ORIGINAL RESEARCH

The Institution of Engineering and Technology WILEY

A novel deep learning technique to detect electricity theft in smart grids using AlexNet

Nitasha Khan[1,2] | **Zeeshan Shahid**[2] | **Muhammad Mansoor Alam**[3,4,5] |
Aznida Abu Bakar Sajak[6] | **Mobeen Nazar**[7] | **Mohd Suud Mazliham**[3]

[1]British Malaysian Institute, Universiti Kuala Lumpur, Sungai Pusu, Malaysia

[2]Electrical Engineering department, Nazeer Hussain University, Karachi, Pakistan

[3]Persiaran Multimedia, Multimedia University, Cyberjaya, Malaysia

[4]USA Faculty of Computing, Riphah International University, Islamabad, Pakistan

[5]School of Computer Science, University of Technology Sydney, Ultimo, New South Wales, Australia

[6]MIIT, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

[7]Software Engineering, Bahria University Karachi, Karachi, Pakistan

Correspondence
Nitasha Khan, British Malaysian Institute, Universiti Kuala Lumpur, Sungai Pusu, 53100, Malaysia.
Email: nitasha.khan@s.unikl.edu.my

M.S Mazliham, Persiaran Multimedia, Multimedia University, Cyberjaya, Malaysia.
Email: mazliham@mmu.edu.my

Abstract
Electricity theft (ET), which endangers public safety, interferes with the regular operation of grid infrastructure, and increases revenue losses, is a significant issue for power companies. To find ET, numerous machine learning, deep learning, and mathematically based algorithms have been published in the literature. However, these models do not yield the greatest results due to issues like the dimensionality curse, class imbalance, inappropriate hyper-parameter tuning of machine learning, deep learning models etc. A hybrid DL model is presented 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, and then the feature extraction technique, AlexNet is used to address the curse of dimensionality. An actual dataset of Chinese smart meters is used in simulations to assess the efficacy of the suggested approach. To conduct a comparative analysis, various benchmark models are implemented as well. This proposed model achieves accuracy, precision, recall, and F1-score, up to 86%, 89%, 86%, and 84%, respectively.

1 | INTRODUCTION

The increased size of the electrical system increased power consumption. With increased energy consumption, electricity theft is rising, posing a danger to the effective operation of power grid systems. Theft of power from distribution networks is known as electricity theft (ET). Meter manipulation, meter bypassing, billing problems, and other tactics are employed. Electricity theft is said to be a major issue that causes financial losses. Manual power theft costs an estimated $6 billion [1, 2]. Electric utilities worldwide lose $25 billion yearly due to ET. Electricity theft costs the United States roughly $6 billion yearly, while it costs the United Kingdom up to $232 million. On the other hand, Pakistan loses 0.89 billion rupees every year, whereas India loses 4.8 billion rupees annually; Brazil is another country that loses $4 billion due to electricity theft [3, 4]. The data on economic losses attributable to ET in various nations are shown in Figure 1.

Many research papers have been published to overcome the challenges outlined above. A gradient boosting approach, for example, is employed to identify power theft in [5, 6]. Furthermore, a particular theft window is created during peak hours to
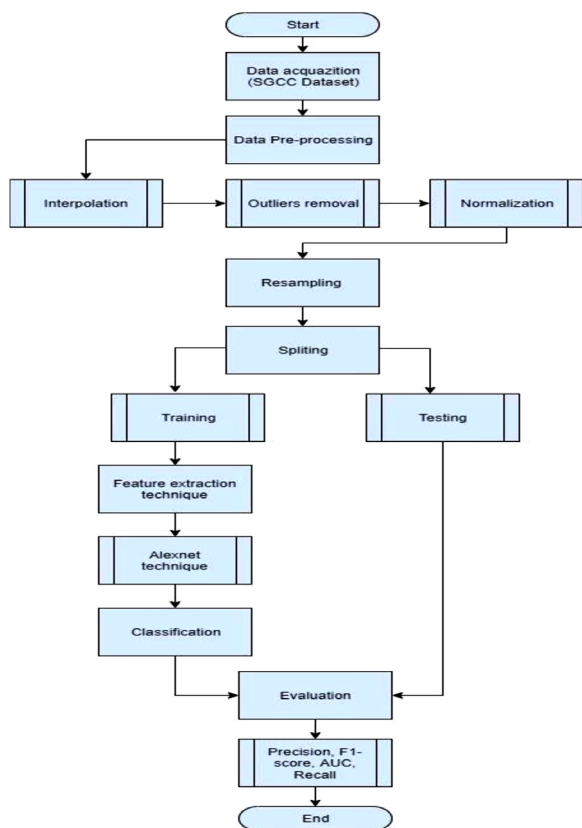
FIGURE 1 Proposed system flowchart.

detect suspect power consumer activity. However, an effective and precise electricity theft detection approach is still mandatory. The ET problem has been addressed in several different ways by researchers. The most prevalent electricity theft detection (ETD) systems are state-based, game theory-based, and machine learning (ML)-based. Hardware elements such as smart meters, distribution transformers, sensors, and other devices are incorporated into state-based systems to detect electricity theft [7]. Some of the most often used artificial intelligence approaches in this discipline include the gradient boosting machine algorithm, genetic algorithm, convolutional neural network, random forest, long short-term memory, bat-based, and deep neural network [8]. One researcher used a state-based approach to identify electricity theft in smart grids that were physically inspired. [8]. A unique type of transformer is connected with smart meters to examine electricity customers' electricity consumption (EC) patterns. The simulation outcomes show that the proposed approach performs better than the base models. In-game theory-based solutions, the power company, and electricity thieves engage in a game. One limitation of this proposed technique is state-based methods of performing ETD, which require more hardware and are more expensive. A game theory-based strategy for smart houses to reduce peak energy costs is presented in [9, 10]. The suggested technique also establishes coordination between smart appliances and minimizes energy losses. The ML-based solutions, on the other hand, utilize the electricity consumption data obtained from smart meters to identify dishonest users of electricity. The

limitation of this proposed technique is that the solutions based on game theory are complicated. The solutions are quite complicated to design and operate since they need to be defined for each player in the game.

Deep learning and convolutional neural networks (CNNs) have made tremendous strides in the field of computer vision. These methods provide robots with the ability to perceive and analyze visual data like the human visual system. CNNs and deep learning both have important roles to play in computer vision applications. They are excellent at automatically recognizing intricate visual patterns from unprocessed pixel data and feature learning and representation. They also make end-to-end learning possible, removing the requirement for human feature engineering and producing more precise models. They have shown to be extremely useful for real-world applications thanks to their capacity to handle complicated patterns and analyze large volumes of data. Pre-trained CNNs may also be used for transfer learning and fine-tuning, allowing them to adapt to particular tasks even with a limited amount of data. Their adaptability to changes, superior object detection, identification, semantic segmentation, and real-time processing further highlight their game-changing influence on computer vision tasks. In general, deep learning and CNNs have transformed computer vision, creating new opportunities in a variety of fields and altering how robots perceive and engage with the visual environment.

The study's emphasis, which is the requirement for an improved activation function in AlexNet for increased performance in the context of energy theft (ET) detection, is introduced in the abstract. ET puts electricity providers in a difficult situation, endangering public safety and costing them money. To solve this problem, researchers have looked at deep learning, machine learning, and mathematical techniques. Existing models, however, have drawbacks such as the dimensionality curse, class imbalance, and inappropriate hyperparameter tuning, which produce unfavourable outcomes. The study suggests a hybrid deep learning (DL) model that integrates preprocessing methods to clean smart meter data and makes use of AlexNet's feature extraction capabilities to solve the curse of dimensionality to address these issues and enhance ET detection. With the use of a genuine dataset of Chinese smart meters, the suggested model is assessed and compared to benchmark models.

The main challenge is to improve AlexNet's activation function so that it can better support the suggested hybrid DL model's detection of power thieves. The goal of the project is to increase accuracy, precision, recall, and F1 score in detecting ET cases by addressing the shortcomings of existing models and making use of AlexNet's feature extraction capabilities. The goal of the project is to advance the field of power theft detection and open the door to more effective and precise ways to address this pressing problem in smart grids.

2 | LITERATURE REVIEW

The table below (Table 1) lists some of the studies conducted on the subject of theft detection. In the table, we covered the

TABLE 1 Previous approach for electricity theft detection (ETD).

Reference	Problem	Dataset used	Technique Used	Performance metrics	Limitations/ Future Work
[22]	Electricity theft in power grids	Ireland and SEAI	CNN- RF	Precision, AUC, recall, and F1 score	Privacy
[2]	Electricity theft	Datasets of different areas randomly	TDTLM	Neglected	The proposed model neglected the focus on performance metrics.
[4]	Electricity theft	SGCC	LSTM (long short-term memory) & bat-based random under-sampling boosting	FI score, precision, recall and ROC-AUC.	The robustness of the system is neglected.
[5]	Electricity theft detection, curse of dimensionality, and Overfitting issues	SEAI	SMOTE	DR, FPR, Time complexity, recall	Overfitting issue of SMOTE, Privacy leakage due to the high sampling rate
[7]	Electricity theft in smart grids	SGCC	Tomek Links, AlexNet, and peephole	PR-AUC, accuracy, precision, recall, F1-score, AUC, and MCC	Considered using low sampling data only
[8]	Electricity theft detection in the commercial area of Brazil	Brazilian	BHA, OPF	Mean accuracy	The dataset is biased on one class, no suitable metrics are used
[9]	Electricity theft	SGCC	Deep artificial neural network	Recall, the F1 score, and AUC.	Experimentation with other supervised learning algorithms
[10]	Electricity theft	Ireland	Gradient boosting machine algorithm, clustering and evolutionary genetic algorithm	Accuracy, F1- score, AUC, and precision	The proposed model does not handle the imbalanced nature of data.
[12]	Electricity theft	Real-time dataset	Load monitoring and AMI networks	ROC-AUC, Accuracy	Security feature results in a slightly low detection rate.
[19]	Electricity theft detection	Malaysia	SVM	Accuracy	Metrics selection is not appropriate.
[21]	Electricity theft detection	SGCC	feature engineered-CatBoost algorithm, SMOTETom ek algorithm	Accuracy, recall, and precision	Improving the system robustness neglected
[23]	Energy theft system		MLP, RNN, LSTM, GRU		The proposed technique has better accuracy and can be implemented in both industrial and commercial sectors.
[24]	Electricity theft detection	Endesa	XG-Boost	TPR, Recall, FPR, Precision, AUC	The proposed model consumes high time on large datasets.
[25]	Electricity theft	Irish	XGBoost	FPR, Recall, AUC, Precision	Not enough training data, limited results, and imbalanced data.
[26]	Electricity theft detection	Brazilian	CSS for ANN-MLP	PSO, SGHS, BP	The proposed model does not handle the imbalanced nature of data.
[27]	Electricity theft detection	Brazilian	ANN-MLP	Accuracy, Precision, Recall	The results of the proposed model are not accurate.
[28]	Electricity theft detection	SEAI	SVM	DR, FPR	The proposed model neglected the accuracy.
[29]	Electricity theft detection	SGCC	CNN-LSTM	MCC, F1- score	The proposed model is consuming high time on datasets.
[30]	Electricity theft detection in a shopping mall in Turkey	BEDAS	Ensemble model (Stacking (LR, RF, KNN)	TPR, FPR, F-measure, precision	The balance of TPR and FPR is neglected in this proposed work.

