frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 08 November 2023
DOI 10.3389/fenrg.2023.1287413

Check for updates

OPEN ACCESS

EDITED BY
Fengji Luo,
The University of Sydney, Australia

REVIEWED BY
Muhammad Faizan Tahir,
South China University of Technology, China
Ning Li,
Xi'an University of Technology, China

*CORRESPONDENCE
Mounir Bouzguenda,
mbuzganda@kfu.edu.sa

RECEIVED 04 September 2023
ACCEPTED 24 October 2023
PUBLISHED 08 November 2023

CITATION
Khan N, Amir Raza M, Ara D, Mirsaeidi S, Ali A, Abbas G, Shahid M, Touti E, Yousef A and Bouzguenda M (2023), A deep learning technique Alexnet to detect electricity theft in smart grids.
Front. Energy Res. 11:1287413.
doi: 10.3389/fenrg.2023.1287413

COPYRIGHT
© 2023 Khan, Amir Raza, Ara, Mirsaeidi, Ali, Abbas, Shahid, Touti, Yousef and Bouzguenda. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

A deep learning technique Alexnet to detect electricity theft in smart grids

Nitasha Khan[1], Muhammad Amir Raza[2], Darakhshan Ara[3], Sohrab Mirsaeidi[4], Aamir Ali[5], Ghulam Abbas[6], Muhammad Shahid[7], Ezzeddine Touti[8], Amr Yousef[9,10] and Mounir Bouzguenda[11]*

[1]British Malaysian Institute, Universiti Kuala Lumpur, Sungai Pusu, Malaysia, [2]Department of Electrical Engineering, Mehran University of Engineering and Technology, Khairpur, Sindh, Pakistan, [3]Department of Information Sciences and Humanities, Dawood University of Engineering and Technology, Karachi, Pakistan, [4]School of Electrical Engineering, Beijing Jiaotong University, Beijing, China, [5]Department of Electrical Engineering, Quaid-e-Awam University of Engineering Science and Technology, Nawabshah, Nawabshah, Sindh, Pakistan, [6]School of Electrical Engineering, Southeast University, Nanjing, China, [7]Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi, Pakistan, [8]Department of Electrical Engineering, College of Engineering, Northern Border University, Arar, Saudi Arabia, [9]Department of Electrical Engineering, University of Business and Technology, Jeddah, Saudi Arabia, [10]Engineering Mathematics Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt, [11]Department of Electrical Engineering King Faisal University, Hofuf, Saudi Arabia

Electricity theft (ET), which endangers public safety, creates a problem with the regular operation of grid infrastructure and increases revenue losses. Numerous machine learning, deep learning, and mathematical-based algorithms are available to find ET. Still, these models do not produce the best results due to problems like the dimensionality curse, class imbalance, improper hyper-parameter tuning of machine learning and deep learning models, *etc.* We present a hybrid deep learning model for effectively detecting electricity thieves in smart grids while considering the abovementioned concerns. Pre-processing techniques are first employed to clean up the data from the smart meters. Then, the feature extraction technique, like AlexNet, addresses the curse of dimensionality. The effectiveness of the proposed method is evaluated through simulations using a real dataset of Chinese intelligent meters. To conduct a comparative analysis, various benchmark models are implemented as well. Our proposed model achieves accuracy, precision, recall, and F1, up to 86%, 89%, 86%, and 84%, respectively.

KEYWORDS

deep learning, electricity theft, smart grid, Chinese smart meter, loss-free intelligent power system

1 Introduction

Due to population growth, the electrical system has grown larger, which increases power consumption (Raza et al., 2023a). ET is believed to be a significant source of revenue losses because of meter manipulation, meter bypassing, billing issues, and other strategies (Rehan et al., 2023a). According to estimates, manual ET costs the USA $6 billion annually, the UK up to $232 million, and electric utilities globally lose $25 billion annually due to ET (Aldegheishem et al., 2021). On the other hand, India loses 4.8 billion rupees annually, Pakistan loses 0.89 billion rupees annually, and Brazil loses $4 billion due to ET (Lepolesa

TABLE 1 Previous approach for ET detection using different algorithms.

References	Problem	Dataset used	Technique used	Performance metrics	Limitations/Future work
Feng et al. (2020)	Electricity theft in power grids	Ireland	Convolutional Neural Network (CNN)	Precision, area under curve, recall and F1 score	Privacy
Chicco (2012)	Electricity theft	Datasets of different areas randomly	Time Division Multiplexing (TDM)	Neglected	The proposed model ignored the focus on performance metrics
Gu et al. (2022)	Electricity theft detection, Curse of dimension, and Overfitting issues	Ireland	Synthetic Minority Over-sampling Technique (SMOTE) and Principal Component Analysis (PCA)	Time complexity and recall	Overfitting issue of SMOTE, Privacy leakage due to the high sampling rate
Pamir et al. (2022)	Electricity theft in smart grids	State Grid Cooperation of China	Tomek Links, AlexNet, and peephole	accuracy, precision, recall, F1-score, and AUC	Considered using low sampling data only
Khan et al. (2020)	Electricity theft detection in the commercial area of Brazil	Brazilian	Binary Black Hole Algorithm (BBHA)	Mean Accuracy	The dataset is biased on one class; no suitable metrics are used
Ahmed et al. (2023)	Electricity theft	State Grid Cooperation of China	Deep Artificial Neural Network (DANN)	Recall, F1 score and AUC.	Experimentation with other supervised learning algorithms
Singh et al. (2018)	Electricity theft	Ireland	Gradient Boosting Machine Algorithm (GBMA), Clustering and Evolutionary Genetic Algorithm (CEGA)	Accuracy, F1- score AUC, and precision	The proposed model does not handle the imbalanced nature of the data
Duarte Soares et al. (2022)	Electricity theft	Real-time dataset	Load monitoring and Advanced Metering Infrastructure (AMI) networks	ROC-AUC Accuracy	Security feature results in a slightly low detection rate
Hasan et al. (2019)	Electricity theft detection	Malaysia	Simplified Memory Bounded (SMB)	Accuracy	Metrics selection is not appropriate
Aslam et al. (2020)	Electricity theft detection	State Grid Cooperation of China	Feature Engineered- CatBoost Algorithm (FECA) Synthetic Minority Oversampling Technique (SMOTE) Algorithm	Accuracy, recall, and precision	Improving the system robustness neglected
Ali et al. (2023a)	Energy theft system	-	Multilayer Perception (MLP), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU)	-	The proposed technique has better accuracy and can be implemented in both industrial and commercial sectors
Badr et al. (2023)	Electricity theft detection	Endesa	Extreme Gradient Boosting (XG-Boost)	TPR, Recall, FPR Precision, AUC	The proposed model consumes time on large datasets
Zheng et al. (2018)	Electricity theft	Irish	XGBoost	FPR, Recall, AUC Precision	Not enough training data, limited results, and imbalanced data
Pereira and Saraiva (2021)	Electricity theft detection	Brazilian	Artificial Neural Network—Multilayer Perception (ANN-MLP)	PSO, SGHS, BP	The proposed model does not handle the imbalanced nature of data
Ahir and Chakraborty (2022)	Electricity theft detection	Brazilian	ANN-MLP	Accuracy, Precision, Recall	The results of the proposed model are not accurate
	Electricity theft detection	SEAI	SMA	DR, FPR	The proposed model neglected the accuracy
Ayub et al. (2022)	Electricity theft detection	State Grid Cooperation of China	CNN-LSTM	MCC, F1-score	The proposed model is consuming high time on datasets

(Continued on following page)

TABLE 1 (*Continued*) **Previous approach for ET detection using different algorithms.**

References	Problem	Dataset used	Technique used	Performance metrics	Limitations/Future work
Ali et al. (2023a)	Electricity theft detection in a shopping mall in Turkey	BEDAS	Ensemble model	TPR, FPR F-measure, precision	The balance of TPR and FPR is neglected in this proposed work
Adil et al. (2020)	Low accuracy, Overfitting, and High FPR in ETD	Self-made dataset	LSTM	Precision, Recall, F1-score, Convergence speed	Not suitable for large datasets

et al., 2022). Numerous researchers have highlighted ET difficulties and potential solutions. Gradient boosting was employed in a study (Punmiya and Choe, 2021) to find ET. A specific theft window is also established during peak hours to identify questionable power consumer activity. However, a reliable and accurate method for ET detection is still needed (Raza et al., 2022a; Raza et al., 2022b; Rehan et al., 2023b). Hardware elements, including sensors, smart meters, distribution transformers, and other equipment, are used by state-based systems to find ET (Raza et al., 2022c). This work (Razavi et al., 2019) employed a state-based methodology to pinpoint ET in physically inspired smart grids. A special kind of transformer was coupled with smart meters to study client electricity consumption trends. The simulation results demonstrate that the suggested strategy outperforms the base models. The power company and electricity thieves play a game in game theory-based solutions. This technique's drawbacks include higher costs, greater complexity, and a need for hardware components for proper implementation (Nabil et al., 2019). Additionally, smart homes employ a game theory-based technique to lower peak energy expenses (Nabil et al., 2019). Many other methods exist to minimize energy losses and establish coordination amongst smart appliances (Raza et al., 2022d; Raza et al., 2022e; Raza et al., 2023b).

