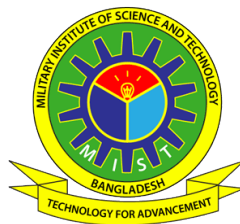


ENHANCED DETECTION OF ELECTRICITY THEFT IN SMART GRIDS USING A MACHINE LEARNING BOOSTING CLASSIFIERS BASED VOTING ENSEMBLE MODEL

MD. SABBIR HOSSAIN MOLLA (SN. 202016028)
MD. NASIF MAHMUD ZISHAN (SN. 202016041)

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Electrical, Electronic and
Communication Engineering



DEPARTMENT OF ELECTRICAL, ELECTRONIC AND
COMMUNICATION ENGINEERING
MILITARY INSTITUTE OF SCIENCE AND TECHNOLOGY
DHAKA, BANGLADESH

MARCH 2024

ACKNOWLEDGEMENTS

Foremost, we would like to express our sincere gratitude to our supervisor, Brigadier General Professor A K M Nazrul Islam (Retd) of the Department of EECE, MIST for the useful comments, remarks and engagement through the learning process of this thesis. We always received appropriate guidelines, learning materials, guidance for solving problems, and opportunities to visit institutions to gather knowledge and experience to make this research fruitful. We would like to further express our gratitude to Brigadier General Md Rezaul Awal, psc, Head, Department of EECE, MIST and Major General Mohammed Saidul Islam, rcds, ndc, psc, Commandant, MIST for their financial support that enabled this study to be conducted. We would like to extend our heartfelt gratitude to all faculty members and staff of the department of Electrical, Electronic and Communication Engineering (EECE) for their support during the research and to the Military Institute of Science and Technology (MIST) for giving us the opportunity to complete the research.

We would like to thank Dhaka Power Distribution Company (DPDC) for giving us insight into their operations. We would also like to acknowledge the contributions of Google LLC for developing a platform like Google Collaboratory that benefits a large number of researchers everyday.

Finally, we must express our profound gratitude to our parents who were immensely supportive throughout the whole research.

ABSTRACT

Enhanced Detection of Electricity Theft in Smart Grids Using a Machine Learning Boosting Classifiers Based Voting Ensemble Model

Electricity theft poses a critical challenge among non-technical losses for electricity providers, resulting in severe consequences such as compromised supply quality, increased generation load, inflated bills for legitimate consumers, and broader economic repercussions. Smart grid technology offers a promising avenue to mitigate such losses through advanced data analytics. With the abundance of data generated by smart grid infrastructure, including individual power consumption patterns, machine learning and deep learning methodologies emerge as effective tools to accurately detect instances of electricity theft. However, existing schemes provide suboptimal performance in electricity theft detection (ETD) due to challenges such as imbalanced data distributions, overfitting issues, handling high-dimensional data, and reliance on individual schemes. In response to these limitations, this paper proposes a voting ensemble model based on machine learning boosting classifiers. In this model, we incorporate Convolutional Neural Networks (CNN), a widely recognized technique for feature extraction. The framework encompasses three key components, such as data preprocessing, data balancing, and classification, each addressing specific challenges in ETD. Notably, the proposed model leverages the strengths of extreme gradient boosting (XGBoost), categorical boosting (CatBoost), and light gradient boosting (LightGBM), enhancing its overall robustness and predictive accuracy. Rigorous validation using diverse metrics underscores the efficacy of the model, as evidenced by extensive simulations. Results indicate superior performance compared to individual models, with the proposed model achieving an impressive test accuracy of 99%.

সারসংক্ষেপ

Enhanced Detection of Electricity Theft in Smart Grids Using a Machine Learning Boosting Classifiers Based Voting Ensemble Model

বিদ্যুৎ সরবরাহকারীদের জন্য অ-প্রযুক্তিগত ক্ষতির মধ্যে বিদ্যুৎ চুরি একটি গুরুতর চ্যালেঞ্জ হয়ে দাঁড়িয়েছে, যার ফলে সরবরাহের মানের সাথে আপস, উৎপাদন বৃদ্ধি, বৈধ গ্রাহকদের জন্য স্থগিত বিল এবং বিস্তৃত অর্থনৈতিক প্রতিক্রিয়ার মতো গুরুতর পরিণতি ঘটে। স্মার্ট গ্রিড প্রযুক্তি উন্নত তথ্য বিশ্লেষণের মাধ্যমে এই ধরনের ক্ষতি হ্রাস করার একটি আশাব্যঞ্জক উপায় প্রদান করে। পৃথক বিদ্যুৎ ব্যবহারের ধরণ সহ স্মার্ট গ্রিড পরিকাঠামো দ্বারা উত্পন্ন তথ্যের প্রাচুর্যের সাথে, মেশিন লার্নিং এবং ডিপ লার্নিং পদ্ধতিগুলি বিদ্যুৎ চুরির ঘটনাগুলি সঠিকভাবে সনাক্ত করার কার্যকর সরঞ্জাম হিসাবে আবির্ভূত হয়। তবে, বিদ্যমান পদ্ধতিগুলির ভারসাম্যহীন তথ্য বিতরণ, ওভারফিটিং সমস্যা, উচ্চ-মাত্রিক তথ্য পরিচালনা এবং পৃথক পদ্ধতিগুলির উপর নির্ভরতার মতো চ্যালেঞ্জের কারণে বিদ্যুৎ চুরি সনাক্তকরণে (ETD) উপ-সর্বোত্তম কর্মক্ষমতা প্রদান করে। এই সীমাবদ্ধতার প্রতিক্রিয়ায়, এই গবেষণাপত্রে মেশিন লার্নিং বুস্টিং ক্লাসিফায়ারের উপর ভিত্তি করে একটি ভোটিং এনসেম্বল মডেলের প্রস্তাব দেওয়া হয়েছে। এই মডেলে, আমরা ফিচার এক্সট্রাকশনের জন্য ব্যাপকভাবে স্বীকৃত কৌশল কনভোলিউশনাল নিউরাল নেটওয়ার্ক (CNN) অন্তর্ভুক্ত করি। কাঠামোটি তিনটি মূল উপাদানকে অন্তর্ভুক্ত করে, যেমন ডেটা প্রিপ্রসেসিং, ডেটা ব্যালেন্সিং এবং ক্লাসিফিকেশন, প্রতিটি বিদ্যুৎ চুরি সনাক্তকরণে নির্দিষ্ট চ্যালেঞ্জ মোকাবেলা করে। উল্লেখযোগ্যভাবে, প্রস্তাবিত মডেলটি এক্সট্রিম গ্রেডিয়েন্ট বুস্টিং (XGBoost), ক্যাটাগরিকাল বুস্টিং (CatBoost) এবং লাইট গ্রেডিয়েন্ট বুস্টিং (LightGBM) এর শক্তি ব্যবহার করে এর সামগ্রিক দৃঢ়তা এবং ভবিষ্যদ্বাণীমূলক নির্ভুলতা বাড়ায়। বিভিন্ন এভালুয়েশন মেট্রিক ব্যবহার করে যথাযথ বৈধতা মডেলের কার্যকারিতাকে নির্দেশ করে, যা ব্যাপক সিমুলেশন দ্বারা প্রমাণিত হয়। ফলাফলগুলি পৃথক মডেলের তুলনায় উচ্চতর কর্মক্ষমতা নির্দেশ করে, প্রস্তাবিত মডেলটি ৯৯% নির্ভুল পরীক্ষণ সক্ষমতা অর্জন করে।

CONTENTS

ABSTRACT	ii
ABSTRACT (BENGALI)	iii
LIST OF FIGURES	vi
LIST OF TABLES	vii
LIST OF ABBREVIATIONS	viii
CHAPTER 1 INTRODUCTION	1
1.1 Introduction	1
1.2 Research Motivation	3
1.3 Research Objectives	4
1.4 Organization of the Thesis	5
CHAPTER 2 RELATED WORKS	6
2.1 Introduction	6
2.2 Theoretical Background and Literature Review	6
2.3 Chapter Summary	13
CHAPTER 3 PROPOSED METHODOLOGY	15
3.1 Introduction	15
3.2 Data Preprocessing	16
3.2.1 Dataset Information	16
3.2.2 Handling the Missing Values	17
3.2.3 Normalization	18
3.2.4 Handling the Class Imbalance	18
3.3 Analysis of Energy Consumption Pattern	20
3.4 Proposed model's algorithm	22
3.4.1 Feature Extraction by CNN	24
3.4.2 Ensemble Boosting Model	25
3.4.2.1 Extreme Gradient Boosting	26
3.4.2.2 Light Gradient Boosting	27
3.4.2.3 Categorical Boosting	29

3.4.3	Soft Voting	30
3.4.4	Essence of Boosting Ensembles for Machine Learning	32
3.4.5	Model Training	33
3.5	Chapter Summary	34
CHAPTER 4 RESULTS AND DISCUSSIONS		36
4.1	Introduction	36
4.2	Evaluation Metrics	36
4.2.1	Analysis of Evaluation Metrics	39
4.3	Comparison With Other Existing Models	45
4.4	Chapter Summary	47
CHAPTER 5 CONCLUSIONS AND FUTURE WORKS		48
5.1	Conclusions	48
5.1.1	Research outcomes	49
5.2	Future Works	50
LIST OF PUBLICATIONS		51
REFERENCES		52

LIST OF FIGURES

Figure 3.1: Normal and theft classes' distribution before SMOTE implementation .	19
Figure 3.2: Normal and theft classes' distribution after SMOTE implementation . .	20
Figure 3.3: Real user consumption pattern	21
Figure 3.4: Fraud user consumption pattern	22
Figure 3.5: Overview of the proposed system model	23
Figure 3.6: CNN architecture for feature extraction	25
Figure 3.7: Soft voting	31
Figure 4.1: Confusion matrix of 2 classes	40
Figure 4.2: SVM model's ROC curve	41
Figure 4.3: LR model's ROC curve	42
Figure 4.4: XGBoost model's ROC curve	43
Figure 4.5: Proposed model's ROC curve	44

LIST OF TABLES

Table 2.1:	Summary of techniques, datasets, contributions, validation metrics, and limitations in some of the studies.	12
Table 3.1:	Dataset Description	17
Table 3.2:	Pseudocode of the proposed model	34
Table 4.1:	Summary of results	45

LIST OF ABBREVIATIONS

AMI	Advanced Metering Infrastructure
AUC	Area Under the Curve
CNN	Convolutional Neural Network
DL	Deep Learning
EC	Electricity Consumption
ET	Electricity Theft
ETD	Electricity Theft Detection
FPR	False Positive Rate
IoT	Internet of Things
LR	Logistic Regression
LSTM	Long Short-Term Memory
ML	Machine Learning
MLP	Multi-layer Perceptron
NaN	Not a Number
NTL	Non-Technical Loss
RF	Random Forest
ROC	Receiver Operating Characteristic
SG	Smart Grid
SGCC	State Grid Corporation of China
SMOTE	Synthetic Minority Over-sampling TEchnique
SMS	Supply Management System
SVM	Support Vector Machine
TL	Technical Loss
TPR	True Positive Rate

CHAPTER 1

INTRODUCTION

1.1 Introduction

Electricity theft (ET), a pervasive global issue, imposes significant financial burdens on utility companies and escalates costs for consumers. The distinction between technical losses (TLs) and non-technical losses (NTLs) underscores the human-driven nature of NTLs, which encompass activities like meter tampering, unauthorized connections, and billing irregularities. These avoidable losses not only impact utility revenues but also disrupt energy demand forecasting and contribute to transmission and distribution inefficiencies. As traditional power grids transition to smart grids (SGs), the integration of Advanced Metering Infrastructure (AMI) offers a promising avenue for detecting instances of ET by providing granular data on electricity consumption (EC). However, the proliferation of AMI introduces security vulnerabilities, necessitating robust fraud detection mechanisms. Various machine learning (ML) and deep learning (DL) models have emerged as potential solutions, ranging from support vector machines (SVM) to deep convolutional neural networks (CNNs). While these models demonstrate promise, challenges persist, including low detection accuracy and high false positive rates (FPR), particularly in the context of imbalanced datasets.

TLs are a part of any power distribution system. Meter manipulation, bypassing meters, direct tapping from the lines, billing anomalies and, most significantly, power theft are human actions rather than the mechanics of electricity transmission that produce NTLs [1]. These avoidable losses are worrisome because they have a direct effect on utility companies' bottom lines, which in turn raises prices for customers and cuts funding for infrastructure upgrades. Not only can ET cause revenue losses and safety issues, but it also makes it harder to accurately predict energy demand, and it's a major contributor to NTLs. Electric power loss is currently one of the biggest problems with both conventional power grids and SGs. Transmis-

sion and distribution losses rose from 11% in 1980 to 16% in 2000, as seen in the statistics [2]. By incorporating AMI with SGs, electricity providers can now collect massive amounts of data on energy use from smart meters in a very short amount of time. In order to detect cases of ET, this data becomes useful [3]. The three main types of AMI security vulnerabilities that might lead to NTL fraud are meter manipulation, network intrusion, and measurement disruption [4]. Various models based on ML and DL have been suggested as solutions to the problem of NTLs rather recently [5]. A few people used the classification-based SVM method to separate the attack samples from the normal samples in the EC database [6]. Further data analysis methods for identifying ET include state estimation [7], linear regression (LR) [8], and matrix decomposition [9]. But when dealing with massive amounts of data, these techniques won't cut it. Zheng et al. [10] introduced a deep CNN model that is both wide and detailed to analyze the ET habits of individual users. To detect power network energy thieves, the authors provide a deep model based on clustering in [11]. The proposed approach divides the EC data into many groups using a density-based clustering technique. EC samples that do not belong to any cluster are called energy thieves. Another source that uses gradient boosting techniques to generate Electricity Theft Detection (ETD) models is [12]. When applied to ETDs, the boosting model yields a more noticeable gain in accuracy. In addition, the problem of class imbalance is addressed by implementing synthetic theft attacks. Yet, the detection accuracy of some of these approaches is rather low. Additionally, several of them have really high FPR levels. These bad results might happen for a variety of reasons. Instead of building a voting ensemble model from several, diverse techniques, we employ the ML classifiers individually in the ways stated above to get better performance in ETD. Also, results from majority class samples are biased due to how the imbalanced class issue is handled. Computer vision and picture categorization are two areas where both traditional and DL approaches have achieved remarkable success [13]. The capacity of DL approaches to process massive datasets, autonomously extract features, and carry out intricate classification tasks led to their incorporation into this study.