(Continues)

TABLE 1   (Continued)

Reference	Problem	Dataset used	Technique Used	Performance metrics	Limitations/ Future Work
[31]	Low accuracy, overfitting, and high FPR in ETD	Self-made dataset	LSTM	Precision, Recall, F1- score, Convergence speed	Not suitable for large datasets

problem, the answer, the approaches utilized to provide the solution, the benefits shown in previous work and any future study, and the constraints of that specific research. In the recognized problem of power theft, temperature-dependent has been presented to work as a solution using smart meter data for the stated problem, which offered superior outcomes in the end [2]. Another study employed the finite mixture model to handle the problem of electricity theft, as well as the gradient boosting machine method, clustering, and evolutionary genetic algorithms. The outcomes reveal it enhanced handling of attack circumstances. The approach has also been recommended for future use in utility corporations [9]. Another study conducted in [8] offered a comparison to determine an appropriate for electricity theft using deep neural network technology, which supplied Recall, F1 score, and AUC. Other supervised learning algorithms have been proposed for further investigation. The electricity problem in smart grids was solved in [7] by employing synthetic monitoring samples, the Tomek, and Peephole techniques. It has been recommended that future power providers follow the suggested model for reducing power losses. Another study published in [4] offered a model for theft detection that uses long short-term memory and a bat-based approach to enhance unbalanced data, parameter optimization, overfitting, and attain F1 score, precision, recall, and ROC-AUC. The proposed paradigm may eventually be applied to electricity information for both commercial and residential buildings. The research in [12] used a Privacy-Preserving Electricity Theft Detection Scheme with Load Monitoring and Billing for AMI Networks to detect fraudulent clients.

The author in [11] proposes an optimal scheduling model for isolated microgrids using automated reinforcement learning-based multi-period forecasting of renewable power generations and loads. It involves a prioritized experience replay automated reinforcement learning (PER-AutoRL) to simplify deployment, a single-step multi-period forecasting method based on PER-AutoRL, and a scheduling model considering demand response to minimize total microgrid operating costs. Simulation results show that this approach significantly reduces system operating costs by improving prediction accuracy. The only thing that might be improved in the future is privacy. The proposed methodology in [13] is an ensemble le machine learning (ML) model for the detection of energy theft in smart grids using customers' consumption patterns. Several algorithms, including adaptive boosting, categorical boosting, extreme boosting, random forest, and extra trees, were tested to find their false positive and detection rates. An extensive analysis based on a practical dataset of 5000 customers revealed that bagging models outperformed other algorithms, with the random forest and extra trees models achieving the highest area under the curve score of 0.90. The precision

analysis showed that the proposed bagging methods perform better.

The paper [14] presents a hybrid deep neural network model that combines a convolutional neural network, particle swarm optimization, and gated recurrent unit. It aims to perform accurate electricity theft detection and overcome issues in existing models. The proposed model is evaluated by performing simulations in terms of accuracy, the area under the curve, F 1 -score, recall, and precision. The results indicate that the proposed hybrid deep neural network model is more efficient in handling class imbalance issues and performing electricity theft detection.

The proposed model in [15] maintained the role of ETD considering cost-efficiency in smart grid and handling the large electricity consumption dataset where researchers used using three modules: data imputation, outlier handling, normalization, on and class balancing algorithms, three different machine learning (ML) methods, and a temporal convolutional network (TCN). Experimental results confirm that the proposed framework yields a highly-accurate, robust classification performance, in comparison to other well-established machine and deep learning models.

The paper [16] compares three gradient boosting machines for electricity theft detection, that is, extreme gradient boosting, light gradient boosting machine, and cat boosting. It conducts experiments on a realistic dataset released by the State Grid Corporation of China with true malicious samples. Experimental results show that gradient-boosting machines outperform the wide and deep convolutional neural networks for electricity theft detection. An ensemble model for electricity theft detection method based on genetic optimization is developed in [17]. Synthetic samples are prepared through SMOTE, features of anomalous electricity consumption are extracted through PCA, and an ensemble deep learning network based on AdaBoost is established to mine implicit information in continuous time series data. The hyperparameters of the deep neural network are optimized based on a genetic algorithm. The results show that the model is superior to other detection methods in terms of sensitivity and AUC. The paper [18] proposes a hybrid method combining an adaptive boosting algorithm (AdaBoost) and convolutional neural networks (CNN) for electricity theft detection. Multiple CNN-based classifiers are trained to extract different features from the electricity consumption data, and AdaBoost combines them into a strong one according to their performance. Experimental results based on the Irish Smart Energy Trial show the hybrid classifier has better performance than other conventional data-driven methods in electricity theft detection.

The research in [19] the table below focuses on the Irish smart energy trail utilizing the XGBoost methodology, which

has great accuracy and resilience. The study has some limitations, such as restricted data collection and outcomes. The costs sustained in Brazil due to ET are significant, with commercial losses reaching $4 billion in 2011. The authors employ the Binary Black Hole Algorithm (BBHA) to solve this issue. Regarding precise NTL identification and execution speed, the method beats current optimization strategies like genetic and particle swarm optimization techniques. However, reliable performance metrics like recall and accuracy are not used to evaluate the model.

A trustworthy assessment metric is critical for measuring model performance in an unbalanced data classification challenge [20]. For IOT-based smart houses, the research in [21] has produced a revolutionary supervised machine learning-based theft detection technique. The suggested model combined SMOTETomek with a feature-engineered CatBoost algorithm. The SMOTETomek approach, which concurrently over- and under-samples the data classes, was employed to prevent data class imbalances.

The CatBoost algorithm's intelligence categorizes data into real and fraudulent consumers. The result shows the model achieved accuracy, recall, and precision. The FDIAs detection algorithm model based on CNN-GRU was introduced in [32] to detect false data injection attacks (FDIAs) in power grid reconstruction and solve the problem of high data dimension and bad abnormal data processing in the power system. The results show that in the IEEE14-bus node and IEEE118-bus node systems, the overall distribution of the state estimated before and after the attack vector injection is consistent with the initial value. In the iFores algorithm, the number of iTree and the number of samples affect the extraction of abnormal score data. shows good detection effects under high attack intensity, with an accuracy rate of more than 95%, and its performance is better than other traditional detection algorithms.

A unique Smart Energy Theft System (SETS) was created in the study [23] to identify energy theft. As part of SETS, a Multi-Model Forecasting System was created that combines machine learning models such as the Long Short-Term Memory (LSTM), Multi-Layer Perceptron (MLP), and Gated Recurrent Unit (GRU). Moreover, SETS made use of the Simple Moving Average statistical model (SMA). Furthermore, SETS used a statistical model known as Simple Moving Average (SMA). The algorithm shows accuracy and future use in the industrial and commercial sectors. Previously, electrical thefts were detected by onsite field inspection, which is a time-consuming and costly task. Many researchers tried to overcome these issues through machine learning and deep learning techniques. Power theft detection is challenging in several ways, including resolving data imbalance [33, 34], choosing useful input features, and maintaining detection accuracy while avoiding false positives. Unbalanced data analysis is one of the key worries, and ETD becomes challenging. The scholar must design the technique to learn irregular and regular patterns. Despite the severely unbalanced data, a trained model can still produce a highly accurate result if it correctly distinguishes between samples from minority and majority classes.

Parameters like the Precision-Recall Curve, AUC, Matthews Correlation Coefficient (MCC), and Area under the Curve of Receiver Operating Characteristics (AUC-ROC) are frequently employed for both majority and minority class anomaly identification because of their high accuracy.

High false positive rates in datasets where many legitimate consumers are mistakenly identified as fraudulent customers and unbalanced data are other issues that arise while detecting theft. The issue is that compared to fraudulent customers in the dataset, most regular customers are also classified as fraudulent, which leads to biased classification and misclassification of minority samples [28]. In addition to those two issues, data resampling techniques have Overfitting and information loss problems. A model is suggested to perform ETD in power networks while keeping the difficulties mentioned above in mind.

