


## Research Article

# Using Hybrid Convolutional Neural Network and Random Forest (CNN-RF) Algorithms to Address Non-Technical Losses in Power Distribution Systems

Babawale Bunmi Folajinmi<sup>1\*</sup> , Emmanuel Majiyebo Eronu<sup>2</sup> , Seyi Josiah Fanifosi<sup>3</sup> 

<sup>1,2</sup>Electrical and Electronics/Faculty of Engineering, University of Abuja, Abuja, Nigeria

<sup>3</sup>Electrical and Computer/School of Engineering, New Mexico State University, New Mexico, USA

\*Corresponding Author: 

Received: 24/Dec/2024; Accepted: 10/Feb/2025; Published: 31/Mar/2025



Copyright © 2025 by author(s). This is an Open Access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited & its authors credited.

**Abstract**— The electricity distribution sector experiences substantial financial losses due to non-technical losses (NTLs) including electricity theft, faulty meters, and commercial losses. This research introduces a combined Convolutional Neural Network and Random Forest (CNN-RF) approach to detect NTLs using metered customer electricity consumption data from the Abuja Electricity Distribution Company. The dataset, covering February 1, 2021, to January 31, 2022, was cleaned, preprocessed, and used to train the model. The CNN part uses a multi-layer design with convolutional layers for automatic feature extraction, followed by dropout layers to mitigate overfitting. Early stopping mechanisms were introduced to optimize training efficiency and prevent model degradation. The RF component was trained on the automatically extracted features by the CNN component and classifies consumers into "energy loss" and "no energy loss" categories. The GridSearchCV algorithm facilitated the RF's hyperparameters fine-tuning to achieve optimal configurations. The proposed model demonstrated a classification accuracy of 97% with a low false positive rate, thereby surpassing the effectiveness of manual inspections in detecting NTLs. This model can enhance the inspection hit rate and serve as an effective tool for detecting NTL activities in the electricity distribution sector.

**Keywords**—Non-Technical Loss Detection, Random Forest, Machine Learning, Deep Learning, Energy Consumption, Convolution Neural Network

## 1. Introduction

The energy sector, particularly the power distribution sector, has been plagued with the problem of NTL, which includes electricity lost due to theft, faulty meters, commercial losses and collection losses. Eighty percent of global energy theft occurs through direct tapping from power lines, making it one of the most common methods of non-technical losses (NTLs) in electricity distribution systems [1]. These losses manifest across the electricity supply chain, from generation to transmission and distribution. Losses are typically categorized into Technical Losses (TLs) and Non-Technical Losses (NTLs). TL results from internal processes within the electrical system, such as energy dissipation in transformers, power lines and other components used to transmit electricity [2]. Conversely, NTL stems from external factors, including electricity theft, inaccurate meter readings, unpaid bills and database management errors. Among NTL, electricity theft is a predominant concern, characterized by unauthorized energy

consumption [3]. This improper conduct often includes meter bypass, tampering with the meter reading, or meter tampering and illegal connection to electricity without paying for the energy consumed. Energy theft can lead to power surges, excessive loads on the electrical system, substantial financial losses for utility companies, and threats to public safety [4]. Overloading transformers and voltage imbalances caused by energy theft degrade power quality and reliability. Detecting electricity theft relies on labour-intensive routine inspections conducted by utility personnel to identify meter tampering, bypasses, and unauthorized connections. However, these methods are resource-intensive, costly, and often yield suboptimal results.

Several strategies have been proposed to address these challenges, including the implementation of smart meters, data analytics and machine learning algorithms. This study investigates the application of deep learning and machine learning techniques to detect and classify NTL cases within

power distribution networks. By utilizing these advanced methods, the research aims to improve the accuracy and efficiency of NTL detection, thereby minimizing financial losses and promoting a more reliable of the electricity supply system.

The paper is structured as follows: Section 1 provides an introduction to NTL. Section 2 examines previous research work on the NTL detection using deep learning and machine learning. Section 3 details the proposed methodology for NTL detection using CNN-RF algorithm. Section 4 outlines the results and discussion analysis. Section 5 discusses conclusions and future scope.