Employing a sophisticated approach, our model integrates a soft voting mechanism to fuse the predictive power of three prominent boosting algorithms: XGBoost, LightGBM, and CatBoost. This ensemble technique synergizes the distinct strengths and perspectives of each algorithm, culminating in a prediction model that exhibits heightened resilience and accuracy. In the realm of ETD, this fusion of DL for feature extraction with ensemble boosting models has proven remarkably effective. This innovative modeling strategy signifies a significant leap forward in harnessing the potential of state-of-the-art ML methods to address pressing real-world challenges. Through this amalgamation of advanced techniques, our research endeavours to push the boundaries of what is achievable in the domain of ETD, ultimately contributing to the advancement of energy security and grid resilience.

1.2 Research Motivation

With escalating energy consumption driven by technological progress and urban growth, tackling ET becomes imperative to safeguard energy security, foster economic resilience, and promote sustainable development. Several factors contribute to the urgency of researching and addressing ETD. Previous cases of ET have demonstrated the significant economic impact it can have on utility companies and the broader economy. For utility companies, ET leads to substantial revenue losses, as NTLs resulting from theft and fraud account for a significant portion of overall revenue. These losses not only affect the financial viability of utility companies but also result in higher electricity prices for consumers to offset the lost revenue. Furthermore, ET undermines the stability and security of energy supply systems, placing strain on the power grid and increasing the risk of blackouts and service interruptions. Such disruptions can have far-reaching consequences, impacting businesses, industries, and critical infrastructure, thereby hampering economic growth and development. Additionally, unauthorized consumption of electricity contributes to excessive energy usage and waste, exacerbating environmental challenges such as greenhouse gas emissions and climate change. Addressing ET is also crucial for promoting social equity, as it disproportionately affects vulnerable communities and low-income households, further widening existing socioeconomic disparities.

Rapid advancements in technology present new opportunities for detecting and preventing ET, with smart meters, data analytics, and ML algorithms offering innovative solutions for identifying suspicious EC patterns. Overall, conducting research on ETD is imperative for mitigating economic losses, enhancing energy security, addressing environmental challenges, promoting social equity, and leveraging technological advancements for the benefit of society.

By leveraging smart meters and advanced data analytics, our research aims to develop robust solutions for identifying and addressing instances of theft and fraud in energy distribution networks. By improving the accuracy and efficiency of detection methods, we seek to not only mitigate financial losses but also enhance the reliability and resilience of the power grid. Ultimately, our efforts align with the broader goals of promoting sustainable energy practices and ensuring equitable access to electricity for all segments of society.

1.3 Research Objectives

In light of the identified gap in the area of theft detection, the research presented in this thesis sets its primary goal to develop an ensemble model for the ETD system as mentioned in the previous section. To carry out the project, the specific objectives of this work are outlined as follows.

- a) To investigate the daily EC patterns of both genuine users and those engaged in fraudulent activities.
- b) To analyze the dataset on power consumption that was obtained from State Grid Corporation of China (SGCC).
- c) To develop machine learning algorithms for detecting electricity theft.
- d) To validate and verify results with the existing models and propose a better model.

The expected outcome of this work is, therefore, that a new theft detection system will be introduced, where ML models will be used to make the detection system.

1.4 Organization of the Thesis

This thesis is organized as follows.

Chapter 2 Captures the background of the proposed research, including previous and current approaches taken for solutions.

Chapter 3 Presents the recommended systematic approach to the detection system.

Chapter 4 Rigorously evaluates the effectiveness of the scheme, analyzing its performance and outcomes.

Chapter 5 Presents the conclusion of the thesis with a summary of the original contributions and future work.

CHAPTER 2

RELATED WORKS

2.1 Introduction

Electricity theft poses a significant challenge to the stability and sustainability of power distribution systems worldwide. As utility companies grapple with the financial ramifications of NTLs incurred through theft and unauthorized consumption, the need for robust detection and mitigation strategies becomes increasingly pressing. In the realm of SGs, where AMI and data analytics hold promise for enhancing operational efficiency and customer service, the issue of ET takes on added complexity. This chapter delves into the multifaceted domain of electricity theft detection within SGs, where the convergence of hardware innovations, data-mining techniques, and ML algorithms offers novel avenues for identifying and mitigating instances of theft. Against the backdrop of escalating energy demand, rising costs, and evolving grid dynamics, the research presented herein seeks to address the critical need for effective and scalable solutions to combat ET. Through an in-depth examination of various methodologies and approaches, this chapter endeavours to elucidate the challenges, opportunities, and emerging trends in the field of ETD within the context of SGs.

2.2 Theoretical Background and Literature Review

ETD is underpinned by a robust theoretical framework encompassing various domains pertinent to the energy sector. Drawing upon principles from electrical engineering and advanced analytics, the effort seeks to understand and combat unauthorized consumption within power grids. By analyzing intricate patterns in consumption data collected from smart meters and other sources, researchers aim to identify anomalies indicative of fraudulent activities. Additionally, insights into the behavioural aspects of electricity theft provide valuable context, informing the development of targeted detection methodologies. Through this interdisciplinary approach, the researchers endeavour to devise effective strategies for mitigating energy theft

and safeguarding the integrity of power distribution systems. Furthermore, the literature review delves into key studies and methodologies employed in the field of ETD. Insights from criminology and behavioural economics shed light on the motivations behind ET, offering valuable perspectives for devising countermeasures. Additionally, advancements in ML and data analytics present promising avenues for enhancing detection accuracy and efficiency. By synthesizing findings from diverse disciplines, the review underscores the importance of interdisciplinary collaboration in addressing the complex challenges associated with ET. Moreover, it highlights the need for scalable and adaptable solutions capable of addressing evolving threats in the energy sector. Through a comprehensive review of existing literature, the research aims to build upon prior knowledge and contribute to the advancement of effective strategies for combating ET.

Research on ETD in SGs has recently gained importance, and researchers have been employing a number of approaches to conduct ETD. The most common ways to classify these approaches are as follows: hardware-based, data-mining-based, or hybrid systems that use elements of both. To resolve ETD in SGs, certain types of hardware, such as sensors, microcontrollers, and circuits, are required [14, 15, 16, 17]. The goal of these techniques is to detect power theft that occurs as a consequence of physical interference between supply management systems (SMS) and distribution power lines. This is not a reliable way for them to detect cyberattacks on energy SMS. Theft of energy from SMS by hacking entails altering EC measurements [18]. As an example, [14] identifies cases of power theft using a hardware class-based approach. The use of temperature sensors allows the authors to both estimate and detect NTL. Additionally, in order to detect energy theft, transformer overloading is employed in [15]. Upon detection of overload at the transformer, a relay circuit is utilized to shut off the transformer. This makes electricity theft less likely. These solutions are costly because they require specialized hardware components that are difficult to procure and keep up-to-date, and they also fail to detect cyberattacks. Class methods for ETD that are hybrid (using both hardware and data mining) [19, 20, 21] employ both data mining (using ML and DL) and

hardware-related approaches to find NTLs. When it comes to ETD in SGs, for instance, the authors utilize SVM in their work [19]. Distribution transformer meters can detect suspicious consumers and areas with a high risk of power theft by looking for unusual EC patterns. On the other hand, by using a standalone machine learning classifier for ETD, the authors get the maximum FPR value. In addition, the authors of [20] highlight the discovery of a new and complex kind of electricity theft called colluding NTL, where many electrical fraudsters collaborate to perpetrate electricity fraud. In order to record the EC of several houses in a community, an observer meter is installed. There are surveillance cameras to prevent cyberattacks and interference-resistant devices to keep observer meters safe from physical interference. In addition, in order to detect SMS that has altered EC data, a mathematical model is created utilizing data collected from both the SMS and an observer meter. However, there is an additional cost associated with the deployment and maintenance of hardware devices due to the specialized hardware components needed for the hybrid category.

Data mining-based ETD strategies have recently attracted a lot of attention from academics looking to combat electricity theft in small-group situations [18, 22, 23, 24]. The reason is that those two types of ETD methods are quite pricey. A deep model for SG non-theft user classification and power theft is presented by the authors of [18]. The problem of not a number (NaN) values is handled by methods of interpolation, while imbalanced data is addressed by methods of synthetic data point production. One way to lower the dimensionality is by using principal component analysis. Bayesian optimization is utilized to enhance the ETD's performance by modifying the model's hyperparameters. Additionally, the adaptive moment estimation (Adam) optimizer is used to optimize the model's parameters for better results. The SGCC dataset is utilized in the analysis of this paper. Some of the performance measurements used in the research include accuracy, precision, recall, F1 score, and Matthews correlation coefficient (MCC). These characteristics are also determined by the time, frequency, and hybrid domains. The use of a Bayesian optimizer to find possible solutions for hyperparameter optimization, on the other hand, is time-consuming. When it comes to EC data, the authors of

[22] recommend a deep stacked autoencoder with a Long Short-Term Memory (LSTM) based structure for anomaly detection. It is believed that deep autoencoders may help identify complicated patterns in data, whereas LSTM can capture large sequences of long-term time series EC data. Hyperparameter optimization also makes use of a sequential grid search optimizer. In order to train and evaluate the suggested and benchmark models, the Irish EC dataset is utilized. Finding ETD in SGs is the objective. Yet, the evolution of stochastic features is neglected. Furthermore, in order to properly classify clients of power theft, [23] developed an LSTM-based DL model. We use consumption statistics from the real SGCC dataset for our analytics. However, separate and independent methods are employed. The outcome is a high FPR with low precision.

The authors construct a mixed DL model to identify NTL in SGs in [24]. The DL model that is hybridized consists of the multilayer perceptron (MLP) and LSTM models. For EC data analysis, LSTM is the tool of choice, whereas MLP is employed for non-sequential information utilization and analysis. The proposed hybrid model for SG NTL identification is trained and evaluated using the Spanish Endesa dataset. But we ignore the problem of data imbalance. In order to detect cases of power theft, a bagging ensemble random forest (RF) is employed in [25]. More so, a stacked autoencoder is used to extract important features, which improves the RF classifier's ETD performance. Electronic Crime Records (ECRs) from Ireland and China are used for theft analysis. Data balancing also makes use of RUS. On the other hand, the proposed classifier becomes underfit because of RUS. Another deep model with low FPR that the authors of [26] recommend is LFPR-DNN. To modify the model's weights, one uses the optimizer of gradient descent. To further reduce the influence of imbalanced data on ETD's efficacy, the focus loss function is employed. The two-stage training method proposed for LFPR-DNN is considered. At the beginning, we tune the hyperparameters using grid search. However, in the second stage, particle swarm optimization is used for fine-tuning. Also, in order to uncover cases of power theft, the Irish EC dataset is examined. In contrast, hyperparameter tuning necessitates the use of grid search, which has a very high temporal complexity.

In addition, the authors of [27] develop a robust detector for electrical theft by combining a bidirectional gated recurrent unit (BiGRU) for the purpose of identifying and categorizing energy theft from typical users with an autoencoder for the purpose of reducing dimensionality. In addition, BiGRU is able to detect drift patterns by learning long-term temporal dependency. In addition, the proposed model's overfitting issue is remedied by employing the dropout regularisation method.

The proposed model is trained and tested on the SGCC dataset. Furthermore, SGCC data is counterbalanced by utilizing six hypothetical theft attacks on actual data. Also, in [28], there is a power theft detector that uses an ensemble gradient boosting approach. The proposed detector is composed of three strategies: XGBoost, LightGBM, and CatBoost. Data from smart ECs in Ireland is used to conduct an investigation on power theft. The three theft detectors mentioned earlier can have their FPR values and detection rates enhanced by using stochastic characteristics. Additionally, feature extraction is executed using a weighted feature significance function to further simplify the training of the theft detectors in terms of both time and space. However, the hyperparameters of the proposed boosting ensemble theft detectors have not been fine-tuned. Using a boosting ensemble with feature engineering, ETD in SGs is achieved in [29]. Data from the SGCC is used to train and evaluate the proposed ETD algorithm. To top it all off, any missing data is filled in using the KNN interpolation approach. Additionally, the data imbalance is addressed using a hybrid over- and under-sampling technique (SMOTE-Tomek). Feature extraction and a scalable hypothesis method are employed to obtain reduced dimensions from the dataset.

Poor ETD performance and local optimum stagnation are the results of ignoring hyperparameter fine-tuning in classifiers. Also, in [30], we see the creation of an ensemble-based DL power theft detector. To get the final classification result, the proposed approach integrates multiple deep learning models and feeds their outputs into the majority voting classifier. The proposed model employs a DL model called a gated recurrent unit (GRU). The SG EC sam-

ples taken from the residential energy disaggregation dataset (REDD) are utilized for theft analysis. To find the best combination for identifying NTLs in SGs, six data balancing methods and fourteen classification approaches are integrated in [31]. These techniques include stacking and maximum voting ensembles. A combination of the stacking classifier, edited nearest neighbour (SMOTE-ENN), and synthetic minority oversampling is believed to be the best approach for ETD in SGs in the end. In addition, the study makes use of the EC data from the SGCC dataset. For further work, the authors of [32] propose ETD theft attacks, the LSTM model, and the GRU (TLGRU) model. The components of TLGRU include a database based on synthetic six theft attacks, a feature extraction method based on LSTM, and a classification method based on GRU. The suggested model is also trained and tested using the SGCC daily dataset. After comparing the proposed TLGRU to the benchmark schemes, the results show that the former is superior. And yet, the hyperparameters of the proposed TLGRU model have not been fine-tuned.