Some of the investigations done on ET detection are listed in Table 1 below. Table 1 presents the problem, the methods used to offer a solution, the advantages suggested by earlier research and potential future research, and the limitations of that particular study. The smart meter data has been used to build a digital solution for the acknowledged ET problem, producing better results. The finite mixture model, the gradient boosting machine approach, clustering, and evolutionary genetic algorithms were all used to address the ET problem in Table 1. Future power providers should adhere to the suggested methodology for minimizing power losses. A model for ET that uses long and short-term memory, as well as a bat-based strategy to improve imbalanced data, parameter optimization, and overfitting and achieve F1 score, precision, recall, and receiver operating characteristics under the area curve (ROC-AUC), was also presented and discussed in Table 1. All research described in Table 1 covered the fundamental concept of ET detection. However, the method used in this paper is novel and has never been used for ET detection in a smart grid. Overall, this study emphasizes the need for building reliable, precise, and effective detection technologies to guarantee the integrity and sustainability of the smart grid and the continued efforts to resist ET detection through creative approaches. The suggested paradigm might eventually be used to apply power data for whole power system structures.

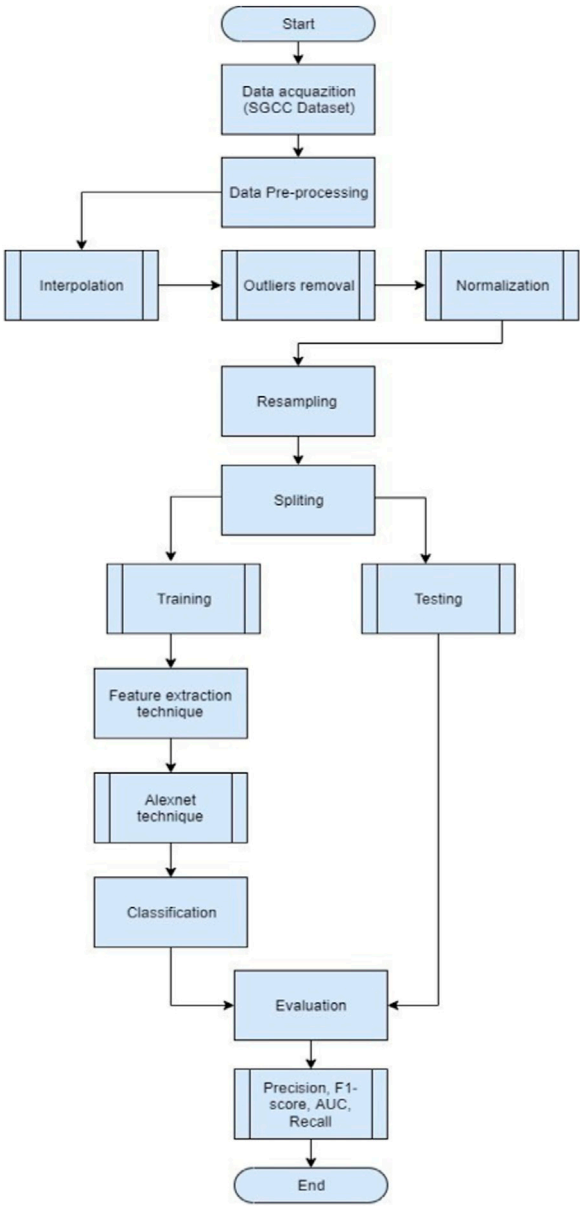

FIGURE 1
Proposed system flowchart for the electricity theft detection in smart grid.

In summary, the literature on ET detection presents a wide range of approaches and techniques to address this critical issue. Researchers have explored various machine learning algorithms to ensemble models for achieving accurate and reliable detection results, including deep neural networks, gradient boosting machines, and many others. Many studies have focused on utilizing intelligent meter data, temperature-dependent solutions, and AMI networks to enhance detection. Privacy-preserving schemes, synthetic monitoring samples, and data imputation techniques have also been proposed to ensure the security and integrity of the electricity grid. Challenges such as data imbalance, high false favorable rates, and overfitting have been recognized and addressed in the literature. Researchers have proposed methods to handle these challenges, including performance metrics, ensemble techniques, and optimization algorithms. Additionally, there is a growing emphasis on system robustness and the need for reliable performance evaluation. However, using AlexNet software, this work offered a revolutionary deep-learning technique for ET detection in smart grids. All research described in the literature covered the fundamental concept of ET detection. However, the method used in this paper is novel and has never been used for ET detection in a smart grid. Overall, this study emphasizes the need for building reliable, precise, and effective detection technologies to guarantee the integrity and sustainability of the smart grid and the continued efforts to resist ET detection through creative approaches. Figure 1 shows the suggested system flowchart for ET detection in the smart grid.

The potential of traditional sampling methods on deep learning technique AlexNet in the significant data context is studied in this work. The main contributions of this research are: a) This paper is focused on dealing with multi-class imbalance problems, which have hardly been investigated and are critical issues in the field of data classification; b) It addresses one of the most popular deep learning methods (AlexNet), a specialized research topic, with details on some particular aspects of the classifier, such as answering the question: Is it pertinent to use methods that work in the features space of classifiers that set the decision boundary in the hidden space? c) Results notice the effectiveness of editing methods on the output AlexNet to improve the curse of dimensionality, class imbalance, and model hyperparameterization problems.

2 The proposed system

This section describes the suggested method in Figure 1, while Figure 5 illustrates the proposed technique's mechanism in all its steps. The proposed system is divided into four steps. First, starting with dataset collection details, then pre-processing the gathered data, then data balancing, and finally, feature extraction. All of them are briefly discussed in the following subsections.

2.1 Dataset collection details

The suggested technique is based on electricity consumption data from the State Grid Corporation of China (SGCC). Table 2 shows the details of the dataset (Shehzad et al., 2022). Most researchers use the SGCC dataset for ET detection due to its extensive coverage. This is because it provides a detailed overview of the geographical, commercial, and technical aspects/data from different parts of China that would help better apprehend ET with higher accuracy. Moreover, this is considered one of the most reliable datasets available for this task thus far, with other datasets still not offering such granular features. Therefore, it is an apt choice amongst research communities working on developing effective models and concepts for detecting unauthorized power consumption or losses throughout distributed network areas spanning vast territories without any manual efforts needing to be expended into collecting actual field readings from those locations directly.

TABLE 2 Information of SGCC dataset (Shehzad et al., 2022).

Explanation	Values
Total consumers	42,372
Data collection period	01-01-2014 to 31-10-2016
Honest consumers	38,575
Theft consumers	3,615

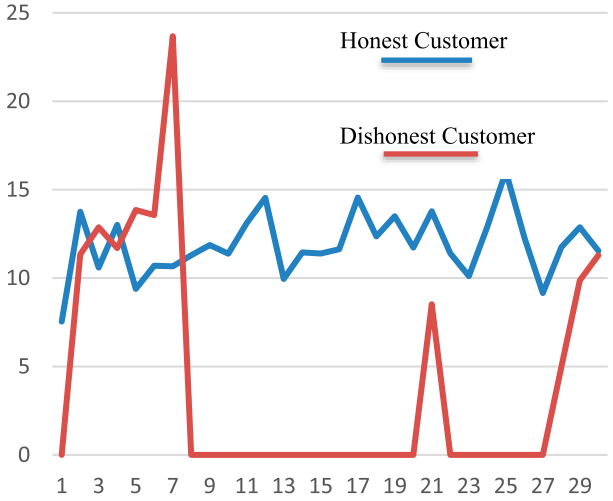

FIGURE 2
Electricity consumption pattern (Shehzad et al., 2022).

