Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Improving Electricity Theft Detection with a Stacked Ensemble Model

Anamika Jain[1], Awanti Karmarkar[2], Shejal Mete[2], Aryan Rai[2]

[1] Computer Engineering, Ajeenkya DY Patil School of Engineering, Lohegaon, Pune

[1] anamika.jain@dypic.in

[2] Dr. Vishwanath Karad MIT World Peace University

Article History:

Received: 14-01-2025

Revised: 15-02-2025

Accepted: 21-03-2025

Abstract:
Energy theft is a major problem for utility providers as it results in huge revenue loss and interruption in power supply. It is shown that traditional detection models cannot adequately cope with different methods of theft and unequal data distributions. This work provided a novel machine learning approach to use a stack ensemble of Random forest, Gradient boost with XGBoost, and Logistic regression as meta classifiers. To solve the problem related to data imbalance, the ADASYN oversampling method is used to increase the number of samples of the minority class. The results are then measured with Recall, FNR, ROC AUC in order to see that the model works effectively to detect theft with good levels of TPR without crossing FDR and FNDR levels. This work provides a useful application to various utility companies designed to identify fluctuations in energy consumption, protect power distribution networks, and minimize energy losses.

Keywords: Energy theft, Machine learning, Ensemble models, meta-learner, Accuracy, Grid security

1. Introduction

Electricity theft along with meter tampering represents major problems leading to annual losses in the billions for utility providers while potentially threatening the integrity of power distribution networks. Exclusive metering fraud consists of meter reading manipulation combined with sophisticated methods that continue to evade detection systems. The financial damage caused by electricity theft extends to electrical infrastructure instability and disrupted payment systems which leads to unequal cost burden on honest energy consumers. Research from Zhou et al. [1] and Aldegheishem et. al. [2] shows that electricity theft creates major safety threats which include network flaws alongside electrical fires. Global deterioration of electricity theft has triggered researchers to develop efficient detection approaches that are also scalable and effective. The insufficient detection abilities of basic visual assessments and fundamental statistical anomaly detection algorithms become ineffective against emerging theft techniques. Traditional approaches used to identify energy theft miss complex usage patterns which results in many theft incidents being reported late according to Ali et al. in [3]. Zhou et al. in [4] noted that the use of observable indicators presents difficulties in theft detection because decision-makers depend solely on traditional methodologies. Advanced detection methods become essential because of rising challenges. Data analytics methods to detect consumption behavior deviations from expected patterns remain important according to research from Khan et al. [5] and

Hussain et al. [6]. The implemented detection methods enhance analysis precision while giving utility providers tools to stop additional losses. Data scientists employ oversampling techniques according to

Ali et al. [7] to fix the irregular distribution between regular and fraudulent patterns in consumption data thus enhancing predictive models' performance. Electricity theft consequences spanning economics and functionality and safety require top priority because of their significance. Advanced analytical tools together with improved data-driven methods will help utility companies achieve better theft prevention capabilities while protecting physical assets and maintaining fair energy distribution. The initiatives support wider global objectives for power system safety as well as reliability.

2. Related Work

Theme theft in smart grid operations represents a major challenge because it reduces monetary earnings while weakening grid stability levels. The extensive utilization of machine learning (ML) and deep learning (DL) methods improves the functionality of electricity theft detection (ETD) systems. Zhou et al. [1] developed a convolutional neural network (CNN)-based system to detect consumption pattern abnormalities. Aldegheishem et al. [2] investigated neural network enhancements for smart grid sustainability through intelligent detection procedures. Ali et al. [3] identified electricity theft patterns through boosting algorithms utilized in Advanced Metering Infrastructure (AMI), while Mujeeb et al. [4] developed automatic labeling systems integrating RUSBoost classification through differential evolution and Jaya algorithms. ETD has witnessed increasing adoption of deep learning methods for its applications. Khan et al. [5] demonstrated that the combination of stacked machine learning with deep learning models achieved better theft detection accuracy because of their integrated multiconcept approach. Hussain et al. [6] showed that supervised ML-based ETD could be strengthened through the use of a Catboost framework with engineered features which proved excellent at identifying optimal features. Ali et al. [7] showed that the detection of theft cyberattacks becomes more effective through ML-based solutions. Arif et al. [8] demonstrated that the integration of big data analytics with supervised ML enables efficient theft behavior detection in microgrids and smart communities. Abraham et al. [9] showed how the integration of real-world attacks with synthesized simulations helps smart homes detect vulnerabilities based on ML ability to recognize dynamic attack patterns. Yan and Wen [10] explored the effectiveness of different models applied to smart grids through performance analysis of ETD techniques. Prusty et al. [11] studied XGBoost optimization methods through hyperparameter optimization as a way to boost detection precision. Pamir et al. [12] demonstrated that Eco-Terrorism detection improvements depend on hybrid models like BiLSTM-LogitBoost stacking ensemble which show better efficiency compared to standard methods. Shehzad et al. [13] showed that combining big data technology with genetic algorithms enables efficient processing of scale power system data for theft detection.