## 2. Related Work

Energy consumers rely on utilities to provide a continuous and reliable supply of electricity characterized by stable voltage, consistent magnitude, and regular frequency [5]. There is an increasing focus on understanding electricity consumption patterns among users in both residential and commercial sectors [6]. However, this expectation is frequently undermined by energy theft, which imposes substantial financial burdens on providers and disrupts power grids [7]. However, the previous techniques have often needed to be improved in effectively detecting instances of energy theft. For example, [4] developed a Deep CNN model utilizing smart meter data to address issues like inconsistent power usage and inefficient energy management. This model outperformed previous methods in accuracy and could automatically extract features, unlike traditional classifiers requiring manual input. However, the Model did not fully consider customer behaviour based on short-term electricity usage in identifying energy theft.

[8] developed a machine learning-based model for detecting Non-Technical Loss (NTL) using feature engineering on data obtained from an electricity distribution firm, considering challenges such as class imbalance, data quality and feature selection. Their approach included classifiers such as Logistic Regression, Support Vector Machine, Decision Tree, and Random Forest, achieving superior results in accuracy, precision, recall, F1 score, and AUC score. However, the limitation of the proposed model was obtaining realistic datasets from utility companies. Similarly, [9] proposed a Bidirectional Gated Recurrent Unit BiGRU-CNN artificial neural network for power theft detection, offering a model architecture conducive to decision-making in the energy sector. Python's keras module was used to program the Model. Several tests were conducted using data from a real electricity provider, confirming the proposed approach was effective. However, the author did not focus on extensively tuning neural network's hyperparameters or consider the temporal patterns in consumer behaviour within the BiGRU-CNN model.

To tackle issues like data imbalances, overfitting, and high-dimensional data, [10] combined Long Short-Term Memory (LSTM) with bat-based Random Under-Sampling Boosting (RUSBoost) methods to detect unusual patterns in electricity

consumption data. While their proposal exhibited strong performance, it remained sensitive to changes in input data and did not account for distinct datasets about residential and commercial buildings. [11] addressed similar challenges by introducing a Bidirectional Gated Recurrent Unit (BGRU) model for that utilized Synthetic Minority Oversampling Technique (SMOTE) and Tomek Link techniques for data balancing, along with Kernel Principal Component Analysis (KPCA) for feature extraction. While this model outperformed other methods, the authors did not explore alternative integration methods to improve its effectiveness.

Furthermore, [12] proposed a Wide and Deep CNN Model to detect electricity theft by analyzing two-dimensional electricity consumption data, which was effective for industrial applications like monitoring marijuana cultivation. The Model outperforms other methods like linear regression and random forest and could be used in industrial applications, such as indoor marijuana cultivation. However, the hybrid nature of the model resulted in longer execution times and issues with data imbalance. [13] developed an adaptive TSRNN architecture for electricity theft detection, which was optimized using Mahalanobis distance and achieved a high accuracy of 95.1%, with minimal false positives. The Model's suitability for large-scale online monitoring of power consumption remained limited.

In a different approach, [14] suggested a Support Vector Machine (SVM)-based approach for theft detection, achieving an accuracy of 81% but only 25% of cases can be accurately classified due to insufficient information on electrical thieves. [15] proposed a supervised machine learning model to identify electricity thieves and recover income losses for utility companies. It uses Adasyn to address class imbalance and uses VGG-16 for balanced data analysis. The model utilized Firefly Algorithm-based Extreme Gradient Boosting (FA-XGBoost) method for classification. While effective for analyzing large datasets, its performance diminished with increased data size. The authors [16] suggest using deep learning instead of artificial intelligence to extract features from large smart meter data for measuring electricity consumption. The method uses one-dimensional sample data and a semi-supervised deep learning model to prevent overfitting. While it outperforms cutting-edge techniques, it is less effective when applied to potential public datasets.

In [17] introduced RUSBoost Manta-Ray Foraging Optimization (rus-MRFO) and RUSBoost Bird Swarm Algorithm models within a CNN framework to detect energy theft, achieving accuracy rates of 91.5% and 93.5% respectively. However, these models lacked a unified real-time environment for electricity theft detection system. Meanwhile, [18] proposed a hybrid deep neural network model combining a CNN-particle swarm optimization with a gated recurrent unit, for effective electricity theft detection. This method, which uses real-time data from China's State Grid Corporation, classifies consumers as either honest or fraudulent. Nevertheless, the approach faces limitation such as extended execution time, overfitting issues and challenges in dealing with electricity thieves in complex real-world