The usage of data mining techniques is employed by a few more articles. However, rather than using them for end-to-end transit, they use them to protect internet of things (IoT) networks from infiltration and cyberattacks, as mentioned in [33, 34, 35]. In order to identify cyberattacks, the writers of [33] employ XGBoost, RF, and KNN. To counter this, the authors of [36] employ a distributed stacking ensemble model for intrusion detection using fog computing. This model incorporates XGBoost, KNN, and Gaussian naive Bayes techniques at level 1. The output of the first-level classifiers is passed on to random forest, which acts as a second-level learner, to complete the final classification at level 2. The authors of [34] employ CNNs for anomaly-based intrusion detection to ensure the security of networks connected to the IoT. Using a sparse evolutionary training-multi layer perceptron, a DL method is employed in [35] to detect many cyber security risks in the context of the industrial IoT.

Before delving into the detailed analysis presented in Table 2.1, it is essential to provide a brief overview of the key components encapsulated within this comprehensive summary. The table

encapsulates a synthesis of various studies, elucidating the diverse techniques, datasets, contributions, validation metrics, and limitations observed across the literature on electricity theft detection. This structured presentation serves as a valuable reference point for understanding the landscape of research in this domain, offering insights into the methodologies employed, the datasets utilized, and the outcomes achieved. Through the systematic examination of these factors, researchers can discern patterns, identify gaps, and glean valuable insights to inform their investigative pursuits in combating electricity theft.

Table 2.1: Summary of techniques, datasets, contributions, validation metrics, and limitations in some of the studies.

Techniques	Dataset	Contributions	Validation Metrics	Limitations
SVM, DT and LR [37, 38]	Smart meter data	To identify fraudulent customers that purposefully steal power	Accuracy	Reliable performance metrics are not used
LSTM, MLP [39]	Endesa	Effectively use sequential data and supplemental information to identify power theft	ROC, PR AUC	Data imbalance
Wide and deep CNN [40]	SGCC	Identify power theft by using data's local and global properties	AUC, MAP	Data imbalance
SMOTE, CNN and LSTM [41]	SGCC	Enhanced ability to identify fraudulent consumers	F1-score, MCC	Overfitting
CNN, RF and SMOTE [42]	EISA	RF is used in the last layer of CNN to prevent local optima	F1-score	High execution time

The quest to combat energy theft has spurred a myriad of approaches, ranging from hardware-based solutions to sophisticated data mining techniques. Yet, despite the diversity of strategies, it is apparent that no single method can fully eradicate the problem. This underscores the necessity for a holistic and multifaceted approach that integrates a variety of perspectives

and technologies. As we conclude this literature review, it becomes clear that the landscape of energy theft detection is characterized by a rich tapestry of research endeavors, each contributing valuable insights and methodologies. From the early hardware-centric solutions to the more recent data-driven approaches, researchers and practitioners alike have explored a wide array of avenues in pursuit of effective countermeasures. However, amidst this diversity, there emerges a common thread—the recognition that a comprehensive solution requires the fusion of diverse expertise and methodologies. It is with this understanding that our research endeavors to build upon the foundational works presented in the literature, drawing upon insights from both academia and industry. By synthesizing these diverse perspectives and leveraging cutting-edge technologies, we aim to develop innovative solutions that not only enhance the resilience and security of modern power grids but also pave the way for a more sustainable and equitable energy future. In doing so, we aspire to contribute to the collective efforts aimed at mitigating the pervasive impact of energy theft and advancing the integrity and efficiency of energy systems worldwide.

2.3 Chapter Summary

In this chapter, our journey encompassed an extensive and meticulous exploration of methodologies geared toward detecting electricity theft within SGs. We traversed a diverse spectrum of approaches, ranging from traditional hardware-based solutions leveraging specialized equipment to sophisticated data-mining techniques harnessing various ML and DL algorithms. Moreover, we ventured into the realm of hybrid methods that intricately blend hardware and data-mining approaches, offering promising avenues for enhanced theft identification. Throughout our discourse, particular emphasis was placed on ensemble methods such as gradient boosting and stacking, renowned for their remarkable efficacy in augmenting theft detection performance. Yet, amidst these promising strides, lingering challenges persisted, notably in the form of imbalanced datasets and elevated False Positive Rates (FPR). These challenges underscored the imperative for ongoing investigation and optimization efforts to refine and validate these methodologies. By shedding light on the nuanced landscape

of ETD within SGs, this chapter underscored the critical need for cultivating robust and scalable theft detection systems meticulously tailored to the intricate dynamics of SG environments. Through a holistic and comprehensive examination, we set the stage for subsequent chapters to delve deeper into the development and evaluation of innovative approaches aimed at addressing these pressing challenges and advancing the state-of-the-art in ETD. The following chapter will examine the methodology that we have put forward.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 Introduction

ETD is a critical endeavour aimed at safeguarding utility systems from illicit consumption practices. This chapter presents a comprehensive overview of the proposed model designed to effectively detect instances of electricity theft. A preliminary examination of the data revealed discernible differences in consumption patterns between two classes: real users (class 0) and fraud users, often indicative of electricity theft (class 1). EC data is typically gathered through smart meters or various sensors deployed at consumer premises, with aggregated data transmitted to centralized servers via communication networks. However, issues such as smart meter failures, sensor malfunctions, or data transmission errors can result in missing or erroneous data entries within the dataset. To mitigate the impact of missing data on the dataset's integrity, a data preprocessing algorithm was developed to address these instances effectively, thereby preserving the dataset's size and facilitating reliable analysis. To tackle this challenge, a synthetic data generation technique, specifically the Synthetic Minority Over-sampling Technique (SMOTE), was employed to augment the minority class (fraud users). After that, the classification model was trained on this balanced dataset to make sure that both classes were fairly represented and to improve the model's ability to correctly identify cases of electricity theft. Leveraging CNN as a feature extractor, we developed an ensemble model integrating three powerful boosting algorithms for classification. Through soft voting, predictions from XGBoost, LightGBM, and CatBoost were combined to enhance the model's predictive capabilities.

3.2 Data Preprocessing

Data preprocessing is a critical stage in ML projects, serving as the foundation upon which accurate and reliable models are built. One of the primary objectives of data preprocessing is to address common issues such as missing values, and class imbalances, which can adversely affect the performance of ML models if left unattended. Additionally, data preprocessing helps standardize and normalize the data, ensuring that all features are on a similar scale and distribution, thereby preventing certain variables from dominating the model training process. Overall, data preprocessing is a crucial step that lays the groundwork for successful ML applications by ensuring that the input data is accurate, consistent, and appropriately formatted for analysis.

3.2.1 Dataset Information

The dataset utilized in this study originates from the SGCC, consisting of real electricity consumption data from 10,152 consumers over two years. It serves as a fundamental component for evaluating the efficacy of the proposed model. Comprising consumer IDs, daily electricity consumptions, and binary labels denoting entries as either real users or fraud users, this dataset offers a comprehensive view of electricity usage patterns. A notable characteristic of the dataset is its imbalanced class distribution, where instances are spread across a wide spectrum. Moreover, the dataset exhibits inconsistencies, including erroneous and missing values, which necessitate preprocessing for accurate analysis. Notably, the dataset provides ground-truth information, revealing that approximately 7.2% of all customers have been identified as engaging in electricity theft. Each customer is assigned a label, either 0 or 1, indicating their classification as a regular consumer or an electrical thief, respectively. These designations are determined through rigorous on-site inspections conducted by SGCC personnel. Structured in a tabular format, the dataset comprises individual customer records arranged in rows, with daily power consumption data for each user represented in columns. Table 3.1 serves as a crucial reference, providing a concise yet comprehensive overview of the dataset's metadata.

Table 3.1: Dataset Description

Description	Values
Duration of data collection	2014-2016
Total consumers	10152
Honest consumers	9466
Fraudulent consumers	686
Ground truth	7.2%

It offers clarity on the dataset's structure, content, and key attributes, facilitating informed decision-making and analysis during subsequent stages of research.

3.2.2 Handling the Missing Values

The dataset often exhibits instances of erroneous or missing values, commonly denoted as NaN. These occurrences can stem from various sources, including malfunctioning smart meters, unforeseen system maintenance, damaged distribution lines, or issues with data storage infrastructure. The presence of missing or erroneous values poses a significant challenge during the training of ML models, as it can severely impair their performance. While a conventional approach to handling such issues involves the deletion of customer records containing missing values, this simplistic solution may lead to the loss of valuable information encoded within these records. To address this challenge, a more sophisticated method is employed in this study to handle missing data effectively. Specifically, a linear imputation approach is adopted, as detailed in Equation 3.1 [40]. This method aims to recover missing data points by leveraging the existing information within the dataset, thereby preserving valuable insights while mitigating the impact of missing values on the analysis.

$$f(x_i) = \begin{cases} \frac{x_{i+1} + x_{i-1}}{2} & \text{if } x_i \in \text{NaN}, x_{i-1} \text{ and } x_{i+1} \notin \text{NaN} \\ 0 & \text{if } x_i \in \text{NaN}, x_{i-1} \text{ or } x_{i+1} \in \text{NaN} \\ x_i & \text{if } x_i \notin \text{NaN} \end{cases} \quad (3.1)$$

Where x_i represents the attribute of the electricity consumption data and NaN represents the non-numeric value. If both x_{i-1} and x_{i+1} are non-numeric values in the dataset, then they are

replaced by zero; otherwise, missing values are replaced by taking the average of the previous and next values in the dataset. The purpose of this imputation method is to recover the missing values while maintaining the temporal continuity of the EC data.

3.2.3 Normalization

After addressing missing values within the dataset, the subsequent step involves normalization, a critical process aimed at standardizing the range of input features. This normalization step is particularly vital for DL models, where consistency in feature scaling greatly influences model performance. Extensive empirical studies consistently highlight the advantages of training DL models on normalized data, underscoring its pivotal role in achieving optimal performance. The min-max normalization method, described by Equation 3.2 [43], provides a structured approach to this standardization process. Through this method, each feature is rescaled to fall within a predefined range, ensuring uniformity and facilitating better model training and analysis. By leveraging the min-max normalization technique, we ensure that the dataset's features are appropriately scaled, thereby bolstering the reliability and efficacy of subsequent analytical processes and model outcomes.

$$x_{i,j} = \frac{x_{i,j} - \min(x_i)}{\max(x_i) - \min(x_i)} \quad (3.2)$$

The $\min(x_i)$ and $\max(x_i)$ represent the minimum and maximum values of EC of consumer i , respectively. By ensuring that the data values are scaled within a consistent range, this transformation helps DL models perform better during training and achieve better convergence.

3.2.4 Handling the Class Imbalance

In machine learning, addressing class imbalance is a critical concern, especially in scenarios where one class significantly outnumbers the other. This imbalance can skew the performance of algorithms, leading to biased predictions that favor the majority class. One of the prominent

techniques employed to mitigate class imbalance [44] is the SMOTE. It is a data augmentation technique designed to alleviate class imbalance by oversampling the minority class. Unlike traditional oversampling methods that replicate existing minority class instances, SMOTE generates synthetic samples based on the characteristics of the minority class. This is achieved by interpolating between existing minority class instances to create new, synthetic examples. Figure 3.1 provides a visual representation of the distribution of normal and theft classes within the dataset before the application of the SMOTE. This visualization offers insights into the imbalance between the two classes and underscores the need for data augmentation techniques to address this imbalance effectively.

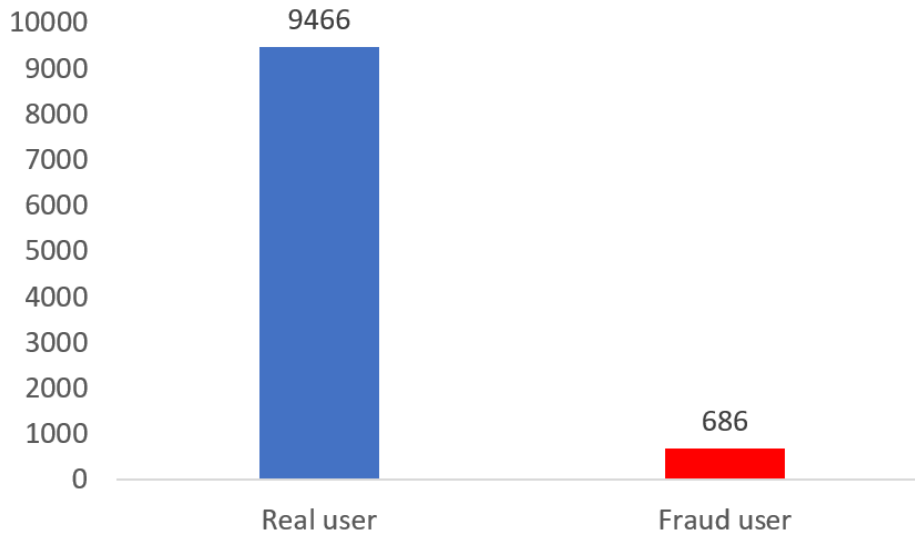


Figure 3.1: Normal and theft classes' distribution before SMOTE implementation

The process of generating synthetic samples involves identifying a minority class instance and its nearest neighbors in the feature space. Then, synthetic instances are created along the line segments connecting the minority class instance to its neighbors. By synthesizing new examples, SMOTE effectively expands the minority class, balancing the distribution of classes in the dataset. One of the key advantages of SMOTE is its ability to address the imbalance issue without introducing bias toward the majority class. By generating synthetic samples that closely resemble existing minority class instances, SMOTE ensures that the model receives

sufficient training data from both classes, facilitating more robust learning. After the implementation of the SMOTE, Figure 3.2 illustrates the distribution of normal and theft classes, showcasing the impact of data augmentation on re-balancing the dataset and facilitating more robust model training.

