is the total abnormal data divided by the total true abnormal data. The recall is the actual number of abnormal data divided by the total number of existing abnormal data. We can calculate F_1 using the following equation.

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{28}$$

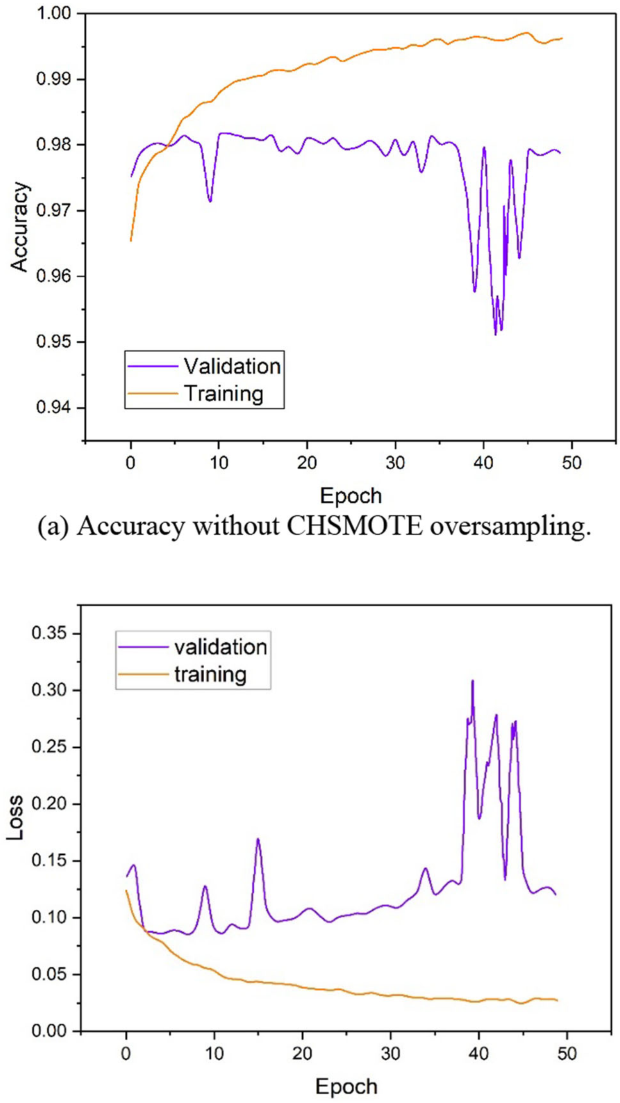
This F_1 value ranges from 0 to 1. The performance improves as the value increases. Moreover, we visually present the performance of tamper detection by plotting the ROC(receiver operator characteristic) curve. We plot this curve in a 2D graph, in which the ordinate is the TPR and the abscissa is the FPR. This curve clearly classifies abnormal consumers and normal consumers. Also, this curve reflects the classification capability of the detection model. The area size under this curve is the value of AUC. We choose AUC to evaluate the final test results as this performance metric has a specific value. AUC ranges from 0.5 to 1.0. The performance of the model improves with increasing AUC. We can calculate the TPR and FPR using the following formulas.

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{29}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{30}$$

In the above equations, FPR and TPR range from 0 to 1. The performance of the model improves as the FPR value decreases. And the performance of the model improves as the TPR value increases. The randomly selected negative sample is given less preference, and the randomly selected positive sample is given more preference. The probability of this statement is represented by the AUC value. We can calculate the AUC with the following equivalent formula:

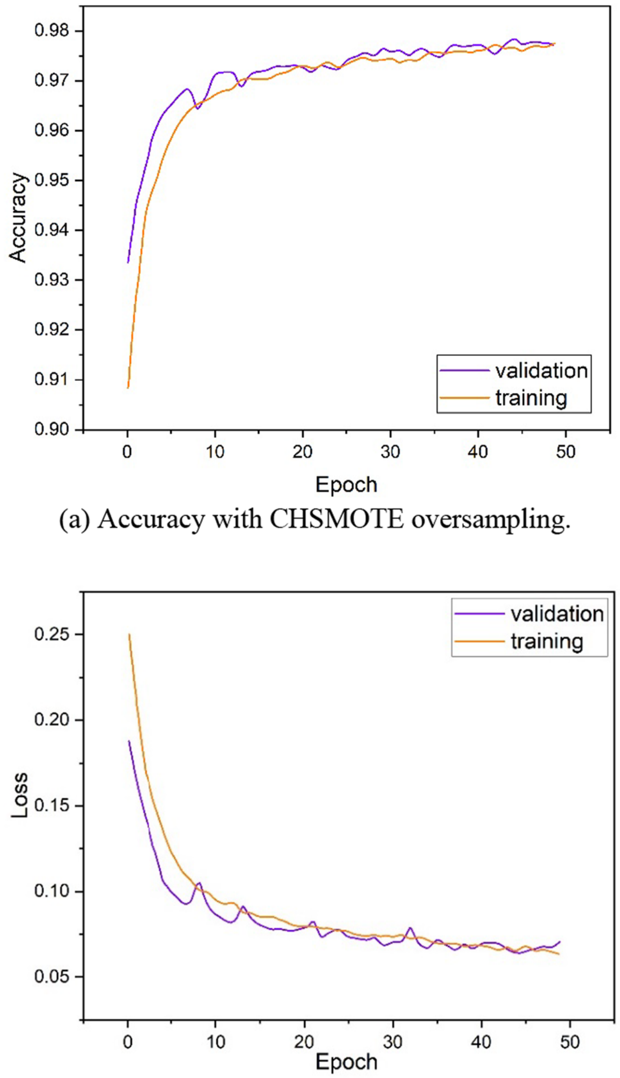
$$\text{AUC} = \frac{\sum_{i \in \text{positiveclass}} \text{rank}_i - \frac{M \times (M+1)}{2}}{M \times N} \tag{31}$$



(a) Accuracy without CHSMOTE oversampling.

(b) Loss without CHSMOTE oversampling.

Fig. 6 Analysis without $CHSMOTE$ oversampling



(a) Accuracy with CHSMOTE oversampling.

(b) Loss with CHSMOTE oversampling.

Fig. 7 Analysis with CHSMOTE oversampling

In the above equation, N is the number of negative samples, M is the number of positive samples, $\sum_{i \in \text{positiveclass}}$ is the addition of the positive sample serial number and rank_i is the i^{th} sample serial number.

4.2 CHSMOTE oversample analysis

We check the performance of the $CHSMOTE$ oversampling method [53], which produces the abnormal consumer sequence. We also check whether this method has a positive impact on the model training. To get trained, our model receives the preprocessed dataset [37]. We compare our model with and without $CHSMOTE$ oversampling step.

Figure 6 shows the results of the model without $CHSMOTE$ method, whereas Fig. 7 shows the results of the model with $CHSMOTE$ method. Without the $CHSMOTE$ method, the model oversamples the abnormal sequence, and it is unable to capture discriminative attributes, as can be seen in Fig. 6(b). Hence, the validation dataset is not converging while the training dataset is gradually converging. The fluctuation is also very significant. In addition to this, the model accuracy changes significantly, as shown in Fig. 6(a). Hence, when we add abnormal data to the dataset with the aid of the $CHSMOTE$ oversampling method, the trained model is unable to detect it efficiently without CHSMOTE oversampling. The trained model has training and validation losses, as shown in Fig. 7. These losses are equal to or closer to the outlier data imbalance. To achieve this, we use more number of abnormal sequences. Moreover, the training and testing datasets are also closer to equal in terms of accuracy.

Table 4 Comparison of different electric power anomaly detection models [37]

Model	Precision (%)	Recall (%)	F_1 (%)	TPR (%)	$1-$ FPR (%)	AUC (%)
Training set = 80%						
IF	77.70	79.10	78.40	79.10	98.12	88.70
kNN	23.10	86.00	36.40	86.00	81.70	78.10
CBLOF	78.30	79.00	78.70	79.00	98.19	88.60
SVM	98.60	56.30	71.60	56.30	99.91	82.30
ADJST	89.60	97.80	93.50	97.80	97.66	97.70
Ours	99.20	98.40	94.60	98.10	99.93	98.90
Training set = 70%						
IF	85.70	72.40	78.50	72.40	99.18	85.80
kNN	12.90	95.90	22.70	95.90	55.80	75.90
CBLOF	81.90	72.30	76.80	72.30	98.91	85.60
SVM	87.80	68.80	77.10	68.80	99.35	84.10
ADJST	89.10	97.70	93.20	97.70	97.37	97.50
Ours	90.30	98.20	93.80	97.90	99.38	98.20
Training set = 60%						
IF	79.20	78.70	78.90	78.70	98.24	88.20
kNN	15.30	93.90	26.00	93.90	67.50	77.10
CBLOF	80.40	78.30	79.30	78.30	98.26	88.30
SVM	99.00	46.30	63.10	46.30	99.96	73.10
ADJST	89.50	97.10	93.10	97.10	96.54	96.80
Ours	99.20	97.30	93.40	97.60	99.97	97.30

Hence, when we use $CHSMOTE$ oversampling method, the dataset quality greatly improves.