High false positive rates in datasets where many legitimate consumers are mistakenly identified as fraudulent customers and unbalanced data are other issues that arise while detecting theft. The issue is that compared to fraudulent customers in the dataset, most regular customers are also classified as fraudulent, which leads to biased classification and misclassification of minority samples [35]. In addition to those two issues, data resampling techniques have Overfitting and information loss problems. A model is suggested to perform ETD in power networks while keeping the difficulties above in mind. This research [36] highlights the significance of smart meters in a smart grid system and emphasizes the potential of machine learning and deep learning approaches for analyzing energy consumption behaviour and detecting theft in smart meter data. The proposed theft detection dataset (TDD2022) and the machine learning-based solution provide valuable resources for automated theft identification in the smart grid, offering a benchmark for comparative studies and demonstrating the effectiveness of the random forest model in achieving improved performance metrics by 10% or more compared to other models. In this research [37], authors emphasize the significance of non-technical loss (NTL) detection in the context of electricity theft, which poses challenges for distribution network operators (DNOs) and affects the quality of the supply. The introduction of a new data set, incorporating location information of missing values, coupled with a neural network model built through neural architecture search (NAS), demonstrates promising results with an excellent AUC value of approximately 0.926. The use of NAS enables automatic model updates, making it a user-friendly tool for engineers without expertise in neural networks, as highlighted by the case study employing Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for missing value pattern analysis.

The authors highlight the issue of non-technical loss (NTL) in the electricity grid system in their research paper [38], emphasizing the threat it poses to sustainability and stability. The proposed approach utilizing deep reinforcement learning (DRL) addresses the challenge of imbalanced electricity usage datasets and eliminates the need for extensive preprocessing or dataset balancing. The simulation results demonstrate the superiority of the proposed method, outperforming

conventional algorithms in detecting NTL across different simulation environments. Non-technical losses (NTLs) pose significant challenges to the electricity distribution system in developing countries, impacting its quality and creating economic issues. Despite regulatory advancements in Brazil, the high levels of unbilled electricity consumption persist, affecting tariffs, investment capacity, and public policy development. This research paper [39] emphasizes the need for coordinated strategic actions, including a cultural shift in attitudes towards electricity theft, and aims to provide valuable insights to regulatory authorities, government, concessionaires, and researchers to develop practical solutions for mitigating NTLs in Brazil.

In summary, the literature on electricity theft detection presents a wide range of approaches and techniques to address this critical issue. Researchers have explored various machine learning algorithms, including deep neural networks, gradient boosting machines, and ensemble models, to achieve accurate and reliable detection results. Many studies have focused on utilizing smart meter data, temperature-dependent solutions, and advanced metering infrastructure (AMI) networks to enhance the detection process [40]. 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 positive rates, and overfitting have been recognized and addressed in the literature. Researchers have proposed methods to handle these challenges, including the use of performance metrics, ensemble techniques, and optimization algorithms. Additionally, there is a growing emphasis on system robustness and the need for reliable performance evaluation.

Future research directions in electricity theft detection may include the exploration of novel algorithms, the integration of advanced technologies such as reinforcement learning and swarm optimization, and the development of hybrid models that combine multiple machine learning techniques. Furthermore, the adoption of real-time monitoring and anomaly detection approaches could enhance the responsiveness and effectiveness of electricity theft detection systems.

Overall, the literature review highlights the ongoing efforts to combat electricity theft through innovative approaches and the importance of developing robust, accurate, and efficient detection systems to ensure the integrity and sustainability of the electricity grid.

3 | THE PROPOSED SYSTEM

This section goes over the suggested method. Figure 1 depicts the suggested technique's flowchart, while Figure 5 illustrates the proposed technique's mechanism in all of 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.

TABLE 2 Information of State Grid Corporation of China (SGCC) dataset.

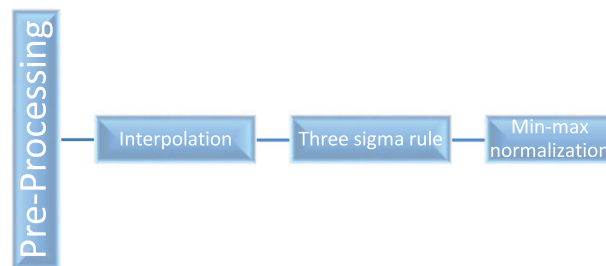| Explanation	Values
Total consumers	42,372
Data collection period	01-01-2014 to 31-10-2016
Honest consumers	38,575
Theft consumers	3,615

FIGURE 2 Pre-processing of data.

3.1 | Dataset details

The suggested technique is based on real electricity consumption data from the State Grid Corporation of China (SGCC) [41]. Table 2 shows the details of the dataset.

Most researchers use the state grid of China dataset for electricity theft 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 in better-apprehending electricity thefts 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 in comparison. Thus, making it 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 over vast territories without any manual efforts needing to be expended into collecting actual field readings from those locations directly.

3.2 | Pre-processing and data

The dataset used in this research often contains outliers and missing values, which can arise from various sources, such as errors in smart meters and sensors. To ensure the accuracy and reliability of the analysis, the implementation of data pre-processing techniques becomes indispensable. In this study, several data pre-processing advantages were leveraged, including data interpolation, outlier removal, and data normalization as illustrated in Figure 2. Data interpolation helps in filling in missing values by estimating them based on existing data points, reducing the impact of incomplete records. Outlier removal

TABLE 3 Advantages of pre-processing.

Steps	Pre-processing steps	Advantages
1	Data normalization	Normalization of input data ensures features are scaled similarly, preventing dominance of certain features due to larger magnitudes. This improves convergence and enhances overall training efficiency.
2	Data augmentation	Data augmentation techniques (rotation, flipping, scaling) increase training dataset diversity. This makes the model more robust, generalizes better to unseen data, reduces overfitting, and improves real-world performance.
3	Local contrast normalization	This step enhances local contrast, normalizes the image, and reduces sensitivity to varying lighting conditions, improving object recognition under different illuminations.
4	Centre cropping and resizing	AlexNet utilizes centre cropping and resizing of images to a fixed size, ensuring consistent image size for simpler model architecture, reduced computational complexity, and preserved important features.
5	Batch processing	Batch training optimizes the learning process by processing data in batches, reducing memory requirements, enabling parallelization, and improving overall training efficiency.
6	Image normalization	Image normalization transforms pixel values to have zero mean and unit variance, controlling model sensitivity to pixel intensities and accelerating the learning process.
7	Feature extraction	Pre-processing steps in AlexNet extract meaningful features from input images, enabling the model to learn hierarchical representations for improved object recognition accuracy.

eliminates erroneous data points that could adversely affect the model's learning process and final predictions. Lastly, data normalization scales the features to a common range, preventing any single feature from dominating the model and ensuring fair contributions from all attributes. Table 3 provides a detailed exploration of the advantages of employing data pre-processing techniques in conjunction with the AlexNet technique for electricity theft detection. By utilizing methods such as data interpolation, outlier removal, and data normalization, the dataset's imperfections are effectively addressed. These pre-processing steps enable the AlexNet technique to handle noise, inconsistencies, and missing values, thereby enhancing its ability to extract meaningful patterns from the data. As a result, the overall performance of the electricity theft detection model is significantly improved, leading to more accurate and reliable results. The successful integration of data pre-processing and the AlexNet architecture underscores its potential as a robust and efficient approach to combating electricity theft and promoting the security and efficacy of power systems.

3.3 | Eliminating the missing values

The model wrongly classifies energy thieves and genuine consumers due to the source data's lost instances. As a result, the EC data's missing values must be filled in. 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.

If the values close by are also missing, the missing value is substituted with 0.

To refill the missing values from [42], the following Equation (1) is employed.

$$(z) = \begin{cases} zi + 1 + zi + 12 \ if \ zi \in NaN, \\ zi - 1 \& and \ zi + 1 \notin NaN, 0 \ if \ zi \in NaN, \\ zi - 1 \ or \ and \ zi + 1 \notin NaN, if \ zi \ NaN, \end{cases} \quad (1)$$

zi represents the value of a customer with electricity consumption data over a period and NaN represents the nonnumeric values.

It contains 42,372 EC records. Where 91 percent of customers are truthful, and 9% are deceitful. The information concerning the defrauded customers is accurate. The disparity between honest and dishonest customers demonstrates the unbalanced nature of data.

The electricity consumption (EC) patterns of two consumers, the dishonest consumer, and the honest consumer, are shown in Figure 3. It demonstrates that the electrical thief has irregular EC patterns and that meter manipulation caused its EC value to decrease. In contrast, an unbiased consumer displays typical EC patterns.

3.4 | Outliers identification and elimination

The outliers are values in the dataset that exhibit unusual behaviour. As specified in the equation, a three-sigma rule is used to remove outliers from the whole dataset in Equation (2),
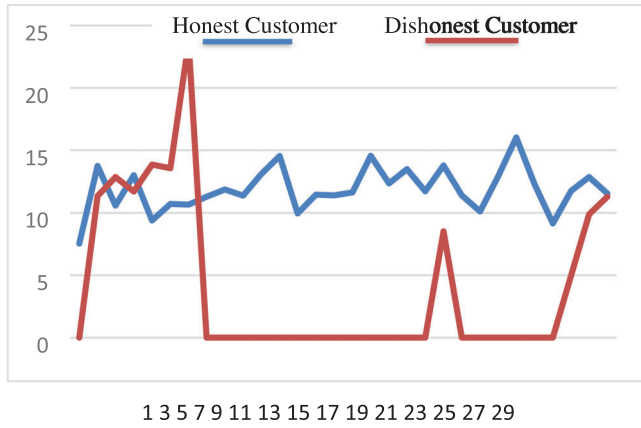
FIGURE 3 Electricity consumption pattern.

which is taken from [42]:

$$f(xi) = \begin{cases} avg(x) + 2\, std(x), if\ xi > avg(x) + 2\, std(x) \\ xi, \qquad else \end{cases} \qquad (2)$$

where x is a day-by-day vector made up of xi, $avg(x)$ is the average value of x, and std (x) is the standard deviation x. It's worth noting that we only look at the positive deviation in Equation (2). This is because each person's electricity use is different. After analyzing the electricity, the user is always larger than 0. Data from 1035 days of consumption. In conclusion, by using this strategy, outliers can be effectively mitigated.

3.5 | Data normalization

Normalization of data is a crucial step that comes after the outliers' removal. It is critical to increase the convergence rate and decrease the execution time in neural networks. Various features in the dataset have different values. As a result, the values are scaled using the min-max normalization procedure.