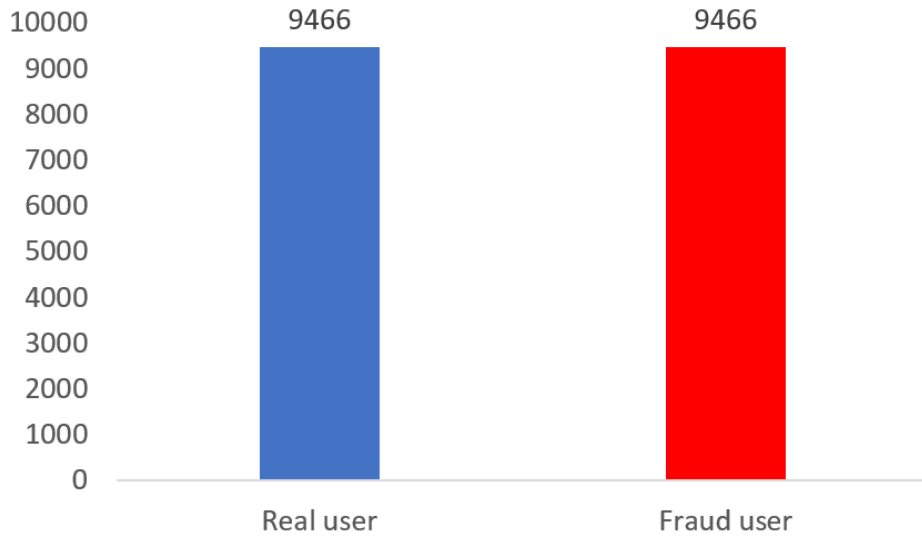


Figure 3.2: Normal and theft classes' distribution after SMOTE implementation

This augmentation technique enhances the generalization capability of classifiers, improving their predictive performance on unseen instances. Moreover, SMOTE can improve the generalization performance of ML models by providing additional training examples for the minority class. This can lead to enhanced model accuracy, particularly in tasks such as fraud detection, where correctly identifying instances of minority classes is of utmost importance.

3.3 Analysis of Energy Consumption Pattern

Understanding energy consumption patterns is crucial for detecting anomalies indicative of electricity theft within smart grid systems. By juxtaposing the consumption patterns of real users and electricity thieves, these figures highlight the significance of identifying irregularities and fluctuations in energy usage data to mitigate the risk of theft and ensure the integrity of power distribution networks. In Figure 3.3, we present the energy consumption pattern of

a typical real user within the dataset. This depiction offers a glimpse into the consistent and relatively stable consumption behavior exhibited by legitimate electricity consumers. This visualization showcases regular energy usage habits, serving as a baseline for identifying abnormal consumption patterns.

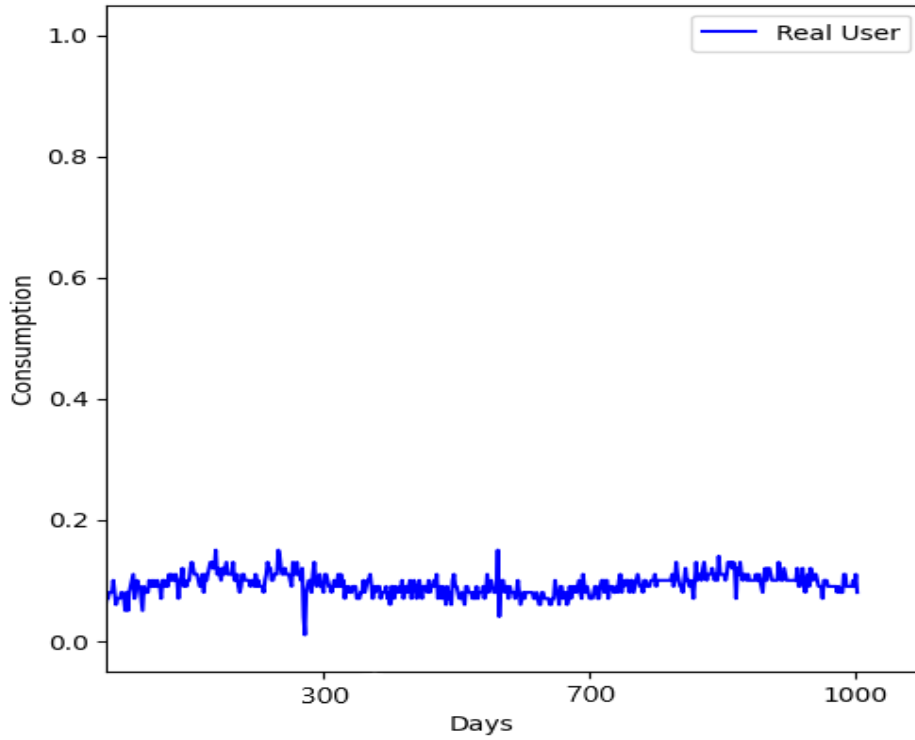


Figure 3.3: Real user consumption pattern

Figure 3.4 provides insight into the energy consumption pattern of an electricity thief, contrasted against that of the real user. Here, we observe distinct fluctuations and irregularities in the consumption curve, indicative of fraudulent activity. These abrupt variations in energy usage patterns serve as key indicators of potential theft or misuse, underscoring the importance of robust detection mechanisms in identifying and addressing such anomalies effectively.

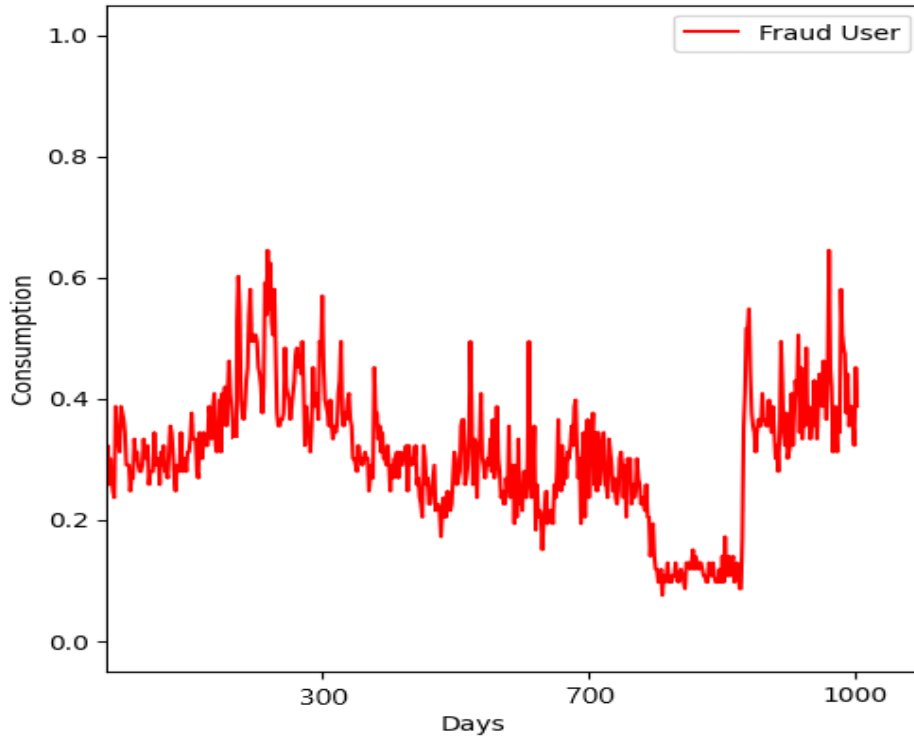


Figure 3.4: Fraud user consumption pattern

The visual analysis presented in the above figures underscores the importance of leveraging data insights to combat electricity theft effectively. By recognizing the distinct consumption patterns of legitimate users and potential fraudsters, utility companies can enhance their detection mechanisms and safeguard the reliability of power distribution systems. These figures serve as a visual reminder of the ongoing efforts to mitigate energy theft and ensure the equitable distribution of electricity resources for all stakeholders.

3.4 Proposed model's algorithm

In our quest for robust electricity theft detection, we embarked on a systematic journey, strategically leveraging CNN as a proficient feature extractor. By harnessing the inherent capabilities of CNN, we aimed to capture nuanced patterns and intricate relationships within the input data, thus facilitating more discerning feature representation. Subsequently, we meticulously crafted an ensemble model by amalgamating the predictive prowess of three eminent boosting

algorithms for classification tasks. This ensemble approach, orchestrated through soft voting, engenders a harmonious collaboration among the individual models, culminating in a collective decision-making process that enhances the overall accuracy and reliability of our detection system. To provide a comprehensive visual elucidation of our proposed methodology, an illustrative diagram in Figure 3.5 delineates the architectural framework of our detection system and elucidates the intricate interplay between feature extraction, classification, and ensemble aggregation strategies. By presenting a holistic overview of the model's architecture, this figure offers invaluable insights into the synergistic integration of diverse components, thus empowering a deeper understanding of the underlying mechanisms driving our detection framework's efficacy and performance.

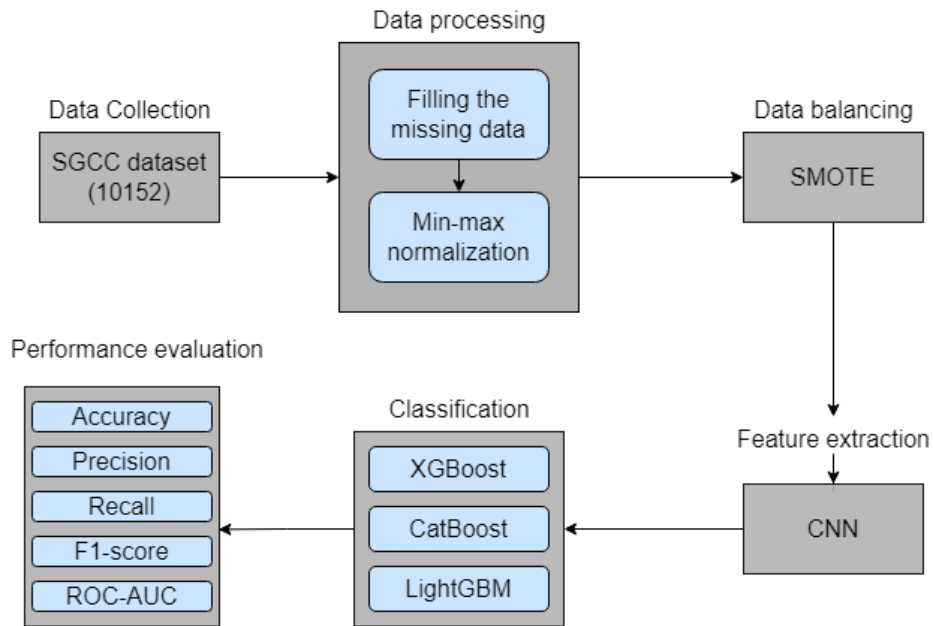


Figure 3.5: Overview of the proposed system model

Our combined approach of utilizing CNN-based feature extraction and ensemble modeling represents a significant advancement in the realm of electricity theft detection for smart grids, demonstrating superior accuracy and efficacy in identifying fraudulent activities within energy distribution systems.

3.4.1 Feature Extraction by CNN

Feature extraction using CNN plays an important role in various domains, including fraud detection in electricity consumption datasets. In the context of this study, CNN is employed to extract meaningful features from the electricity consumption data, which are subsequently used for classification tasks to distinguish between normal and abnormal consumption patterns. CNN is a class of deep learning models specifically designed for processing structured grid-like data, such as images, time series, and sequences. The architecture of CNN consists of multiple layers, including convolutional layers, pooling layers, and fully connected layers. These layers work collaboratively to extract hierarchical representations of input data, capturing both local and global patterns. In the case of electricity consumption data, CNN is applied to the daily consumption readings of consumers over a specified period. Each consumer's consumption data is treated as a time series, with each time step representing a day's consumption.

The CNN architecture in [45] is configured to analyze these sequential data points and extract discriminative features that capture underlying consumption patterns. The feature extraction process begins with the input layer, where the consumption data is fed into the network. Convolutional layers play a crucial role in feature extraction by applying filters across the input data and identifying spatial and temporal patterns present in the consumption sequences. These filters, also known as kernels, slide across the input data, performing element-wise multiplications and aggregations to produce feature maps. Pooling layers are interspersed between convolutional layers to downsample the feature maps, reducing the dimensionality of the data while retaining essential information. Max-pooling, for example, selects the maximum value from each region of the feature map, preserving the most significant features. As the data passes through successive convolutional and pooling layers, it undergoes hierarchical feature extraction, with deeper layers capturing increasingly abstract representations of the input data. The extracted features are then flattened and passed through fully connected layers,

which further process the features and map them to the output layer for classification.

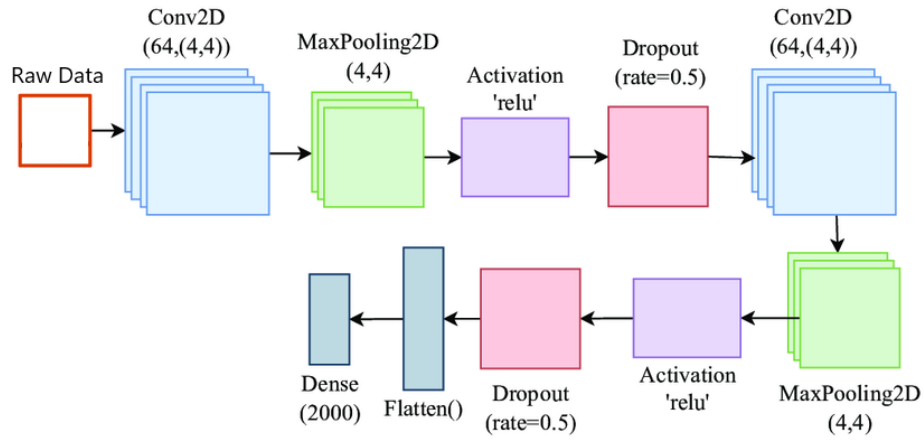


Figure 3.6: CNN architecture for feature extraction

In the context of fraud detection in electricity consumption datasets, CNN is adept at capturing subtle consumption patterns indicative of fraudulent behavior. By analyzing sequential consumption data, CNN can identify anomalies, irregularities, or fluctuations in consumption patterns that deviate from normal usage. These extracted features serve as valuable inputs to downstream classification models, enabling accurate detection of fraudulent activities. Overall, feature extraction using CNN empowers fraud detection systems to leverage the inherent structure and temporal dependencies present in electricity consumption data. By capturing relevant patterns and anomalies, CNN enhances the effectiveness of classification models, enabling more robust and accurate identification of fraudulent behavior.