Prusty et al. [11] achieved better classification outcomes through the blending of Particle Swarm Optimization with Jaya methods through XGBoost-based ETD models. Pamir et al. [14] demonstrated the use of stacking models combined with boosting classifiers to identify non-technical losses in smart grids through ensemble learning techniques. Soares et al. [15] showed that BiGRU-CNN hybrid neural networks have achieved significant success when detecting energy theft. Yan and Wen [16] analyzed AMI data with XGBoost and showed this algorithm effectively identifies complex theft patterns. Chen et al. [17] showed how intelligent algorithms employing data-driven approaches have benefited ETD accuracy by introducing sophisticated feature selection methods. Yang et al. [18] implemented updated approaches to self-decision ant colony clustering developed enhanced clustering based theft detection

models. Nirmal et al. [19] implemented CNN-AdaBoost hybrid models to boost classification performance. Appiah et al. [20] showed that temperament-based modeling techniques, specifically the extremely randomized trees (ETs) have proven useful for ETD applications because they generate solutions that are simple to interpret and maintain stability.

Nawaz et al. [21] demonstrated that secure smart grids benefit from improved classification precision after integrating CNN and XGBoost techniques. Ullah et al. [22] introduced deep neural networks that include both CNN architectures alongside GRU designs which consistently delivered enhanced cross-dataset generalization. Zheng et al. [23] showed that wide and deep CNNs have remarkable success at protecting smart grids from electricity theft. The SGCC Electricity Consumption Dataset [24] serves as an important publicly available dataset for constantly training and testing different ML and DL models used in ETD while enabling verification and performance comparison among approaches Although there have been many advances in the field of electricity theft detection, some of the gaps exist in the field. The problem with many of them is that they can be scaled down for use in large databases and often fail to make balanced attacks such as theft mimic normal use. The issues related to the limited datasets, noise, and imbalance class are still challenging even if applying methods as SMOTE and ADASYN.

Models that either depend on a set of previous data or large complex computer structures are currently not fit for real-time use; advanced models such as graph-based models and some deep learning include the use of hybrid approaches, however, the overall performance must still be fine-tuned for practical use. Furthermore, many feature engineering methods and managing temporal spatial patterns introduced require further enhancement to be more stable and applicable for practical smart grid systems.

After analyzing the above literature, we have identified most important research objectives to addressed. The goal of this study were developed to succeed in achieving those objectives below, which was aimed at responding to some of the hurdles in detecting electricity theft.

1. One of the primary objectives was to achieve the highest possible value of ROC AUC as to distinguish between genuine and theft events.

2. Furthermore, measures were taken to reduce FPR and FNR which will not punish the genuine users and at the same time ensure that the theft incidence is detected. Specifically, to address the problem of unpaid cases dominating the datasets, the ADASYN oversampling method was applied to increase the number of features corresponding to thefts.

3. Last, the performance of various base and ensemble models were compared in order to check which methodology would be most effective to use for theft detection in enhancing the model's robustness.

3. Methodology

The methodology used in this research is designed to systematically address the challenges of detecting electricity theft, including class imbalance, data preprocessing, and model evaluation. The proposed solution integrates advanced ensemble techniques, culminating in a stacked model configuration. Each aspect of the methodology is elaborated upon in the sections below, providing an expansive and

detailed understanding of the process. The overall block diagram of the proposed work has been shown in figure 1. Each block of the proposed work has been discussed in the following subsections.