Equation (3) is used for the min-max normalization and is referenced in [42]:

$$f(xi) = xi - \min(x) \max(x) - \min(x) \qquad (3)$$

where max (x) is the maximum value in x and $\min(x)$ is the minimum value in x.

3.6 | Sampling of imbalanced data

Using (RUS) random under-sampling techniques, the data imbalance has been addressed. Undersampling results in the removal of some real customer samples during training. Using a different number as a random seed, the RUS technique eliminates the samples of honest customers.

Figure 4 illustrates the outcomes after eliminating the customer data with a higher likelihood of being mistaken for sincere clients. The picture also displays the outcomes of a ran-
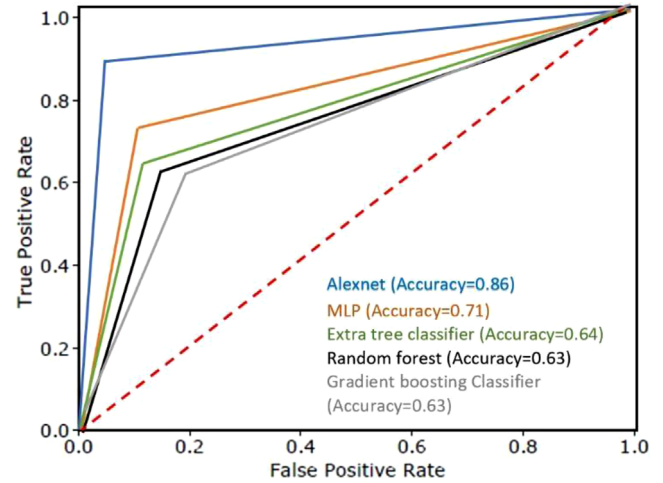

FIGURE 4 Performance graph.

dom under-sampling experiment using various random seeds. Under-sampling appears to considerably raise the accuracy score. Undersampling significantly boosts recall and precision performance.

3.7 | Generation of feature

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

3.7.1 | Feature generation using an AlexNet technique

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

AlexNet is a deep neural network technology that can be used as a feature extractor for detecting electricity theft. It has proven to have great potential and accuracy for this type of 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 it comes to adding additional features such as recognizing multiple types of fraud or incorporating temperature sensing devices into existing infrastructure. Additionally, if

new technologies are implemented for electrical networks with better speed performance characteristics than present sensors, AI algorithms will become even faster, allowing AlexNet techniques greater ability to scale up automatically with improved efficiency and precision at matching patterns found in energy.

For any detection approach to be successfully scaled up, it must remain efficient even as new data points get added over time or certain parameters change suddenly (such as the power supply interruption). In terms of scalability, the proposed electricity theft detection framework relies on advanced deep learning models that can automatically adapt their parameters. This allows them to perform consistently despite unexpected changes, whether from natural causes like lightning strikes or criminal activity like tampering with transformers etc. To conclude, its ability to scale itself dynamically during runtime given a suitable training dataset and parameter tuning strategy enabled via AI support, along with the other measures mentioned above, makes the proposed electricity theft method relatively robust compared to traditional approaches employed so far, making implementation much more viable.

The computational cost of the AlexNet approach for detecting electricity theft is relatively low due to the design decisions taken in its architecture. While initially devised as an image recognition convolutional neural network (CNN) by Krizhevsky et al., subsequent researchers have applied it to other problems such as outlier and anomaly detection, where the class imbalance between classes represents a challenge. The effective utilization of pre-trained weights further reduces computational costs associated with training a deep model from scratch while maintaining high performance on highly imbalanced datasets. As such, AlexNet has been found useful for applications related to power fraud and leakage assessment tasks, providing significant financial benefits within an electric utility setting via real-time intrusion detection algorithms at a minimal computational cost. By leveraging machine learning algorithms such as convolutional neural networks (CNN), the AlexNet model can take inputs of electrical current analyzer patterns it finds using deep-learning methods, and make predictions about likely instances of tampering or misrepresentation. Accuracy rates are high for this method, making it a cost-effective solution for detecting fraudsters quickly and reliably without the need for human intervention.

Smart meters are used to capture EC data. It frequently contains values that are missing or noisy. Inconsistent EC readings, missing records, overlapping and redundant records, anomalies, outliers, and other noise can all be discovered in EC data. These sounds must be managed, or the suggested ETD model may provide erroneous findings and increase the FPR even further. 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.

Furthermore, the AlexNet model discards irrelevant and noisy features. The AlexNet model automatically selects essential features and minimizes noise effects. Furthermore, selecting appropriate EC characteristics is critical for completing effective ETD. 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 [37]. AlexNet's architecture is comparable to the LeNet paradigm. However, as compared to the LeNet model contains more filters. Convolution, pooling, and fully connected layers are included.

Convolution layers are utilized to obtain abstract and latent features, whereas pooling layers are useful for obtaining high-level features, reducing the dimensionality curse. Instead of regularization techniques, dropout layers are also utilized to control the overfitting problem. Dropout layers, on the other hand, lengthen the AlexNet model's training time. Authors tune the parameters of the AlexNet detection method for electricity theft detection with high accuracy by various steps including splitting the dataset into training, validation, and test sets then pre-processing the data by normalizing it and splitting it into smaller batches. After that, we initialize the hyperparameters, such as learning rate, batch size, and the number of epochs, 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 tune the model's hyperparameters further and prevent overfitting. And at last, we evaluate 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.

Figure 5 illustrates the fundamental architecture of the AlexNet model. Each component's detailed explanation is presented below, offering insights into the inner workings of the model and its key elements.

3.8 | Layerwise classification of AlexNet technique

3.8.1 | Layer one (Convolutional layer)

Each neuron is one of the convolutional kernels that make up the convolutional layer. The convolution operation becomes a correlation operation if the kernel is symmetric [31].

The method used by convolutional kernels involves cutting the image into tiny sections, known as receptive fields. The extraction of feature motifs is made easier by segmenting an image into smaller parts. The kernel multiplies its components by the pertinent components of the receptive field, then convolves with the pictures using a particular set of weights [42]. One method to describe a convolution operation is as follows:

$$f_l^k(p,q) = \sum_c \sum_{x,y} i_c(x,y).e_l^k(u,v) \tag{4}$$

where (u,v) x, is an element of the input image tensor. Convolutional operations can share their weights, allowing for extracting various sets of features from an image by sliding kernels with the same set of weights, making CNN parameters more effective than fully linked networks. Based on the kind and size of
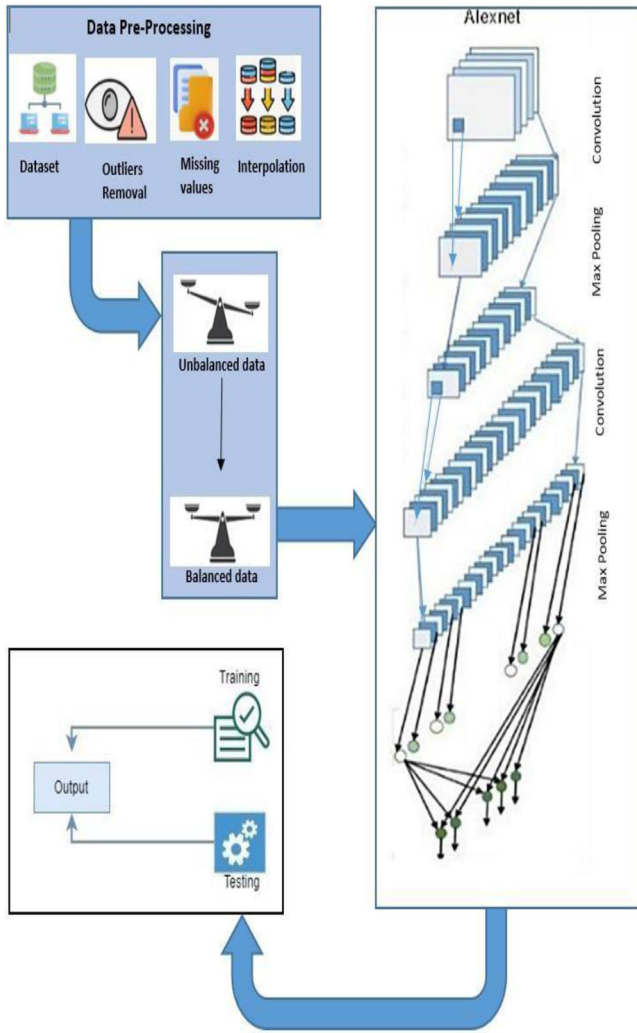
FIGURE 5 Proposed model.

filters, the type of padding, and the direction of convolution, convolution operation can be further divided into many types [43].

3.8.2 | Layer two (Pooling layer)

The convolution procedure produces feature patterns that can appear in various places throughout the image. As long as a feature's approximate position concerning other features is kept once it has been retrieved, its precise location becomes less crucial. A fascinating local procedure is pooling or down-sampling [43]. It compiles similar information around the receptive field and generates the response that dominates this particular small area. Equation (5) gives an example of how to pool data.

$$Z_l^k = g_p \left(F_l^k \right) \tag{5}$$

In the equation above, k Fl, the result of a convolution, is employed. It is provided to the activation function (.) a g, which incorporates nonlinearity and generates a modified output, k

Tl, for the lth layer. The literature uses a variety of activation functions, such as the sigmoid, tanh, max-out, SWISH, ReLU, and ReLU variants, such as the leaky ReLU, ELU, and PReLU, to instill non-linear combinations of traits. However, ReLU and its modifications are preferred as they help to address the vanishing gradient problem. The pooling technique can obtain a mixture of robust features to translational shifts and small distortions [35, 41, 45]. In addition to controlling the network's complexity, shrinking the feature map to an invariant feature set enhances generalization by reducing overfitting. CNN employs a variety of pooling formulations, including average, max, L2, spatial pyramid pooling, overlapping etc.