4.3 Comparative analysis

We compare anomaly detection models such as support vector machine (SVM), cluster-based local outlier factor ($CBLOF$), k-nearest neighbours detector (kNN), Isolation Forest (IF), and the recently developed Anomaly Detection by Joint Spatial–Temporal learning ($ADJST$) [37] with our model to assess the performance of the proposed model. We browse the open-source library $PyOD$ and download the codes of these anomaly detection models. We use the same dataset division for a fair comparison. In other words, we analyze the 80%, 70%, and 60% experimental results of the training dataset. The comparison of anomaly detection performance of various models, including our model, is presented in Table 4.

The training and testing datasets are the same for all the models. We use the training dataset, which consists of some normal and abnormal sequences that the $CHSMOTE$ oversampling method generated. We use the test dataset, which consists of remaining normal and original anomalous sequences. Figure 8 shows the results of each performance metric as a radar chart. The radar chart intuitively illustrates the detection results of the model. Various performance metrics show that our model achieves excellent detection results.

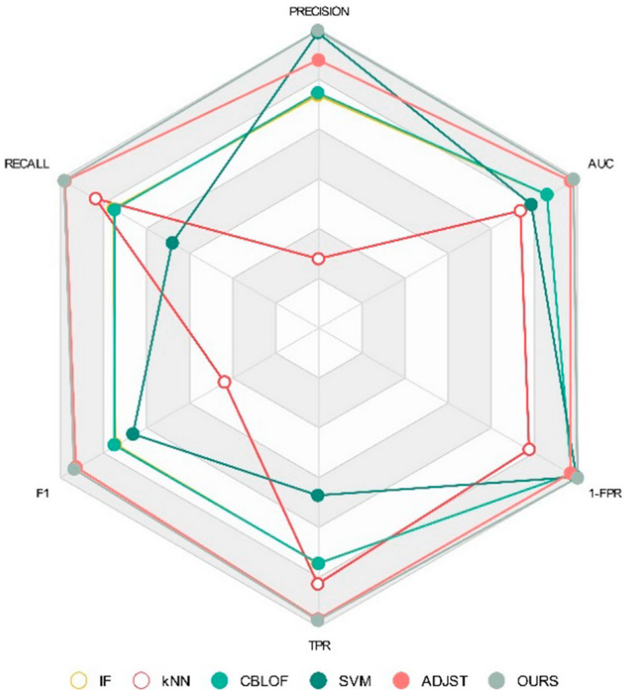


Fig. 8 Radar chart for different models

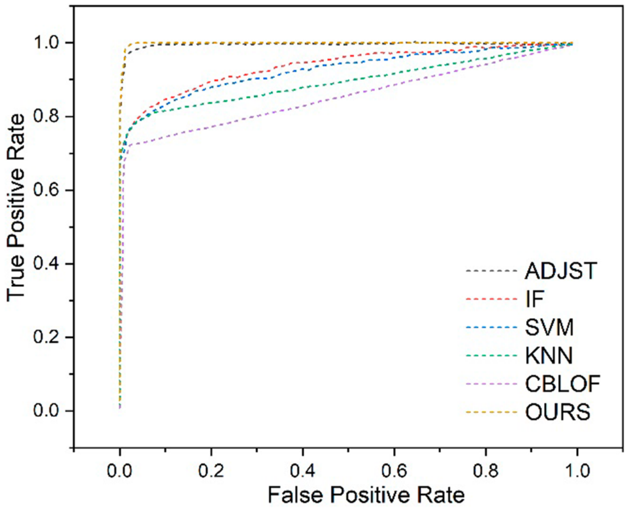


Fig. 9 ROC curve for different models

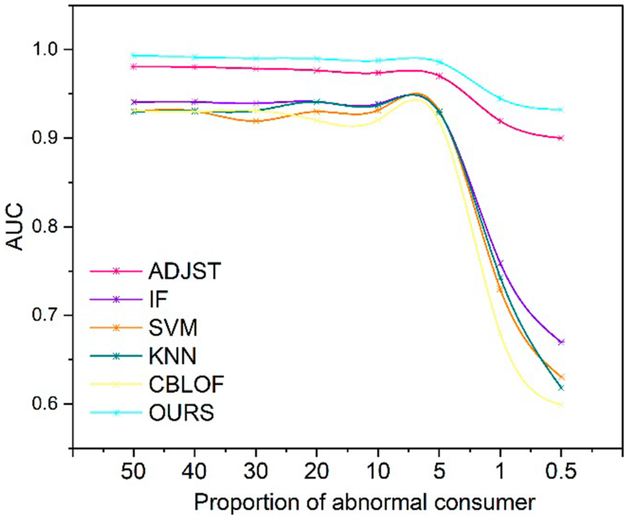


Fig. 10 AUC values for different proportions of abnormal consumers

The F_1 score of our model is greater than 94%, whereas that of other models are lesser than this value. Moreover, the AUC metric of our model is superior to other existing detection models. Also, our model is about 2% superior to the ADJST model, which was proposed in recent years [37]. Figure 9 shows the comparative experimental results as the ROC curves [37]. Nonetheless, anomalous consumers constitute a minority in the real-world scenario. It is, therefore, important to confirm that our proposed model is able to produce accurate results even in the presence of extreme imbalances in the dataset.

Figure 10 displays different proportions of abnormal consumers and the corresponding AUC values of the various models [37]. When the abnormal consumer proportion exceeds 5%, all models have stable detection accuracy, as can be seen in Fig. 10.

However, the existing comparison models deliver poor AUC values when the abnormal consumer proportion continues to decrease. Our model remains above 0.9 even though the abnormal consumer proportion is decreased.

4.4 Ablation study