3.4.2 Ensemble Boosting Model

In our pursuit of enhancing the effectiveness of fraud detection systems, we adopted a strategic ensemble learning approach. By integrating three powerful gradient-boosting models - XGBoost, LightGBM, and CatBoost - we aimed to capitalize on their strengths while mitigating inherent weaknesses. This comprehensive strategy not only diversifies the learning process but also ensures a more robust and accurate fraud detection system. Through the technique of soft voting, we amalgamated the predictions of these models, facilitating a thorough analysis

of the data and ultimately leading to improved system performance and reliability. Detailed explanations of each model are provided below for a comprehensive understanding of their contributions.

3.4.2.1 Extreme Gradient Boosting

It is also known as XGBoost, an essential component of the ensemble model utilized for fraud detection in this study, and operates on a foundational principle rooted in gradient boosting, a robust technique in machine learning renowned for its ability to construct predictive models by sequentially training decision trees. Within the context of electricity consumption data, XGBoost leverages this technique to iteratively refine predictions by correcting errors made by preceding models, ultimately capturing intricate non-linear relationships between input features and the target variable.

The mechanism behind XGBoost's effectiveness lies in its iterative approach [46], where each subsequent decision tree is trained to rectify the errors of its predecessors. Through a process of gradient descent, XGBoost minimizes a predefined loss function, effectively optimizing the model's predictive capabilities with each iteration. Additionally, XGBoost introduces regularization techniques to prevent overfitting, ensuring the model's generalizability to unseen data. XGBoost optimizes the objective function outlined in Equation 3.3.

$$\text{Obj}(\Theta) = \sum_{i=1}^n L(y_i, \hat{y}_i) + \sum_{k=1}^K \Omega(f_k) \quad (3.3)$$

$L(y_i, \hat{y}_i)$ represents the loss function, which measures the model's error in predicting the target y_i compared to the predicted value $\hat{y}_i$. $\Omega(f_k)$ is a regularization term that penalizes model complexity. It discourages the creation of overly complex decision trees, which can lead to overfitting.

Furthermore, XGBoost incorporates weighted sampling techniques to address class imbal-

ance, a common challenge in fraud detection datasets where instances of fraud (class 1) are significantly outnumbered by normal activities (class 0). By assigning higher weights to minority class samples during training, XGBoost mitigates the risk of bias towards the majority class, enabling more accurate detection of fraudulent behaviors. In addition to its robustness to class imbalance, XGBoost offers insights into feature importance through its built-in functionality for evaluating variable importance. By analyzing the contribution of each feature to model performance, domain experts can gain valuable insights into the underlying factors driving fraudulent activities in electricity consumption datasets. Moreover, XGBoost's parallelized implementation and optimization algorithms ensure scalability, making it well-suited for handling large-scale datasets commonly encountered in fraud detection scenarios. Its efficient training and inference processes enable real-time detection capabilities crucial for safeguarding against potential threats to electricity consumption infrastructures.

3.4.2.2 Light Gradient Boosting

Light Gradient Boosting is also known as LightGBM, a critical component of the ensemble model utilized for fraud detection, and is a gradient-boosting framework developed by Microsoft. It stands out for its efficiency, scalability, and high-performance capabilities, making it well-suited for handling large-scale datasets commonly encountered in fraud detection scenarios.

At the heart of its mechanism [47] lies the concept of gradient boosting, which involves iteratively training an ensemble of decision trees to improve predictive accuracy. LightGBM, however, introduces several innovative techniques to enhance the efficiency and effectiveness of gradient boosting. One of its key innovations is its histogram-based approach to decision tree construction. Unlike traditional algorithms that use level-wise or depth-wise tree growth strategies, it employs a leaf-wise growth strategy. This strategy selects the leaf with the maximum delta loss, resulting in a more balanced tree structure and reducing computational costs. Moreover, it implements a gradient-based one-side sampling (GOSS) technique to speed up

the training process. It focuses on retaining the instances with large gradients during the sampling process while discarding instances with small gradients. This selective sampling approach preserves the information crucial for model training while reducing computational overhead. It optimizes an objective function comprising the components outlined in Equation 3.4.

$$\text{Obj}(\Theta) = \sum_{i=1}^n L(y_i, \hat{y}_i) + \sum_{k=1}^K \frac{1}{2} \lambda \|w_k\|^2 + \gamma |w_k| \quad (3.4)$$

$L(y_i, \hat{y}_i)$ represents loss function. λ and γ are regularization parameters. $\|w_k\|$ represents weights of decision tree leaves.

Additionally, it utilizes a distributed computing framework that enables parallel and distributed training across multiple machines. This distributed training capability significantly accelerates the model training process, making LightGBM well-suited for large-scale fraud detection applications where timely decision-making is critical. Furthermore, it incorporates built-in support for handling class imbalance, a common challenge in fraud detection datasets where instances of fraud are significantly outnumbered by normal activities. By incorporating class weights or adjusting the threshold for decision-making, it can effectively address class imbalances and improve the detection of fraudulent activities.

Its significance within the ensemble model extends beyond its capabilities, playing a pivotal role in enhancing the overall performance and efficacy of the ensemble. Its unique strengths, including its efficient training process, scalability, and adeptness at handling class imbalances, energize those of other algorithms like XGBoost and CatBoost. Through this harmonious integration, it contributes to the diversification and robustness of the ensemble, enabling it to navigate complex data landscapes with greater accuracy and reliability. By harnessing its capabilities, the ensemble model not only achieves heightened levels of accuracy in detect-

ing fraudulent activities but also exhibits enhanced efficiency in processing and analyzing vast volumes of EC data. Thus, it emerges as a cornerstone element within the ensemble, augmenting its overall performance and reinforcing its utility in combating electricity theft within SG environments.

3.4.2.3 Categorical Boosting

Categorical Boosting is also known as CatBoost, an integral part of the ensemble model employed for fraud detection, and is a gradient-boosting framework developed by Yandex. It is renowned for its robustness, scalability, and native support for categorical features, making it well-suited for handling complex datasets commonly encountered in fraud detection scenarios.

At the core of its mechanism [48] lies the gradient boosting algorithm, which iteratively trains an ensemble of decision trees to improve predictive accuracy. However, CatBoost incorporates several innovative techniques to enhance performance and address challenges inherent in fraud detection datasets. One of its key innovations is its implementation of ordered boosting, which minimizes the impact of overfitting by considering the order of categorical features during tree construction. Unlike traditional gradient boosting algorithms that rely on random or predefined feature orders, it automatically selects the optimal feature ordering based on statistical significance, leading to more accurate and robust models. Moreover, it introduces the concept of oblivious trees, which enables parallelization of tree construction without compromising accuracy. By splitting categorical features into multiple numerical features, CatBoost facilitates parallel processing, thereby accelerating training without sacrificing predictive performance. Its direct handling of categorical variables enhances its usability and effectiveness in real-world data analysis tasks. It optimizes an objective function that incorporates the following components, as depicted in Equation 3.5.

$$\text{Obj}(\Theta) = \sum_{i=1}^n L(y_i, \hat{y}_i) + \sum_{j=1}^m \frac{1}{2}(g_j + h_j) \quad (3.5)$$

$L(y_i, \hat{y}_i)$ represents the loss function, measuring the model's error in predicting the target y_i compared to the predicted value $\hat{y}_i$. g_j and h_j are the first and second-order gradients for categorical features.

It incorporates a novel technique known as learning-to-rank, which optimizes model performance by directly optimizing ranking metrics such as ROC-AUC (Receiver Operating Characteristic - Area Under the Curve). This approach is particularly beneficial in fraud detection scenarios where the focus is on ranking instances based on their likelihood of being fraudulent. It offers built-in support for handling missing values, categorical features, and class imbalance, a common challenge in fraud detection datasets where instances of fraud are significantly outnumbered by normal activities. By automatically handling these complexities, it simplifies the model development process and enhances the reliability of fraud detection systems.

The importance of CatBoost in the ensemble model lies in its ability to complement other algorithms, such as XGBoost and LightGBM, by providing diversity and resilience to the model ensemble. By leveraging its robustness, native support for categorical features, and optimization for ranking metrics, the ensemble model can achieve superior performance in identifying fraudulent activities in electricity consumption data.

3.4.3 Soft Voting

Soft voting, also known as weighted averaging, is a popular ensemble learning technique used to combine the predictions of multiple base models to make a final decision. In the context of a fraud detection project, where an ensemble model consisting of XGBoost, LightGBM, and CatBoost classifiers is employed, soft voting plays an important role in aggregating the

individual predictions of these classifiers to arrive at a consensual prediction. The soft voting process involves assigning weights to the predictions of each base model based on their respective confidences or probabilities. Instead of simply counting the votes of each model equally (hard voting), soft voting considers the confidence levels associated with each prediction. Specifically, the predicted probabilities generated by each base model for each class (0 for real users and 1 for fraud users) are averaged or weighted according to their importance.

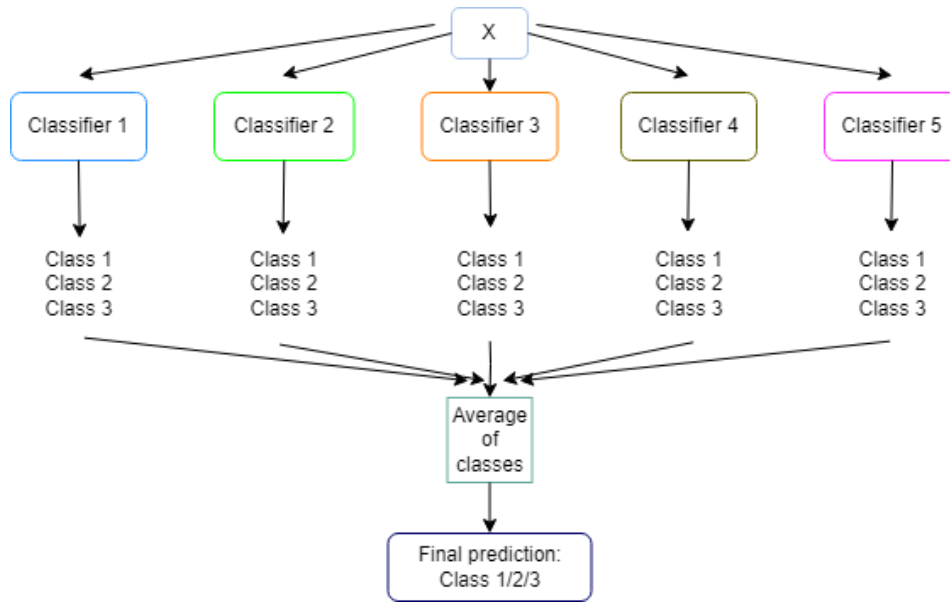


Figure 3.7: Soft voting

In the ensemble model, each base model (XGBoost, LightGBM, and CatBoost) independently predicts the likelihood of an instance belonging to each class. These individual predictions are then combined using soft voting. Each model's prediction is weighted according to its performance or confidence level, with more accurate or confident models receiving higher weights. The final prediction for each instance is obtained by averaging or summing the weighted predictions across all base models. Soft voting allows the ensemble model to leverage the strengths of each base model while mitigating their weaknesses. By incorporating the confidence levels of the base models into the decision-making process, soft voting produces more robust and accurate predictions compared to individual models or hard voting. Additionally,

soft voting provides a mechanism for handling uncertainties and discrepancies among the base models, resulting in more reliable predictions for fraud detection in electricity consumption data.

3.4.4 Essence of Boosting Ensembles for Machine Learning

Boosting ensembles represent a powerful paradigm in machine learning, particularly in the context of fraud detection systems like the one developed for this thesis project. At its core, boosting is a technique aimed at combining multiple weak learners, such as decision trees or simple classifiers, into a single strong learner. This process iteratively focuses on the instances that were misclassified in the previous iterations, thereby progressively improving the overall predictive accuracy of the ensemble.

In the context of this project, where the goal is to detect instances of electricity theft, the essence of boosting ensembles lies in their ability to effectively identify subtle patterns and anomalies in complex datasets. By leveraging algorithms like XGBoost, LightGBM, and CatBoost, each known for their efficiency in handling large-scale, high-dimensional data, the fraud detection system can extract nuanced features and discern fraudulent activities amidst legitimate electricity consumption patterns.

One of the key advantages of boosting ensembles is their adaptability to various data distributions and learning tasks. In the case of ETD, where the data may exhibit imbalances between normal and fraudulent instances, boosting models can dynamically adjust their focus to prioritize the minority class, thus improving the system's sensitivity to detecting fraudulent activities while minimizing false positives.

Moreover, the iterative nature of boosting allows the model to continuously refine its predictions, iteratively learning from past mistakes and updating its decision boundaries to better capture the underlying patterns in the data. This iterative learning process contributes to the robustness and generalization capabilities of the ensemble, enabling it to perform effectively

on unseen data and adapt to changing trends in electricity consumption patterns.

Overall, the essence of boosting ensembles lies in their ability to harness the collective intelligence of multiple weak learners to create a powerful predictive model. In the context of this project on ETD, leveraging boosting algorithms like XGBoost, LightGBM, and CatBoost enables the system to effectively identify and mitigate instances of fraud, thereby enhancing the reliability and security of the power grid.