3.8.3 | Layer three (Activation layer)

The activation function acts as a decision-making function and aids in recognizing complex patterns. Therefore, choosing the right activation function can speed up the learning process. The equation defines the activation function for a convolved feature map (3).

$$T_l^k = g_p \left(F_l^k \right) \tag{6}$$

MISH, one of the most recently proposed activation functions, beat ReLU in most of the previously proposed deep networks when tested on benchmark datasets [44]

3.8.4 | Layer four (Normalization of batch layer)

Batch normalization solves the issues brought on by the internal covariance shift in feature maps. The hidden units' distribution values are altered by the internal covariance shift, which slows convergence (by capping the learning rate at a low value) and calls for careful parameter setting. The equation shows batch normalization for a modified feature map, k Fl (4).

$$N_l^k = \frac{F_l^k - \mu_\beta}{\sqrt{\sigma_B^2 + \varepsilon}} \tag{7}$$

Equation (7) shows the mean and variance of a feature map for a micro-batch as well as the normalized feature map (N_l^k) and input feature map (F_l^k), respectively. By setting feature-map values to have a zero mean and unit variance, batch normalization unifies the distribution of those values. Additionally, it functions as a regulator and smoothens the gradient flow, enhancing the network's generalization.

3.8.5 | 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
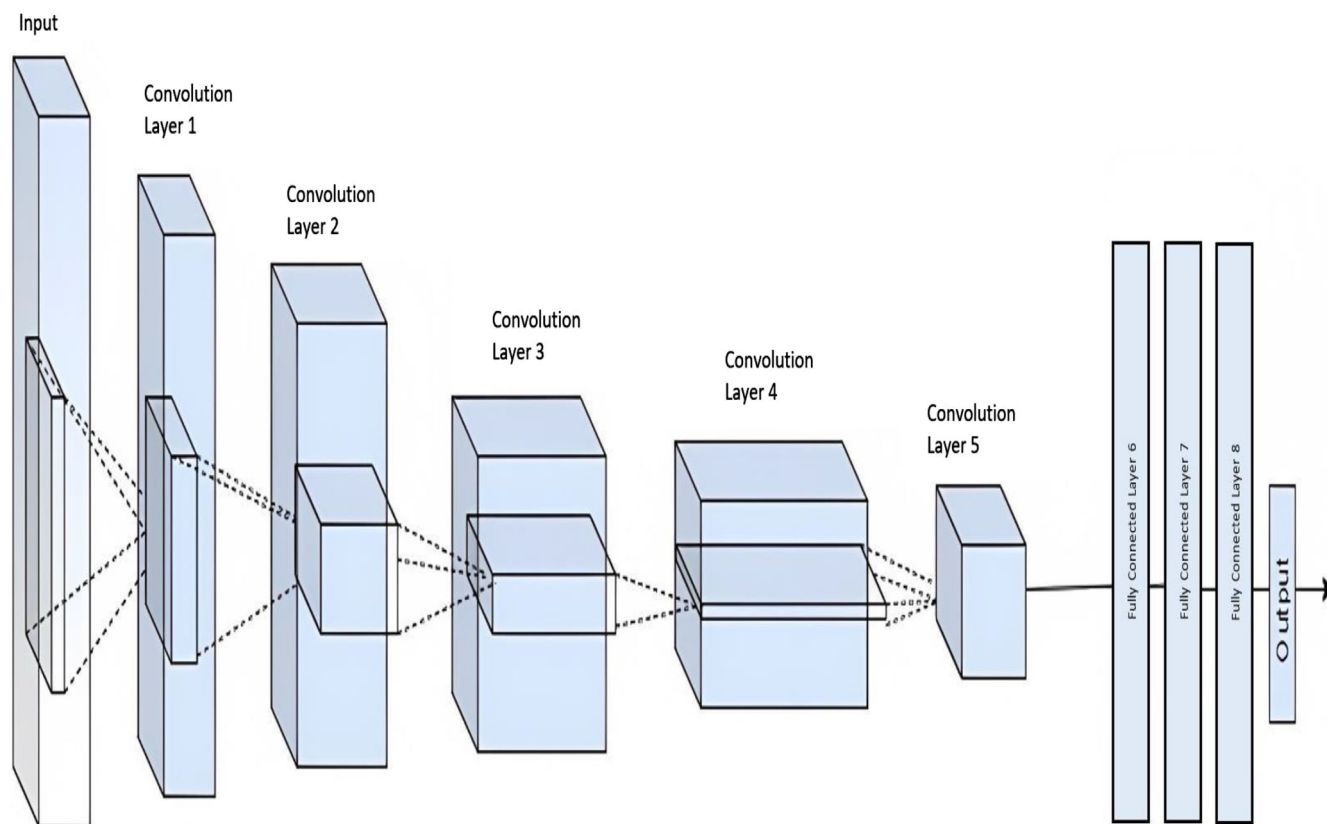
FIGURE 6 AlexNet block diagram.

connections that learn a non-linear relation collaborate, Overfitting in NNs 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 selected design, all suggested networks are approximated.

3.8.6 | Layer six (Flatten layer)

After the operations above, feature maps are converted into 1D data to discriminate between valid and fraudulent EC patterns. However, because the output of the flattened layer minimizes the overlapping and noisy data, it is taken into account as an extracted feature set in this study. This feature set offers a more accurate representation of the EC data.

3.8.7 | Layer seven (Fully connected layer)

At the network's end, classification is often done using the fully linked layer. Unlike pooling and convolution, it is a global operation. With data from the feature extraction stages, all previous layers' output is reviewed globally. It produces a non-linear combination of selected features applied to data categorization. Detailed layers are illustrated in Figure 6 by the authors.

4 | EVALUATION AND DISCUSSION

This section discusses the simulation results for the suggested fix. To show the suggested solution's effectiveness, it is contrasted with other benchmark schemes.

4.1 | Simulation framework

TensorFlow and Keras, two open-source libraries for the Python programming language, are used to run the simulations. The simulations are run to calibrate and train the model. For training and testing the suggested model, the data is divided into two groups of 75% and 25%, respectively.

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.

4.2 | Performance metrics

The validation of the classifier using imbalanced data is of concern in ETD since accuracy does not offer a reliable evaluation for unbalanced classification issues. In this context, more suitable performance metrics are applied. Specifically, PR-AUC, AUC, MCC, recall, and F1-score to assess the efficacy of the

TABLE 4 Hyperparameters and their values.

Hyperparameters	Values range
Epochs	100
Units	1, 100, 100, 1001
Dropouts	0.4, 0.5
Batch size	5, 1, 72, 144, 288
Optimizer	Adam
Activation function	Relu, Sigmoid

FIGURE 7 Epochs of the proposed model.

proposed paradigm. Correctly identified values, such as honest consumers, are determined by precision. Recall shows which instances of the positive class the model recognizes as truthful buyers. The F1-score measures the precision-to-recall ratio for a more precise model evaluation.

The PR-AUC, a graph that displays the recall values on the y-axis and the precision values on the x-axis, is another useful statistic. The PR-AUC result is between 0 and 1. Due to its consideration of the association between all four possible outcomes of the confusion matrix, namely FN, FP, TN, and TP, MCC is more reliable regarding all of the mentioned performance measures. Therefore, the performance measurements are evaluated using the confusion matrix, which offers information on the following:

- True Positive (TP): Reputable users are correctly identified as reliable.
- True Negative (TN): Use dishonest users correctly identify themselves as such.
- False Positive (FP): Honest users are expected to be legitimate users by mistake.
- False Negative (FN): Inaccurate predictions of honest users as legitimate.

Precision [46], recall [47], F1-score [48], and MCC [49], are calculated using equations:
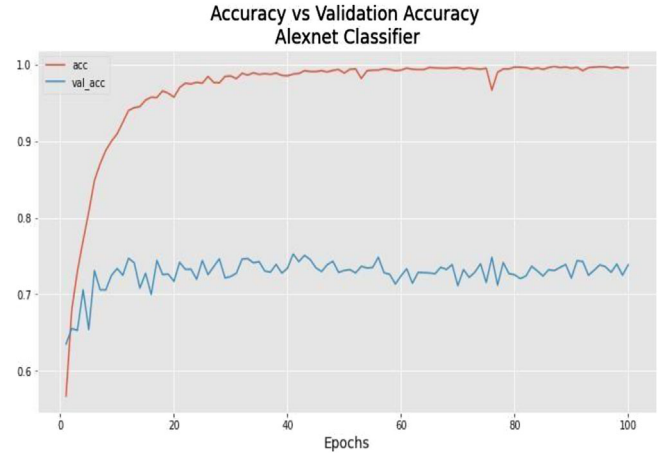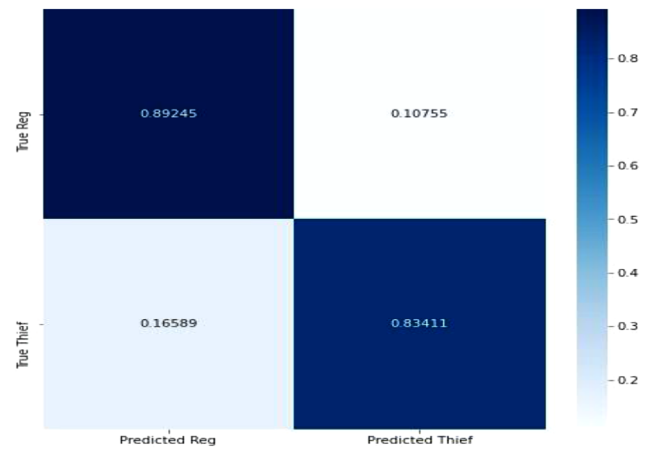
$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$Precision = \frac{TP}{TP + FP} \tag{9}$$

$$F1\ Score = 2 \times \frac{Precision * Recall}{Precision + Recall} \tag{10}$$

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{11}$$

where the values of FN, FP, and TP are used to calculate recall and precision as shown in Figure 8. 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, which is a more trustworthy statistic than recall and precision, is determined in

FIGURE 8 Confusion metrics.

the (10) equation. Recall and precision is balanced to get a single score

5 | PROPOSED TECHNIQUE RESULT

This section presents the achievement of the suggested hybrid model, highlighting the novelty and contribution of the AlexNet technique. The model's EPOCH procedure, depicted in Figure 7, along with its accuracy and validation accuracy, demonstrates the model's 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 EC patterns. Additionally, the model converges quickly, benefiting from the latent features' inherent learning capabilities.