We perform an ablation study to demonstrate the performance of the proposed model and to verify how efficiently two modules of our model perform. The results obtained from the ablation study are given in Table 5. Both modules have significantly contributed to the performance improvement of the model. To be more specific, the $LSTM : AE$ module effectively detects the abnormal consumption time, while the VGAE module effectively detects the abnormal consumption routes. The losses of the two modules are shown in Fig. 11. It further demonstrates that the $LSTM : AE$ and $VGAE$ modules are effectively detecting the abnormal consumption time and abnormal consumption route, respectively. We substitute GAT to the GCN layer of $VGAE$. The performance of GAT and GCN is shown in Table 5. Due to the attention weights for the relationships between different consumption patterns, the GAT performs better, as can be witnessed in Table 5.

4.5 Discussion

The performance of our model is discussed in this subsection. Different performance metrics are used to assess the performance of the model thoroughly. The precision, recall, TPR, FPR, F_1 score, and AUC are used in this study as the performance metrics of the model. Prior to assessing the proposed model, the CHSMOTE oversample method is analysed primarily to ascertain the efficiency of abnormal consumption sequences generated by the CHSMOTE oversample method in influencing the training of the model. Figure 7 demonstrates that validation and training losses closely align with the outlier data imbalance, which is addressed by incorporating a substantial quantity of generated abnormal consumption sequence. The training and testing datasets exhibit similarity in terms of accuracy. Hence, it is evident that the utilization of the CHSMOTE oversample method significantly enhances the quality of the dataset.

To assess the performance of the proposed model over existing models, a comparative analysis is conducted on widely used anomaly detection models: SVM, CBLOF, kNN, IF, and ADJST. Table 4 presents a result comparison between our model and other existing models. Figure 8 displays the radar chart created based on the results of the performance metrics. Figure 9 shows the ROC curves drawn using the results obtained from the experiments. Figure 10 presents the AUC values of all models across various percentages of abnormal consumers. It is evident that our model provides

Table 5 Ablation study on $LSTM : AE$ and $VGAE$ modules of our model

Configuration	Precision	Recall	F_1 (%)	TPR (%)	$1 - \text{FPR}$ (%)	AUC (%)
Without *LSTM:AE*	85.27	97.85	91.12	97.98	96.22	96.94
Without *VGAE*	85.68	98.72	91.89	98.75	96.39	96.53
GAT replaces *GCN*	86.46	97.37	91.59	97.44	96.73	96.98
Our whole model	91.65	98.93	95.27	98.68	98.82	98.36