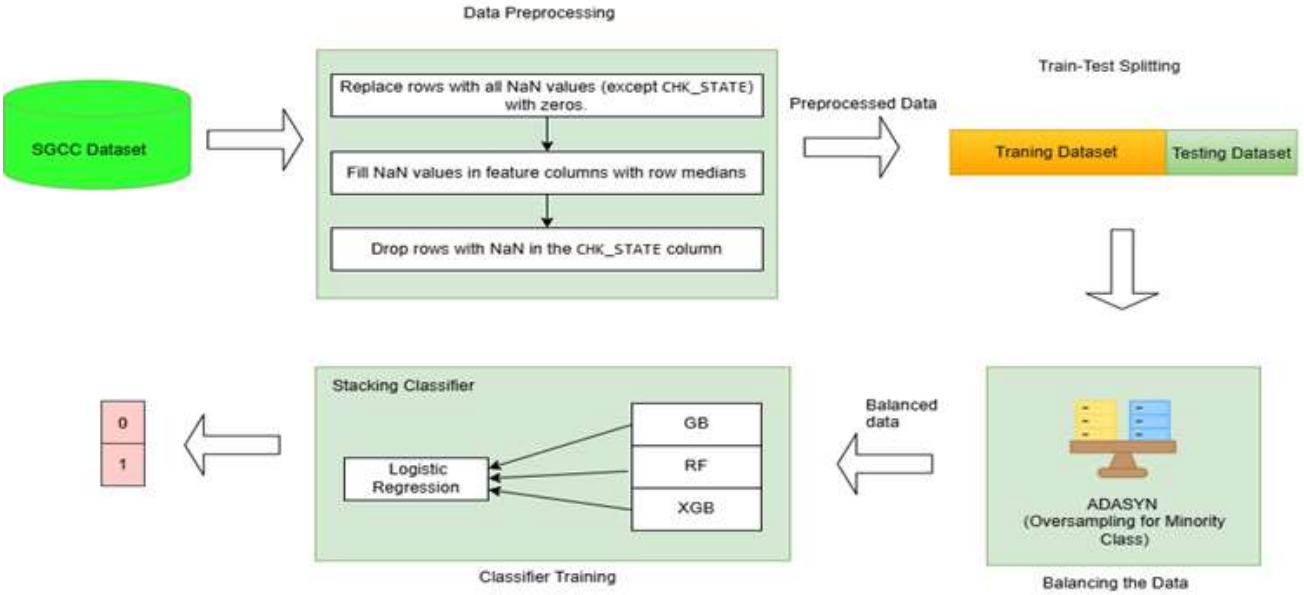

Figure 1: Stacking-Based Framework for Electricity Theft Detection

3.1.1. Data Preprocessing

In this section we make sure that the dataset is clean internally consistent with machine learning specified before feeding the dataset into the model. Challenges to this research included how to deal with missing data and how to balance the classes of the data so that useful intelligence could be made out of the cases involving electricity theft. Figure 2 illustrates the comprehensive framework employed for electricity theft detection. This framework includes data preprocessing steps such as handling missing values, performing train-test splits, and applying oversampling techniques like ADASYN to balance the dataset. The stacking ensemble methodology integrates RF, GB, and XGB as base learners, with LR serving as the meta-learner.

i. Missing Data Imputation

The problem inherent to such datasets– some data is missing because of inaccurate record-keeping. When some variables were incomplete, an imputation procedure was conducted systematically. For the rows with percentage of NaN values equal to 100% then such rows were imputed with zeros. It provided constructive means of maintaining the structural features of the dataset without excluding any potentially useful data. But if some of the data were missing for some of the rows, the median value of the certain characteristic was proceeded. The median is less sensitive to extreme values of features compared to the mean and hence became a better measure for datasets that have high variance in terms of their feature data. Thus, in accomplishing missing data via these strategies, the exactness of the dataset later on was secured due to holism and consistency.

ii. Addressing Class Imbalance

Class imbalance was another problem since legitimate instances(Class 0) are several times more frequent than theft instances (Class 1). In the absence of balancing operations such models are easily prone to develop a bias towards the majority class hence poor theft cases detection. To address this problem, the ADASYN strategy was used as it is an improvement of the synthetic sampling technique. ADASYN enhances minority class instance density by synthesizing samples in low density areas of input space. It is done by estimating the density of provided minority class examples and by placing new points in areas with a low density of such classes. ADASYN, unlike ordinary oversampling that leads to overfitting since the samples are replicated identically, creates a variety of synthetic patterns that can better be used to improve the model's generalization. It was found that after augmentation the class distribution was almost 49.3% for legitimate cases and 50.7% for theft cases. Besides, it enhanced performance in terms of sensitivity to theft cases and, at the same time, helped to maintain fairness of the prediction in classes. The benefit of ADASYN has been discussed in terms of being able to tackle the source of the imbalance and cater to the samples from where it is difficult to generate the samples.

3.1.2. Stacking Model

In this section we describe stacking ensembles to overcome the problems associated with electricity theft detection presented in Table 1. Stacking is the powerful approach where predictions of the base models are f inalized using a meta-learner for making ensemble models combined together by covering the strength of diverse models. As the base learners, we had chosen RF, GB, and XGB, while the meta-learner was LR. LR as a method was used due to its linearity and ease of aggregating base model output, justifying the method selection. This configuration harnesses the performance of three solid base learners to solve the complexity of electricity theft detection efficiently. In selecting the base learners for the ensemble, each was selected based on the individual contribution it would make. The process of creating a decision tree within RF lower variance through bagging it, especially in cases of imbalance data and noise in the prediction. GB improves predictions in a step-by-step way, stacking new models one after the other and, as a result of this sequential process, it is very valuable when it is necessary to deal with complicated patterns or outlier cases. XGB, which is an improved version of GB, brings more improvement to the ensemble method due to its computational advantages, additional regularization measures, and a powerful capability of detecting rare class samples with high accuracy. Altogether, the discussed models cover different aspects of the electricity theft detection problem, including the class imbalance issue and complex data characteristics, ensuring the high quality of the stacking ensemble. The proposed model has the highest ROC AUC score, and recall rate, which shows a good trade-off between precision and recall. Superior results in class imbalance management, as well as its flexibility for the specific problem type, proved that this model was the most effective one for electricity theft identification. The above studies demonstrate the ability of the stacking ensembles to provide better accurate models and generalization when compared to other models in complex environments. In our case, some future enhancements could be the inclusion of other advanced base learners or use of other forms of features which are specific to a particular domain for construction of the stacking model. Therefore, it is necessary to carefully design the stacking configurations in order to f it specific issues and this paper lays the groundwork for future development of electricity theft detection using ensemble based approaches.