scenarios. A novel XGBoost-based model is proposed by [19] for detecting electricity theft by examining customer electricity use trends. The Model employs six synthetic theft attacks, outperforming existing benchmarks. It achieves a 96% detection rate and 3% false positive rate but faces data privacy issues. [20] introduced a hybrid CNN-RF model which uses convolution and downsampling methods to extract features from smart energy meter consumption datasets. The Model then uses a random forest to detect theft. Experiments show the model outperforms other methods but consumers' privacy concerns remain and with additional synthetic data generated to represent malicious customers this use of synthetic data may not fully represents complexities inherent in authentic real-world scenarios.

### 3. Experimental Method

This section outlines the methodology adopted by this paper, which utilizes a hybrid CNN-RF model designed to detect cases of NTL within power distribution systems and classify them as either energy loss or no energy loss incidents. Illustrated in Figure 1, the framework for the NTL detection method provides a visual representation of the methodological approach. Below, we delve into the various components of the NTL detection framework.

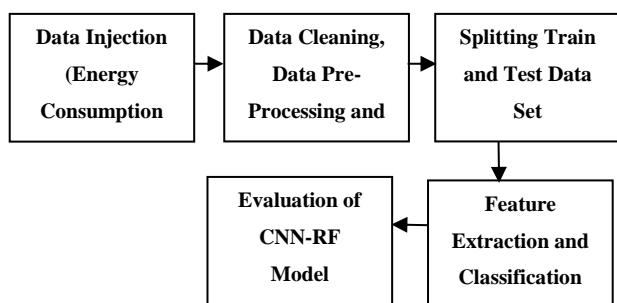


Figure 1. Framework of Non-Technical Loss Detection Method

#### 3.1 Data Injection (Energy Consumption Dataset)

The dataset used in this study comprises monthly energy consumption records of metered customers (residential, commercial, industrial and special) obtained from a power distribution company, Abuja Electricity Distribution Company (AEDC). The dataset spans from February 1, 2021, to January 31, 2022, and includes 653,534 customers with 52 features. A key feature is the "violation" column, which indicates meter conditions based on field inspections. The "violation" column classifies customers into two categories: No energy loss (labeled as "meter okay"). Energy loss (labeled as "meter bypass," "faulty meter," "burnt meter," "tampered meter," and "obsolete meter"). This classification helps identify fraudulent behaviour among consumers.

#### 3.2 Data Cleaning, Data Preprocessing and Analysis

The dataset was cleaned and preprocessed to ensure data quality and suitability for analysis. The rows with missing values in the "violation" column were removed, reducing the dataset to 43,322 customers. Missing values for energy consumption and vending information were replaced with

zeros. The ineffective columns were dropped, retaining 34 relevant features. New features were created, including total annual energy consumption, total annual vending, weekday, and season (rainy or dry). The "violation" column was label encoded: "0" for no energy loss and "1" for energy loss. Categorical variables such as month, weekday, meter make, tariff bands, tariff class, and phase were encoded. The dataset was normalized to ensure consistency and improve model performance.

After preprocessing, the dataset contained 43,322 rows and 34 columns, with 15,729 instances of energy loss and 27,593 cases of no energy loss. This represents a class imbalance, with 63.7% of instances being no energy loss and 36.3% being energy loss. The analysis of the energy consumption dataset is presented in Table 1, showing records of violations committed by customers, as identified during field inspections conducted by AEDC staff.

Table 1. Types of Violation recorded in the datasets

Violation	Frequency
Meter Okay	27593
Meter Bypass	6899
Energy Recovery	4084
Faulty Meter	2513
Tampered Meter	1773
Obsolete Meter	344
Burnt Meter/Faulty Meter	77
Blank/Faulty Meter	26
Abandoned Meter	13