SGCC data contains 42,372 energy consumption records, where 91% of customers are truthful and 9% are deceitful (Shehzad et al., 2022). The information concerning the defrauded customers is accurate. The disparity between honest and dishonest customers demonstrates the unbalanced nature of data. The electricity consumption patterns of two consumers, the fraudulent consumer and the conscientious consumer, are shown in Figure 2 (Shehzad et al., 2022). It demonstrates that the electrical thief has irregular electricity consumption patterns and that meter manipulation caused its electricity consumption value to decrease. In contrast, an unbiased consumer displays typical electricity consumption patterns.

2.2 Pre-processing and data

The dataset usually comprises outliers and missing values. These figures result from incorrect measuring equipment, such as smart

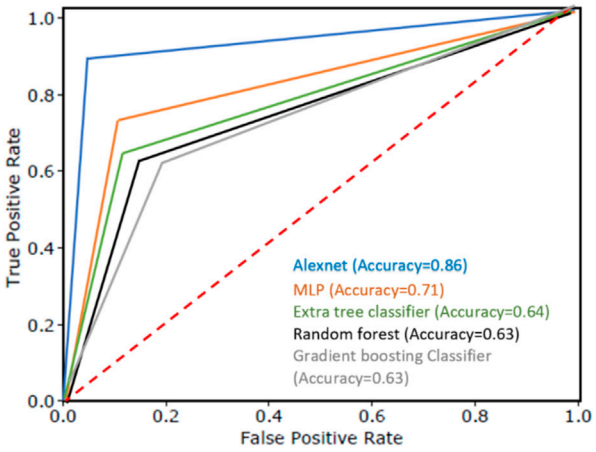

FIGURE 3
Performance graph (Pereira and Saraiva, 2021).

meters and sensors. The use of data pre-processing processes is essential in this matter. As a result, a series of data pre-processing techniques are used in this research, including data interpolation, outlier removal, and normalization of data.

1. Eliminating the missing values: The model wrongly classifies energy thieves and genuine consumers due to the data's lost instances. As a result, the electricity consumption data's missing values must be filled in from (Ali et al., 2023b). The missing values are handled using the data interpolation technique in this instance. This approach fills in the missing value using the average of the closest numbers
2. Outliers identification and elimination: The outliers are values in the dataset that exhibit unusual behavior. A three-sigma rule is used to remove outliers from the whole dataset.
3. Data Normalization: As a result, the values are scaled using the min-max normalization procedure.

2.3 Sampling of imbalanced data

The data imbalance has been addressed using random under-sampling (RUS) techniques, sampling results in removing some actual customer samples during training. Using a different number as a random seed, the RUS technique eliminates the samples of honest customers (Pereira and Saraiva, 2021). Figure 3 illustrates the outcomes after stopping the customer data with a higher likelihood of being mistaken for sincere clients (Pereira and Saraiva, 2021). The picture also displays the outcomes of a random under-sampling experiment using various random seeds. Under-sampling appears to raise the accuracy score considerably. Undersampling significantly boosts recall and precision performance.

2.4 Generation of feature

The baseline electricity consumption dataset is univariate and contains just one electricity consumption feature. However, more statistical traits must be developed for ET to be effective. Therefore, the authors use the original electricity consumption data to compute key statistical parameters, including median, mean, mode, max, and min, to enhance the ET detection performance.

2.4.1 Feature generation using an AlexNet technique

The electricity sector faces various challenges, the main among them being the growing problem of illegal ET. This has led to substantial financial losses for utilities and is also a primary environmental concern, as stolen power usually comes from unsustainable sources or those detrimental to the environment. Therefore, there is an urgent need to develop solutions to detect and deter ET to protect consumers' pockets and the environment.

AlexNet is a deep neural network technology that can be used as a feature extractor for detecting ET (Ullah et al., 2022). It has proven great potential and accuracy for this task, effectively recognizing non-metered customers and fraudulent activities within power grids. The scalability of this system depends on the size of the data set that needs to be processed, as larger datasets may require more computing resources depending on hardware capability. This method also offers scalability when adding additional features, such as recognizing multiple types of fraud or incorporating temperature-sensing devices into existing infrastructure (Raza et al., 2022f; Ullah et al., 2022). Additionally, if new technologies are implemented for electrical networks with better speed performance characteristics than present sensors, artificial intelligence (AI) algorithms will become even faster, allowing AlexNet techniques more remarkable ability to scale up automatically with improved efficiency and precision at matching patterns found in energy (Javaid, 2021).

Smart meters are used to capture electricity consumption data. It frequently contains values that are missing or noisy. Inconsistent electricity consumption readings, missing records, overlapping and redundant records, anomalies, outliers, and other noise can all be discovered in electricity consumption data. These sounds must be managed, or the suggested ET detection model may provide erroneous findings and further increase the false positive rate. We use fundamental pre-processing approaches in this paper to deal with the sounds. The three sigma rule deals with anomalies and outliers, whereas LI is used to fill in missing values, and normalization is used to deal with inconsistent values (Khan et al., 2020).

Furthermore, the AlexNet model discards irrelevant and noisy features. The AlexNet model automatically selects essential features and minimizes noise effects. Again, selecting appropriate electricity consumption characteristics is critical for completing effective ET detection. As a result, we use AlexNet to extract hidden and dense characteristics from the profiles of customers. It was created to address the flaws of the time's traditional models, such as LeNet, which is considered CNN (Habib et al., 2022). AlexNet's architecture is comparable to the LeNet paradigm. The LeNet model includes more filters and convolution, pooling, and fully connected layers. Convolution layers obtain abstract and latent features, whereas pooling layers help get high-level features to reduce the dimensionality curse. Instead of regularisation techniques, dropout layers are also used to control the overfitting problem. Dropout layers, on the other hand, lengthen the AlexNet model's training time. The authors tune the parameters of the AlexNet detection method for ET detection with high accuracy

TABLE 3 Hyperparameters and their values.

Hyperparameters	Values range
Epochs	100
Units	1, 100, 100, 1,001
Dropouts	0.4, 0.5
Batch size	5, 1, 72, 144, 288
Optimizer	Adam
Activation function	Relu, Sigmoid

by splitting the dataset into training, validation, and test sets, then pre-processing the data by normalizing it and dividing it into smaller batches. After that, we initialize the hyperparameters, such as learning rate, batch size, and the number of epochs, as shown in Table 3, and finally, by training the AlexNet model using the training set and adjusting the hyperparameters accordingly to improve accuracy. The authors used the correct validation set to further tune the model's hyperparameters and prevent overfitting. At last, we evaluated the model's performance on the test set and adjusted its hyperparameters. For fine-tuned hyperparameters of the AlexNet model, we also used the RUS sampling technique that perfectly balanced the dataset. The AlexNet model's basic design is shown in Figure 4. Furthermore, the AlexNet block diagram is given in Figure 5, and each component is described in sub-sections.

2.4.2 Layerwise classification of Alexnet technique

Layerwise description is listed below.