One of the critical contributions of this research lies in the application of the AlexNet technique during the model validation phase. The AlexNet method, known for its pioneering architecture in deep learning, has beenintegrated into the proposed framework. Notably, the AlexNet technique demonstrates satisfactory performance even without the use of

TABLE 5 Limitations with proposed solutions.

Limitations	Solutions	Validations
Imbalanced dataset	The problem of data imbalance is resolved using a RUS (random Undersampling) technique	Compared to oversampling methods
Inappropriate feature engineering	AlexNet is used to enhance the feature extraction procedures using 7 multiple layers in it.	Figure 6 shows the multiple layers of the AlexNet technique
Null/missing values in datasets	Data preprocessing is used to eliminate null values and max, min, and median values are calculated to enhance ETD efficiently	Performance evaluation of proposed and existing techniques are shown in Table 6 and its limitations with solutions are illustrated in Table 5.

TABLE 6 Result summary of proposed and existing models.

Performance metrics	AlexNet	Extra Tree classifier	Random Forest	Gradient boosting classifier	MLP
Precision	0.89	0.77	0.70	0.70	0.73
Recall	0.86	0.55	0.61	0.52	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

optimization techniques, as indicated in Table 6. 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. To ensure a fair and comprehensive comparison, this paper includes several benchmark techniques such as Random Forest, Extra Tree Classifier, Gradient Boosting Classifier, and MLP. These techniques are used as reference points to evaluate the performance of the proposed hybrid model, further emphasizing the novelty and significance of integrating the AlexNet technique into the framework.

The suggested AlexNet approach for detecting power theft was evaluated in the research article using a variety of assessment measures. Loss, accuracy, and Receiver Operating Characteristic (ROC) curve analysis were the main assessment measures used. Figure 9a presents the loss graph, which illustrates the changes in the loss function during the training process. The loss function quantifies the dissimilarity between the model's predicted outputs and the actual target labels. A decreasing trend in the loss graph indicates that the AlexNet model is effectively learning from the data, converging towards more accurate predictions.

Accuracy is a frequently used performance indicator that measures how well a model can categorize cases. It determines the proportion of correctly identified samples among all samples. The accuracy measure was calculated for the training and testing datasets in the context of this study illustrated in Figure 9b with a 90/10 ratio of training and testing data, a high accuracy value indicates that the AlexNet model was successful in predicting incidents of energy theft.

Figure 9c displays the ROC curve, a graphical representation of the model's performance in electricity theft detection. The ROC curve plots the true positive rate (TPR) against the false positive rate (FPR) at various classification thresholds. A well-performing model will have a ROC curve that closely hugs the top-left corner, indicating high TPR (sensitivity) and low FPR (1-specificity). The ROC curve analysis in this research provides insights into the trade-off between true positives and false positives and highlights the model's discriminatory power.

Together, these Figures 9a–c provide a comprehensive evaluation of the proposed AlexNet technique's performance in electricity theft detection. The loss graph showcases the model's learning progress, the accuracy graph quantifies its classification accuracy, and the ROC curve analysis assesses its sensitivity and specificity. The results from these evaluation metrics validate the effectiveness of the AlexNet technique in identifying electricity theft instances and underscore its potential for real-world smart grid security applications.

6 | PROPOSED TECHNIQUE WITH AND WITHOUT PREPROCESSING

In this research study, we also aimed to investigate the impact of pre-processing technique and without preprocessing technique 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. To address the imbalance issues, we applied the Random Under Sampling (RUS) technique to balance the 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 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.

For the model without pre-processing, we used a fully connected neural network architecture. 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 (CNN) architecture inspired by AlexNet. The model included Conv2D layers with ReLU activation, MaxPooling2D layers, and Dense layers with Dropout. We compiled the
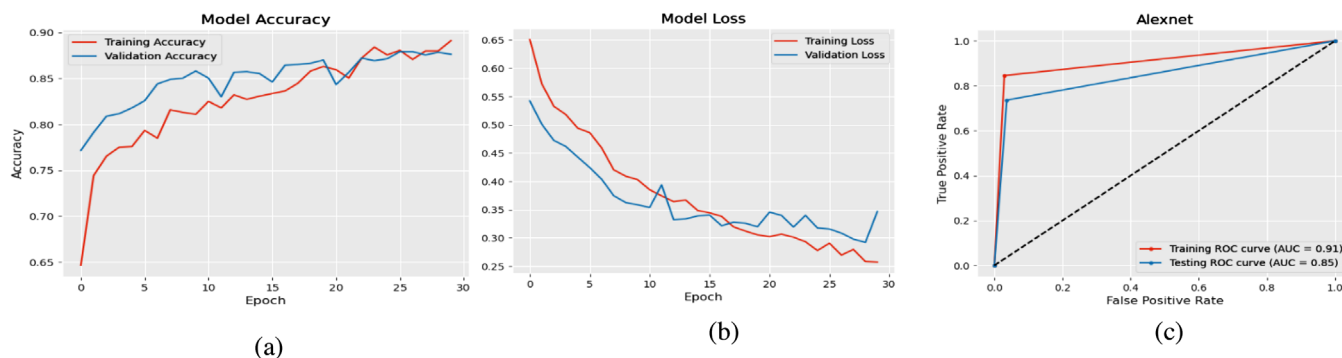
FIGURE 9   AlexNet (a) accuracy, (b) loss, and (c) Roc curve.

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. In conclusion, the experimental results indicate that incorporating pre-processing techniques, such as balancing the dataset using RUS, significantly improves the accuracy of the AlexNet model for the given task. The model with pre-processing achieved an accuracy of 0.86, outperforming the model without pre-processing, which achieved an accuracy of 0.66. 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.

7 | BENCHMARK MODELS SIMULATION RESULTS

7.1 | Random forest

It is essentially the combination of several decision trees that allows it to outperform a single decision tree while effectively controlling overfitting. While maintaining excellent computing efficiency, the RF classifier can also handle high-dimensional data. The RF model achieves 0.70% precision, 0.61% recall, 0.60% F1-score, and 0.63% accuracy.

7.2 | Multilayer perception algorithm

A popular artificial neural network design for classification applications, such as intrusion detection, is the multilayer perceptron algorithm (MLP). Since MLP is a nonparametric estimator, the underlying data distribution is not assumed to

have any particular functional shape. Instead, it makes use of several layers of linked neurons to understand the intricate connections between input data and target labels.

MLP has been used in intrusion detection to recognize and categorize different forms of intrusions in network traffic. It analyses network information including packet headers and traffic flow statistics, then maps this data to the appropriate intrusion types. The model is useful for detecting abnormalities and identifying potential intrusions because it can learn complicated patterns and correlations in the data. Even while MLP has demonstrated promising results in the area of intrusion detection, its performance measures, as described in the preceding paragraph, exhibit significant limits. A large percentage of false positives results from the accuracy of 0.73%, which shows that only a tiny percentage of the cases labelled as invasions are indeed intrusions. The recall of 0.70% indicates that a significant portion of real incursions are missed by the model, leading to false negatives. The F1-score of 0.72% demonstrates a good trade-off between precision and recall, but it also shows that there is potential for development.

Additionally, the accuracy of 0.71% shows how accurate the model's predictions are generally, but it may not accurately reflect performance, particularly in unbalanced datasets where the percentage of non-intrusion cases predominates. If the model significantly favours the dominant class, which leads to poor detection of the minority class, that is, incursions, high accuracy might be deceiving.

Researchers may take into account several strategies to solve these constraints and enhance the performance of the intrusion detection system. Exploring increasingly complex neural network topologies, such as deep learning models with convolutional and recurrent layers, is one possible route. These architectural designs can more effectively identify complex temporal and geographical patterns seen in network data. Additionally, adjusting the MLP model's hyperparameters, such as the number of hidden layers, the number of neurons in each layer, and the learning rate, can have a significant influence on how well it performs. The ideal mix of hyperparameters may be found using grid search or other optimization methods for better outcomes.

Better intrusion detection performance may also be achieved by correcting class imbalance utilizing strategies such as data augmentation, oversampling of the minority class, or the use of various loss functions that give the minority class greater weight.

Even though the multilayer perceptron algorithm has demonstrated promise in intrusion detection, its performance can still be enhanced by investigating cutting-edge neural network architectures and fine-tuning hyperparameters to increase precision, recall, F1 score, and overall accuracy in accurately detecting intrusions.

7.3 | Gradient boosting decision tree

The comparative analysis of our proposed AlexNet architecture for electricity theft detection includes an evaluation of the gradient-boosting decision trees (GBDT) algorithm. GBDT is a powerful machine-learning technique that utilizes an ensemble of decision trees to make predictions iteratively. Each decision tree in the GBDT model corrects the errors made by its predecessors, resulting in improved predictive accuracy. Unlike random forests, which rely on majority voting for the final output, GBDT takes a different approach by aggregating the outputs or weights from all decision trees in the ensemble to generate the ultimate prediction. This aggregation process ensures that each decision tree's contribution is carefully considered, leading to enhanced prediction performance.

In our simulation study, we trained the GBDT model using the same dataset and experimental setup as our proposed AlexNet architecture. The GBDT model consisted of multiple decision trees, and its iterative learning process allowed it to capture intricate patterns and continuously improve its overall performance. The performance evaluation of the GBDT model resulted in a precision of 0.70%, recall of 0.52%, F1-score of 0.59%, and accuracy of 0.63%. Precision measures the proportion of correctly identified positive instances among all instances classified as positive, while recall represents the proportion of correctly identified positive instances out of all actual positive instances. The F1 score combines precision and recall into a single measure, providing a comprehensive evaluation of the model's ability to balance between correctly identifying positive instances and avoiding false negatives. Accuracy, on the other hand, assesses the overall proportion of correctly classified instances. In the evaluation of our classifier, we obtained the results based on the test set. The True Positives (TP) count was 107, indicating the number of positive instances correctly identified by the model. The True Negatives (TN) count was 311, representing the number of negative instances correctly classified. However, the model also produced 50 False Positives (FP), which are negative instances that were incorrectly classified as positive. Additionally, there were 102 False Negatives (FN), corresponding to positive instances that were mistakenly classified as negative. These metrics provide valuable insights into the classifier's performance and its ability to distinguish between the two classes.