In the Table 1, the terms 'Meter Okay' within the dataset signify instances of no recorded energy loss. In contrast, the categories 'Meter Bypass,' 'Energy Recovery,' 'Faulty Meter,' 'Tampered Meter,' 'Obsolete Meter,' 'Burnt Meter/Faulty Meter,' 'Blank/Faulty Meter,' and 'Abandoned Meter' are classified as energy loss or Non-Technical Loss (NTL). The dataset has cases of honest metered customers, which is 'Meter Okay', accounting for 27,593 times, and the total number of energy loss cases amounts to 15,729, with 'Meter Bypass' being the most prevalent, accounting for 6,899 cases. The analysis of the dataset, as illustrated in Figure 2, presents the distribution of recorded violations across different weekdays. The y-axis represents the violation status, where "1" indicates instances of energy loss, while "0" signifies no energy loss. The x-axis represents the count of violations. Focusing on category "1", which highlights cases of energy loss, the data reveals a significant concentration of violations during weekdays. Notably, Wednesdays and Thursdays exhibit the highest spikes, suggesting that energy theft is more frequently detected on these days. This trend may be attributed to increased monitoring efforts or specific consumption patterns that make fraudulent activities more detectable on these days.

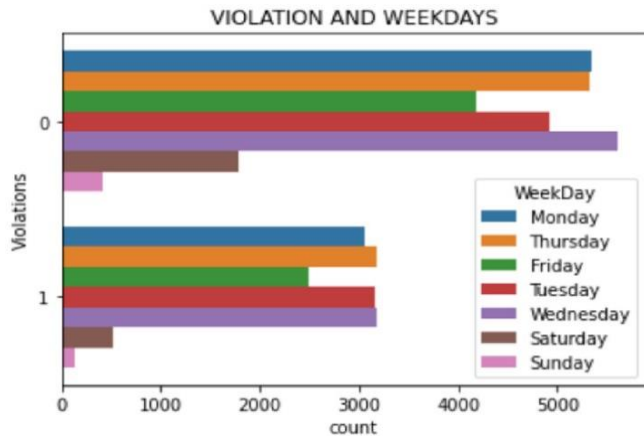


Figure 2. Violations during weekdays

Similarly, as illustrated in Figure 3, the distribution of recorded violations across different months is presented. Focusing on category "1", which highlights cases of energy loss, the data reveals a significant concentration of violations in specific months. Notably, February and March exhibit the highest spikes, indicating that energy loss incidents were more frequently recorded during these periods. This trend may be attributed to seasonal variations in energy consumption, intensified inspection activities, or other operational factors that influence the detection of violations.

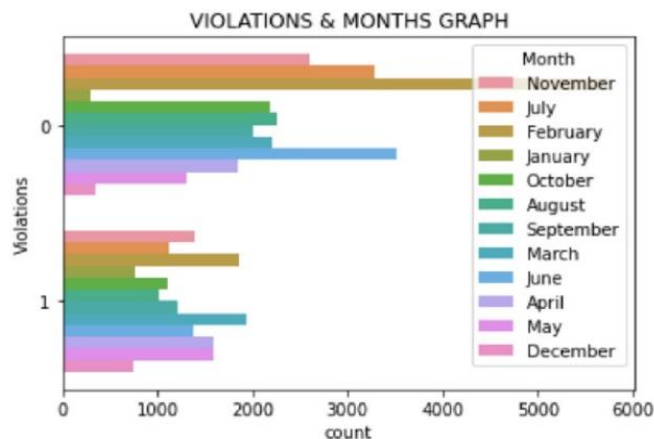


Figure 3. Violations during the month

### 3.3 Splitting Train and Test Dataset

The dataset shows a significant class imbalance, with 63.7% representing legitimate electricity consumers, far outweighing the 36.3% of theft instances. To address this imbalance is essential to avoid bias and enhance the model's capacity to accurately distinguish between the two categories. To achieve this, the Synthetic Minority Over-Sampling Technique (SMOTE) was used. This enhances the minority class, typically representing NTL cases, by creating synthetic samples based nearest neighbours. This technique was chosen because it prevents the model from overfitting to the majority class while ensuring the minority class is well represented. After balancing, the preprocessed dataset was divided into segments for effective training and evaluation of the CNN-RF model. A cross-validation method was used, splitting the datasets into 70% for training and 30% for testing. This split ensures that the model is trained on one portion of the data

and evaluated on another, unseen portion, minimizing the risk of overfitting.

