


RESEARCH

Open Access



Integrated encoder-decoder-based wide and deep convolution neural networks strategy for electricity theft arbitration

Manoj Kumawat¹, Adeniyi Onaolapo², Gulshan Sharma², Ibrahim Cagri Barutcu³, Temitope Adefarati⁴ and Ramesh Bansal^{5,6*} 

*Correspondence:
rcbansal@ieee.org

¹ Department of Electrical Engineering, National Institute of Technology Delhi, Delhi, India

² Department of Electrical Engineering Technology, University of Johannesburg, Johannesburg 2006, South Africa

³ Department of Electricity and Energy, Çölemerik V.H.S., Hakkari University, Hakkari 30000, Turkey

⁴ Department of Electrical and Electronics Engineering, Federal University Oye Ekiti, Oye Ekiti, Nigeria

⁵ Department of Electrical Engineering, University of Sharjah, Sharjah, United Arab Emirates

⁶ Department of Electric, Electronic and Computer Engineering, University of Pretoria, Pretoria, South Africa

Abstract

Integrating energy systems with information systems in smart grids offers a promising avenue for combating electricity theft by leveraging real-time data insights. Suspicious activity indicative of theft can be identified through anomalous consumption patterns observed in smart networks. However, a smart model is required for capturing and analysing the data intelligently to accurately detect electricity theft. In the paper, electricity theft has been detected using an encoder-decoder-based classifier that integrates two models of convolutional neural networks (CNN). The aim is to scan the strength of the data and built a smart model that analysed the connections in complex data and determine the pattern of theft. The model comprises three compartments: the auto-encoder, the wide convolutional neural network (1-D CNN model), and the deep convolutional neural network (2-D CNN model). The auto-encoder has been trained on the complex and in-depth linkage between the theft data and the normal data as it removes noise and unnecessary information. The 1-D CNN model gathers relevant connections and general features, while the 2-D CNN model determines the rate at which energy theft occurs and differentiates between the energy-stealing consumers and normal consumers. The efficacy of the approach is underscored by its superiority over traditional deep learning and machine learning techniques. This paper elucidates the distinct advantages and applications of the proposed model in combating electricity theft within smart grid environments.

Keywords: Convolutional neural networks, Deep learning, Power system, Electricity theft, Smart grid

Introduction

In the modern era, every technological innovation is linked to electricity. Contemporary life would be incomplete without electricity. However, electricity losses remain a key problem for the utilities. Technical and non-technical losses are the two types of losses in the power system [1]. The technical losses have been compressed in significant amounts in the restructured power system [2]. Meanwhile, non-technical loss as an electricity theft plays a major role. Therefore, this paper pivots around electricity theft,

accounting for significant global financial losses for power utilities. The utilities in developing and developed countries have experienced serious financial losses due to electricity theft [3]. Manually inspecting bypassed meter connections, analyzing meter readings to identify normal and anomalous situations, and verifying malfunctioning meters are the traditional techniques for identifying electricity theft [4]. These techniques are inefficient and slow. More research is needed to unravel novel technologies with high efficiency for electricity theft detection [5].

Literature has conducted much research on electricity theft, but there is room for more improvement [6, 7]. Electricity theft can be detected in two ways, namely, the hardware-based approach and the data-driven approach. The hardware-based approach is a simple method that detects theft by smart meters and specific infrastructure designs without the use of the software. It makes use of advanced anti-tampering sensors and smart meters [8]. The disadvantages of the hardware-based approach are (i) requirement of specific smart meter devices manufactured for this purpose, (ii) the difficulty in maintaining these devices, (iii) high costs of implementation, and (iv) failure of the devices due to weather conditions [9]. The data-driven approach leverages extensive customer electricity consumption data, employing advanced machine learning algorithms and data science techniques to extract intricate patterns and pertinent insights from the dataset [10]. The integration of smart grid technologies such as advanced metering infrastructure (AMI), smart meters, and conventional power grids facilitates the acquisition of customers' consumption data [11–13]. Moreover, smart grids facilitate two-way communication between electricity consumers and utilities. This fosters the development of a network characterized by heightened reliability, security, and intelligence [14–16].

Electricity theft detection techniques explored in the literature use different machine learning and statistical approaches, such as the Naïve Bayes, KNN, Random Forest, Decision Tree, and Support Vector Machine [17–20]. These approaches have the advantage of low computational time for training and testing. However, their prediction accuracies have required more improvements. Therefore, deep learning methods, such as CNN-GRU [21], CNN-LSTM [22], CNN [23], and MLP [24], are used to find hidden patterns and innate features in datasets [25, 26]. Supervised learning methods are impossible to deploy in instances of pseudonymous data; rather, unsupervised learning methods map the data's natural cluster to different groups, and assign new data to the created groups [27, 28]. Consumers' data of the existing electricity theft detection methods are highly imbalanced. A dataset is regarded as imbalanced when some class instances are scarce than the other classes. The classification algorithms focus on maximizing prediction accuracies and are thus susceptible to misclassification of minority classes as dominant classes since the fundamental principle of classification algorithms is finding the boundary among the classes. At times, the minority classes do not possess sufficient data to find boundaries with other classes; this is referred to as an anomaly [29, 30].

The model proposed in this paper uses an auto-encoder neural network to address the anomaly. The auto-encoder neural network primarily creates a substantial gap between each class by transforming the dimensions of the dataset, thereby removing the redundancy and noise of the dataset. Auto-encoder neural networks have been widely used in detecting anomalies in fraud detection, industrial control systems, and intrusion detection [31]. About 5–10% of the entire consumption data is the portion

belonging to theft scenarios. So, extracting the information and features of minority class data for an unbiased classification is a big challenge. The autoencoder model is comprehensively explained in section III. Also, the existing electricity theft detection algorithms contain many non-malicious factors, like trends in customers' consumption data, stationarity, seasonality, and temporal dependency. Some factors are emphasized in the literature because of their importance in categorizing the characteristics and patterns of the dataset [32]. Such factors include weekends, holidays, seasonal requirements, and weather conditions. These factors produce uncertainty in the simplification of electricity theft detection algorithms. To tackle these problems, a deep complex convolutional neural network classifier that can automatically recognize the boundary between classes and learn the time-dependent features is proposed in this research.

The deep complex convolutional neural network is designed in two stages, the auto-encoder neural networks and the two collaborative convolution neural networks with different feature extraction and configuration capabilities. In collaborative learning, the output's generalization error is reduced, and overall performance is improved by combining the predictions of many independent models. Therefore, this research constructs a technique for detecting electricity theft by overcoming the problems described above. The auto-encoder-based collaborative model of 1-D and 2-D Convolutional Neural Networks (CNN), which identify electricity burglars more accurately by learning complex patterns of electricity consumption data, are developed in this research. The data is encoded (or compressed) into a small code by the auto-encoder and then decoded (or decompressed) to replicate the input. Thereby learning the non-linear and complex patterns of both the normal and abnormal electricity data and converts the input features to various nonlinear vector spaces [33]. Thus, it successfully filters inappropriate noise and redundant information in the dataset and differentiates between the normal and abnormal data. These pre-processed datasets are passed through two complex concatenated deep learning networks, which are the Wide (i.e., 1-D) CNN network and the Deep (i.e., 2-D) CNN Network [28]. Wide (1-D) component network is made up of a layer of neural networks trained on a one-dimensional dataset and a layer of the convolutional neural network, while Deep (2-D CNN) component network is made up of two-dimensional, deep dense, dropout, pooling, and convolutional layers [26].