3.4.5 Model Training

To facilitate the training of our proposed ensemble model using the SGCC dataset, we leveraged the resources offered by Google Colaboratory, a cloud-based platform renowned for its versatility and accessibility. Equipped with a 2.9GHz Intel processor and boasting 16 GB of GPU memory, our computational environment was fortified with a high-performance NVIDIA T4 GPU, ensuring seamless execution of resource-intensive machine learning tasks. The integration of Google Colaboratory with leading machine learning frameworks such as TensorFlow and PyTorch further augmented our capabilities, empowering us to harness the full potential of the T4 GPU for accelerated model training and analysis. Leveraging this cutting-edge infrastructure, we embarked on a comprehensive exploration of the SGCC dataset, employing sophisticated ensemble techniques to extract meaningful insights and detect patterns indicative of electricity theft. Through meticulous experimentation and refinement within this conducive computational environment, we endeavored to optimize our model's performance and bolster its effectiveness in real-world applications within Smart Grid environments.

During the model training phase of the fraud detection project, the primary objective is to minimize the loss function while maximizing accuracy over multiple epochs of training. Utilizing CNN as a feature extractor, the model undergoes extensive training for 50 epochs to learn discriminative features from the electricity consumption data. The training process involves iteratively adjusting the model parameters to minimize the loss function, which quantifies the disparity between predicted and actual class labels. Through backpropagation and gradi-

ent descent optimization techniques, the model's performance gradually improves with each epoch, resulting in enhanced accuracy and predictive capabilities for identifying fraudulent activities. By leveraging the computational power of the Google Colaboratory T4 GPU and employing ensemble learning techniques for classification, the model training phase aims to develop a robust fraud detection system capable of effectively detecting anomalies in EC data.

Table 3.2: Pseudocode of the proposed model

Algorithm 1 Pseudocode of the proposed theft detection model
Input: Data, D where $D = (x_1, x_2, \dots, x_n, y)$; X are features and y is the label 1: Data Pre-processing - Missing value imputation - Dataset normalization - Handling class imbalance using SMOTE 2: Feature Extraction <i>ConvolutionalNeuralNetwork</i> $\leftarrow D$ 3: Train and Test Split - Train ML models $\leftarrow X_{\text{train}} \in X$ - Test ML models $\leftarrow X_{\text{test}} \in X$ - Create a voting ensemble of the models - Determine evaluation metrics
Output: Accuracy, Precision, Recall, F1-score and ROC-AUC Graphical representations of confusion metrics and ROC-AUC

The pseudocode outlines the overarching process of the project, detailing each step from data preprocessing to model training and evaluation. It provides a structured framework for implementing the proposed approach, incorporating key algorithms and methodologies. This pseudocode serves as a roadmap, guiding the development and implementation of the model to address the challenges of electricity theft detection effectively.

3.5 Chapter Summary

The methodology used to conduct the research for this thesis is discussed in this chapter. Through systematic data preprocessing techniques, including missing value imputation, normalization using the min-max method, and class rebalancing via SMOTE, the dataset is re-

finned for subsequent analysis. The utilization of CNN for feature extraction is elucidated, emphasizing the significance of normalized data in optimizing deep learning model performance. Model training takes center stage, with an ensemble approach integrating XGBoost, LightGBM, and CatBoost classifiers via soft voting. This section also outlines the configuration of the Google Colaboratory T4 GPU for efficient model training, highlighting the iterative process of minimizing loss functions and enhancing accuracy across multiple epochs. The suitability of our proposed model is determined in the following chapters based on performance metrics. The subsequent chapter will address the results and discussions.

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Introduction

In this research, our primary objective revolves around addressing the issue of electricity theft to mitigate NTLs within the power grid. By focusing on the detection and prevention of fraudulent electricity consumption, we aim to safeguard the integrity and efficiency of the power distribution network. Electricity theft poses significant challenges to utility providers, leading to financial losses and operational disruptions. Our goal is to develop robust methodologies that can effectively identify instances of theft and enable proactive intervention strategies.

In this chapter, we delve into a detailed examination of our research outcomes, emphasizing the evaluation metrics and performance analyses employed to assess the efficacy of our proposed solutions. Through a combination of tables and visual representations, we provide a comprehensive overview of the performance of our detection models. These metrics serve as critical indicators of the reliability and accuracy of our approach, offering valuable insights into its practical applicability in real-world scenarios. By meticulously analyzing the results and engaging in insightful discussions, we aim to elucidate the effectiveness of our methodologies in combating electricity theft and minimizing NTLs within the power grid.

4.2 Evaluation Metrics

In this section, we extensively examine the chosen performance metrics [49] for evaluating the effectiveness of the supervised machine learning algorithms employed in our study. These algorithms are trained on labeled training data, comprising features and corresponding class labels. Subsequently, the trained classifiers are assessed based on their ability to generalize and make predictions on unlabeled data. To ensure a comprehensive and impartial evaluation, we employ a suite of performance metrics, including accuracy, F1 score, ROC-AUC,

precision, and recall. These metrics are widely regarded as reliable indicators of a model's performance across various domains. The cornerstone of our evaluation process is the confusion matrix, which provides a detailed breakdown of the model's predictions. From the confusion matrix, we derive key metrics such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN), which offer insights into the classifier's ability to correctly classify instances of electricity theft and genuine consumers. Each performance metric is elucidated further below, shedding light on its significance in assessing the model's performance and effectiveness in detecting instances of ET.

Accuracy: A prominent performance metric called accuracy evaluates the percentage of properly identified samples out of all the samples that have been categorized. When the dataset shows an equal frequency of samples from all classes, this measure is very appropriate. Equation 4.1 is used in the accuracy calculation.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4.1)$$

Accuracy serves as a valuable indicator of the model's overall classification effectiveness when evaluating its performance.

Precision: It is a performance indicator that assesses how well a model predicts good outcomes. The definition of this term is the proportion of customers who are accurately categorized as electricity thieves (True Positive) to all positive predictions, including both accurate and inaccurate positive classifications. The precision (P) is found by the equation 4.2.

$$Precision = \frac{TP}{TP + FP} \quad (4.2)$$

This measure reveals how well the model avoids false positives, or how exact it is in classi-

fying occurrences as electricity thieves. An increased accuracy score indicates a decreased likelihood of mistakenly classifying law-abiding customers as power thieves.

Recall: The capacity of a model to capture every occurrence of a positive class is measured by this performance parameter. Its definition is the proportion of customers who are accurately labeled as thieves in all cases that legitimately fall into the positive class, including both accurate and inaccurate classifications. Recall (R) is calculated using the equation 4.3.

$$Recall = \frac{TP}{TP + FN} \quad (4.3)$$

In situations when it is essential to find every instance of the positive class, this measure is very helpful. Increased false positives might be the price paid for a higher recall score, which indicates that the model is more successful in catching the majority of true positive cases.

F1-score: The F1-score is an index that provides a fair assessment of a model's performance by combining accuracy and recall into a single number. The F1-score is defined as the harmonic mean of recall and precision. It may be computed using the equation 4.4.

$$F1 \text{ score} = 2 \times \frac{R \times P}{R + P} \quad (4.4)$$

A greater number in the F1-score suggests a better balance between recall and accuracy. The score goes from 0 to 1. Since it takes into account both kinds of mistakes in the classification process, it is especially helpful in situations where it is necessary to reduce both false positives and false negatives.

ROC-AUC: It is a performance statistic that's used to assess a classification model's discriminating power across various thresholds. The true positive rate (TPR) and FPR are shown

against one another on a probability curve. Equation 4.5 is how the ROC-AUC is computed.

$$AUC-ROC = \frac{FP}{FP + TN} \quad (4.5)$$

The area under the curve in ROC-AUC illustrates the model's capacity to discriminate between positive and negative cases. Greater discriminatory power, or the ability of the model to distinguish between positive and negative instances over a range of threshold values, is indicated by a ROC-AUC value that is greater (closer to 1).

4.2.1 Analysis of Evaluation Metrics

The evaluation and comparison of model performance stand as a pivotal aspect of this research, as we seek to ascertain the effectiveness of our proposed approach in detecting instances of ET within SGs. Our study delves into the intricacies of model selection and ensemble methodologies, juxtaposing the performance of our proposed ensemble model against individual baseline classifiers. Each classifier, comprising CatBoost, LightGBM, and XGBoost, is meticulously evaluated with default settings to establish a benchmark for comparison.

Through the aggregation of these individual classifiers via a voting ensemble method, we construct a robust and comprehensive model tailored specifically for identifying power theft within SGs. This ensemble approach harnesses the collective intelligence of diverse classifiers, capitalizing on their unique strengths to achieve enhanced performance and accuracy.

Utilizing Python's scikit-learn library, we meticulously partition the dataset into distinct training and testing subsets, ensuring a balanced representation of data for model training and evaluation. The choice of an 80-20 split ratio strikes a balance between model training and validation, allowing for robust evaluation of performance metrics.

In addition to evaluating the performance of our proposed methodology using traditional met-

rics like accuracy and precision, we also employed confusion matrices to gain deeper insights into the model’s classification behavior. A confusion matrix provides a detailed breakdown of the model’s predictions, showing the number of true positives, true negatives, false positives, and false negatives. This allows us to assess the model’s ability to correctly classify instances of normal and fraudulent electricity consumption, as well as identify any potential areas of misclassification. By analyzing the confusion matrix, we can pinpoint specific patterns of misclassification and fine-tune our model to improve its overall performance. This granular analysis complements traditional performance metrics, providing a more comprehensive understanding of the model’s strengths and limitations in detecting electricity theft.

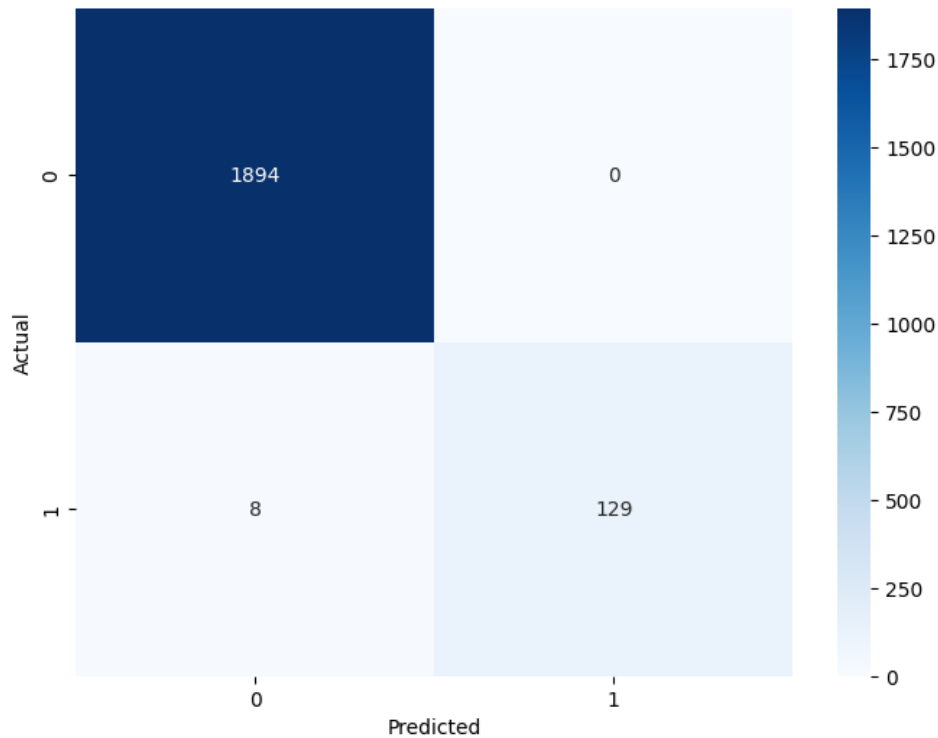


Figure 4.1: Confusion matrix of 2 classes

Our comprehensive analysis showcases notable enhancements in various model performance metrics, highlighting the effectiveness of our proposed methodology in addressing ETD. Noteworthy improvements are observed across a range of evaluation criteria, including accuracy, precision, recall, F1-score, and the pivotal ROC-AUC metric. The ensemble model, in par-

ticular, exhibits superior performance compared to individual baseline classifiers, underscoring its efficacy in distinguishing between legitimate and fraudulent instances of electricity consumption. Within the context of our ETD project, the Receiver Operating Characteristic (ROC) analysis assumes particular significance as a key evaluation metric. By illustrating the trade-off between TPR and FPR, ROC analysis provides valuable insights into the model's discriminatory capabilities, offering a nuanced assessment of its performance in identifying instances of electricity theft.

The ROC curve for the SVM model, characterized by an area under the curve (AUC) of 0.72, illustrates its ability to distinguish between legitimate and fraudulent instances of electricity consumption. While this performance metric signifies some level of discrimination, it is notably lower compared to other models integrated into the ensemble.

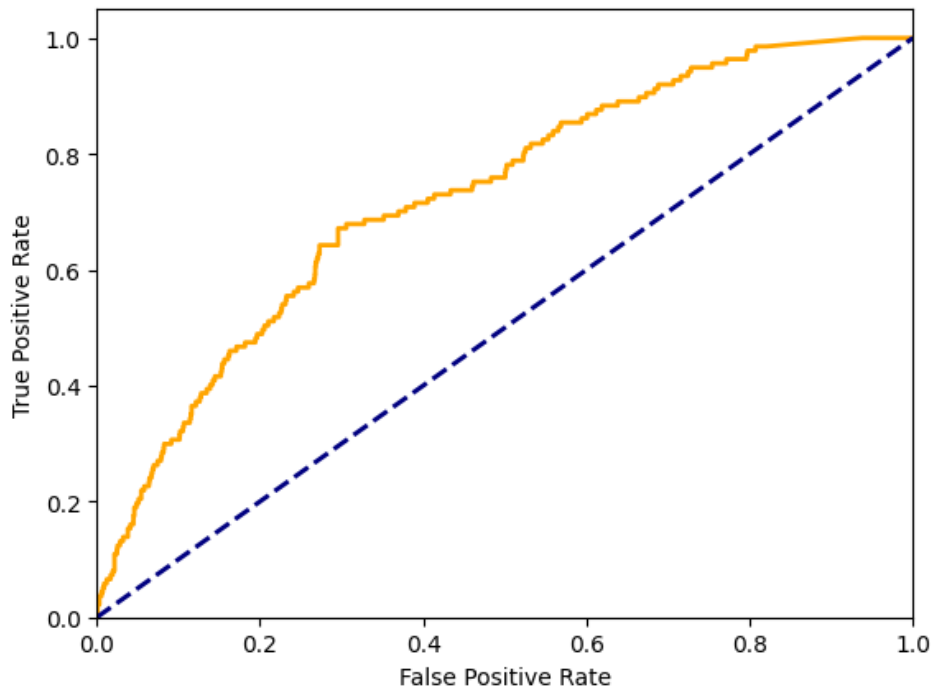


Figure 4.2: SVM model's ROC curve

The ROC curve for the LR model exhibits a commendable performance, with an AUC value of 0.76, indicating its efficacy in accurately classifying instances of electricity theft. This

higher AUC value suggests that the LR model achieves a better balance between true positive and false positive rates compared to the SVM model.