### 3.4 Feature Extraction and Classification using CNN-RF Model

The hybrid CNN-RF model was developed in two main stages. First, the Convolutional Neural Network (CNN) model was constructed using the Sequential API in TensorFlow. The CNN architecture consisted of six convolutional layers, each employing 64 filters with a kernel size of 3, followed by the Rectified Linear Unit (ReLU) activation function. After the first convolutional layer, a max-pooling layer with a pool size of 2 was added to reduce the spatial dimensions of the data by taking the maximum value within a 2-unit window. This down-sampling step helped prioritize the most significant features and reduce computational complexity. To prevent overfitting, a dropout layer with a rate of 20% was incorporated, randomly deactivating neurons during training. After the convolutional layers, a flattening layer was used to convert the multi-dimensional data into a one-dimensional vector, which was then passed through two dense layers. The first dense layer contained 100 neurons with ReLU activation, while the final output layer consisted of a single neuron with a sigmoid activation function for binary classification. The model was compiled using the Adam optimizer with a learning rate of 0.001 and a binary cross-entropy loss function. The training was conducted for 100 epochs using a batch size of 32, and the model's performance was evaluated using validation data. Early stopping was implemented to monitor the validation loss during training, halting the process if no improvement was observed for five consecutive epochs, ensuring optimal performance without overfitting. This approach allowed the model to learn effectively while avoiding excessive training that could lead to overfitting. Table 2 shows the architecture of the CNN Model.

Table 2. The architecture of the CNN Model

Layer (Type)	Output Shape	Param#
Conv1d (Conv1D)	(None, 31, 64)	256
max_pooling1d (MaxPooling1D)	(None, 15, 64)	0
conv1d_1 (Conv1D)	(None, 13, 64)	12352
conv1d_2 (Conv1D)	(None, 13, 64)	12352
conv1d_3 (Conv1D)	(None, 13, 64)	12352
conv1d_4 (Conv1D)	(None, 7, 64)	12352
conv1d_5 (Conv1D)	(None, 5, 64)	12352
dropout (Dropout)	(None, 5, 64)	0
flatten (Flatten)	(None, 320)	0
dense (Dense)	(None, 100)	32100
dense_1 (Dense)	(None, 1)	101

In the second stage, features were extracted from the CNN's second-to-last layer, which served as input for the Random Forest (RF) classifier. The RF model was optimized using GridSearchCV to identify the best hyperparameters for the binary classification task. The optimal configuration included 50 trees (n\_estimators), a maximum depth of 9 (max\_depth), the square root of the total number of features for node splitting (max\_features), and a maximum of 9 leaf nodes per tree (max\_leaf\_nodes). The RF model was trained on the features extracted from the CNN, enabling it to classify

instances into energy loss and no energy loss categories effectively. This hybrid approach leverages the feature extraction capabilities of CNNs and the robust classification performance of Random Forests, making it well-suited for detecting Non-Technical Losses (NTLs) in power distribution systems.

#### 4. Results and Discussion

The model development and programming were done using Python 3.11 on a laptop computer system with the following specifications: Windows 10 Enterprise Operating System, Intel(R) Core (TM) i7-6500U CPU@2.50GHz 2.60 GHz processor and 8.00 GB RAM. The CNN architecture was implemented using TensorFlow, while the interface connecting the CNN and the RF was implemented using Scikit-learn. All code execution was performed on Jupyter notebook server version 7.0.1. This study addressed NTL detection as a binary classification problem, categorizing each customer as either "Energy loss" or "No Energy loss". To evaluate the performance of CNN-RF model, a real-world dataset comprising 12,997 customers' monthly energy consumption records for the duration of one year was used (February 1, 2021 - January 31, 2022). The model's performance was evaluated using five key metrics: accuracy, precision, recall, F1-score, and Receiver Operating Characteristics Area Under Curve (ROC-AUC). These metrics were derived from the confusion matrix, which provides detailed insights into the model's classification outcomes. The confusion matrix, derived from the test dataset of 12,997 metered customers, is shown in Figure 4. It provides a breakdown of the model's classification results.