The Wide 1-D component learns the inter-relationship and universal information of the data, while the Deep 2-D CNN component apprehends irregularities and explores periodicity in the electricity consumption data [33]. Hence, the proposed model combines the benefits of an advanced anomaly detection system with that of collaborative deep learning models to present a high-performance electricity theft detector. Deep learning models (ANN and CNN) and machine learning models (SVM, KNN, and LDA), which are capable of learning complex patterns of data, were also implemented for comparison purposes. The following are the contributions of this research:

- The research paper proposes a combination of auto-encoder and collaborative 1-D and 2-D CNN models. The composition of proposed model is highly lucrative in that:

- i. The encoder-decoder arrangement effectively eliminates the noise and extraneous information, thereby enhanced the differentiation between theft data and normal data.
 - ii. The utilization of the wide component is facilitated the retention of pertinent relationships and global features.
 - iii. The deep component is accurately recognized the non-periodic patterns in electricity theft data and periodic patterns in normal data, showcasing its ability to learn non-linear and complex relationships. This capability significantly enhances the accuracy of the electricity theft detection system.
- An intensive experimentation is conducted in the paper, employed on a real-life electricity dataset to validate the superiority of the proposed model over existing ones.

Problem analysis

Power utilities nowadays are confronted with many problems, one of which is electricity theft. A huge sum (between 5 and 10% of electricity) produced is being stolen daily. This act has excessive negative effects on the economy and impacts grid security, monitoring, and proper regulation. Electricity theft is performed in different malicious ways, like hacking digital meters, tempering the readings of energy meters, and bypassing the digital meter. Breakthroughs in technologies, such as deep learning and machine learning, and the availability of a large amount of power consumption data, have given rise to the popularity of data-driven electricity theft detection methods. Electricity theft can be detected using optimized tools and advanced data science algorithms. In this research, data were acquired from the State Grid Corporation of China (<http://www.sgcc.com.cn>) and analyzed. The data is made up of thirty-three thousand, eight hundred and forty-one (33,841) electricity consumption data from customers between Jan 1, 2014, to Oct 31, 2016 (i.e., 1035 days) [34]. The data were first pre-processed for outlier and empty values and normalized for an independent analysis of individual consumers, as explained in “Methods”. Visualization of a sample of consumption data, randomly selected for both customer types (i.e., the normal usage and theft data), was performed after pre-processing. The plot is shown in Fig. 1.

The plot shows a lot of fluctuations in both electricity theft and normal consumption data, and difficult to find critical differences between normal consumption and electricity theft data but drawing the data approximate lines revealed that normal usage data has much less uncertainty and fluctuations than the theft data.

Similar observations were made in other randomly selected customer data samples as well. Figure 2 shows the plot of the scenario between the theft data and normal electricity usage data of August 2016, selected randomly for some customers.

It could be observed in Fig. 2 the clear differences in patterns and fluctuations showing satisfactory results from deep and machine-learning classification models. Random customer weekly datasets for both normal usage and electricity data were plotted for better insight, as reported in Figs. 3 and 4.

Figures 3 and 4 were plotted from a month’s randomly selected theft and normal data. It is discovered from the plots that the glance of periodicity is clearly observed in the patterns of the normal usage data. The consumption patterns for each day are

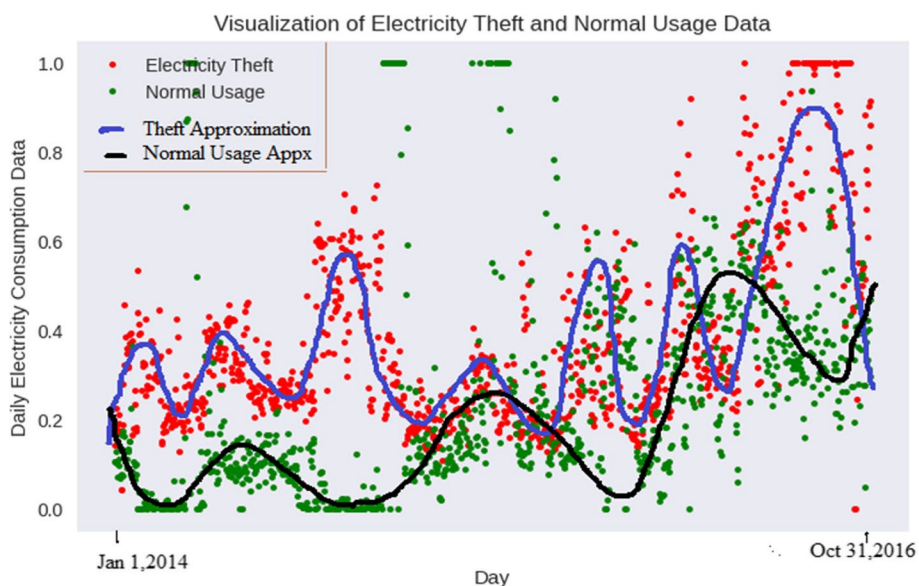


Fig. 1 Electricity theft and normal usage electricity consumption data

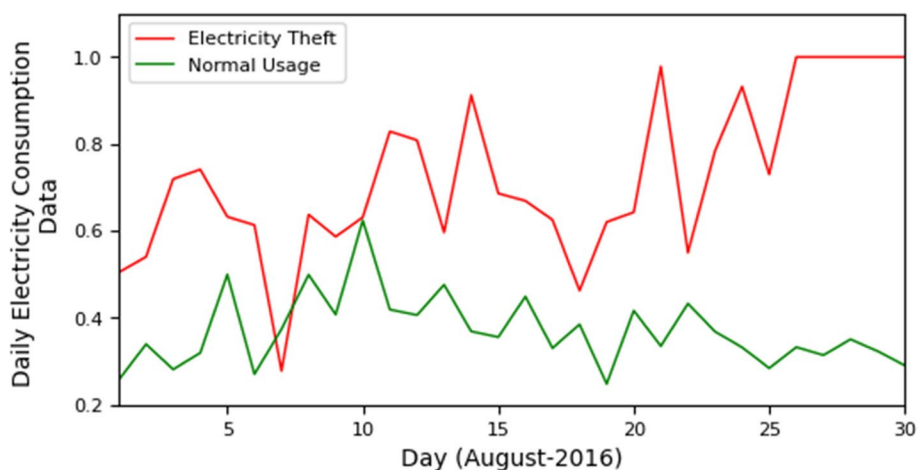


Fig. 2 Visualization of 1-month electricity theft and normal usage electricity consumption data

similar; for instance, the highest consumption is observed on days 4 or 5, while low consumptions are peculiar to days 7. The frequency variation, fluctuations, and noise trends are more in the theft data patterns. Hence, theft data patterns become less periodic. Random data were plotted from the entire dataset for easy visualization and simplicity; the findings for different customers were observed to be similar. Similar findings on elements of periodicity in fluctuations and noise were observed in other studies which used similar datasets [8].