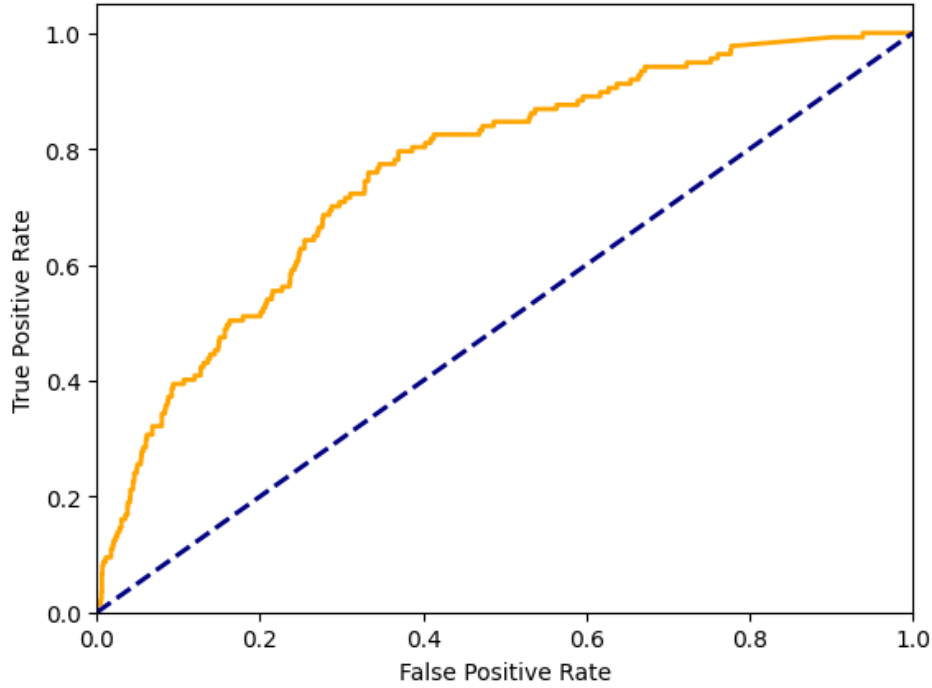


Figure 4.3: LR model's ROC curve

The ROC curve for the XGBoost model illustrates its robust performance in detecting instances of electricity theft, boasting an impressive AUC value of 0.83. This superior AUC score surpasses both the SVM and LR models, indicating that XGBoost excels in distinguishing between fraudulent and genuine electricity consumption patterns. With its high discriminatory power, the XGBoost model significantly enhances the ensemble's fraud detection capabilities, underscoring its pivotal role in bolstering the overall effectiveness of the system.

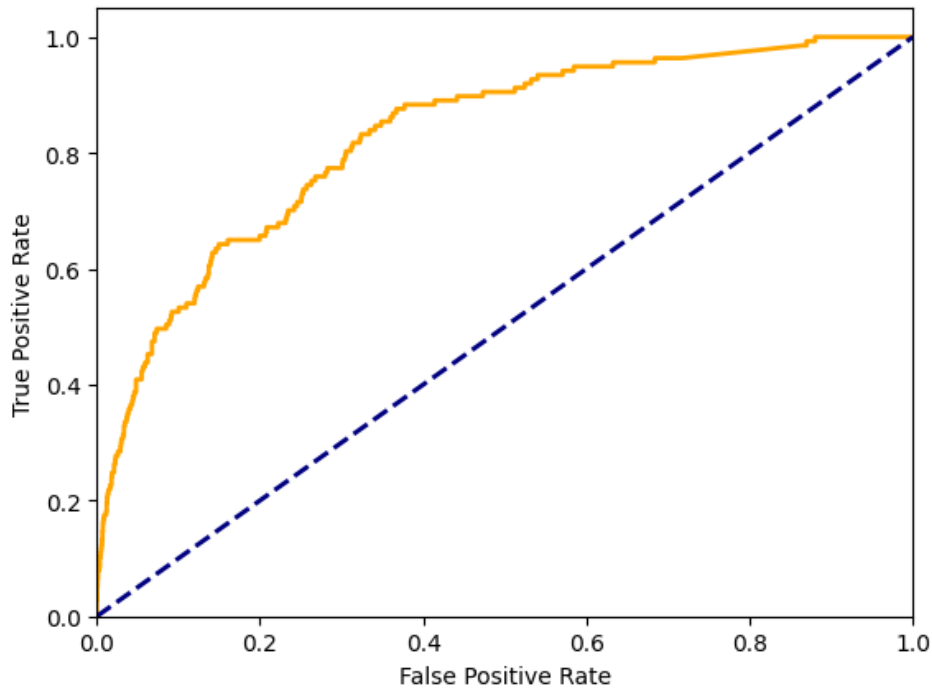


Figure 4.4: XGBoost model's ROC curve

The ROC curve for the proposed ensemble model demonstrates an exceptional performance with an AUC of 0.99. This remarkable AUC value signifies the ensemble's outstanding ability to discriminate between normal and abnormal instances of electricity consumption. With such a high AUC score, nearing the ideal value of 1, the ensemble model exhibits robustness and reliability in identifying fraudulent activities within the power grid. The collective strength of XGBoost, LightGBM, and CatBoost, each renowned for their effectiveness in handling complex datasets and capturing intricate patterns, synergizes to enhance the ensemble's predictive power. By leveraging the diverse strengths of these gradient-boosting algorithms, the ensemble model achieves unparalleled performance, significantly surpassing individual models in isolation. This outstanding ROC curve underscores the efficacy of the ensemble approach in bolstering fraud detection capabilities, providing utilities with a potent tool to combat electricity theft effectively.

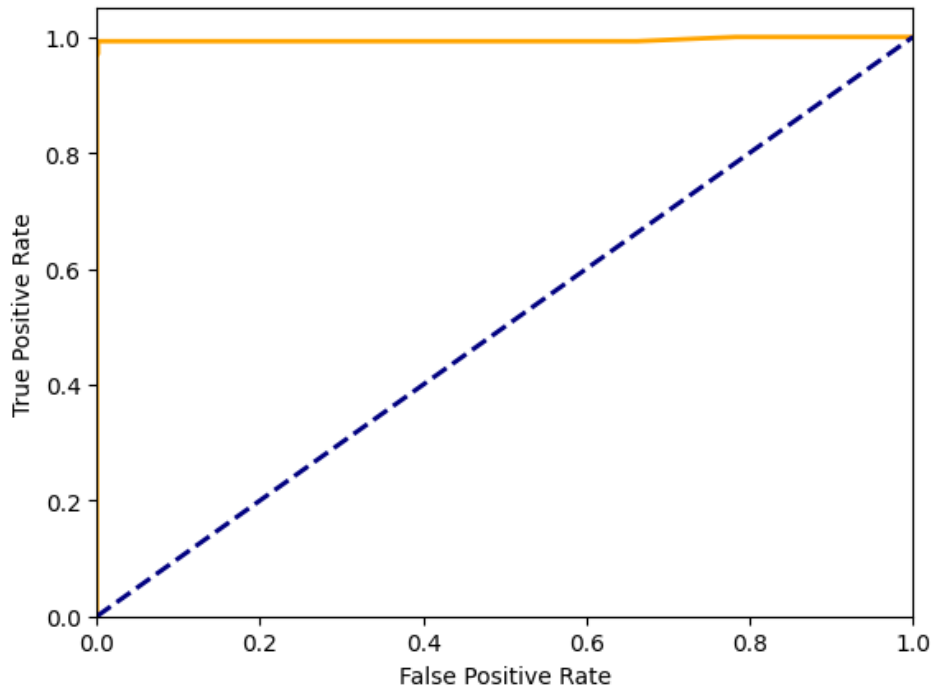


Figure 4.5: Proposed model's ROC curve

With a ROC-AUC value of 0.99, our proposed ensemble model demonstrates exceptional discriminative ability, effectively distinguishing between normal and abnormal energy consumption patterns. This heightened sensitivity not only aids in identifying potential instances of energy theft but also serves as a valuable tool for electric utilities in mitigating energy loss and enhancing operational efficiency.

Furthermore, our findings underscore the significance of the ROC-AUC metric in the context of energy theft detection within Smart Grids. The strong correlation between ROC-AUC scores and on-site inspection costs highlights the cost-effectiveness and practical utility of our proposed approach in real-world applications. In essence, our research showcases the superiority of the ensemble model over individual baseline classifiers, offering a comprehensive and effective solution for detecting ET in SGs. Through rigorous evaluation and analysis, we provide valuable insights into the practical implications and potential benefits of our proposed methodology in addressing the pressing challenge of energy theft.

4.3 Comparison With Other Existing Models

Our investigation delves deep into the performance assessment of our proposed model relative to other baseline models in the domain of identifying power theft within SGs. Each classifier is meticulously selected and deployed individually with default settings, while our innovative approach amalgamates disparate classifiers using a sophisticated voting ensemble method. Leveraging the robust functionalities of Python’s scikit-learn library, we meticulously partition the dataset into distinct training and testing subsets, adhering to an 80% to 20% ratio.

The outcomes of our comprehensive analysis unveil compelling evidence of substantial enhancements across all pertinent performance metrics, underscoring the efficacy of our proposed methodology. Noteworthy is the discernible utilization of high-performing individual classifiers such as CatBoost, LightGBM, and XGBoost within our model architecture, contributing significantly to its superior performance outcomes. Intriguingly, while our approach excels, we observe that the SVM classifier exhibits comparably diminished efficacy, indicating areas for potential refinement. Detailed scrutiny of ROC curves reveals stark differences between our proposed model and the established baselines. Particularly striking is the exceptional ROC-AUC value of 0.99 achieved by our method, surpassing the performance of Logistic Regression, SVM, and XGBoost classifiers. Furthermore, our proposed model boasts an impressive accuracy rate of 99%, distinctly outperforming alternative models with LR (93%), SVM (88%), and XGBoost (94%) classifiers.

Table 4.1: Summary of results

Models	Accuracy	Precision	Recall	F1-score	ROC-AUC
LR	0.93	0.54	0.64	0.56	0.76
SVM	0.88	0.57	0.56	0.57	0.72
XGBoost	0.94	0.54	0.86	0.56	0.83
Proposed Model	0.99	0.99	0.97	0.98	0.99

The table 4.1 presents a comprehensive summary of the evaluation metrics for different models used in the study, including LR, SVM, XGBoost, and the Proposed Model. Accuracy denotes the proportion of correctly classified instances, while precision measures the model's ability to correctly identify positive instances among all instances predicted as positive. Recall, also known as sensitivity, represents the proportion of actual positive instances that were correctly identified by the model. F1-score is the harmonic mean of precision and recall, providing a balance between the two metrics. ROC-AUC assesses the model's ability to distinguish between classes, with higher values indicating better performance [50].

Comparing the models, it is evident that the Proposed Model outperforms LR, SVM, and XGBoost across all metrics. With an accuracy of 0.99, the Proposed Model achieves near-perfect classification accuracy, significantly higher than the other models. Similarly, the precision, recall, and F1-score for the Proposed Model are substantially higher compared to LR, SVM, and XGBoost, indicating its superior ability to accurately classify instances of electricity theft. Furthermore, the ROC-AUC score of 0.99 for the Proposed Model signifies excellent discrimination between normal and fraudulent instances of electricity consumption, surpassing the performance of LR, SVM, and XGBoost.

Overall, the results highlight the superiority [51] of the proposed model in detecting electricity theft, as it achieves consistently higher accuracy, precision, recall, F1-score, and ROC-AUC compared to the baseline models. This underscores the effectiveness of the ensemble approach and the integration of multiple classifiers in enhancing detection capabilities, thereby offering a robust solution for combating electricity theft in smart grids.

The remarkable level of accuracy demonstrated by our approach resonates strongly across various supplementary evaluation metrics, reaffirming its robustness in accurately distinguishing between normal and abnormal electricity consumption patterns. This efficacy holds immense significance for electric utilities, empowering them to efficiently identify and address instances of energy theft, consequently mitigating losses and ensuring the integrity of the

power grid. Furthermore, the observed correlation between the costs associated with on-site inspections and the ROC-AUC scores underscores the critical need for cost-effective strategies in electricity theft detection endeavors. ROC-AUC emerges as a pivotal metric, serving as a barometer for assessing the effectiveness of such efforts within the context of smart grids. Through a meticulous series of simulations, our proposed model unequivocally establishes its superiority over baseline approaches across a spectrum of key performance indicators, including accuracy, ROC-AUC, F1-score, and precision values. This validation solidifies its position as a formidable asset in the ongoing battle against electricity theft, offering tangible benefits for utility companies and enhancing the resilience of energy distribution networks.