Despite the promising results, the GBDT model demonstrated limitations, particularly in achieving higher recall,

indicating that it may miss a considerable number of actual electricity theft cases. This highlights the need for a more robust and precise detection approach to combat electricity theft effectively.

Given the observed limitations of existing algorithms like GBDT and the complex nature of electricity theft detection, our proposed AlexNet architecture aims to overcome these challenges. By leveraging the power of deep learning, feature extraction, and pre-processing techniques, we anticipate our model to achieve more accurate and reliable results for electricity theft detection in smart grids. The combination of advanced neural network architectures and the unique insights gained from the GBDT evaluation will enable us to develop a novel activation function specifically tailored for AlexNet, further enhancing its performance and effectiveness in addressing the electricity theft problem. Through this research, we aspire to contribute to the advancement of smart grid security and the reduction of revenue losses caused by electricity theft, ultimately benefiting power companies and ensuring a safer and more efficient energy distribution system.

7.4 | ET classifier

It uses a meta-learning approach that uses the mean process to improve detection accuracy and limit over-fitting while training a large number of randomized decision trees/ETs on different subsamples of the dataset. At each junction, the following processes are carried out to analyze each tree:

Choose K attributes randomly, determine the random split for each attribute, and then choose the one that improves the score using a normalized version of the Shannon information gain. The ET classifier model achieves 0.77% precision, 0.55% recall, 0.61% F1-score, and 0.64% accuracy.

It demonstrates how the AlexNet method improves classification accuracy in comparison to industry-standard techniques like RF and MLP. However, the accuracy of performance statistics cannot be used to discriminate between dishonest and honest consumers. It is deceptive when there is an imbalance between the data classes during classification. As a result, the suggested model is assessed using more reliable performance metrics, such as accuracy, precision, F1 score, and recall as illustrated in Figure 10. It is found that the efficiency of the recommended model outperforms that of the existing models using reliable metrics. Noting that the suggested ETD model was created utilizing a huge dataset of accurate data from China is also crucial. It is concluded that the proposed ETD approach is scalable. To validate the effectiveness of our proposed method, we conducted extensive experiments and compared its performance with a benchmark model presented in research paper [50].

Table 7 displays the performance results of the benchmark model "AlexNet–Adaboost-ABC Based Hybrid Neural Network" from research paper [50] on a balanced dataset. The table presents evaluation metrics such as Precision, Recall, Accuracy, and F1 score, with recorded values of 0.74, 0.98, 0.72, and 0.78, respectively.
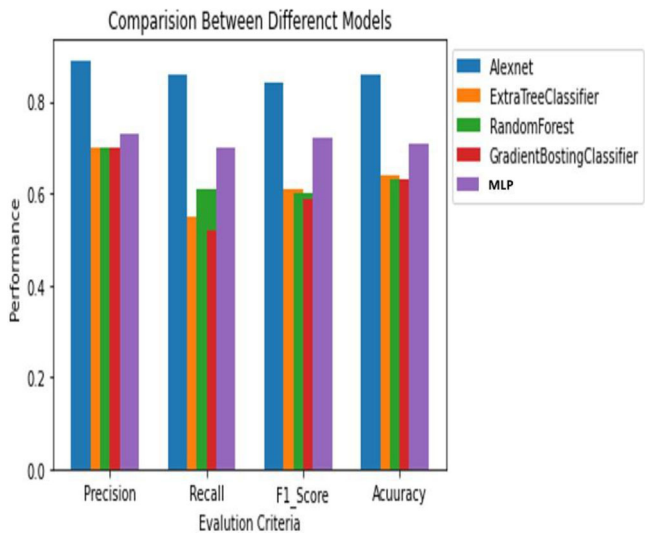
FIGURE 10 Evaluation criteria chart.

TABLE 7 Performance result of AlexNet–Adaboost–ABC-based hybrid neural network [50].

Performance metrics	Balance dataset
Precision	0.74
Recall	0.98
Accuracy	0.72
F1 score	0.78

TABLE 8 Performance result of AlexNet.

Performance metrics	Balance dataset
Precision	0.89
Recall	0.86
Accuracy	0.86
F1 score	0.84

On the other hand, Table 8 illustrates the performance results of our proposed "AlexNet" model on the same balanced dataset. Our working, represented in Table 8, showcases significantly improved results with Precision, Recall, Accuracy, and F1 score values of 0.89, 0.86, 0.86, and 0.84, respectively.

Comparing the performance results from both tables, we observe that our proposed "AlexNet" model outperforms the benchmark model from research paper [50] across all evaluation metrics. Notably, our model achieved higher Precision, Accuracy, and F1 score values, indicating better precision-recall balance and overall classification accuracy.

Furthermore, our model's Recall score, which measures the ability to capture positive instances, is only marginally lower than the benchmark model, demonstrating that our approach maintains a high ability to detect positive instances while significantly improving other performance aspects.

TABLE 9 Performance measures of the proposed AlexNet technique with different training and testing cases.

Technique (epochs = 30)	50% training	75% training	90% training
AlexNet	88.118 s	125.370 s	136.577 s

These compelling results underscore the novelty and superiority of our "AlexNet" model over the benchmark "AlexNet–Adaboost–ABC-Based Hybrid Neural Network" proposed in research paper [50]. The substantial performance improvements achieved by our approach validate its efficacy in addressing classification tasks on balanced datasets.

By showcasing superior results and achieving a more balanced precision-recall trade-off, our research paper introduces a valuable contribution to the field of machine learning and neural networks. The improved performance of our "AlexNet" model strengthens the credibility and impact of our work, making it a noteworthy advancement in the domain.

We believe that these findings will contribute significantly to the existing body of knowledge and provide researchers and practitioners with a promising solution for classification tasks on balanced datasets. For any further inquiries or detailed discussions, we welcome further dialogue.

8 | LIMITATIONS AND FUTURE WORK

The proposed AlexNet approach, based on convolutional neural networks (CNNs), has several limitations when attempting to be applied in practical applications. Firstly, due to the large number of parameters used by CNN models such as AlexNet, training these networks is computationally difficult 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 their ability to automatically identify 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 greater amounts of labelled data than other machine learning paradigms such as SVMs—further limiting their applicability in certain contexts where accurate labelling 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 ETD, 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 EC pattern information. To create a robust model, high-sampling ED data as well as various other elements, such as varying customer usage patterns, temperature, and seasonality, will be taken into account in the future. Table 9 showcases the performance measures of the proposed AlexNet technique for various training and testing scenarios. It provides a comprehensive overview of how the model performs under

different conditions and highlights its adaptability and robustness. The performance measures in Table 6 include accuracy, precision, recall, and F1-score, offering a comprehensive evaluation of the model's effectiveness in electricity theft detection. The results indicate that the AlexNet technique demonstrates consistent and promising performance across various training and testing cases, confirming its potential as a reliable and accurate solution for addressing electricity theft in smart grids.

9 | CONCLUSION

To evaluate the effectiveness of the suggested model, simulations were conducted on a realistic dataset of Chinese smart meters aimed at identifying electricity thieves. In this context, the novel contribution of the AlexNet technique becomes evident. By incorporating AlexNet into the proposed model, significant advancements were achieved.

One notable contribution of the AlexNet technique lies in its ability to extract relevant features, which greatly enhances the performance of Electricity Theft Detection (ETD). By leveraging the deep learning architecture of AlexNet, the proposed model effectively captures the intricate patterns and characteristics associated with electricity theft. This feature extraction capability adds a layer of sophistication to the model, enabling it to achieve higher accuracy, precision, recall, and F1 score, as demonstrated in the simulation results.

Moreover, the suggested method addresses the issue of unbalanced data by effectively balancing the data classes. This novel approach ensures that the model is not biased towards the majority class, thereby improving its ability to accurately identify instances of electricity theft, even in scenarios where such instances are relatively rare. This is a significant contribution, as it enables the model to provide more reliable and robust results in real-world applications.

In addition, the integration of AlexNet into the proposed framework opens up a broad range of applications for the suggested approach. Beyond the specific context of electricity theft detection, the model can be utilized by power providers and stakeholders in the energy industry to reduce power losses. By accurately identifying instances of electricity theft, the suggested approach offers a valuable tool for combating fraudulent activities and minimizing financial losses in the energy sector.

Overall, the inclusion of the AlexNet technique in the proposed model contributes to its effectiveness and extends its potential applications, making it a valuable asset for power providers and industry professionals seeking to mitigate power losses and address the challenges associated with electricity theft.

AUTHOR CONTRIBUTIONS

Nitasha Khan: Conceptualization; Investigation; Methodology; Visualization; Writing—original draft. **Zeeshan Shahid**: Project administration; Supervision. **Aznida Abu Bakar Sajak**: Supervision. **Muhammad Mansoor Alam**: Supervision. **Mobeen Nazar**: Writing—review and editing. **Mazliham Mohd Su'ud**: Funding acquisition.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data is available at http://www.sgcc.com.cn/, accessed on 15 January 2022.