1. Layer One (Convolutional layer): The extraction of feature motifs is made more accessible by segmenting an image into smaller parts. The kernel multiplies its components by the pertinent components of the receptive field and then convolves with the pictures using a particular set of weights (Janthong et al., 2023).
2. Layer Two (Pooling Layer): Pooling layers are used to reduce the dimensions of the feature maps. Thus, it reduces the number of learning parameters and the computation performed in the network. The pooling layer summarises the features present in a region of the feature map generated by a convolution layer.
3. Layer Three (Activation Layer): The activation function acts as a decision-making function and aids in recognizing complex patterns. Therefore, choosing the proper activation function can speed up the learning process.
4. Layer Four (Normalization of Batch Layer): Batch normalization is essential because it helps address the internal covariate shift problem in deep neural networks. It normalizes the intermediate outputs of each layer within a batch during training, making the optimization process more stable and faster.
5. Layer Five (Dropout Layer): Dropout produces regularization inside the network by randomly omitting some units or connections with a certain probability, subsequently improving generalization. When numerous connections that learn a non-linear relation collaborate,

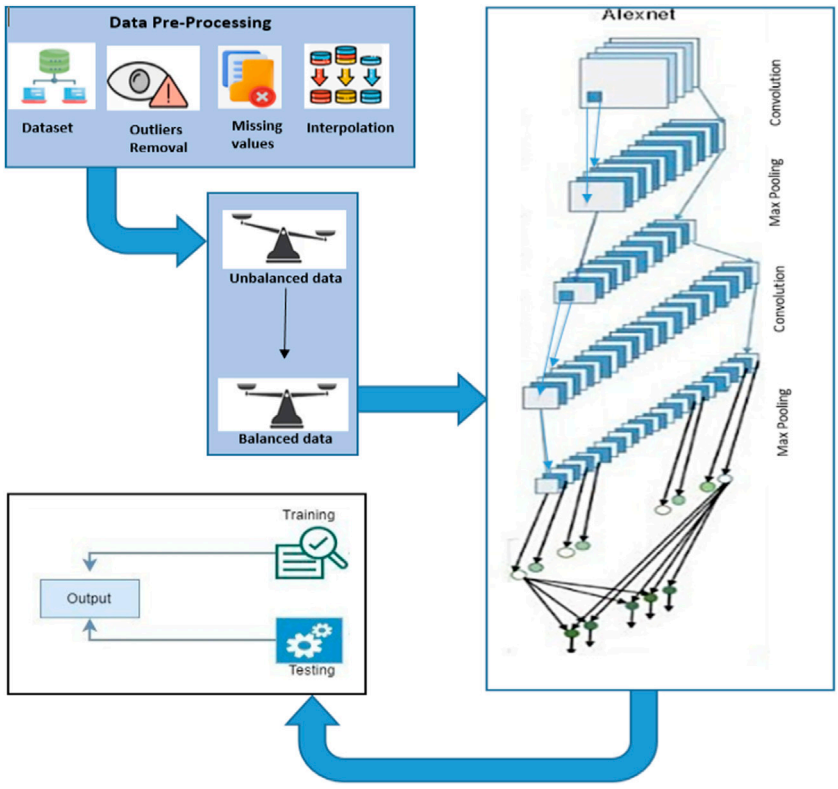

FIGURE 4
Proposed model.

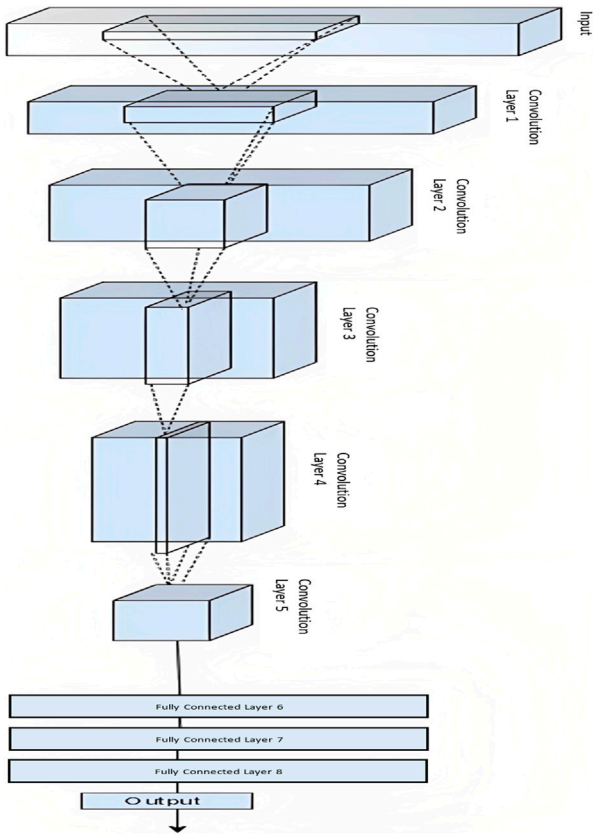

FIGURE 5
Alexnet block diagram.

overfitting in neural networks happens. The reduced network topologies produced by this discretionary elimination of some connections or units are then used to select one representative network with low weights. Then, using this design chosen, all suggested networks are approximated.

6. Layer Six (Flatten Layer): After the operations above, feature maps are converted into 1D data to discriminate between valid and fraudulent electricity consumption patterns. However, because the output of the flattened layer minimizes the overlapping and noisy data, it is considered an extracted feature set in this study. This feature set offers a more accurate representation of the electricity consumption data.
7. Layer Seven and Eight (Fully Connected Layer): AlexNet's last links the neurons of earlier layers with those of later levels. Additionally, from the given feature maps, it extracts global features. Additionally, it gathers the results of the preceding layer to carry out the final categorization.

3 Evaluation and discussion on the AlexNet model

This section discusses the simulation results for the suggested fix. It is contrasted with other benchmark schemes to show the proposed solution's effectiveness.

3.1 Simulation framework

TensorFlow and Keras, two open-source Python libraries, are used to run the simulations. The hyperparameters and their appropriate values obtained during the tuning of the existing AlexNet model are shown in Table 4. Due to their lengthy computation, we did, however, investigate fewer hyperparameters.

3.1.1 Performance metrics

Since accuracy does not provide a trustworthy evaluation for unbalanced classification difficulties, the validation of the classifier using imbalanced data is of concern in the ET detection process. More appropriate performance measurements are used in this situation. PR-AUC, AUC, MCC, recall, and F1-score, in particular, are used to evaluate the effectiveness of the suggested paradigm. The precision determines correctly detected values, such as honest consumers. Which positive class occurrences does the model perceive as the recall indicates trustworthy purchasers? For a more accurate model evaluation, the F1-score assesses the precision-to-recall ratio. Another helpful statistic is the PR-AUC, a graph that shows the recall values on the y-axis and the precision values on the x-axis. The PR-AUC result ranges from 0 to 1. MCC is more trustworthy in terms of all of the performance indicators listed since it takes into account the link between all four possible confusion matrix outputs, namely, false negative (FN), false positive (FP), true negative (TN), and true positive (TP). As a result, the confusion matrix is used to evaluate the performance metrics and provide the following information.

- TP: Reputable users are correctly identified as reliable.
- TN: Use dishonest users to identify themselves as such correctly.
- FP: Honest users are expected to be legitimate users by mistake.

TABLE 4 Limitations with proposed solutions.

Limitations	Solutions	Validation
Imbalanced dataset	The problem of data imbalance is resolved using the RUS technique	Compared to the sampling method
Null/missing values in datasets	Data pre-processing eliminates the null values, and max, min, and median values are calculated to enhance ET detection efficiently	Performance evaluation of proposed and existing techniques is shown in Table 5. Alongside its limitations, the proposed solutions are presented in Table 4
Inappropriate feature engineering	AlexNet is used to enhance the feature extraction procedure using multiple layers	Figure 5 shows the multiple layers of the AlexNet technique

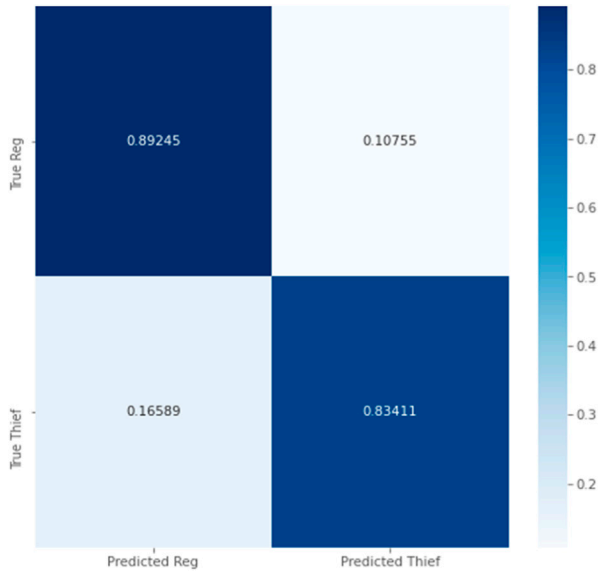

FIGURE 6
Confusion metrics.