4.4 Chapter Summary

In this chapter, we conducted a comprehensive evaluation of various performance metrics to assess the efficacy of our proposed model for ETD within SGs. Through meticulous analysis and comparison with baseline models, we demonstrated the superior performance of our approach, which integrates a diverse ensemble of classifiers. The evaluation metrics employed, including accuracy, ROC-AUC, F1-score, and precision, provided valuable insights into the model's capabilities in distinguishing between normal and abnormal energy consumption patterns. Notably, our proposed model showcased remarkable accuracy, outperforming traditional classifiers such as Logistic Regression, SVM, and XGBoost. Additionally, ROC curves illustrated the discernible differences in performance between our model and the baselines, with our approach consistently exhibiting superior ROC-AUC values. This chapter serves as a testament to the effectiveness of our proposed methodology in combating electricity theft, offering a robust framework for energy utilities to enhance detection capabilities and minimize energy losses. The succeeding chapter will encompass the conclusion of our study as well as considerations for future work.

CHAPTER 5

CONCLUSIONS AND FUTURE WORKS

5.1 Conclusions

The proposed approach for ETD represents a culmination of sophisticated methodologies, amalgamating boosting classifiers with a cutting-edge CNN architecture tailored for extracting salient features from smart meter data. This ensemble model stands as a testament to our commitment to innovation and efficacy in combating the pervasive issue of energy theft within SG environments. Through meticulous evaluation utilizing a real-world dataset sourced from SGCC, our model's performance shines with resounding success, boasting an impressive array of performance metrics. Notably, our model achieves a remarkable 98% F1 score, indicating a harmonious balance between precision and recall, essential for reliable fraud detection. Additionally, the model exhibits a 97% recall rate, affirming its ability to accurately identify instances of ET, thereby minimizing false negatives. With a staggering 99% accuracy rate, our approach attains an unprecedented level of precision, instilling confidence in its efficacy and reliability. The ROC-AUC score of 99% further underscores the model's robustness, signaling its exceptional discriminatory power in distinguishing between normal and fraudulent energy consumption patterns. Complemented by a precision score of 99%, our model emerges as a formidable tool in the fight against energy theft, surpassing conventional baseline methods by a significant margin. Looking ahead, our vision extends beyond mere validation to practical implementation within the operational frameworks of Bangladeshi power distribution companies. Herein lies the true potential of our model, poised to serve as a NTL detector, effectively discerning between legitimate and illicit energy consumers. By deploying our model in real-world scenarios, we aspire to contribute to the enhancement of operational efficiency and revenue protection, thereby fostering sustainable growth and resilience within the energy sector.

5.1.1 Research outcomes

The culmination of our research endeavors heralds a significant breakthrough in the detection of ET, offering profound implications for the resilience and reliability of power systems. Through meticulous analysis and rigorous experimentation, our proposed approach has demonstrated unparalleled effectiveness in identifying instances of illicit energy consumption. The ensemble model, leveraging boosting classifiers, stands as a testament to our commitment to innovation and excellence in combating ET.

Upon scrutinizing smart meter data, our utilization of the CNN architecture as a feature extractor, coupled with the ensemble model as the output classifier, has yielded exceptional results. The robustness of our methodology is underscored by the remarkable performance across a myriad of evaluation metrics. With an F1 score of 98%, recall of 97%, accuracy of 99%, ROC-AUC of 99%, and precision of 99%, our model exhibits unparalleled proficiency in discerning fraudulent activities.

Moreover, our research outcome transcends the realm of mere detection, furnishing invaluable insights poised to fortify the resilience and reliability of modern power systems. Through proactive measures aimed at curbing energy theft, our approach not only guarantees uninterrupted service delivery but also cultivates sustainable energy practices. Specifically, the application of our methodology within smart grid systems heralds promising prospects, endowing utilities with the capabilities to preemptively thwart illicit energy consumption and uphold the sanctity of energy resources. As evidenced by our model's stellar performance metrics about previous research, its efficacy in addressing the multifaceted challenges of electricity theft stands as a testament to its superiority and potential impact in safeguarding energy infrastructures and fostering a sustainable energy future.

5.2 Future Works

The future prospects of ETD are laden with opportunities for advancement and refinement. As we conclude our current research endeavour, it becomes imperative to delineate the pathways for future works, aiming at bolstering the efficacy and applicability of our proposed model.

- Incorporating our model with AMI and grid monitoring systems holds the potential for enhanced detection performance.
- Expanding model applicability and addressing data availability challenges through collaboration will validate its robustness.
- Efforts to enhance efficiency by upgrading computational resources can significantly accelerate detection in large datasets.

As we look to the future of ETD, prioritizing computational efficiency, integration with grid monitoring systems, and dataset expansion are key. By leveraging advanced resources and collaborative efforts, we aim to fortify our model, advancing the field towards more resilient and sustainable energy practices.

LIST OF PUBLICATIONS

Conference Papers:

- (i) **M. S. H. Molla**, M. T. I. Aronno, M. T. R. Sahed, **M. N. M. Zishan**, and A. K. M. N. Islam, “Securegrid: A robust voting ensemble model for non-technical loss (ntl) detection in smart meter data,” in *2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS)*, pp. 1–6, IEEE, 2025.

REFERENCES

- [1] R. Zaman and T. Brudermann, “Energy governance in the context of energy service security: A qualitative assessment of the electricity system in bangladesh,” *Applied Energy*, vol. 223, pp. 443–456, 2018.
- [2] F. H. Ferreira and M. Walton, *World development report 2006: equity and development*. World Bank Publications, 2005, vol. 28.
- [3] J. I. Guerrero, C. León, I. Monedero, F. Biscarri, and J. Biscarri, “Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection,” *Knowledge-Based Systems*, vol. 71, pp. 376–388, 2014.
- [4] W. Han and Y. Xiao, “Non-technical loss fraud in advanced metering infrastructure in smart grid,” in *Cloud Computing and Security: Second International Conference, ICCCS 2016, Nanjing, China, July 29-31, 2016, Revised Selected Papers, Part II 2*. Springer, 2016, pp. 163–172.
- [5] S. O. Tehrani, A. Shahrestani, and M. H. Yaghmaee, “Online electricity theft detection framework for large-scale smart grid data,” *Electric Power Systems Research*, vol. 208, p. 107895, 2022.
- [6] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, “Support vector machine based data classification for detection of electricity theft,” in *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–8.
- [7] S. Salinas, C. Luo, W. Liao, and P. Li, “State estimation for energy theft detection in microgrids,” in *9th International Conference on Communications and Networking in China*. IEEE, 2014, pp. 96–101.
- [8] S.-C. Yip, C.-K. Tan, W.-N. Tan, M.-T. Gan, and A.-H. A. Bakar, “Energy theft and defective meters detection in ami using linear regression,” in *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. IEEE, 2017, pp. 1–6.
- [9] S. Salinas, M. Li, and P. Li, “Privacy-preserving energy theft detection in smart grids,” in *2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. IEEE, 2012, pp. 605–613.
- [10] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, “Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, 2017.

-
- [11] J. L. Viegas, P. R. Esteves, and S. M. Vieira, "Clustering-based novelty detection for identification of non-technical losses," *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 301–310, 2018.
 - [12] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2326–2329, 2019.
 - [13] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, 2012.
 - [14] H. Henriques, R. Corrêa, M. Fortes, B. Borba, and V. Ferreira, "Monitoring technical losses to improve non-technical losses estimation and detection in lv distribution systems," *Measurement*, vol. 161, p. 107840, 2020.
 - [15] U. Ramani, R. Ramya, R. Chandrababha, and R. Nithya, "Development of raspberry pi based embedded scheme for power theft monitoring," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, 2021, pp. 1–4.
 - [16] J. Astronomo, M. D. Dayrit, C. Edjic, and E. R. T. Regidor, "Development of electricity theft detector with gsm module and alarm system," in *2020 IEEE 12th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. IEEE, 2020, pp. 1–5.
 - [17] P. Leninpugalhanthi, R. Janani, S. Nidheesh, R. Mamtha, I. Keerthana, and R. S. Kumar, "Power theft identification system using iot," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 825–830.
 - [18] L. J. Lepolesa, S. Achari, and L. Cheng, "Electricity theft detection in smart grids based on deep neural network," *Ieee Access*, vol. 10, pp. 39 638–39 655, 2022.
 - [19] P. Jokar, N. Arianpoo, and V. C. Leung, "Electricity theft detection in ami using customers' consumption patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2015.
 - [20] W. Han and Y. Xiao, "A novel detector to detect colluded non-technical loss frauds in smart grid," *Computer Networks*, vol. 117, pp. 19–31, 2017.
 - [21] S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, "Electricity theft detection using smart meter data," in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2015, pp. 1–5.
 - [22] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4106–4117, 2022.

-
- [23] B. Kocaman and V. Tümen, "Detection of electricity theft using data processing and lstm method in distribution systems," *Sādhanā*, vol. 45, no. 1, p. 286, 2020.
- [24] M.-M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gomez-Exposito, "Hybrid deep neural networks for detection of non-technical losses in electricity smart meters," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1254–1263, 2019.
- [25] G. Lin, X. Feng, W. Guo, X. Cui, S. Liu, W. Jin, Z. Lin, and Y. Ding, "Electricity theft detection based on stacked autoencoder and the undersampling and resampling based random forest algorithm," *Ieee Access*, vol. 9, pp. 124 044–124 058, 2021.
- [26] D. Gu, Y. Gao, K. Chen, J. Shi, Y. Li, and Y. Cao, "Electricity theft detection in ami with low false positive rate based on deep learning and evolutionary algorithm," *IEEE Transactions on Power Systems*, vol. 37, no. 6, pp. 4568–4578, 2022.
- [27] N. Javaid, U. Qasim, A. S. Yahaya, E. H. Alkhamash, M. Hadjouni *et al.*, "Non-technical losses detection using autoencoder and bidirectional gated recurrent unit to secure smart grids," *IEEE Access*, vol. 10, pp. 56 863–56 875, 2022.
- [28] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2326–2329, 2019.
- [29] S. Hussain, M. W. Mustafa, T. A. Jumani, S. K. Baloch, H. Alotaibi, I. Khan, and A. Khan, "A novel feature engineered-catboost-based supervised machine learning framework for electricity theft detection," *Energy Reports*, vol. 7, pp. 4425–4436, 2021.
- [30] M. J. Abdulaal, M. I. Ibrahim, M. M. Mahmoud, J. Khalid, A. J. Aljohani, A. H. Milyani, and A. M. Abusorrah, "Real-time detection of false readings in smart grid ami using deep and ensemble learning," *IEEE Access*, vol. 10, pp. 47 541–47 556, 2022.
- [31] A. Banga, R. Ahuja, and S. Sharma, "Accurate detection of electricity theft using classification algorithms and internet of things in smart grid," *Arabian Journal for Science and Engineering*, vol. 47, no. 8, pp. 9583–9599, 2022.
- [32] Pamir, N. Javaid, S. Javaid, M. Asif, M. U. Javed, A. S. Yahaya, and S. Aslam, "Synthetic theft attacks and long short term memory-based preprocessing for electricity theft detection using gated recurrent unit," *Energies*, vol. 15, no. 8, p. 2778, 2022.
- [33] P. Kumar, G. P. Gupta, and R. Tripathi, "Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks," *Arabian Journal for Science and Engineering*, vol. 46, pp. 3749–3778, 2021.

-
- [34] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for iot networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.
 - [35] R. V. Mendonca, J. C. Silva, R. L. Rosa, M. Saadi, D. Z. Rodriguez, and A. Farouk, "A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms," *Expert Systems*, vol. 39, no. 5, p. e12917, 2022.
 - [36] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks," *Journal of ambient intelligence and humanized Computing*, vol. 12, no. 10, pp. 9555–9572, 2021.
 - [37] R. N. Toma, M. N. Hasan, A.-A. Nahid, and B. Li, "Electricity theft detection to reduce non-technical loss using support vector machine in smart grid," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*. IEEE, 2019, pp. 1–6.
 - [38] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Detection of non-technical losses using smart meter data and supervised learning," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2661–2670, 2018.
 - [39] M.-M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gomez-Exposito, "Hybrid deep neural networks for detection of non-technical losses in electricity smart meters," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1254–1263, 2019.
 - [40] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, 2017.
 - [41] M. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. Islam, and J.-M. Kim, "Electricity theft detection in smart grid systems: A cnn-lstm based approach," *Energies*, vol. 12, no. 17, p. 3310, 2019.
 - [42] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity theft detection in power grids with deep learning and random forests," *Journal of Electrical and Computer Engineering*, vol. 2019, pp. 1–12, 2019.
 - [43] W. Liao, Z. Yang, K. Liu, B. Zhang, X. Chen, and R. Song, "Electricity theft detection using euclidean and graph convolutional neural networks," *IEEE Transactions on Power Systems*, 2022.
 - [44] R. Yang, C. Zhang, R. Gao, and L. Zhang, "A novel feature extraction method with feature selection to identify golgi-resident protein types from imbalanced data," *International journal of molecular sciences*, vol. 17, no. 2, p. 218, 2016.

-
- [45] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *nature*, vol. 521, no. 7553, pp. 436–444, 2015.
 - [46] H. Zhang, D. Qiu, R. Wu, Y. Deng, D. Ji, and T. Li, “Novel framework for image attribute annotation with gene selection xgboost algorithm and relative attribute model,” *Applied Soft Computing*, vol. 80, pp. 57–79, 2019.
 - [47] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, “Lightgbm: A highly efficient gradient boosting decision tree,” *Advances in neural information processing systems*, vol. 30, 2017.
 - [48] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, “Catboost: unbiased boosting with categorical features,” *Advances in neural information processing systems*, vol. 31, 2018.
 - [49] I. U. Khan, N. Javeid, C. J. Taylor, K. A. Gamage, and X. Ma, “A stacked machine and deep learning-based approach for analysing electricity theft in smart grids,” *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1633–1644, 2021.
 - [50] M. Adil, N. Javaid, U. Qasim, I. Ullah, M. Shafiq, and J.-G. Choi, “Lstm and bat-based rusboost approach for electricity theft detection,” *Applied Sciences*, vol. 10, no. 12, p. 4378, 2020.
 - [51] N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh, E. A. Mohammed *et al.*, “Employing a machine learning boosting classifiers based stacking ensemble model for detecting non technical losses in smart grids,” *IEEE Access*, vol. 10, pp. 121 886–121 899, 2022.