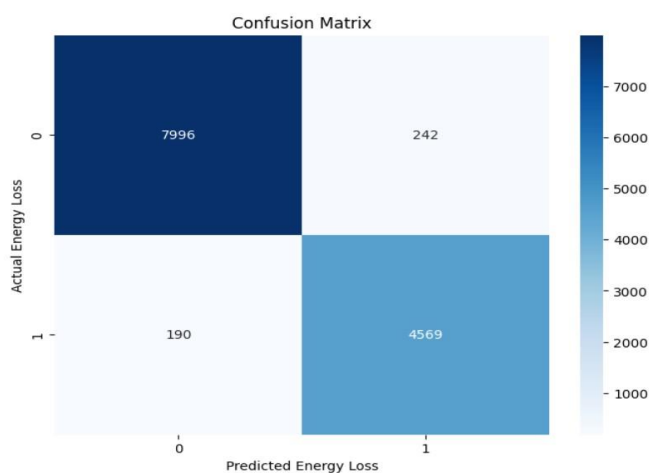


Figure 4. Confusion Matrix of the CNN-RF Model

The model correctly classified 7,996 cases as "No Energy Loss", indicating accurate identification of customers with no fraudulent activity. However, it incorrectly classified 242 instances as "Energy Loss" when they were actually "No Energy Loss". These are cases where the model flagged legitimate customers as potential fraudsters, which could lead to unnecessary investigations. Similarly, the model incorrectly classified 190 cases as "No Energy Loss" when they were actually "Energy Loss". These are instances where

the model failed to detect fraudulent activity, which could result in revenue loss for the utility company. On the other hand, the model correctly classified 4,569 instances as "Energy Loss", demonstrating its ability to accurately identify cases of energy theft or meter tampering. The confusion matrix highlights the model's strong ability to distinguish between "Energy Loss" and "No Energy Loss" cases, with a relatively low number of false positives and false negatives. This indicates that the model is both precise and reliable in detecting NTL.

The model's performance was evaluated using several key metrics. Accuracy, which measures the proportion of correctly classified instances (both "Energy Loss" and "No Energy Loss") out of the total number of instances, was 97%. This high accuracy indicates that the model correctly classified the vast majority of cases, demonstrating its overall effectiveness in NTL detection. Precision, which measures the proportion of correctly predicted "Energy Loss" cases out of all cases predicted as "Energy Loss", was 95%. This means that 95% of the flagged cases were actual instances of energy loss, while 5% were false alarms. This high precision reduces the risk of unnecessary investigations into legitimate customers. Recall, which measures the proportion of actual "Energy Loss" cases that were correctly identified by the model, was 96%. This indicates that the model successfully detected 96% of all energy loss cases, minimizing the risk of undetected fraud. The F1-score, which is the harmonic mean of precision and recall, was 96%. This balanced measure ensures that the model is both accurate and comprehensive in detecting NTL. Finally, the ROC-AUC value of 0.99 confirms the model's excellent ability to distinguish between "Energy Loss" and "No Energy Loss" cases. The ROC-AUC curve, shown in Figure 5, provides a graphical representation of the model's performance across different classification thresholds. The ROC curve plots the True Positive Rate (TPR), also known as recall or sensitivity, against the False Positive Rate (FPR) at various threshold settings. The TPR represents the proportion of actual "Energy Loss" cases correctly identified by the model, while the FPR represents the proportion of "No Energy Loss" cases incorrectly classified as "Energy Loss".