The presence of non-periodic patterns in electricity theft data and periodic patterns in normal usage data is also illustrated using the Pearson correlation coefficient (PCC), as shown by the PCC matrices in Table 1. It is observed that the PCC values of most of the normal usage weekly data are greater than 0.70, hence, indicating a

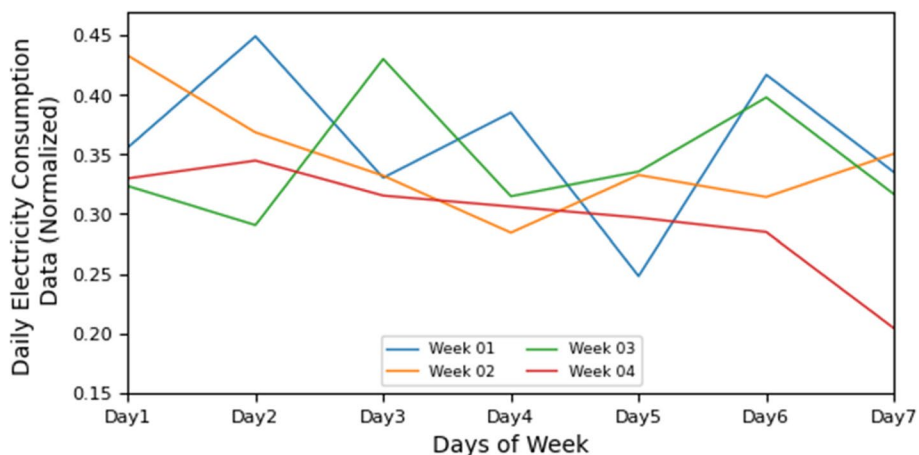


Fig. 3 Weekly plot of a normal usage customer

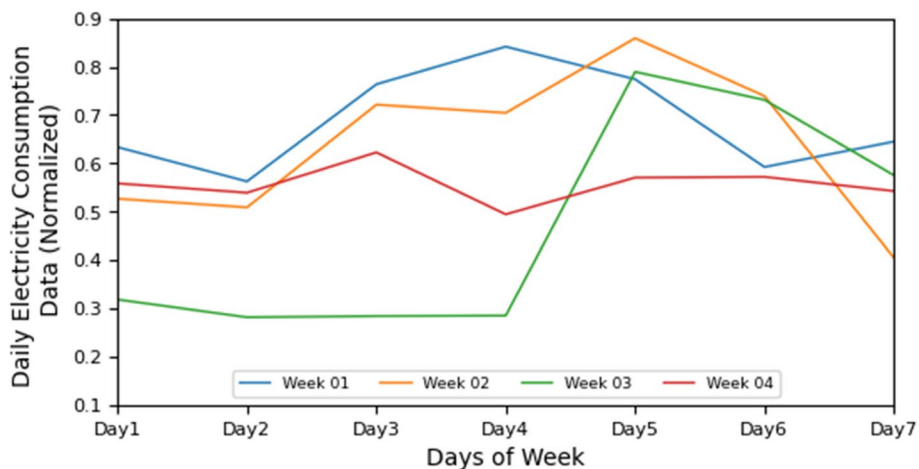


Fig. 4 Weekly plot of a customer having electricity theft

Table 1 Electricity theft and normal usage data's Pearson correlation coefficient

Pearson correlation coefficient of normal usages					Pearson correlation coefficient of electricity theft				
Week1	1	0.70	0.82	0.71	Week1	1	0.50	-0.35	-0.45
Week2	0.70	1	0.74	0.90	Week2	0.50	1	-0.12	-0.45
Week3	0.82	0.74	1	0.85	Week3	-0.35	-0.12	1	-0.36
Week4	0.71	0.90	0.85	1	Week4	-0.45	-0.45	-0.36	1
	Week1	Week2	Week3	Week4		Week1	Week2	Week3	Week4

strong correlation. While the PCC values of most of the electricity theft weekly data are mostly between negative value and zero, hence, indicating a weak correlation [35].

The partial autocorrelation and the autocorrelation function of the normal usage and theft customers are plotted in Figs. 5 and 6, respectively. It was discovered that while normal usage data has clearly defined lag values, the theft data has no definite

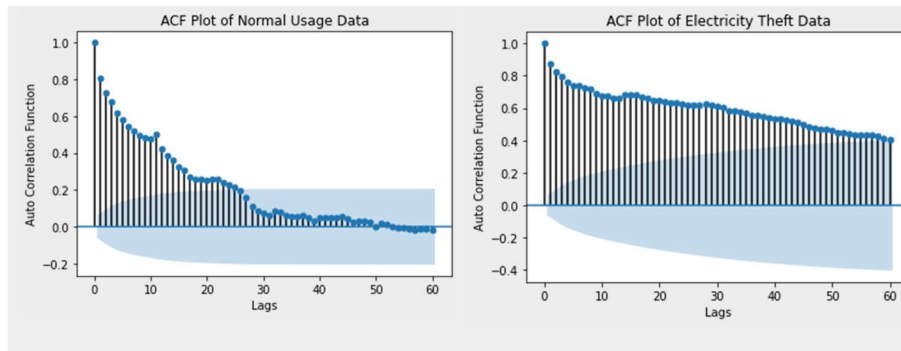


Fig. 5 ACF plots of electricity theft and normal usage data

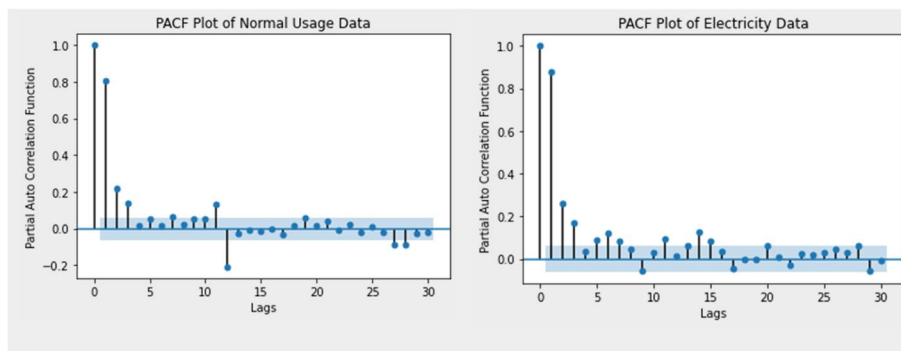


Fig. 6 PACF plots of electricity theft and normal usage data

relationship with its historical values. Hence, the visual and statistical analysis of theft data revealed that they are non-periodic or less periodic as compared to normal usage data. This observation is consistent with the findings from other countries [05]. However, the 1-D dataset nature, huge noise, and massive size make it difficult to visualize the dependency and periodicity of previous day data.

Methods

Data pre-processing

Outliers and missing values are usually contained in the electricity consumption data as a result of the maintenance schedules, storage issues, and failures in smart meters, sensors, and transmit and receive systems [3]. It is, therefore, required to handle these missing values by using a well-accepted method. The outliers or missing values are handled in this research using a popular interpolation technique as expressed in the following equations.

$$f(x_i) = \begin{cases} \frac{x_{i-1} + x_{i+1}}{2}, & x_i \in NaN, x_{i-1}, x_{i+1} \notin NaN \\ 0, & x_i \in NaN, x_{i-1} \text{ or } x_{i+1} \in NaN \\ x_i, & x_i \notin NaN \end{cases} \quad (1)$$

where x_i is a customer consumed electricity on an i th day (spanning between Jan 1, 2014, and Oct 31, 2016). NaN is the outlier value on that particular day.