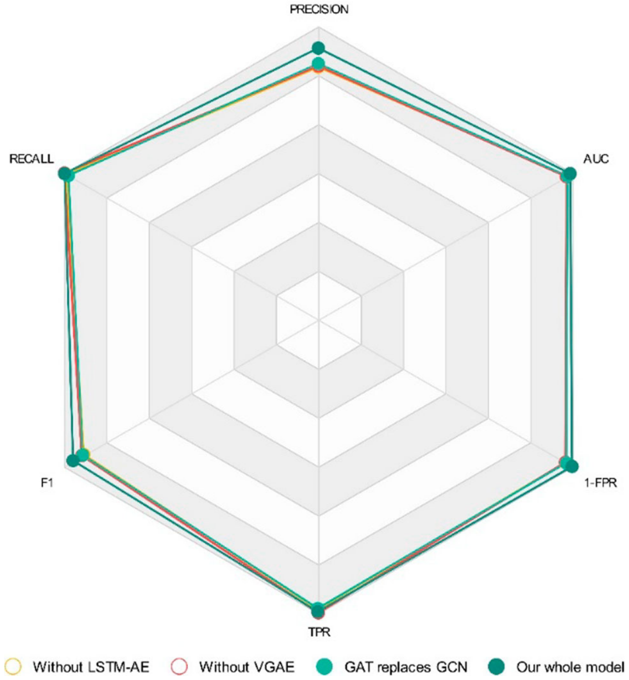


Fig. 11 Radar chart of ablation study

excellent detection results across all performance metrics. Finally, an ablation study is conducted to show the performance of the model and to confirm that all modules of the proposed model are efficient. Table 5 displays the results of the ablation study. In addition, Fig. 11 depicts its radar chart. The modules of the proposed model are efficient, according to the results of the ablation study.

4.6 Limitations

This work is subject to some limitations. Firstly, the proposed trace-based graph deep learning model is primarily suitable for identifying whether a consumer is normal or abnormal. Further research, as outlined in [61], is required to classify the consumers according to theft types. Secondly, the GCN is the core of the proposed model. The GNN exhibits a lack of robustness when dealing with noise present in graph data. The presence of noise in a graph, either through edge deletion/addition or node perturbation, has a negative impact on the output of the GNN. Thirdly, when compared to existing anomaly detection models, such as IF, kNN, CBLOF, SVM, and ADJST, the proposed model exhibits computation complexity, as it considers the entire electric power distribution network in the form of a graph. However, it is acceptable and justifiable because the proposed model outperforms the existing anomaly detection models. Finally, several consumption values are missing in the SGCC dataset. The dataset has approximately 1, 12, 33, 528 missing values, accounting for approximately 22% of the dataset. If these missing values are ignored, the dataset may end up being smaller, which makes it much harder to perform reliable analysis.

5 Conclusion

We propose a trace-based graph deep learning model in this paper. The model is based on unsupervised encoder-decoder anomaly detection. In the proposed model, the $LSTM$ extracts temporal attributes, and the GNN extracts spatial attributes. This model integrates the consumption attributes and traces using a unified graph representation. To analyze the impacts of the implementation of our model on the smart grid, we conduct experiments on a real-world dataset to assess the performance of the proposed model. The proposed model performs better than the existing anomaly detection models in terms of performance metrics. Our model achieves a precision of 99.20%, recall of 98.40%, F_1 of 94.60%, TPR of 98.10%, $1 - \text{FPR}$ of 99.93%, and AUC of 98.90%. On the basis of this research work, a few interesting future research directions have emerged. First, future work may apply the proposed model to a multi-class electricity theft detection dataset described in the recent research work by [62]. This dataset is a collection of electricity consumption information from various sources, including hospital, office, school, private industry, laboratories, institutions, etc. It contains energy consumption for 16 different types of consumers. Second, our proposed model is a general network that can be easily applied to other applications, such as vehicle theft detection [63], detection of unauthorized consumption in water supply systems [64], and detection system for cyber-attacks [65]. Finally, future research may attempt to employ machine learning methods [66] to obtain more precise and accurate models. The model we propose in this paper could be a good starting point for developing enhanced detection models, and our research work would be a blueprint to construct those new models.

Acknowledgements The authors would like to thank the editor-in-chief and the associate editor for their consideration.

Author contributions SIE: Conceptualization, Methodology, Software, Formal analysis, Data curation, Writing—original draft, Investigation. SD: Conceptualization, Writing—Review & Editing. PPA: Methodology, Supervision, Verification. MCT: Writing, Validation, Revision, Review & Editing.