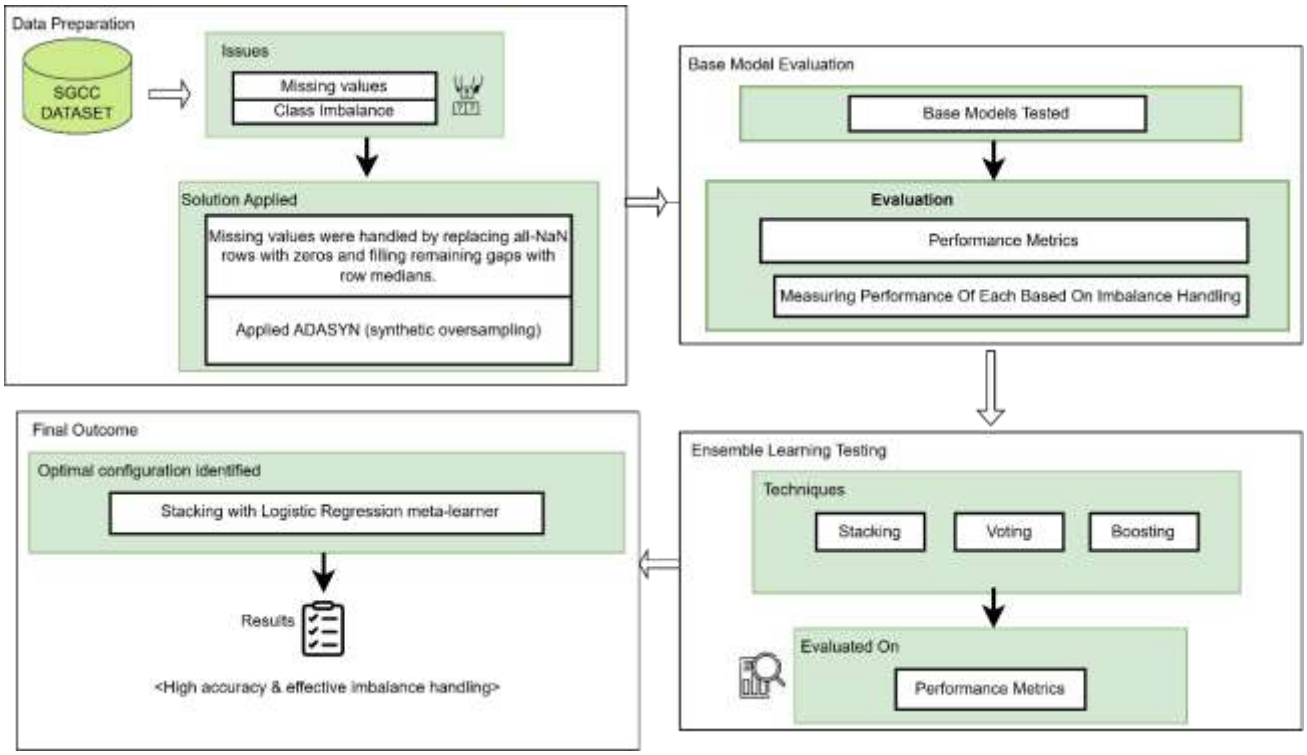

Figure 2: Comprehensive Methodology for Electricity

Model Configuration	TPR	FPR	TNR	FNR	ACCURACY	AUC
Stacking (RF, GB, BRF) + XGBoost Meta Learner	0.933	0.0592	0.9408	0.0667	0.9370	0.9791
Stacking (RF, GB, BRF) + Logistic Regression Meta Learner	0.945	0.0586	0.9414	0.0548	0.9433	0.9841
Stacking (RF, GB, XGB) + Logistic Regression Meta Learner	0.948	0.0569	0.9431	0.0514	0.9459	0.9867

Table 1: Classification Metrics for stacking Model

4. Experimental Setup

It describes how the experiment was designed in the initial stage in terms of the characteristics of the data and computational environment, as well as concrete goals defining the research direction.

4.1.1 Dataset Description

The data used for this study was collected from the SGCC dataset of electrical energy consumption of 9958 users drawn in 2015. This dataset contains measurements of daily usage and time stamp for each user, which could be used to identify unusual phenomena including electricity theft. However, there is one major problem, which is the skewed class distribution: only 14.02% belongs to Class 1 (theft cases), while the rest 85.98% belongs to Class 0 (legitimate cases) [24].

4.1.2 Computational Environment

All these experiments were performed in Google Colab, the environment that can be useful when performing computational analysis. Hardware configuration consisted of ; NVIDIA Tesla T4 GPU, Intel Xeon CPU, and 12.6 GB RAM. The computational demand for training a large ensemble of models was met by the NVIDIA Tesla T4 GPU, with plenty of memory due to seamless data processing and the optimization of hyperparameters of the chosen model. One of the peculiarities of the cloud-based infrastructure was the effectiveness of the organization of collaborative research with data and code sharing among the research team members.