- FN: Inaccurate predictions of honest users as legitimate.

Precision (Hand and Christen, 2018), recall (Gu et al., 2019), F1-score (Douzas et al., 2019), and MCC (Greff et al., 2016) are calculated using equations:

$$Recall = \frac{TP}{TP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$F1\ Score = 2^{*}\frac{Precision * Recall}{Precision + Recall} \tag{3}$$

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{4}$$

Where FN, FP, and TP values are used to calculate recall and precision, as shown in Figure 6, while recall identifies the instances of the positive class that the model correctly recognizes as honest consumers, precision displays those values that are reliably classified as such. The F1-score, a more trustworthy statistic than recall and precision, is determined in Eqn. 11. Recall and precision are balanced to get a single score.

4 Proposed technique result

The proposed model AlexNet was trained and tested considering three cases: a 50:50% ratio for training and testing the model, and the second case considering 75: 25% and 90:10% training and testing sets. The model could achieve remarkable performance by outperforming the accuracy confusion matrix, as shown in Figure 7. The model correctly classified all theft consumers (True Positive) without missing many theft consumers in the dataset (False Negative). This exceptional accuracy underscores the effectiveness of the AlexNet model for theft detection, making it a significant accomplishment for theft detection and energy saving in power systems.

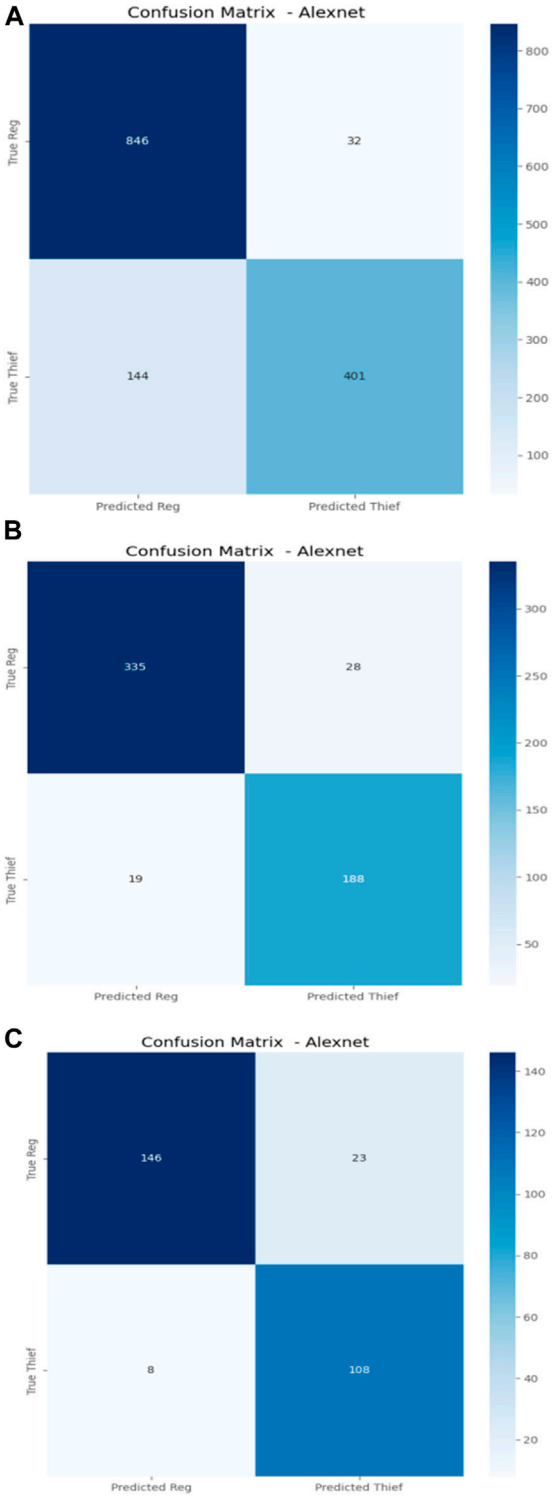

FIGURE 7
Confusion matrix outcomes for the AlexNet model **(A)** (50%, 50%), **(B)** (75%, 25%), **(C)** (90%, 10%).

Our experiments revealed promising outcomes for electric theft detection using AlexNet, as shown in Figure 8. In the first case

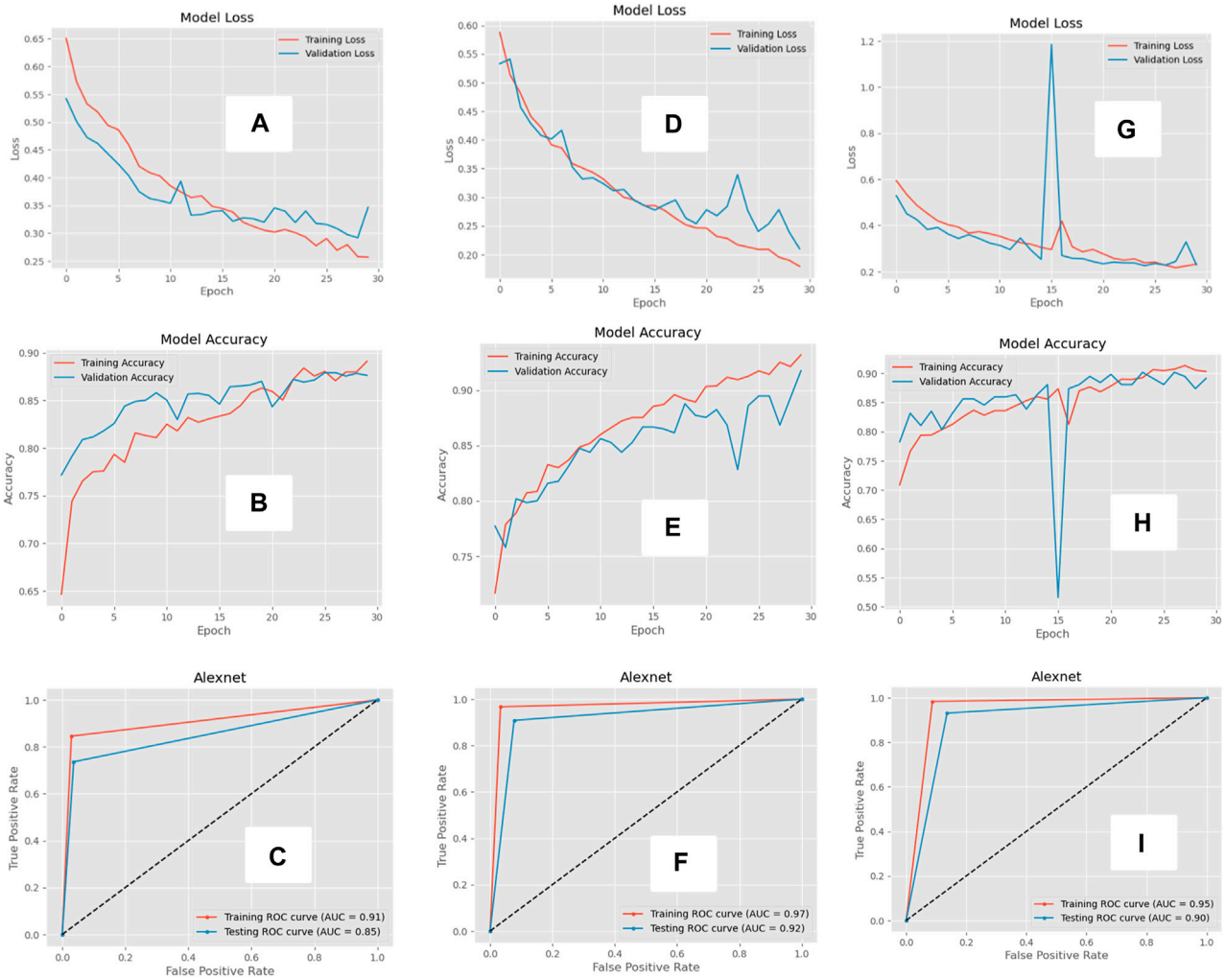

FIGURE 8
The AlexNet results for the first case (50% 50%); Loss **(A)**, accuracy **(B)**, and ROC-AUC; second case (75% 25%); Loss **(D)**, accuracy **(E)**, and ROC-AUC **(F)**; third case (90% 10%); Loss **(G)**, accuracy **(H)**, and ROC-AUC **(I)**.