Funding No funding was received.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Lewis FB (2015) Costly throw-ups: electricity theft and power disruptions. Electr J 28(7):118–135
2. de Oliveira ME, Padilha-Feltrin A, Candian FJ (2006) Investigation of the relationship between load and loss factors for a Brazilian electric utility. In: Proceedings of the 2006 IEEE PES transmission and distribution conference and exposition. Latin America
3. Kumar RS, Raghunatha T, Deshpande RA (2013) Segregation of technical and commercial losses in an 11 kV feeder. In: Proceedings of the 7th IEEE GCC conference and exhibition, p 76–79
4. Buevich M, Jacquiau-Chamski A, Schnitzer D, Thacker J, Escalada T, Rowe A (2015) Short paper: microgrid losses—when the whole is greater than the sum of its parts. In: Proceedings of the 2nd ACM international conference on embedded systems for energy-efficient built environments, p 95–98
5. Antmann P (2009) Reducing technical and non-technical losses in the power sector (background paper for the World Bank Group energy sector Strategy). Tech. Rep.
6. Smith TB (2004) Electricity theft: a comparative analysis. Energy Policy 32(18):2067–2076
7. Depuru SSSR, Wang L, Devabhaktuni V (2011) Electricity theft: overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 39(2):1007–1015
8. de Souza Savian F, Siluk JC, Garlet TB, do Nascimento FM, Pinheiro JR, Vale Z (2021) Non-technical losses: a systematic contemporary article review. Renew Sustain Energy Rev 147:111205
9. Klug TW, Beyene AD, Meles TH, Toman MA, Hassen S, Hou M, Klooss B, Mekonnen A, Jeuland M (2022) A review of impacts of electricity tariff reform in Africa. Energy Policy 1(170):113226
10. Tehrani SO, Shahrestani A, Yaghmaee MH (2022) Online electricity theft detection framework for large-scale smart grid data. Electr Power Syst Res 1(208):107895
11. Kotsampopoulos P, Dimeas A, Chronis A, Saridaki G, Hatziargyriou N, Maiti S, Chakraborty C (2022) EU-India collaboration for smarter microgrids: RE-EMPOWERED project. In: 2022 IEEE PES innovative smart grid technologies conference Europe (ISGT-Europe), pp 1–6
12. Viegas JL, Vieira SM, Melício R, Mendes VM, Sousa JM (2016) Classification of new electricity customers based on surveys and smart metering data. Energy 15(107):804–817
13. Battaglini A, Lilliestam J, Haas A, Patt A (2009) Development of SuperSmart grids for a more efficient utilisation of electricity from renewable sources. J Clean Prod 17(10):911–918
14. Malik FH, Lehtonen M (2016) A review: agents in smart grids. Electr Power Syst Res 1(131):71–79
15. Elzinga D, Heinen S (2011) Technology roadmap: smart grids. International Energy Agency, Paris, France
16. Welsch M, Howells M, Bazilian M, DeCarolis JF, Hermann S, Rogner HH (2012) Modelling elements of smart grids: enhancing the OSeMOSYS (open-source energy modelling system) code. Energy 46(1):337–350
17. Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen XS (2014) Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 19(2):105–120
18. Abaide AR, Canha LN, Barin A, Cassel G (2010) Assessment of the smart grids applied in reducing the cost of distribution system losses. In: Proceedings of the 7th international conference on the European energy market (EEM 2010), p 1–6
19. Serrano-Guerrero X, Escrivá-Escrivá G, Roldán-Blay C (2018) Statistical methodology to assess changes in the electrical consumption profile of buildings. Energy Build 164:99–108. https://doi.org/10.1016/j.enbuild.2017.12.059
20. Serrano Guerrero X, Escrivá-Escrivá G, Luna-Romero S, Clairand J-M (2020) A time-series treatment method to obtain electrical consumption patterns for anomalies detection improvement in electrical consumption profiles. Energies 13:1046. https://doi.org/10.3390/en13051046
21. Kozitsin V, Katser I, Lakontsev D (2021) Online forecasting and anomaly detection based on the arima model. Appl Sci 11(7):3194. https://doi.org/10.3390/app11073194
22. Wang X, Ahn S-H (2020) Real-time prediction and anomaly detection of electrical load in a residential community. Appl Energy 259:114145. https://doi.org/10.1016/j.apenergy.2019.114145
23. Rashid H, Singh P (2018) Monitor: an abnormality detection approach in buildings energy consumption, pp. 16–25. https://doi.org/10.1109/CIC.2018.00-44
24. Punmiya R, Choe S (2019) Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. IEEE Trans Smart Grid 10:2326–2329. https://doi.org/10.1109/TSG.2019.2892595
25. Amara korba A, Karabadji N (2019) Smart grid energy fraud detection using SVM. In: 2019 International conference on networking and advanced systems (ICNAS), pp 1–6. https://doi.org/10.1109/ICNAS.2019.8807832
26. Zhang L, Wan L, Xiao Y, Li S, Zhu C (2019) Anomaly detection method of smart meters data based on GMM-LDA clustering feature learning and PSO support vector machine. In: 2019 IEEE sustainable power and energy conference (iSPEC), pp 2407–2412. https://doi.org/10.1109/iSPEC48194.2019.8974989
27. Cody C, Ford V, Siraj A (2015) Decision tree learning for fraud detection in consumer energy consumption. In: IEEE international conference on machine learning applications. https://doi.org/10.1109/ICMLA.2015.80
28. Kammerer K, Hoppenstedt B, Pryss R, Stkler S, Reichert M (2019) Anomaly detections for manufacturing systems based on sensor data—insights into two challenging realworld production settings. Sensors 19(24):5370. https://doi.org/10.3390/s19245370
29. Atemkeng M, Osanyindoro V, Rockefeller R, Hamlomo S, Mulongo J, Ansah-Narh T, Tchakounte F, Fadja AN (2023) Label assisted autoencoder for anomaly detection in power generation plants. arXiv preprint: https://arxiv.org/abs/2302.02896.
30. Touzani S, Granderson J, Fernandes S (2018) Gradient boosting machine for modeling the energy consumption of commercial buildings. Energy Build 158:1533–43. https://doi.org/10.1016/j.enbuild.2017.11.039