The presence of many outlier values was observed in the data; these values should be subjected to an acceptable range to get a more accurate and better-generalized outcome. The “Three-sigma rule of thumb” [9] technique was used in this research to remove the missing data values. The original value is expressed as follows:

$$f(x_i) = \begin{cases} avg(x) + 2.std(x), & \text{if } x_i > avg(x) + 2.std(x), \\ x_i & \text{otherwise} \end{cases} \tag{2}$$

where x is a vector or list of the energy consumption record for the 35-month period. The i th element of the vector x is the i th day customers’ energy consumption (i.e., x_i), the $avg(x)$ is the total average energy consumption per customer per day, and $std(x)$ is the standard deviation of the total energy consumption per customer.

After the necessary pre-processing, normalization of the datasets is essential because of the sensitivity of neural networks to different data. Normalization is done using the min–max scaling technique as:

$$f(x_i) = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{3}$$

where $\min(x)$ and $\max(x)$ are the respective minimum and maximum customer energy consumption values over the period of data acquisition.

Proposed machine learning model

The proposed classification model is made up of the (i) auto-encoder network and the (ii) ensemble of 1-D and 2-D convolutional neural networks, as shown in Fig. 7.

(i) Auto-encoder network

Auto-encoder is made up of unsupervised artificial neural networks which encode and compress data efficiently and reconstruct it back to a depiction that is the original input’s feasible replica. Auto-encoder learns to avoid data noise, thereby reducing data dimensionality [36]. Auto-encoder neural networks receive wide acceptance for anomaly detection among unsupervised models [37, 38]. Several layers make up the model structure of the auto-encoder, with various arrangements of neurons in each layer, as depicted in Fig. 7. The neuron number in each encoder-decoder network’s layer decreases to a particular extent

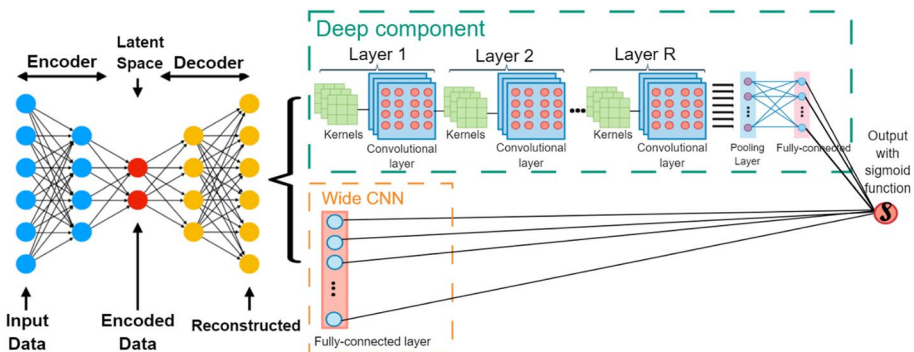


Fig. 7 Proposed ensemble auto-encoder dependent model

and then increases to a particular extent, as could be seen in Fig. 7. Noise and redundant information are filtered in the auto-encoder network. The gap between theft data and normal usage data is also increased by converting the input (x) to linear independent vector space (\underline{x}) using the latent space (z) in order to allow the proposed model to identify customers easily. With a training set, given as: $S = \{x_i | x_i \in R^d\}, 1 \leq i \leq n$, the auto-encoder is modeled as:

$$\begin{cases} z = h(w_e, b_e; x) \\ r = k(w_d, b_d; z) \end{cases} \tag{4}$$

where the neural networks implemented decoder and encoder functions are $k(\cdot)$ and $h(\cdot)$ respectively. The encoder parameters are w_e and b_e , while the decoder parameters are w_d and b_d . If $h(\cdot)$ and $k(\cdot)$ are neural networks, then b_i and w_i are the bias vectors and weight matrices with respect to encoder and decoder, $h(\cdot)$ and $k(\cdot)$ neural networks. Training an auto-encoder is by optimizing (i.e., minimizing) the loss function as:

$$J(\theta) = \frac{1}{n} \sum_{i=1}^n \|x_i - r_i\|^2 \tag{5}$$

where $\theta = (w_e, b_e; w_d, b_d)$. The gradient descent algorithm is applied to solve Eq. (5) optimization problem.

(ii) Integration of wide and deep components of convolutional neural network

Classification problems have been widely addressed using deep learning algorithms such as convolution neural networks. Images can be analyzed using common feed-forward neural networks like the convolutional neural network (CNN or ConvNet). A CNN is a multi-layer network with simple pattern detection and specialized feature extraction attributes. CNN has its respective input, hidden, and output layers, just like any deep learning model. Hidden layers work by taking input from the preceding layer, transforming it into some form of output using the weights, and sending it to the next layer. Transformation, here, is defined as the convolution of different kernels or filters in relation to the hidden layers. Hidden layers are referred to as convolution layers when they use convolution operations. Convolution layers have links with different filters and can detect objects, shapes, and patterns in images. The structure of a CNN model has different convolutional layers, filters, complex (non-linear) activation functions, Down-sampling layers, and MLP classification output layers, as shown in Fig. 8. The weights of MLP and convolution layer kernels are updated using efficient learning algorithms (stochastic and gradient descent momentum). CNN's description and working principles are further explained in the literature [36].

The common deep neural networks (DNN), which are multi-layered neural networks, are simply made up of the input layers, hidden layers, and output layers, but CNN has an additional convolutional layer, which serves as the key operation in the discrete convolution. In each grid, the input I has a value, while the output S of the convolution is:

$$S(i, j) = \sum_{k_i=0}^1 \sum_{k_j=0}^1 I(i + k_i, j + k_j)K(k_i, k_j) \tag{6}$$

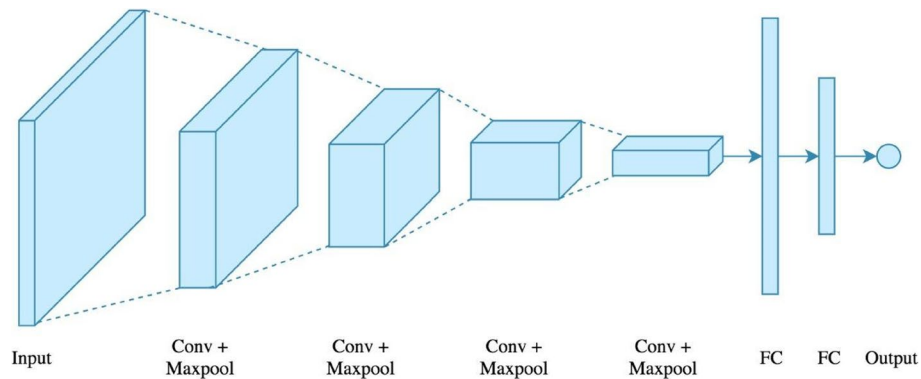


Fig. 8 The architecture of a CNN model

The abovementioned wide and deep convolutional neural networks contain different configurations of parameters and layers. As earlier observed, the data are less stable and thereby fluctuate more than normal usage data, and its nature is less periodic. Hence, electricity consumers' datasets can be treated as 1-D time series data. The handling of normal usage data's periodic nature is done using a deep CNN model whereby 1-D power usage data is transformed into 2-D information as indicated by 11 days (done by a trial-and-error method which produces the best accuracy). The 2-D CNN model is made up of several layers, poolings, neurons, and filters. The network structure is produced using trial-and-error methods vis-à-vis the knowledge of the domain. The use of the grid search method is also explored in this research, combining the hyperparameters, and returning those producing the best result.