(50%:50% ratio), the model demonstrated remarkable accuracy and lower training and validation losses a), indicating accuracy that the model effectively learned the underlying patterns of electric theft from the dataset. The training and validation losses in b) are slightly more significant in the case first case. The ROC-AUC curve in c) showcases the model's ability to distinguish between positive and negative instances with high sensitivity and specificity. In the second case (75%:25% ratio), the model exhibited better accuracy levels with slightly lower losses during training and validation d). However, the overall performance remained robust, indicating that the model generalizes well to unseen data, which meant the model could have lower training and validation losses in e) compared to the first case. The ROC-AUC curve f) reinforced the model's proficiency in differentiating electricity theft occurrences from standard electricity consumption patterns. In the third case (90%:10% ratio), the model's accuracy remained consistently high in g), with decreased training and validation losses h). This indicates that increasing the training data leads to improved model generalization. The ROC-AUC curve i) exhibited excellent performance, affirming the model's competence in distinguishing electric theft events from average electricity consumption. However, the limitations of the proposed solutions are presented in Table 4.

4.1 Propose Technique with and Without Pre-processing

In this research study, we also aimed to investigate the impact of pre-processing and without pre-processing techniques on the accuracy of the AlexNet model for a specific task. The task involved predicting a binary flag based on consumer kWh (kilowatt-hour) data. We conducted experiments using both the AlexNet model without pre-processing and with pre-processing. First, we loaded the raw data and separated the features (kWhs) and labels. We applied the RUS technique to balance the dataset to address the imbalance dataset. The RUS technique randomly selects samples from the majority class and removes them until a balance is achieved. After pre-processing, we split the data into train and test

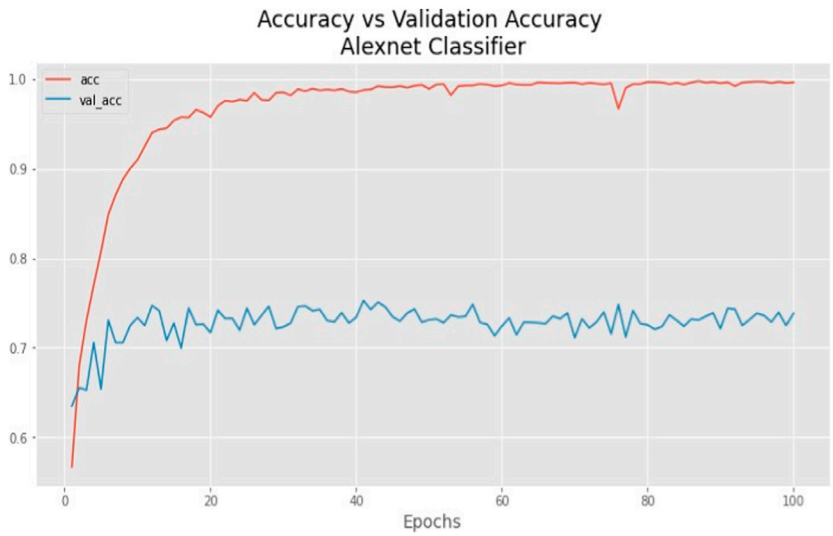

FIGURE 9
Epochs of the proposed model.

TABLE 5 Result summary of proposed and existing models.

Performance metrics	AlexNet	Extra tree classifier	RF classifier	GBDT classifier	MLP algorithm
Precision	0.89	0.77	0.70	0.70	0.73
Recall	0.86	0.55	0.61	0.53	0.70
F1-Score	0.84	0.61	0.60	0.59	0.72
Accuracy	0.86	0.64	0.63	0.63	0.71

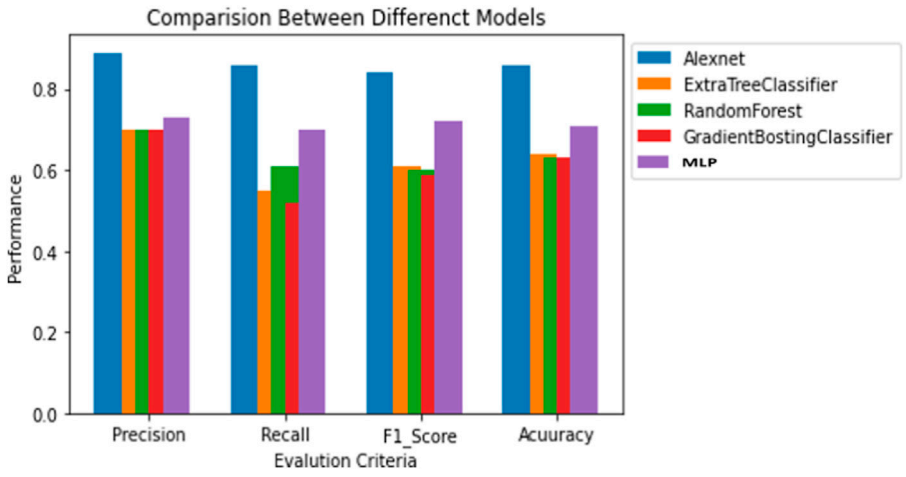

FIGURE 10
Comparison of AlexNet, Extra tree classifier, RF classifier, GBDT classifier, and MLP algorithm.

sets with a 50% test size. We then performed feature scaling using the standard scaler to normalize the data and bring all features to a similar scale.

We used a fully connected neural network architecture for the model without pre-processing. The model consisted of multiple dense layers with ReLU activation functions and dropout layers to

prevent overfitting. We compiled the model using binary cross-entropy loss, SGD optimizer, and metrics, including accuracy and AUC. We trained the model with 30 epochs and a batch size of 32. For the model with pre-processing, we used a convolutional neural network architecture inspired by AlexNet. The model included Conv2D layers with ReLU activation, MaxPooling 2D layers, and dense layers with dropout. We compiled the model with the same loss function, optimizer, and evaluation metrics as the model without pre-processing. The input shape of the model was adjusted to match the reshaped data. We trained the model with pre-processing using the reshaped and scaled data. Again, we used 30 epochs but reduced the batch size to 16 to account for the larger input size and convolutional layers. After training both models, we evaluated their performance on the test set. The model without pre-processing achieved an accuracy of 0.66, while the model with pre-processing achieved a higher accuracy of 0.86. These findings highlight the importance of data pre-processing in improving the performance of deep learning models for specific tasks, such as predicting binary flags based on consumer kWh data.

4.2 Comparison of AlexNet model with other benchmark models results

4.2.1 AlexNet

This section highlights the novelty and contribution of the AlexNet technique. The model's EPOCH procedure, depicted in Figure 9, along with its accuracy and validation accuracy, demonstrates its performance. The orange curve represents the accuracy, while the blue curve represents the validation accuracy. The increasing accuracy in the graphic indicates that the suggested model effectively learns electricity consumption patterns. Additionally, the model converges quickly, benefiting from the latent features' inherent learning capabilities. One of this research's critical contributions is applying the AlexNet technique during the model validation phase. The AlexNet method, known for its pioneering architecture in deep learning, has been integrated into the proposed framework. Notably, the AlexNet technique demonstrates satisfactory performance even without using optimization techniques. The results show that the proposed model achieves over 0.89% precision, 0.86% accuracy, 0.84% F1-score, and 86% recall. This highlights the effectiveness of the AlexNet technique in capturing relevant patterns and classifying the data accurately, as indicated in Table 4. To ensure a fair and comprehensive comparison, this paper includes several benchmark techniques such as random forecast (RF), extra tree classifier, GBDT classifier, and MLP and compares results with the AlexNet model. All these techniques are used as reference points to evaluate the system's performance, further emphasizing the novelty and significance of integrating the AlexNet technique into the framework. The comparison of the AlexNet model with other benchmark models is indicated in Table 5.