31. Bontemps L, Cao VL, Mcdermott J, Le-Khac NA (2016) Collective anomaly detection based on long short-term memory recurrent neural networks, pp 141–152. https://doi.org/10.1007/978-3-319-48057-2_9
32. Silva AD, Guarany IS, Arruda B, Gurjao EC, Freire RS (2019) A method for anomaly prediction in power consumption using long short-term memory and negative selection, pp 1–5. https://doi.org/10.1109/ISCAS.2019.8702152
33. Wang X, Zhao T, Liu H, He R (2019) Power consumption predicting and anomaly detection based on long short-term memory neural network, pp 487–491. https://doi.org/10.1109/ICCCBDA.2019.8725704
34. Hollingsworth K, Rouse K, Cho J, Harris A, Sartipi M, Sozer S, Enevoldson B (2018) Energy anomaly detection with forecasting and deep learning, pp 4921–4925. https://doi.org/10.1109/BigData.2018.8621948
35. Fenza G, Gallo M, Loia V (2019) Drift-aware methodology for anomaly detection in smart grid. IEEE Access 7:9645–9657. https://doi.org/10.1109/ACCESS.2019.2891315
36. Ali S, Wang G, Cottrell RL, Anwar T (2017) Detecting anomalies from end-to-end internet performance measurements (PingER) using cluster based local outlier factor. In: 2017 IEEE international symposium on parallel and distributed processing with applications and 2017 IEEE international conference on ubiquitous computing and communications (ISPA/IUCC), pp 982–989. IEEE
37. Kong J, Jiang W, Tian Q, Jiang M, Liu T (2023) Anomaly detection based on joint spatio-temporal learning for building electricity consumption. Appl Energy 334:120635
38. Wu Z, Pan S, Chen F, Long G, Zhang C, Philip SY (2020) A comprehensive survey on graph neural networks. IEEE Trans Neural Netw Learn Syst 32(1):4–24
39. Chen J, Liu F, Jiang J, Zhong G, Xu D, Tan Z, Shi S (2023) TraceGra: a trace-based anomaly detection for microservice using graph deep learning. Comput Commun 204:109–117
40. Ester M, Kriegel HP, Sander J, Xu X (1996) A density-based algorithm for discovering clusters in large spatial databases with noise. Inkdd 96(34):226–231
41. Malhotra P, Vig L, Shroff G, Agarwal P (2015) Long short term memory networks for anomaly detection in time series. In: Proceedings 89: 89–94
42. Kipf TN, Welling M (2016b) Variational graph auto-encoders. In: Proc. NIPS workshop bayesian deep learning
43. Velicˇkovic’ P, Cucurull G, Casanova A, Romero A, Lio P, Bengio Y (2018) Graph attention networks. In: International conference on learning representations (ICLR)
44. Weng J, Wang JH, Yang J, Yang Y (2017) Root cause analysis of anomalies of multitier services in public clouds. In: 2017 IEEE/ACM 25th international symposium on quality of service (IWQoS), pp 1–6
45. Wang T, Zhang W, Xu J, Gu Z (2020) Workflow-aware automatic fault diagnosis for microservice-based applications with statistics. IEEE Trans Netw Serv Manag 17(4):2350–2363
46. Zhang Y, Yang Q (2022) A survey on multi-task learning. IEEE Trans Knowl Data Eng 34(12):5586–5609
47. Sharma R, Joshi AM, Sahu C, Nanda SJ (2023) Temporal and consumer driven cluster analysis for identification of FDI attacks in smart grid. Int J Numer Modell Electron Netw Devices Fields, p e3145