4.1.3 Software Environment

For this study, the software stack used was developed with Python 3.8 and other libraries and frameworks. For pre-processing the data, enhancing the model accuracy as well as for almost all machine learning operations, scikit-learn was used. XGBoost(XGB) was used when dealing with boosting, gradient classifiers, and hyperparameters. The oversampling techniques such as ADASYN were implemented with the help of the Imbalanced-learn library Data handling and numerical computations were done using Pandas and NumPy. Matplotlib and Seaborn were used to perform visualization of data and results obtained after data analysis. The fact that all these tools were runned in the Google Colab environment allowed for sequenced experimentations and guaranteed the replicability of the solution.

4.2 Experimentation with Models and Ensemble Techniques

In the testing phase, results for the preprocessed dataset were checked with single base models in order to understand how they perform on each other and what issues might have occurred. All evaluated instances, namely Random Forest (RF), Gradient Boosting (GB), XGB, Balanced Random Forest (BRF), Easy Ensembles, Support Vector Classifier (SVC), and Multi-Layer Perceptron (MLP), are listed in Table 1 alongside True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR), False Negative Rate (FNR), Accuracy and ROC AUC.

4.2.1 Key Observations of Base Models

Various base models were explored to evaluate their suitability for the task. The RF Classifier was employed due to its ensemble nature, combining decision trees using bootstrapped aggregation (bagging) to enhance predictive accuracy and mitigate overfitting tendencies. XGB was investigated for its ability to handle high dimensional and imbalanced datasets, leveraging its robust feature-capturing capabilities. Additionally, GB was utilized to focus on capturing intricate data patterns and handling borderline cases effectively. These models were selected to provide a diverse set of approaches for understanding the data and addressing the complexities of the electricity theft detection problem, serving as foundational components for further analysis or ensemble modeling. Ensemble methods, which integrate base classifiers, were employed to enhance accuracy and generalization. Several approaches were explored, with key findings outlined below.

4.2.2. Key Observations of Varying Ensemble Models

The Easy Ensemble Classifier applied a bagging-based strategy and resampled the majority class to create balanced datasets for constructing weak learners. While this approach aimed to address class imbalance, it exhibited poor recall values for theft detection cases, making it less effective for standalone use. Voting classifiers, encompassing both soft and hard voting techniques, were implemented to combine results from multiple models. Soft voting slightly improved the ROC AUC and recall, while hard voting demonstrated stable performance. However, the benefits of soft voting, such as balanced precision-recall division, were not prominent in this study. Weighted bagging, utilizing Random Forest (RF) as the base learner, emphasized the

minority class. While it improved sensitivity toward theft cases, calibration of evaluation factor weights was necessary to prevent overemphasis and maintain balance. Stacking, an advanced ensemble technique, employed Logistic Regression (LR) as a meta-learner and used predictions from RF, Gradient Boosting (GB), and Extreme Gradient Boosting (XGB) as inputs. Stacking effectively addressed the limitations of individual models, offering a robust solution to challenges posed by imbalanced datasets.

The strengths of the base learners—RF for generalization, GB for capturing complex patterns, and XGB for advanced optimization—were leveraged to achieve superior performance. LR aggregated these diverse outputs in a straightforward yet efficient manner, reducing overfitting through regularization and ensuring balanced predictions. Two alternative stacking configurations were also tested. The first used XGB as the meta-learner with RF, GB, and Balanced Random Forest (BRF) as base learners. This setup enhanced recall and precision through XGB's gradient boosting but struggled with class imbalance. The second variant used LR as the meta-learner with the same base learners, abbreviated as LR-RF, LR-GB, and LR-BRF. This approach balanced recall and precision, with LR's linear predictions simplifying the integration of base model outputs. While this configuration generalized well, it achieved only moderate control over false positives.

In summary, individual classifiers exhibited unique strengths: RF excelled in generalization, XGB ranked high in recall, and GB was adept at capturing complex patterns. Ensemble techniques—especially stacking—capitalized on these strengths to achieve better performance. Stacking, with LR as the meta learner, provided an outstanding solution for handling imbalanced data and detecting electricity theft cases by effectively combining the outputs of diverse models. Alternative configurations demonstrated potential, but their limitations in addressing class imbalance indicated stacking with LR as the meta-learner was the most effective strategy. This experimental configuration demonstrated the ensemble methodology's ability to handle imbalanced data, detect challenging patterns, and combine outputs from diverse models. Future enhancements could include incorporating deep learning models as base learners and integrating domain-specific features to further improve accuracy and stability.

4.2.3. Experimentation with Multi-View Ensemble Learning and Variance-Based Dynamic Classifier Selection

Two advanced methodologies, Multi-View Ensemble Learning and Variance-Based Dynamic Classifier Selection, were implemented and analyzed to enhance electricity theft detection. The Multi-View Ensemble Learning approach involves segmenting the dataset into distinct "views" that reflect daily, weekly, and seasonal electricity consumption patterns. These views are generated by aggregating data over specific temporal intervals, capturing unique aspects of user behavior. Separate machine learning models, including XGBoost, Random Forest, Support Vector Machine (SVM), and Gradient Boosting, are trained on these views, emphasizing short-term anomalies and long-term trends. These models are combined into an ensemble using a VotingClassifier with soft voting, leveraging their collective strengths. The approach also employs robust preprocessing steps, including filling missing values using the median, standardization via StandardScaler, and handling class imbalance with ADASYN and Tomek Links. The Variance-Based Dynamic Classifier Selection approach employs a dynamic strategy to select the most suitable classifier for each test sample based on its variance. The feature space is divided into low, medium, and high variance regions, with Balanced Random Forest, k-Nearest Neighbors (k-NN), and Isolation Forest selected, respectively, for these regions. This strategy ensures optimal handling of varying levels of data variability, enabling the model to adapt to complex patterns and outliers.