Each neuron in the fully connected layer produces its probability score using the following equations:

$$y_i = \sum_{i=1}^n w_{i,j} x_i + b_1 \quad (7)$$

where y_i is the output of the fully connected layer. $w_{i,j}$ is the weight of the j th neuron and i th input value. n is the length of input data, and b_1 is the bias term. The wide model controls the extent at which this prediction influences further step prediction using the activation function. The activation function used in this research is the rectified linear unit (ReLU), as expressed in the equation below:

$$u_j = f(y_j) = \max(0, y_j) \quad (8)$$

where u_j and f are the output and the activation function, respectively. The main reason to use ReLU is used mainly because of its good learning abilities and effective prevention of over-fitting in forwarding propagation.

Experimental setting

Power consumption data

Real-life electricity consumption data acquired from the State Grid Corporation of China (SGCC) was used in carrying out the experiment. Table 2 shows the metadata information of this dataset.

Table 2 Meta data information of dataset

Description	Value
Time duration of data collection	Jan 1, 2014–Oct 31, 2016
Total no of customers	33,841
Total no of thieves	3615
Total number of normal usage customers	30,226

Electricity consumption data of 32,841 consumers, spanning 1035 days (from January 1, 2014, to October 31, 2016), were acquired for this research. Outliers and missing values in the data were pre-processed, as explained earlier. SGCC confirmed that 3615 customers' data were discovered to be involved in electricity theft, while the rest data are normal electricity usage data. The proposed model was also evaluated using this theft data as ground truth. The proposed algorithm has been implemented on PARAM Shavak with 2.2 GHz Dual socket Intel Xeon E5-2600.

Performance matrix

The proposed model's performance was evaluated in this research using some standard parameters, such as F1 score, recall, precision, and area under the curve (AUC) Accuracy [39, 40]. AUC is particularly used to authenticate the classification model, which is the possibility that positive sample ranks selected randomly are greater than a randomly selected negative sample. AUC is expressed as:

$$AUC = \frac{\sum_{i \in +ve \text{ class}} Rank_i - \frac{P(1+P)}{2}}{P * N} \quad (9)$$

where P, N, and $Rank_i$ are the number of positive samples, negative samples, and the rank of i th. The samples were arranged in ascending order depending on the probability score before feeding them into Eq. (9). The indices used for performance evaluation are defined as follows:

Accuracy: stands for the number of classes that were correctly predicted over the overall classes.

Precision: stands for the number of positively predicted classes that are truly positive.

Recall: stands for the ratio of positive class predictions to that of all-positive classes.

F1 Score: stands for the harmonic mean of recall and precision. This can be expressed as:

$$F1_{score} = \frac{2P_r R_c}{P_r + R_c} \quad (10)$$

Table 3 Optimization parameters and input features for the model

Methods	Features	Parameters
SVM [19]	Raw(1-D)	C = 100, Degree = 10, Kernel = 'rbf'
MLP [27]	Raw(1-D)	Neurons = 500, Hidden Layer = 5, Epochs = 200, Batch size = 5
CNN [34]	Raw(2-D)	Filters = 64, Dropout = 0.2, Hidden Layer = 7, Epochs = 180, Batch size = 10
KNN [20]	Raw (1-D)	Leaf size = 30, neighbours = 3, weight = 'uniform'
LDA [25]	Raw(1-D)	n_components = 3, solver = 'svd'
Proposed method	Raw (1-D and 2-D)	Filters = 32 & 64, Hidden Layer = (1 for wide component and 6 for deep Component), Lag = 11 day, Epochs = 100, Batch size = 5

Table 4 Performance comparison with other models

Methods	Training ratio = 60%					Training ratio = 80%				
	AUC	ACC	Precision	Recall	F1 Score	AUC	ACC	Precision	Recall	F1 Score
SVM [19]	0.716	0.897	87	90	88.47	0.729	0.897	87	90	88.47
KNN [20]	0.640	0.892	86	89	87.47	0.630	0.887	85	89	86.95
MLP [27]	0.797	0.907	89	91	89.99	0.818	0.909	90	91	90.49
CNN [34]	0.880	0.938	93	94	93.49	0.910	0.944	94	94	94.00
LDA [25]	0.664	0.883	86	89	87.47	0.682	0.896	87	90	88.47
PM	0.891	0.956	95	96	95.49	0.956	0.974	97	97	97.00

where P_r and R_c are the value of Precision and Recall, respectively.

Baseline models

Other conventional methods were also implemented for analyzing the performance of the proposed model, and their outcomes are reported in Table 4.

Some classifiers, which are support vector machine (SVM), linear decrement analysis (LDA), and K-Nearest Neighbours (KNN) were implemented on Python's machine learning library, Scikit-learn. An open-source Deep Learning Framework, Keras, was used to implement the proposed model, convolutional neural network (CNN), and the Multi-Layer Perceptron Model (MLP). Table 3 shows the optimization parameters for each model and their range.

Results and discussion

Performance comparison of the implemented model

The entire dataset is divided into two for model training and testing. The training ratio was chosen on two groups of the dataset, 60 and 80%, so as to generalize the conclusion of the machine-learning model's performances. The training and testing samples were randomly selected for each group of experiments. The training ratio is selected as:

$$\text{Training Ratio} = \frac{\text{Number of samples used for training}}{\text{Total number of samples}} \times 100 \quad (11)$$

The electricity consumption data of 20,304 customers were used for training, while that of 13,537 customers was used for testing in the first group of experiments. Also,

the electricity consumption data of 27,072 customers were used for training the classification model, while that of 6769 customers was used for testing the performance in the second group of experiments. The outcomes of the performance evaluation parameters for different classification models are shown in Table 4. Several factors contribute to the consistency of the model as the complexity of the model architecture utilized enables it to capture intricate patterns within the dataset efficiently, potentially reaching a performance plateau with additional training data. The dataset characteristics: exhibiting moderate complexity and sufficient variability facilitate the model's generalization across various training data sizes. Additionally, the model's strong generalization ability suggests it has learned robust features representative of the underlying data distribution, ensuring stable performance regardless of training data size. The possibility that evaluation metrics used are not highly sensitive to minor changes in model performance could explain minimal observed differences between different training data percentages.

(i) The performance at the train-test ratio of 60%

The results in Table 4 show the outstanding performance of the proposed methods, an ensemble of wide and deep convolutional neural networks. It has an accuracy of 95.59%, which is far better than that of the conventional models. The proposed model's F1 score is 95.49%, which surpasses that of all the conventional classifiers. The values of the proposed model for all other indices (such as recalls, precision, and AUC) are also better than that of the conventional methods.