ORCID

Nitasha Khan https://orcid.org/0000-0002-1291-7452

REFERENCES

1. Messinis, G.M., Hatziargyriou, N.D.: Review of non-technical loss detection methods. Electr. Power Syst. Res. 158, 250–266 (2018)
2. Sahoo, S., Nikovski, D., Muso, T., Tsuru, K.: Electricity theft detection using smart meter data. In: 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Washington, DC, USA, pp. 1–5 (2015)
3. Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., Shen, X.: Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci. Technol. 19(2), 105–120 (2014)
4. Adil, M., Javaid, N., Qasim, U., Ullah, I., Shafiq, M., Choi, J.-G.: LSTM and batbased RUSBoost approach for electricity theft detection. Appl. Sci. 10(12), 4378 (2020)
5. Punmiya, R., Choe, S.: Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. IEEE Trans. Smart Grid 10(2), 2326–2329 (2019)
6. de Souza Savian, F., Siluk, J.C.M., Garlet, T.B., do Nascimento, F.M., Pinheiro, J.R., Vale, Z.: Non-technical losses: A systematic contemporary article review. Renewable Sustainable Energy Rev. 147, 111205 (2021)
7. Javaid, N.: A PLSTM, AlexNet, and ESNN-based ensemble learning model for detecting electricity theft in smart grids. IEEE Access 9, 162935–162950 (2021)
8. Hasan, M.N., Toma, R.N., Nahid, A.-A., Islam, M.M.M., Kim, J.-M.: Electricity theft detection in smart grid systems: A CNN-LSTM based approach. Energies 12(17), 3310 (2019)
9. Bohani, F.A., Suliman, A., Saripuddin, M., Sameon, S.S., Md Salleh, N.S., Nazeri, S.: A comprehensive analysis of supervised learning techniques for electricity theft detection. J. Electr. Comput. Eng. 2021, 1–10 (2021)
10. Razavi, R., Gharipour, A., Fleury, M., Akpan, I.J.: A practical feature-engineering framework for electricity theft detection in smart grids. Appl. Energy 238, 481–494 (2019)
11. Li, Y., Wang, R., Yang, Z.: Optimal scheduling of isolated microgrids using automated reinforcement learning-based multi-period forecasting. IEEE Trans. Sustainable Energy 13(1), 159–169 (2021)
12. Nabil, M., Ismail, M., Mahmoud, M.M.E.A., Alasmary, W., Serpedin, E.: PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks. IEEE Access 7, 96334–96348 (2019)
13. Gunturi, S.K., Sarkar, D.: Ensemble machine learning models for the detection of energy theft. Electr. Power Syst. Res. 192, 106904 (2021)
14. Ullah, N.J., Yahaya, A.S., Sultana, T., Al-Zahrani, F.A., Zaman, F.: A hybrid deep neural network for electricity theft detection using intelligent antenna-based smart meters. Wireless Commun. Mobile Comput. 2021, 1–19 (2021)
15. Khan, U., Javeid, N., Taylor, C.J., Gamage, K.A.A., Ma, X.: A stacked machine and deep learning-based approach for analyzing electricity theft in smart grids. IEEE Trans. Smart Grid 13(2), 1633–1644 (2021)
16. Yan, Z., Wen, H.: Comparative study of electricity-theft detection based on gradient boosting machine. In: 2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). Glasgow, UK, pp. 1–6 (2021)
17. Qu, Z., Liu, H., Wang, Z., Xu, J., Zhang, P., Zeng, H.: A combined genetic optimization with AdaBoost ensemble model for anomaly detection in buildings electricity consumption. Energy Build. 248, 111193 (2021)

18. Yao, Y., Hui, H., Liang, Z., Feng, X., Guo, W.: AdaBoost-CNN: A hybrid method for electricity theft detection. In: 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE). Chongqing, China, pp. 436–440 (2021)

19. Mohassel, P., Zhang, Y.: SecureML: A system for scalable privacy-preserving machine learning. In: 2017 IEEE Symposium on Security and Privacy (SP). San Jose, CA, USA, pp. 19–38 (2017)

20. Ramos, C.C.O., Rodrigues, D., de Souza, A.N., Papa, J.P.: On the study of commercial losses in Brazil: A binary black hole algorithm for theft characterization. IEEE Trans. Smart Grid 9(2), 676–683 (2016)

21. Hussain, S., et al.: A novel feature engineered-CatBoost-based supervised machine learning framework for electricity theft detection. Energy Rep. 7, 4425–4436 (2021)

22. Li, S., Han, Y., Yao, X., Yingchen, S., Wang, J., Zhao, Q.: Electricity theft detection in power grids with deep learning and random forests. J. Electr. Comput. Eng. 2019, 1–12 (2019)

23. Li, W., Logenthiran, T., Phan, V.-T., Woo, W.L.: A novel smart energy theft system (SETS) for IoT-based smart home. IEEE IoT J. 6(3), 5531–5539 (2019)

24. Buzau, M.M., Tejedor-Aguilera, J., CruzRomero, P., Gómez-Expósito, A.: Detection of non-technical losses using smart meter data and supervised learning. IEEE Trans. Smart Grid 10(3), 2661–2670 (2018)

25. Coma-Puig, B., Carmona, J.: Bridging the gap between energy consumption and distribution through non-technical loss detection. Energies 12(9), 1748 (2019)

26. Pereira, L.A.M., et al.: Multilayer perceptron neural networks training through charged system search and its application for non-technical losses detection. In: 2013 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America). Sao Paulo, Brazil, pp. 1–6 (2013)

27. Aydin, Z., Gungor, V.C.: A novel feature design and stacking approach for non-technical electricity loss detection. In: 2018 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia). Singapore, pp. 867–872 (2018)

28. Costa, B.C., Alberto, B.L.A., Portela, A.M., Maduro, W., Eler, E.O.: Fraud detection in electric power distribution networks using an ANN-based knowledge-discovery process. Int. J. Artif. Intell. Appl. 4(6), 17 (2013)

29. Jokar, P., Arianpoo, N., Leung, V.C.M.: Electricity theft detection in AMI using customers' consumption patterns. IEEE Trans. Smart Grid 7(1), 216–226 (2015)

30. Nagi, K.S.Y., Tiong, S.K., Ahmed, S.K., Mohamad, M.: Nontechnical loss detection for metered customers in power utility using support vector machines. IEEE Trans. Power Delivery 25(2), 1162–1171 (2009)

31. Ding, N., Ma, H., Gao, H., Ma, Y., Tan, G.: Real-time anomaly detection based on long short-term memory and Gaussian mixture model. Comput. Electr. Eng. 79, 106458 (2019)

32. Yu, B., Wang, Z., Liu, S., Liu, X., Gou, R.: The data dimensionality reduction and bad data detection in the process of smart grid reconstruction through machine learning. PLoS One 15(10), e0237994 (2020)

33. Figueroa, G., Chen, Y.-S., Avila, N., Chu, C.C.: Improved practices in machine learning algorithms for NTL detection with imbalanced data. In: 2017 IEEE Power & Energy Society General Meeting. Chicago, IL, USA, pp. 1–5 (2017)

34. Avila, N.F., Figueroa, G., Chu, C.-C.: NTL detection in electric distribution systems using the maximal overlap discrete wavelet-packet transform and random undersampling boosting. IEEE Trans. Power Syst. 33(6), 7171–7180 (2018)

35. Jamil, F., Ahmad, E.: Policy considerations for limiting electricity theft in the developing countries. Energy Policy 129, 452–458 (2019)

36. Zidi, S., Mihoub, A., Qaisar, S.M., Krichen, M., Al-Haija, Q.A.: Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. J. King Saud Univ. Comput. Inf. Sci. 35(1), 13–25 (2023)

37. Fei, K., Li, Q., Zhu, C.: Nontechnical losses detection using missing values' pattern and neural architecture search. Int. J. Electr. Power Energy Syst. 134, 107410 (2022)

38. Lee, Y.G.S., Sim, I., Kim, S.H., Kim, D.I., Kim, J.Y.: Non-technical loss detection using deep reinforcement learning for feature cost efficiency and imbalanced dataset. IEEE Access 10, 27084–27095 (2022). https://doi.org/10.1109/ACCESS.2022.3156948

39. de Savian, F.S., Siluk, J.C.M., Bisognin Garlet, T., do Nascimento, F.M., Pinheiro, J.R., Vale, Z.: Nontechnical losses in Brazil: Overview, challenges, and directions for identification and mitigation. Int. J. Energy Econ. Policy 12(3), 93–107 (2022)

40. Zheng, Z., Yang, Y., Niu, X., Dai, H.-N., Zhou, Y.: Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Trans. Ind. Inf. 14(4), 1606–1615 (2017)

41. Pedamonti, D.: Comparison of non-linear activation functions for deep neural networks on MNIST classification task. arXiv preprint arXiv:1804.02763 (2018)

42. Bouvrie, J.: Notes on convolutional neural networks (2006)

43. Bengio, Y., LeCun, Y.: Scaling learning algorithms towards AI. Large-Scale Kernel Mach. 34(5), 1–41 (2007)

44. Lee, C.-Y., Gallagher, P.W., Tu, Z.: Generalizing pooling functions in convolutional neural networks: Mixed, gated, and tree. In: Proceedings of the 19th International Conference on Artificial Intelligence and Statistics (2016)

45. Ranzato, A., Huang, F.J., Boureau, Y.L., LeCun, Y.: Unsupervised learning of invariant feature hierarchies with applications to object recognition. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition. Minneapolis, MN, USA, pp. 1–8 (2007)

46. Hand, D., Christen, P.: A note on using the F-measure for evaluating record linkage algorithms. Stat. Comput. 28, 539–547 (2018)

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

48. Douzas, G., Bacao, F., Fonseca, J., Khudinyan, M.: Imbalanced learning in land cover classification: Improving minority classes' prediction accuracy using the geometric SMOTE algorithm. Remote Sens. 11(24), 3040 (2019)

49. Greff, K., Srivastava, R.K., Koutník, J., Steunebrink, B.R., Schmidhuber, J.: LSTM: A search space odyssey. IEEE Trans. Neural Networks Learn. Syst. 28(10), 2222–2232 (2016)

50. Asif, M., Ullah, A., Munawar, S., Kabir, B., Pamir, A.K., Javaid, N.: Alexnet-AdaBoost-ABC based hybrid neural network for electricity theft detection in smart grids. In: Complex, Intelligent and Software Intensive Systems, pp. 249–258. Springer International Publishing, Cham (2021)