Figure 10 demonstrates how the suggested model reduces overfitting and produces the best classification outcomes on unobserved data. Compared to industry-standard methods like the RF classifier and MLP algorithm, it shows how the AlexNet method increases classification accuracy. However, it is impossible to differentiate between dishonest and honest customers using the accuracy of performance statistics. When there is an imbalance between the data classes during categorization, it is misleading. As a result, the proposed model is evaluated using more trustworthy performance criteria, including recall, F1 score, accuracy, and precision. It is discovered that the recommended model performs more efficiently than the current models while using valid measurements. It is also vital to note that the suggested ET detection technique was developed using a sizable collection of precise data from China. The proposed ET detection method is found to be scalable.

5 Conclusion

Simulations employing a large Chinese smart-meter dataset were used to evaluate the AlexNet model's power theft detection capabilities. The goal of these simulations was to identify unauthorized electricity users. AlexNet's new contribution is evident in this case. AlexNet, in the suggested model, made significant progress. The AlexNet method is known for extracting relevant information and improving electricity theft detection. The AlexNet deep learning architecture efficiently captures electricity theft trends and characteristics in the suggested model. The simulation results show that this feature extraction capability increases the model's complexity, improving accuracy, precision, recall, and F1 score. The proposed method also balances dataset types to reduce skewed data. This innovative methodology ensures that the model remains neutral towards the dominant class, allowing it to detect electricity theft even in rare cases. This addition improves the model's reliability and resilience in practical situations. AlexNet's inclusion in the proposed framework opens up many applications for the recommended technique. Power providers and stakeholders can use the model to reduce power losses and detect electricity theft. The proposed technology detects electricity theft, reducing energy sector fraud and financial losses.

The AlexNet technique improves the suggested model's efficacy and reach, making it a significant resource for power providers and industry professionals trying to reduce power losses and address electricity theft. Future power theft detection research could examine innovative algorithms, incorporate cutting-edge technologies like reinforcement learning and swarm optimization, and create hybrid models that combine multiple machine learning methods. In addition, real-time monitoring and anomaly detection can increase electricity theft detection systems' efficiency and timeliness.

6 Limitations and future work

The proposed AlexNet approach, based on CNNs, has several limitations when applied in practical applications. Firstly, due to the large number of parameters used by CNN models such as AlexNet, training these networks is computationally challenging to handle as it requires a significant amount of time, which may be difficult or impossible for some users. Additionally, while CNN architectures are renowned for automatically identifying features from inputs that could otherwise not have been detected with traditional methods, they can suffer from overfitting if given too few input data points and

under-fitting problems if given too many. Finally, these types of networks tend to require more significant amounts of labeled data than other machine learning paradigms, such as SVMs - further limiting their applicability in specific contexts where accurate labeling might not always be possible or efficient. In terms of categorization, the suggested model outperforms the current models. Even though the proposed model is the best option for effective ET detection, there are some sudden variations in the proposed model's performance regarding the input data. The suggested model is also trained on sparse sample data, which hinders its ability to capture finer details of electricity consumption pattern information. To create a robust model, high-sampling ET detection data and various other elements, such as varying customer usage patterns, temperature, and seasonality, will be considered in the future.

Nomenclature.

Electricity theft (ET); Receiver Operating Characteristics under the Area Curve (ROC-AUC); Convolutional Neural Network (CNN); Time Division Multiplexing (TDM); Synthetic Minority Over-sampling Technique (SMOTE); Principal Component Analysis (PCA); Binary Black Hole Algorithm (BBHA); Deep Artificial Neural Network (DANN); Gradient Boosting Machine Algorithm (GBMA); Clustering and Evolutionary Genetic Algorithm (CEGA); Advanced Metering Infrastructure (AMI) networks; Simplified Memory Bounded (SMB); Feature Engineered - CatBoost Algorithm (FECA); Synthetic Minority Oversampling Technique (SMOTE) Algorithm; Multilayer Perception (MLP), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Gated recurrent Unit (GRU); Extreme Gradient Boosting (XG-Boost); Artificial Neural Network–Multilayer Perception (ANN-MLP); State Grid Corporation of China (SGCC).

Data availability statement

The original contributions presented in the study are included in the article/Supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

NK: Conceptualization, Writing–original draft. MAR, Formal Analysis, Writing–original draft, Writing–review and editing. DA: Investigation, Software, Supervision, Writing–original draft. SM: Visualization, Writing–original draft. AA: Formal Analysis, Investigation, Validation, Writing–review and editing. GA: Conceptualization, Writing–original draft, Writing–review and editing. MS: Software, Validation, Writing–review and editing. ET: Software, Supervision, Writing–review and editing. AY: Supervision, Resources, Formal Analysis, Writing–review and editing. MB: Funding, Supervision, Formal Analysis, Writing–review and editing.

Acknowledgments

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was funded by the Deanship of Scientific Research, King Faisal University, Project No. GRANT4741.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Adil, M., Javaid, N., Qasim, U., Ullah, I., Shafiq, M., and Choi, J. G. (2020). LSTM and bat-based RUSBoost approach for electricity theft detection. *Appl. Sci.* 10 (12), 4378. doi:10.3390/app10124378

Ahir, R. K., and Chakraborty, B. (2022). Pattern-based and context-aware electricity theft detection in smart grid. *Sustain. Energy, Grids Netw.* 32, 100833. doi:10.1016/j.segan.2022.100833

Ahmed, M. A., Abbas, G., Jumani, T. A., Rashid, N., Bhutto, A. A., and Eldin, S. M. (2023). Techno-economic optimal planning of an industrial microgrid considering integrated energy resources. *Front. Energy Res.* 11, 1–12. doi:10.3389/fenrg.2023.1145888

Aldegheishem, A., Anwar, M., Javaid, N., Alrajeh, N., Shafiq, M., and Ahmed, H. (2021). Towards sustainable energy efficiency with intelligent electricity theft detection in smart grids emphasising enhanced neural networks. *IEEE Access* 9, 25036–25061. doi:10.1109/ACCESS.2021.3056566

Ali, A., Abbas, G., Keerio, M. U., Koondhar, M. A., Chandni, K., and Mirsaeidi, S. (2023b). Solution of constrained mixed-integer multi-objective optimal power flow problem considering the hybrid multi-objective evolutionary algorithm. *IET Gener. Transm. Distrib.* 17 (1), 66–90. doi:10.1049/gtd2.12664

Ali, A., Abbas, G., Keerio, M. U., Mirsaeidi, S., Alshahr, S., and Alshahir, A. (2023a). Multi-objective optimal siting and sizing of distributed generators and shunt capacitors considering the effect of voltage-dependent nonlinear load models. *IEEE Access* 11, 21465–21487. doi:10.1109/ACCESS.2023.3250760

Aslam, Z., Javaid, N., Ahmad, A., Ahmed, A., and Gulfam, S. M. (2020). A combined deep learning and ensemble learning methodology to avoid electricity theft in smart grids. *Energies* 13 (21), 5599. doi:10.3390/en13215599

Ayub, N., Ali, U., Mustafa, K., Mohsin, S. M., and Aslam, S. (2022). Predictive data analytics for electricity fraud detection using tuned CNN ensembler in smart grid. *Forecasting* 4 (4), 936–948. doi:10.3390/forecast4040051

Badr, M. M., Mahmoud, M. M. E. A., Abdulaal, M., Aljohani, A. J., Alsolami, F., and Balamsh, A. (2023). A novel evasion attack against global electricity theft detectors and a countermeasure. *IEEE Internet Things J.* 11, 11038–11053. doi:10.1109/jiot.2023.3243086

Chicco, G. (2012). Overview and performance assessment of the clustering methods for electrical load pattern grouping. *Energy* 42 (1), 68–80. doi:10.1016/j.energy.2011.12.031

Douzas, G., Bacao, F., Fonseca, J., and Khudinyan, M. (2019). Imbalanced learning in land cover classification: improving minority classes' prediction accuracy using the geometric SMOTE algorithm. *Remote Sens.* 11 (24), 3040. doi:10.3390/rs11243040

Duarte Soares, L., de Souza Queiroz, A., López, G. P., Carreño-Franco, E. M., López-Lezama, J. M., and Muñoz-Galeano, N. (2022). BiGRU-CNN neural network applied to electric energy theft detection. *Electronics* 11 (5), 693. doi:10.3390/electronics11050693

Feng, X., Hui, H., Liang, Z., Guo, W., Que, H., Feng, H., et al. (2020). A novel electricity theft detection scheme based on text convolutional neural networks. *Energies* 13 (21), 5758. doi:10.3390/en13215758

Greff, K., Srivastava, R. K., Koutnik, J., Steunebrink, B. R., and Schmidhuber, J. (2016). LSTM: a search space odyssey. *IEEE Trans. neural Netw. Learn. Syst.* 28 (10), 2222–2232. doi:10.1109/tnnls.2016.2582924

Gu, D., Gao, Y., Chen, K., Shi, J., Li, Y., and Cao, Y. (2022). Electricity theft detection in AMI with low false positive rate based on deep learning and evolutionary algorithm. *IEEE Trans. Power Syst.* 37 (6), 4568–4578. doi:10.1109/tpwrs.2022.3150050

Gu, Y., Cheng, L., and Chang, Z. (2019). Classification of imbalanced data based on MTS-CBPSO method: a case study of financial distress prediction. *J. Inf. Process. Syst.* 15 (3), 682–693.