(ii) Performance when the train-test ratio is 80%

Here, the train data are more than the 60% train-test ratio scenario. The model learning is observed to have improved, hence, an improvement in the results of all parameters. It has an accuracy of 97.44%, which is far better than that of the conventional models. For every performance evaluation index, there is an improvement in our proposed model than other existing models. Hence, there is greater accuracy and better feature generalization in the proposed model's learning of patterns and electricity consumption data behaviors.

The ROC-AUC curves were also plotted for the two groups of experiments (i.e., at 60 and 80% training ratios, respectively) for the models' outcomes and for visualizing the analysis of the AUC, as reported in Figs. 9, 10 and 11. The areas covered by the red and

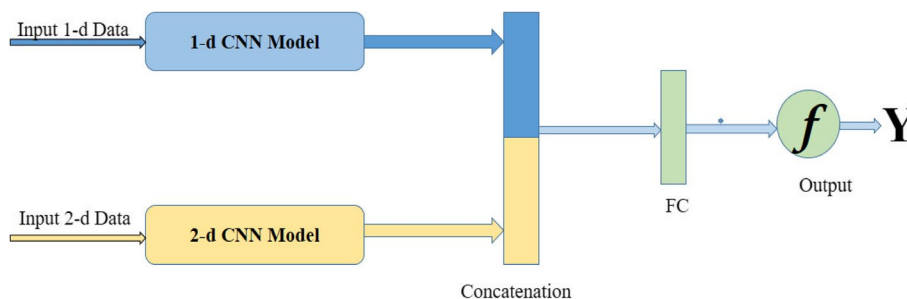


Fig. 9 The Framework of a wide and deep convolution neural networks (CNN)

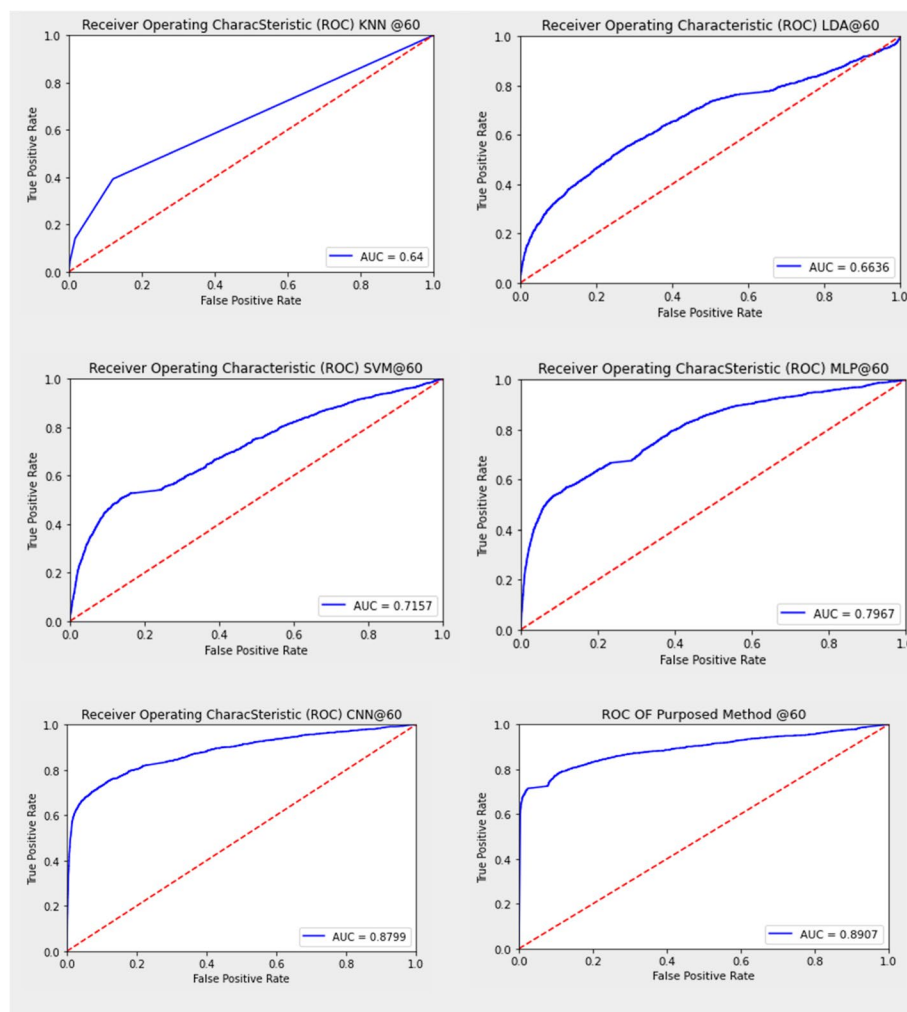


Fig. 10 ROC-AUC plot of all the implemented models when training ratio is 60%

blue curves in Figs. 9, 10 and 11 are the AUC values. AUC value is directly proportional to the classification model's performance. The higher the AUC value, the higher the accuracy of the model, and vice versa. The AUC value results for the KNN model and other existing models in Figs. 9 and 10 are far lower than that of the proposed model (which is 89.07%), ditto for the AUC value results for the KNN model and other existing models in Figs. 9 and 10 are far lower than that of the proposed model (which is 95.55%).

It could also be observed from Figs. 9, 10 and 11 that the performance of the machine learning algorithms is better at the training data scenario of 80% than at the training data scenario of 60%. There is also an improvement in the ROC plot of the proposed model compared to that of the existing models. Thus, all the performance indices for the proposed model (i.e., auto-encoder-based wide and deep CNN) are better than that of the conventional models.

The confusion matrix was also plotted for all the models, as shown in Fig. 12. A confusion matrix is a convergence of accurately forecasted classes as well as falsely forecasted classes in a classification method.