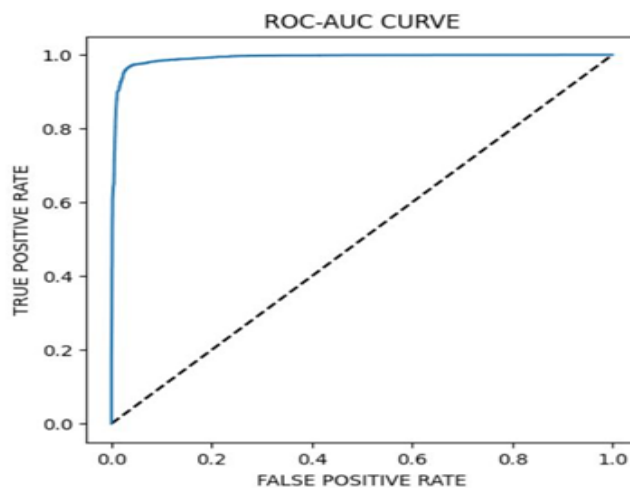


Figure 5. ROC-AUC Curve of the CNN-RF Model

The Area Under the Curve (AUC) quantifies the model's ability to distinguish between the two classes. An AUC value of 0.99, which is very close to the maximum value of 1, indicates that the model has an excellent ability to differentiate between "Energy Loss" and "No Energy Loss" cases. This means that the model can achieve a high true positive rate while maintaining a low false positive rate, making it highly effective for NTL detection. The steep rise of the ROC curve in Figure 5 further illustrates this, as the model quickly achieves a high TPR with minimal increase in FPR. This performance is particularly important in real-world applications, where minimizing false positives (incorrectly flagging legitimate customers) is crucial to avoid unnecessary investigations, while maximizing true positives (correctly identifying energy theft) is essential to reduce revenue losses. To validate the performance of the proposed CNN-RF model, its results were compared with several baseline machine learning models, including Random Forest, Stochastic Gradient Descent, Gaussian Naive Bayes, Decision Tree, and Logistic Regression. As illustrated in Figure 6, the ROC-AUC curves of these models were compared, revealing that the CNN-RF model consistently outperformed the baseline models. The ROC-AUC curve of the CNN-RF model is significantly closer to the top-left corner of the graph, indicating a higher TPR and lower FPR compared to the other models. This demonstrates the CNN-RF model's superior ability to distinguish between "Energy Loss" and "No Energy Loss" cases, as reflected by its AUC value of 0.99, which is higher than the AUC values of the baseline models.

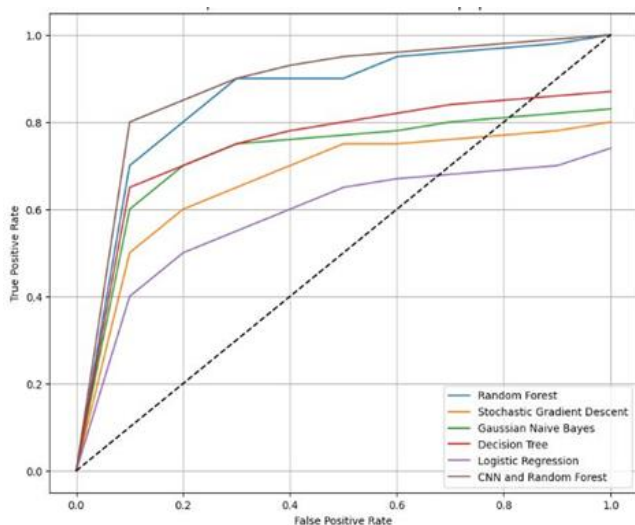


Figure 6. ROC-AUC based comparison of CNN-RF with ML Model

As illustrated in Figure 7, the CNN-RF model also outperformed these baseline models across all performance metrics (accuracy, precision, recall, and F1-score). Specifically, the CNN-RF model achieved higher accuracy (97%) compared to the baseline models, indicating its superior ability to correctly classify both "Energy Loss" and "No Energy Loss" cases. The higher precision (95%) of the CNN-RF model suggests that it produces fewer false positives compared to the baseline models, reducing the risk of incorrectly flagging legitimate customers. The higher recall (96%) indicates that the CNN-RF model is more effective at

detecting actual instances of energy loss, minimizing the risk of undetected fraud. The higher F1-score (96%) demonstrates that the CNN-RF model achieves a better balance between precision and recall compared to the baseline models. These results underscore the robustness and reliability of the CNN-RF model in detecting NTL, making it a superior choice for energy theft detection in power distribution systems.