The preprocessing pipeline includes handling missing values with forward and backward fill methods, standardizing features using StandardScaler, and addressing class imbalance with ADASYN. These experiments demonstrate the potential of advanced ensemble methods and dynamic classifier selection to

enhance the detection of electricity theft. By addressing diverse temporal patterns and varying data variability, both methodologies significantly improve detection accuracy and reliability.

5. Results and Discussion

This section aims at different methods and approaches used in identifying Electricity Theft as well as different configurations. We proposed three strategies, namely multi view learning, dynamic classifier selection and stacking; and evaluated them. The outcomes of these experiments and analysis are provided in the Table 2 below, where the discussion of these findings follows next. Average measures on different sorts of electricity theft detection models, such as multiview ensembles, dynamic classifiers, and stacking configurations, are presented in Table 2. These are TPR (Recall), FPR, TNR (Specificity), FNR,Accuracy and ROC AUC Curves which will give a clear indication of the weaknesses and strengths of the different models.

In the multiview ensemble approach we divide the dataset into three distinct views: and divide daily, weekly, and seasonal consumption. There are two views each of which is passed through a different model and the final prediction is made using soft voting of the two models. In this we have tested two configurations : The first set of models which included: Logistic Regression, RF, Support Vector Machine(SVM), and GB had an accuracy of 86.82%; sensitivity of 86.15%; and ROC AUC of 0.94. Second configuration, which had XGB, achieved a higher accuracy of 93.16 %, TPR of 95.75 %, and AUC of 0.97 but had a higher FPR of 9.23% The concluding model that used XGB, RF, SVM, and GB as base learners with LR as the final learner computed better recall and had higher specificity, and an excellent F1 score at 0.8929. Whilst being much improved over previous methods, there is still room for improving both in eliminating false positives and in increasing the computational speed for real world applications.

Model	**TPR**	**FPR**	**TNR**	**FNR**	**ACCURACY**	**AUC**
Ensemble (LR, RF, SVM, GB) – Soft Voting	0.8615	0.141	0.879	0.1385	0.8682	0.94
Ensemble (XGB, RF, SVM, GB) – Soft Voting	0.9575	0.0923	0.9077	0.0425	0.9316	0.97
Dynamic Classifier (RF, Boosting, SVM, IF)	0.8755	0.086	0.914	0.1245	0.89	0.9092
Dynamic Classifier (RF, KNN, SVM, IF)	0.877	0.0857	0.913	0.1217	0.9	0.9
Stacking (RF, GB, BRF) + XGBoost Meta Learner	0.933	0.0592	0.9408	0.0667	0.937	0.9791
Stacking (RF, GB, BRF) + LR Meta-Learner	0.9452	0.0586	0.9414	0.0548	0.9433	0.9841
Stacking (RF, GB, XGB) + LR Meta-Learner	0.9486	0.0569	0.9431	0.0514	0.947	0.9867

Table 2: Classification Metrics for Electricity Theft Detection Models

Dynamic classifiers go further with the detection system by choosing appropriate models for the specific regions of feature space according to their variance limits. The classification of samples is given as follows: Low variance sample (variance < 0.5) utilization BRF, Medium variance samples (0.5 <= variance < 1.5) utilized k-Nearest Neighbors [k-NN] and samples having high variance (variance >= 1.5) employed Isolation Forest. An integration of RF, boosting, SVM, and the isolation forest reported an accuracy of 89.00% with a TPR of 87.55% and ROC-AUC of 0.9092. Changing Boosting to k-NN improved the accuracy marginally to a 90,00 percent

while the ROC AUC stayed at 0.90. Although this approach proves flexibility, the model still requires higher sensitivity to minority classes considering its moderate impact on addressing class imbalance. Stacking models use RF, GB and XGB as base models and either XGB or LR as a meta learner. Our proposed system when the meta-learner is the XGBoost classifier attains accuracy of 93.70%, TPR of 93.33%, and 0.9791 the ROC AUC. With LR as the meta-learner, the performance increased up to 94.33% as accuracy, 94.52% as TPR, and 0.9841 as ROC AUC, and decreased FPR up to 5.%. The highest accuracy, TPR and ROC AUC were recorded by the Stacking (RF, GB, XGB) + LR model at 94.59%, 94.86%, and 0.9867 respectively with the lowest FPR of 5.69%.This configuration exploits the fact that XGB can learn relatively complex decision boundaries while being somewhat insensitive to them but LR is insensitive in general but its decision boundaries are relatively simple. In general, the proposed Stacking (RF, GB, XGB) + LRmodel had the highest accuracy, strong discriminative capability, and few false positives. By addressing both efficiency and reliability, its application in electricity theft detection systems is well recommended for real world use. In order to test the applicability of our proposed model, we compared the results obtained with state of the art technique as listed in the following Table 3.