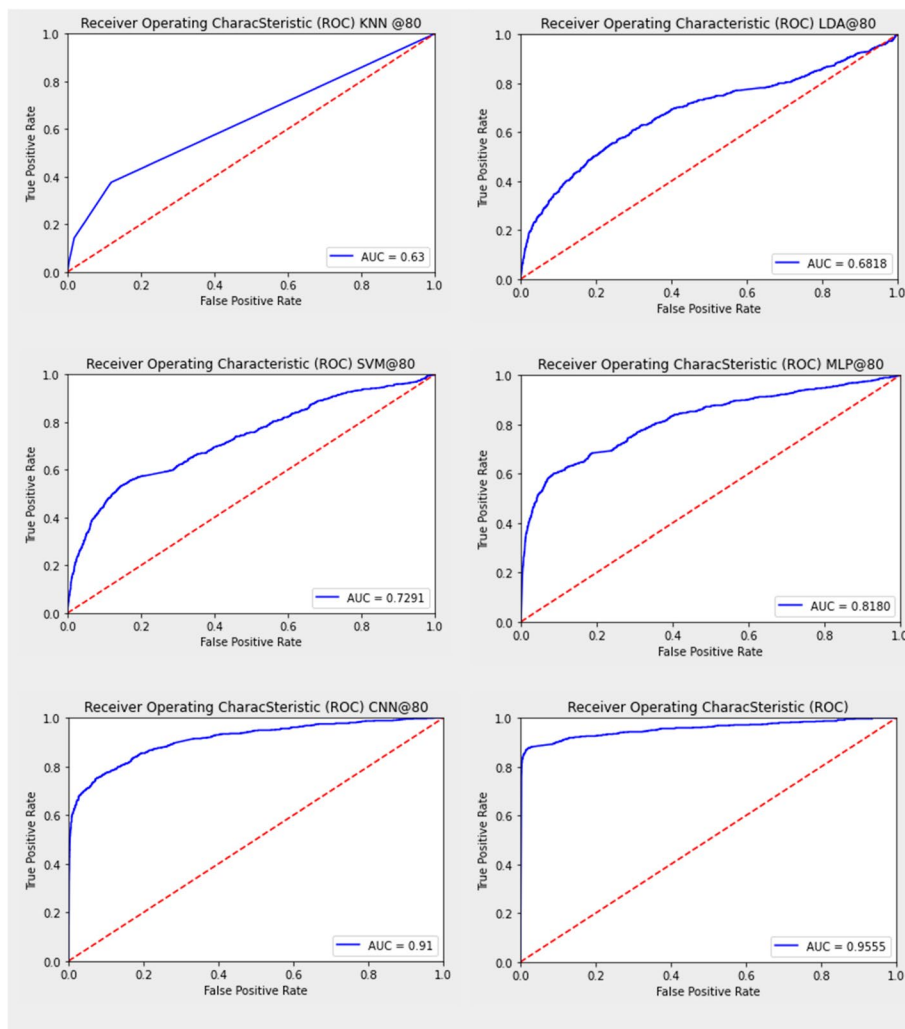


Fig. 11 ROC-AUC Plot of all the implemented models when the training ratio is 80%

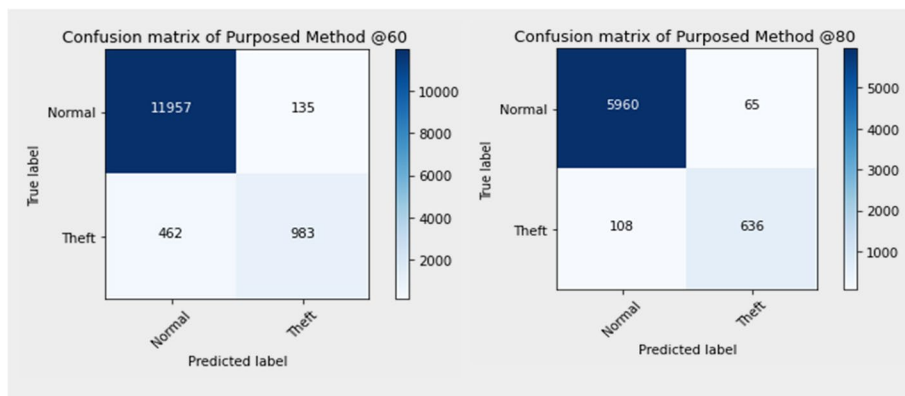


Fig. 12 Confusion matrix of proposed models when the training ratio is 60 and 80%

In Fig. 12, it can be observed that when the training ratio is 60%, 983 theft and 11,957 normal customers were classified accurately by the proposed model, while only 462 theft and 135 normal customers were classified inaccurately. Meanwhile, when the training ratio is 80%, a reduction in the percentage of inaccurate predictions is observed; there were only 65 inaccurate classifications out of 6025 normal customers, while only 108 inaccurate classifications out of 744 theft customers. Hence, the superior performance and significant generalization and accuracy of the proposed model (irrespective of the training ratio) as compared to the conventional models have been demonstrated.

Convergence analysis of the proposed methods and the effects of hyper-parameter

The ensemble of two convolutional networks makes up the proposed methods. Hence, the system results are impacted greatly by the hyper-parameters, such as the number of dense layers, pooling layers, filters, and neurons. The hyper-parameter is first selected by the trial-and-error method and in accordance with the best domain knowledge. Then, the exact hyper-parameters of models are found using the grid search method. The performance of the model improved during training when the number of epochs is increased up to 100, but when the number of epochs is increased beyond 100, the model's performance degraded. Also, the performance of the model improved when the batch size decreases and vice versa, as the batch size is calculated using grid search techniques.

Conclusions

This paper is applied a data-driven electricity theft detection approach using data that were encoded and decoded and passed through an ensemble of wide and deep CNN models. The dataset was projected on a less noisy vector space by the auto-encoder and informatively compared to the raw data. The global features learning of the electricity theft dataset of wide convolutional neural networks is another benefited of the proposed model. Therefore, the model has the ability to learn the periodic and non-periodic natures of theft and normal usage data, which is typical of deep convolutional neural networks. Moreover, the ensemble of two convolutional neural networks has delivered the benefits of conjecture and consciousness. In the paper, the dataset acquired from the State Grid Corporation of China was utilized to validate the accuracy and efficiency of the model. The results demonstrate the generalization and accuracy of classification of the theft and normal customers by the proposed auto-encoder-based ensemble model of wide and deep CNN. Anomaly detection ability of proposed approach is much higher than that of conventional models, such as CNN, MLP, SVM, LDA, and KNN. The proposed ensemble-based wide and deep CNN model has undergone rigorous testing and validation, demonstrating its robustness and suitability for a wide range of industrial applications.

Abbreviations

b_d	Bias parameters for decoder
b_e	Bias parameters for encoder
b_i	Bias vectors
$h(\cdot)$	Neural networks implemented encoder functions
$J(\theta)$	Loss function
$k(\cdot)$	Neural networks implemented decoder functions

N	Negative samples
n	Length of input data
NaN	Outlier value on that particular day
P	Number of positive samples
P_r	Value of Precision
$Rank_i$	Rank of i th
R_c	Value of Recall
R^d	Number of layer of deep component
r	Rate of learning
u_j	Output of activation function
w_e	Weight parameters for encoder
w_d	Weight parameters for decoder
w_i	Weight matrices
x_i	Customer consumed electricity i th day
y_i	Output of the fully connected layer
z	Latent space

Acknowledgements

Authors would like their universities for the support provided.

Authors' contributions

All authors planned the study and contributed to the idea and field of information; introduction, MK; software, MK, and GS; writing—original draft preparation; MK and AO, writing—review and editing, IB and TA; supervision, RB, review and editing and corresponding author. All authors have read and approved the manuscript.

Funding

Not received.

Availability of data and materials

Data will be made available on suitable request.

Declarations

Competing interests

Na.