Habib, S., Abbas, G., Jumani, T. A., Bhutto, A. A., Mirsaeidi, S., and Ahmed, E. M. (2022). Improved whale optimization algorithm for transient response, robustness, and stability enhancement of an automatic voltage regulator system. *Energies* 15 (14), 5037. doi:10.3390/en15145037

Hand, D., and Christen, P. (2018). A note on using the F-measure for evaluating record linkage algorithms. *Statistics Comput.* 28, 539–547. doi:10.1007/s11222-017-9746-6

Hasan, M. N., Toma, R. N., Nahid, A. A., Islam, M. M. M., and Kim, J. M. (2019). Electricity theft detection in smart grid systems: a CNN-LSTM based approach. *Energies* 12 (17), 3310. doi:10.3390/en12173310

Janthong, S., Chalermyanont, K., and Duangsoithong, R. (2023). Unbalanced data handling techniques for classifying energy theft and defective meters in the provincial electricity authority of Thailand. *IEEE Access* 11, 46522–46540. doi:10.1109/access.2023.3274543

Javaid, N. (2021). A PLSTM, AlexNet, and ESNN based ensemble learning model for detecting electricity theft in smart grids. *IEEE Access* 9, 162935–162950. doi:10.1109/access.2021.3134754

Khan, Z. A., Adil, M., Javaid, N., Saqib, M. N., Shafiq, M., and Choi, J. G. (2020). Electricity theft detection using supervised learning techniques on smart meter data. *Sustainability* 12 (19), 8023. doi:10.3390/su12198023

Lepolesa, L. J., Achari, S., and Cheng, L. (2022). Electricity theft detection in smart grids based on deep neural network. *IEEE Access* 10, 39638–39655. doi:10.1109/ACCESS.2022.3166146

Nabil, M., Ismail, M., Mahmoud, M. M. E. A., Alasmary, W., and Serpedin, E. (2019). PPETD: privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks. *IEEE Access* 7, 96334–96348. doi:10.1109/access.2019.2925322

Pamir, Javaid, N., Javaid, S., Asif, M., Javed, M. U., Yahaya, A. S., et al. (2022). Synthetic theft attacks and long short term memory-based preprocessing for electricity theft detection using gated recurrent unit. *Energies* 15 (8), 2778. doi:10.3390/en15082778

Pereira, J., and Saraiva, F. (2021). Convolutional neural network applied to detect electricity theft: a comparative study on unbalanced data handling techniques. *Int. J. Electr. Power and Energy Syst.* 131, 107085. doi:10.1016/j.ijepes.2021.107085

Punmiya, R., and Choe, S. (2021). ToU pricing-based dynamic electricity theft detection in smart grid using gradient boosting classifier. *Appl. Sci.* 11 (1), 401. doi:10.3390/app11010401

Raza, M. A., Aman, M. M., Abro, A. G., Shahid, M., Ara, D., Waseer, T. A., et al. (2023a). A simulation model of climate policy analysis for sustainable environment in Pakistan. *Environ. Prog. Sustain. Energy* 42, e14144. doi:10.1002/ep.14144

Raza, M. A., Aman, M. M., Abro, A. G., Tunio, M. A., Khatri, K. L., and Shahid, M. (2022c). Challenges and potentials of implementing a smart grid for Pakistan's Electric Network. *Energy Strategy Rev.* 43, 100941. doi:10.1016/j.esr.2022.100941

Raza, M. A., Aman, M. M., Rajpar, A. H., Bashir, M. B. A., and Jumani, T. A. (2022d). Towards achieving 100% renewable energy supply for sustainable climate change in Pakistan. *Sustainability* 14 (24), 16547. doi:10.3390/su142416547

Raza, M. A., Aman, M. M., Tunio, N. A., Soomro, S. A., Shahid, M., Ara, D., et al. (2023b). Energy transition through bioelectricity in Pakistan: implications for limiting global mean temperature below 1.5 C. *Environ. Prog. Sustain. Energy* 42 (4), e14189. doi:10.1002/ep.14189

Raza, M. A., Khatri, K. L., and Hussain, A. (2022e). Transition from fossilized to defossilized energy system in Pakistan. *Renew. Energy* 190, 19–29. doi:10.1016/j.renene.2022.03.059

Raza, M. A., Khatri, K. L., Israr, A., Ul Haque, M. I., Ahmed, M., Rafique, K., et al. (2022b). Energy demand and production forecasting in Pakistan. *Energy Strategy Rev.* 39, 100788. doi:10.1016/j.esr.2021.100788

Raza, M. A., Khatri, K. L., Memon, M. A., Rafique, K., Haque, M. I. U., and Mirjat, N. H. (2022f). Exploitation of Thar coal field for power generation in Pakistan: a way forward to sustainable energy future. *Energy Explor. Exploitation* 40 (4), 1173–1196. doi:10.1177/01445987221082190

Raza, M. A., Khatri, K. L., Ul Haque, M. I., Shahid, M., Rafique, K., and Waseer, T. A. (2022a). Holistic and scientific approach to the development of sustainable energy policy framework for energy security in Pakistan. *Energy Rep.* 8, 4282–4302. doi:10.1016/j.egyr.2022.03.044

Razavi, R., Gharipour, A., Fleury, M., and Akpan, I. J. (2019). A practical feature-engineering framework for electricity theft detection in smart grids. *Appl. Energy* 238, 481–494. doi:10.1016/j.apenergy.2019.01.076

Rehan, M., Amir Raza, M., Ghani Abro, A., M Aman, M., Mohammad Ibrahim Ismail, I., Sattar Nizami, A., et al. (2023a). A sustainable use of biomass for electrical energy harvesting using distributed generation systems. *Energy* 278, 128036. doi:10.1016/j.energy.2023.128036

Rehan, M., Raza, M. A., Aman, M., Abro, A. G., Ismail, I. M. I., Munir, S., et al. (2023b). Untapping the potential of bioenergy for achieving sustainable energy future in Pakistan. *Energy* 275, 127472. doi:10.1016/j.energy.2023.127472

Shehzad, F., Javaid, N., Aslam, S., and Umar Javed, M. (2022). Electricity theft detection using big data and genetic algorithm in electric power systems. *Electr. Power Syst. Res.* 209, 107975. doi:10.1016/j.epsr.2022.107975

Singh, S. K., Bose, R., and Joshi, A. (2018). Entropy-based electricity theft detection in AMI network. *IET Cyber-Physical Syst. Theory and Appl.* 3 (2), 99–105. doi:10.1049/iet-cps.2017.0063

Ullah, A., Javaid, N., Asif, M., Javed, M. U., and Yahaya, A. S. (2022). Alexnet, adaboost and artificial bee colony based hybrid model for electricity theft detection in smart grids. *Ieee Access* 10, 18681–18694. doi:10.1109/access.2022.3150016

Zheng, K., Chen, Q., Wang, Y., Kang, C., and Xia, Q. (2018). A novel combined data-driven approach for electricity theft detection. *IEEE Trans. Industrial Inf.* 15 (3), 1809–1819. doi:10.1109/tii.2018.2873814