Model	**TPR**	**FPR**	**TNR**	**FNR**	**ACCURACY**	**AUC**
BiLSTM- LogitBoost	0.9241	0.0368	0.9632	0.0759	0.8945	-
Stacking (RF, GB, XGB) + LR Meta-Learner (Proposed)	**0.9486**	0.0569	0.9431	**0.0514**	**0.947**	0.9867

Table 3: Comparison of the Proposed method with The State of the Art of The Model

The comparative outcome of the stacking model proposed in this study has been shown in Table 3 against benchmark model BiLSTM-LogitBoost model. The following table 3 shows the compromise between recall, specificity or identification of true positives and true negative or overall accuracy. From table 3 it is observed that we have acheived lower false negative rate as compared to the BiLSTM-logitboost method. Accuracy of the propsed work is higher with the state of the art method.

We focused on comparing the stacking model against two benchmark models: Optimized XGB-PSO [11] and BiLSTM-LogitBoost [12].The evaluation standard were TPR , FPR, TNR FNR, Accuracy, and ROC AUC. We observe that our stacking model produced a comparatively lower FPR (5.69%) as opposed to the Optimized XGB-PSO's (8.58%) and a high accuracy rate of 94.59% and TPR of 94.86%. While the Optimized XGB-PSO model detected more instances with 96% recall and 96% accuracy, their lag in FPR is higher and will produce more false alarms.

Our improved stacked model achieved a lower FPR of 3.68% high TNR of 96.32% compared to BiLSTM LogitBoost but it was less accurate with 89.45% and a TPR of 92.41%. As for the stacking configuration, these results prove that our proposed setup provides the best balance of recall, specificity,and obvious accuracy to be used in real-world electricity theft detection systems. Future work can emerge in refining the model even further and performing real time studies in very large organisations.

6. Conclusion

In this paper, we discussed and compared numerous techniques of estimating electricity theft such as multiview ensemble models, dynamic classifier selection and the stacking approach. Out of these, we found that the Stacking (RF, GB, XGB) + LR meta-learner was the most effective with TPR=94.86%, Accuracy = 94.70%, and FPR=5.69%. This shows how using various base models along with a simple and lightly parameterized meta-learner provides high sensitivity and specificity as well as high accuracy. Moreover, a comparison with

standard models such as Optimized XGB-PSO and BiLSTM-LogitBoost also confirmed the effectiveness of the described approach, as it had higher recall with less number of false positives in comparison with the listed methods. Examining the overall performance of the proposed model, the following limitations can be observed. The computational complexity of the stacking approach can significantly limit the possibilities for real time application in massive or in conditions of a lack of resources. Further, it is prominent that the model keeps minority class samples in consideration which essentially suggests that methods to address class imbalance should be strengthened. ADASYN has limitations when used for balancing; one of them is when it introduces new instances that may distort the ability to generalize. Furthermore, the hyperparameters were tuned with respect to the SGCC dataset, and its generalization capacity towards other unseen datasets is still unknown.

7. Future Scope

Future advancements in electricity theft detection will focus on the development of computationally efficient algorithms that can handle large-scale, high-dimensional data from modern power systems. Techniques like adaptive sampling and cost-sensitive learning show promise in addressing class imbalance, improving prediction reliability in skewed datasets. Additionally, the integration of explainable AI (XAI) will enhance model transparency, increasing trust and enabling easier deployment in regulatory and operational settings. The adoption of advanced deep learning architectures, such as Transformer models, Graph Neural Networks (GNNs), and Recurrent Neural Networks (RNNs), will improve the ability to capture complex patterns in electricity consumption data, enhancing model precision and generalization. Moreover, the incorporation of real time data streams and edge computing will enable faster, distributed decision-making, transforming detection systems for dynamic environments. These developments will lead to more scalable, efficient, and interpretable solutions for electricity theft detection.

References

[1] Wei Zhuang, Wen Jiang, Min Xia, and Jun Liu. Dynamic generative residual graph convolutional neural networks for electricity theft detection. IEEE Access, 12:42737–42750, 2024.

[2] Arwa Alromih, John A Clark, and Prosanta Gope. Electricity theft detection in the presence of prosumers using a cluster-based multi-feature detection model. In 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pages 339–345. IEEE, 2021.

[3] Ivan Petrlik, Pedro Lezama, Ciro Rodriguez, Ricardo Inquilla, Julissa Elizabeth Reyna-González, and Roberto Esparza. Electricity theft detection using machine learning. International Journal of Advanced Computer Science and Applications, 13(12), 2022.

[4] Yu Yao, Hengyu Hui, Ziyang Liang, Xiaofeng Feng, and Wenchong Guo. Adaboost-cnn: a hybrid method for electricity theft detection. In 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE), pages 436–440. IEEE, 2021.

[5] Inam Ullah Khan, Nadeem Javeid, C James Taylor, Kelum AA Gamage, and Xiandong Ma. A stacked machine and deep learning-based approach for analysing electricity theft in smart grids. IEEE Transactions on Smart Grid, 13(2):1633–1644, 2021.