Received: 16 January 2024 Accepted: 10 April 2024

Published online: 22 April 2024

References

- Liao W, Bak-Jensen B, Pillai JR, Xia X, Ruan G, Yang Z (2024) Reducing annotation efforts in electricity theft detection through optimal sample selection. *IEEE Trans Instrum Meas* 73:1–11
- Kumawat M, Gupta N, Jain N, Bansal RC (2017) Swarm-intelligence-based optimal planning of distributed generators in distribution network for minimizing energy loss. *Electr Pow Compo Syst* 45(6):589–600
- Jokar P, Arianpoo N, Leung VCM (2016) Electricity theft detection in ami using customers' consumption patterns. *IEEE Trans Smart Grid* 7(1):216–226
- Liao W, Yang Z, Liu K, Zhang B, Chen X, Song R (2023) Electricity theft detection using Euclidean and graph convolutional neural networks. *IEEE Trans Power Syst* 38(4):3514–3527
- Gerasopoulos SI, Manousakis NM, Psomopoulos CS (2022) Smart metering in EU and the energy theft problem. *Energy Efficiency* 15:12. <https://doi.org/10.1007/s12053-021-10011-y>
- Raza MH, Rind YM, Javed I, Zubair M, Mehmood MQ, Massoud Y (2023) Smart meters for smart energy: a review of business intelligence applications. *IEEE Access* 11:120001–120022
- Nabil M, Ismail M, Mahmoud MMEA, Alasmay W, Serpedin E (2019) PPETD: Privacy-Preserving Electricity Theft Detection Scheme with load monitoring and billing for AML networks. *IEEE Access* 7:96334–96348
- Orlando M et al (2022) A Smart meter infrastructure for smart grid IoT applications. *IEEE Internet Things J* 9(14):12529–12541. <https://doi.org/10.1109/JIOT.2021.3137596>
- Gu D, Gao Y, Chen K, Shi J, Li Y, Cao Y (2022) Electricity theft detection in AML with low false positive rate based on deep learning and evolutionary algorithm. *IEEE Trans Power Syst* 37(6):4568–4578
- Duan N, Huang C, Sun C-C, Min L (2022) Smart meters enabling voltage monitoring and control: the last-mile voltage stability issue. *IEEE Trans Industr Inf* 18(1):677–687. <https://doi.org/10.1109/TII.2021.3062628>
- Mbungu NT, Bansal RC, Naidoo R (2019) Smart energy coordination of autonomous residential home. *IET-Smart Grid* 2(3):336–346
- Mbungu NT, Bansal RC, Naidoo R (2019) Overview of the optimal smart energy coordination for microgrid applications. *IEEE Access* 7:163063–163084
- Mbungu NT, Naidoo R, Bansal RC, Bettayab M, Siti MW, Bipath M (2020) A dynamic energy management system through smart metering. *Appl Energy* 280(115990):1–12
- Onaolapo K, Pillay Carpanen R, Dorrell DG, Ojo EE (2023) Event-driven power outage prediction using collaborative neural networks. *IEEE Trans Ind Inform* 19(3):3079–3087

15. Onaolapo K, Pillay Carpanen R, Dorrell DG, Ojo EE (2022) A Comparative assessment of conventional and artificial neural networks methods for electricity outage forecasting. *Energies* 15(2):511
16. Onaolapo K, Pillay Carpanen R, Dorrell DG, Ojo EE (2021) Reliability evaluation and financial viability of an electricity power micro-grid system with the incorporation of renewable energy sources and energy storage: A case study of KwaZulu-Natal, South Africa. *IEEE Access* 9:159908–159924
17. Jindal A, Dua A, Kaur K, Singh M, Kumar N, Mishra S (2016) Decision Tree and SVM-based data analytics for theft detection in smart grid. *IEEE Trans Ind Inf* 12(3):1005–1016
18. Li S, Han Y, Yao X, Yingchen S, Wang J, Zhao Q (2019) Electricity theft detection in power grids with deep learning and random forests. *J Electric Comput Eng* 4136874:1–12
19. Khan ZA, Adil M, Javaid N, Saqib MN, Shafiq M, Choi J-G (2020) Electricity theft detection using supervised learning techniques on smart meter data. *Sustainability* 12(19):8023
20. Zhuang W, Jiang W, Xia M, Liu J (2024) Dynamic generative residual graph convolutional neural networks for electricity theft detection. *IEEE Access* 12:42737–42750
21. Onaolapo K, Pillay Carpanen R, Dorrell DG, Ojo EE (2020) Transmission Line Fault Classification and Location Using Multi-Layer Perceptron Artificial Neural Network. *IEEE Industrial Electronics Society Conference (IECON)*. pp 5182–5187
22. Onaolapo K, Akindeji KT, Adetiba E (2019) Simulation experiments for faults detection, classification and location in smart distribution networks using IEEE 13 node test feeder and artificial neural network. *J Phys: Conf Ser* 1378(3):032021
23. Onaolapo K, Akindeji KT (2019) Application of Artificial Neural Network for Fault Location in Distribution Network. *Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA)*. pp 299–304
24. Bansal RC (2006) Overview and literature survey of artificial neural networks applications to power systems (1992–2004). *J Inst Eng (India) Electric Eng* 86(1):282–296
25. Buzau MM, Tejedor-Aguilera J, Cruz-Romero P, Gomez-Exposito A (2020) Hybrid deep neural networks for detection of non-technical losses in electricity smart meters. *IEEE Trans Power Syst* 35(2):1254–1263
26. Plathottam J, Salehfar H, Ranganathan P (2017) Convolutional Neural Networks (CNNs) for power system big data analysis. *North American Power Symposium (NAPS)*
27. Lu X, Zhou Y, Wang Z, Yi Y, Feng L, Wang F (2019) Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid. *Energies* 12(18):3452
28. Ullah A, Javaid N, Samuel O, Imran M, Shoaib M (2020) CNN and GRU based Deep Neural Network for Electricity Theft Detection to Secure Smart Grid. *International Wireless Communications and Mobile Computing (IWCMC)*
29. Aligholian, Farajollahi M, Mohsenian-Rad H (2019) Unsupervised Learning for Online Abnormality Detection in Smart Meter Data. *IEEE Power & Energy Society General Meeting (PESGM)*
30. Rouzbahani HM, Karimipour H, Lei L (2020) An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*
31. Chandola V, Banerjee A, Kumar V (2009) Anomaly detection. *ACM Comput Surv* 41(3):1–58
32. Yuan F-N, Zhang L, Shi J-T, Xia X, Li G (2019) Theories and applications of auto-encoder neural networks: a literature survey. *Jisuanji Xuebao/Chin J Comput* 42:203–230
33. Li J, Ji C, Yan G, You L, Chen J (2020) An Ensemble Net of Convolutional Auto-Encoder and Graph Auto-Encoder for Auto-Diagnosis. *IEEE Trans Cogn Dev Syst* 13(1):189–199. March 2021
34. Zheng Z, Yang Y, Niu X, Dai H, Zhou Y (2018) Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. *IEEE Trans Industrial Informatics* 14(4):1606–1615
35. Bansal RC (2019) *Power System Protection in Smart Grid Environment*. CRC Press, New York, USA
36. Zhai J, Zhang S, Chen J, He Q (2018) Autoencoder and Its Various Variants. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. pp 415–419
37. Fan F, Xiao Y, Zhao J (2018) Wang, "Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data." *Appl Energy* 211:1123–1135
38. Antwarg L, Miller RM, Shapira B, Rokach L (2021) Explaining anomalies detected by autoencoders using Shapley Additive Explanations. *Expert Syst Appl* 186(30):115736
39. Sharma T, Shrivastava V, Kumawat M (2022) "A Comprehensive Study on Electricity Theft Detection Using Data Analysis," *IEEE 10th Power India International Conference (PIICON)*. New Delhi, India, pp 1–6
40. Xin R, Zhang J, Shao Y (2020) Complex network classification with convolutional neural network. *Tsinghua Science and Technol* 25(4):447–457

Publisher's Note

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