48. Jain H, Kumar M, Joshi AM (2021) Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection. Electr Eng, pp 1–16
49. Yogarajan G, Vinosh JA, Prakash SKA, Kumar SMM (2021) Interpolation search-based malicious user detection in smart grids. Electr Eng 103:1899
50. Sharma R, Joshi AM, Sahu C, Nanda SJ (2023) Detection of false data injection in smart grid using PCA based unsupervised learning. Electr Eng 105:2383
51. Zheng Z, Yang Y, Niu X, Dai H-N, Zhou Y (2018) Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Trans Ind Inf 14(4):1606–1615. https://doi.org/10.1109/TII.2017.2785963
52. Khan H, Wang X, Liu H (2021) Missing value imputation through shorter interval selection driven by Fuzzy C-Means clustering. Comput Electr Eng 1(93):107230
53. Yuan X, Chen S, Zhou H, Sun C, Yuwen L (2023) CHSMOTE: convex hull-based synthetic minority oversampling technique for alleviating the class imbalance problem. Inf Sci 1(623):324–341
54. Han H, Wang WY, Mao BH (2005) Borderline-smote: a new over-sampling method in imbalanced data sets learning. In: ICIC, Springer, pp 878–887
55. Noble WS (2006) What is a support vector machine? Nat Biotechnol 24(12):1565–1567
56. Sáez JA, Luengo J, Stefanowski J, Herrera F (2015) SMOTE–IPF: addressing the noisy and borderline examples problem in imbalanced classification by a resampling method with filtering. Inf Sci 291:184–203
57. Yogarajan G, Revathi T (2018) Nature inspired discrete firefly algorithm for optimal mobile data gathering in wireless sensor networks. Wirel Netw 24:2993–3007
58. Yogarajan G, Revathi T (2018) Improved cluster based data gathering using ant lion optimization in wireless sensor networks. Wirel Pers Commun 98:2711–2731
59. Mukherjee D, Ghosh S, Misra RK (2022) A novel false data injection attack formulation based on CUR low-rank decomposition method. IEEE Trans Smart Grid 13(6):4965–4968
60. Mukherjee D (2022) Data-driven false data injection attack: a low-rank approach. IEEE Trans Smart Grid 13(3):2479–2482
61. Mukherjee D, Chakraborty S, Ghosh S (2022) Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. Electr Eng 104(1):259–282
62. Zidi S, Mihoub A, Qaisar SM, Krichen M, Al-Haija QA (2023) Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. J King Saud Univ-Comput Inf Sci 35(1):13–25
63. Tseng PY, Lin PC, Kristianto E (2023) Vehicle theft detection by generative adversarial networks on driving behavior. Eng Appl Artif Intell 1(117):105571
64. Stramari MR, Kalbusch A, Henning E (2023) Random forest for the detection of unauthorized consumption in water supply systems: a case study in Southern Brazil. Urban Water J 20(3):394–404
65. Stabili D, Romagnoli R, Marchetti M, Sinopoli B, Colajanni M (2023) A multidisciplinary detection system for cyber attacks on powertrain cyber physical systems. Future Gener Comput Syst 1(144):151–164
66. Chakir O, Rehaimi A, Sadqi Y, Krichen M, Gaba GS, Gurtov A (2023) An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0. J King Saud Univ-Comput Inf Sci 35(3):103–19

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.