[6] Saddam Hussain, Mohd Wazir Mustafa, Touqeer A Jumani, Shadi Khan Baloch, Hammad Alotaibi, Ilyas Khan, and Afrasyab Khan. A novel feature engineered-catboost-based supervised machine learning framework for electricity theft detection. Energy Reports, 7:4425–4436, 2021.

[7] Abdelfatah Ali, Mohamed Mokhtar, and Mostafa F Shaaban. Theft cyberattacks detection in smart grids based on machine learning. In 2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pages 1–4. IEEE, 2022.

[8] Arooj Arif, Nadeem Javaid, Abdulaziz Aldegheishem, and Nabil Alrajeh. Big data analytics for identifying electricity theft using machine learning approaches in microgrids for smart communities. Concurrency and Computation: Practice and Experience, 33(17):e6316, 2021.

[9] Olufemi Abiodun Abraham, Hideya Ochiai, Md Delwar Hossain, Yuzo Taenaka, and Youki Kadobayashi. Electricity theft detection for smart homes: Harnessing the power of machine learning with real and synthetic attacks. IEEE Access, 12:26023–26045, 2024.

[10] Zhongzong Yan and He Wen. Performance analysis of electricity theft detection for the smart grid: An overview. IEEE Transactions on Instrumentation and Measurement, 71:1–28, 2021.

[11] Sashikanta Prusty, Debasish Swapnesh Kumar Nayak, Meena Moharana, Sushree Gayatri Priyadarsini Prusty, Manmohan Sahoo, and Jyotirmayee Rautaray. Optimizing xgboost for enhanced electrical theft detection: A fusion of particle swarm and jaya optimization techniques. In 2024 IEEE 4th International Conference on Sustainable Energy and Future Electric Transportation (SEFET), pages 1–4. IEEE, 2024.

[12] Nadeem Javaid, Ahmad Almogren, Muhammad Adil, Muhammad Umar Javed, Mansour Zuair, et al. Rfe based feature selection and knnor based data balancing for electricity theft detection using bilstm-logitboost stacking ensemble model. IEEE Access, 10:112948–112963, 2022.

[13] Mahdi Emadaleslami, Mahmoud-Reza Haghifam, and Mansoureh Zangiabadi. A two stage approach to electricity theft detection in ami using deep learning. International Journal of Electrical Power & Energy Systems, 150:109088, 2023.

[14] Nadeem Javaid, Mariam Akbar, Abdulaziz Aldegheishem, Nabil Alrajeh, Emad A Mohammed, et al. Employing a machine learning boosting classifiers based stacking ensemble model for detecting non technical losses in smart grids. IEEE Access, 10:121886–121899, 2022.

[15] Lucas Duarte Soares, Altamira de Souza Queiroz, Gloria P López, Edgar M Carreño-Franco, Jesús M López-Lezama, and Nicolás Muñoz-Galeano. Bigru cnn neural network applied to electric energy theft detection. Electronics, 11(5):693, 2022.

[16] Zhongzong Yan and He Wen. Electricity theft detection base on extreme gradient boosting in ami. IEEE Transactions on Instrumentation and Measurement, 70:1–9, 2021.

[17] Junde Chen, YA Nanehkaran, Weirong Chen, Yajun Liu, and Defu Zhang. Data-driven intelligent method for detection of electricity theft. International Journal of Electrical Power & Energy Systems, 148:108948, 2023.

[18] Zhengqiang Yang, Linyue Liu, Ning Li, and He Li. Corrigendum to “a self-decision ant colony clustering algorithm for electricity theft detection” [eng. appl. artif. intell. 133, part e (july 2024), 108442]. Eng. Appl. Artif. Intell., 135(C), September 2024.

[19] Santosh Nirmal, Pramod Patil, and Jambi Ratna Raja Kumar. Cnn-adaboost based hybrid model for electricity theft detection in smart grid. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 7:100452, 2024.

[20] Stanley Yaw Appiah, Emmanuel Kofi Akowuah, Valentine Chibueze Ikpo, and Albert Dede. Extremely randomised trees machine learning model for electricity theft detection. Machine Learning with Applications, 12:100458, 2023.

[21] Asif Nawaz, Tariq Ali, Ghulam Mustafa, Saif Ur Rehman, and Muhammad Rizwan Rashid. A novel technique for detecting electricity theft in secure smart grids using cnn and xg-boost. Intelligent Systems with Applications, 17:200168, 2023.

[22] Rui Xia, Yunpeng Gao, Yanqing Zhu, Dexi Gu, and Jiangzhao Wang. An attention-based wide and deep cnn with dilated convolutions for detecting electricity theft considering imbalanced data. Electric Power Systems Research, 214:108886, 2023.

[23] Zibin Zheng, Yatao Yang, Xiangdong Niu, Hong Ning Dai, and Yuren Zhou. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Transactions on Industrial Informatics, 14(4):1606–1615, 2017.

[24] Sgcc electricity theft detection. http://https: //www.kaggle.com/datasets/bensalem14/ sgcc-dataset. Accessed: 2025-01-31