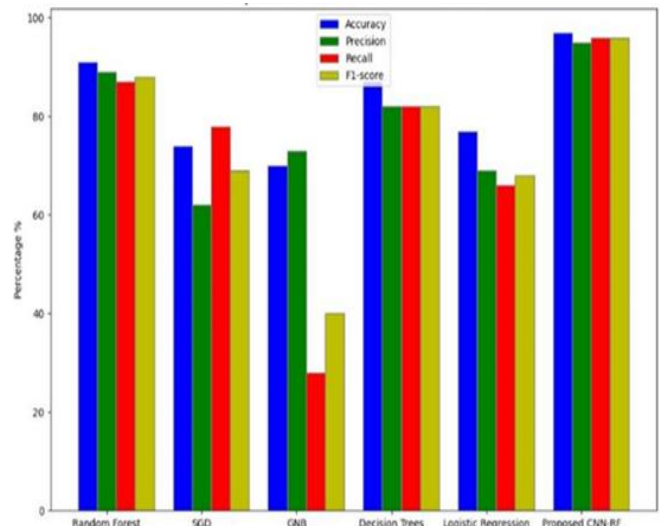


Figure 7. Performance comparison of CNN-RF with ML Model

The results demonstrate that the proposed CNN-RF model is highly effective in detecting Non-Technical Losses (NTL) in power distribution systems. The model's ability to achieve 97% accuracy, 95% precision, 96% recall, and an F1-score of 96% highlights its strong predictive capabilities. Additionally, the ROC-AUC value of 0.99 confirms the model's excellent ability to distinguish between "Energy Loss" and "No Energy Loss" cases. The low number of false positives (242) and false negatives (190) indicates that the model is both precise and reliable, minimizing the risk of unnecessary investigations and undetected fraud. The comparison with baseline models further validates the superiority of the CNN-RF model, as it consistently outperformed other machine learning techniques across all performance metrics.

These findings have significant implications for power distribution companies, as the CNN-RF model can help reduce revenue losses caused by energy theft and improve the overall efficiency of energy distribution systems. By accurately identifying instances of energy loss, the model enables utility companies to take targeted actions, such as conducting inspections or implementing preventive measures, to mitigate NTL.

## 5. Conclusion and Future Scope

This study introduced a hybrid model combining Convolutional Neural Network (CNN) and Random Forest (RF), referred to as the CNN-RF model, to detect Non-Technical Losses (NTLs) in electricity consumption patterns of customers. The original dataset, sourced from the Abuja Electricity Distribution Company (AEDC), contained inconsistencies and missing data. To address these

challenges, comprehensive data preprocessing techniques were applied, including normalization and the Synthetic Minority Over-Sampling Technique (SMOTE) to address class imbalances. The CNN component, with its layers of convolution and pooling, efficiently and automatically extracted features from metered customers' electricity consumption patterns, a process that traditionally requires significant manual input when using conventional classifiers. The CNN architecture also mitigated the risk of overfitting through the implementation of dropout layers and early stopping mechanisms, allowing the model to effectively learn from high-dimensional data while preventing degradation during training. The RF component, trained on the output of the CNN, classified the data into energy loss and non-energy loss categories.

Our results show that the CNN-RF model achieved an accuracy of 97% with a low false positive rate. Testing with real-world data confirmed that our model outperformed other approaches in terms of accuracy, precision, recall, and F1-score. The model's ROC-AUC value of 0.99 further demonstrated its excellent ability to distinguish between "Energy Loss" and "No Energy Loss" cases. These findings highlight the robustness and reliability of the CNN-RF model in detecting NTLs, making it a valuable tool for electricity distribution companies. While the CNN-RF model has demonstrated strong performance in detecting NTLs, there are several areas for future research to further enhance its effectiveness and applicability: The current model may exhibit bias when dealing with customers who have newly installed meters or those with less than a year of meter installation. Future research could focus on developing strategies to improve the model's performance for this specific customer category, such as incorporating additional data sources or using transfer learning techniques and also investigate the integration of the CNN-RF model with advanced metering infrastructure (AMI) and other smart grid components. This would enable more comprehensive monitoring and detection of NTLs across the entire power distribution network.

#### Data Availability

The data use in this research will be provided upon request.

#### Conflict of Interest

The authors confirm that they have no known financial conflicts of interest or personal affiliations that could have influenced the work presented in this paper.

#### Funding Source

This research was conducted without any financial support from any organization.

#### Authors' Contributions

Babawale Bunmi Folajinmi was responsible for data gathering, analysis, preprocessing, model development, and the research write-up. Seyi Josiah Fanifosi reviewed and proofread the manuscript, while Emmanuel Majiyebo Eronu provided supervision and guidance throughout the research.

#### Acknowledgements

We acknowledged God the giver of knowledge and his divine guidance in the course of this research work.

#### References

- [1] U. Soni and U. Kumari, "Prevention of Power Theft Using Concept of Multifunction Meter and PLC," *International Journal of Computer Sciences and Engineering* Open Access Survey Paper, Vol.6, Issue.12, pp.443-447, 2018.
- [2] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J. G. Choi, "Electricity theft detection using supervised learning techniques on smart meter data," *Sustain.*, Vol.12, No.19, pp.1-25, 2020.
- [3] O. Olaoluwa, "Electricity theft and power quality in Nigeria," *Int. J. Eng. Res.*, Vol.6, No.6, pp.1180-1184, 2017.
- [4] E. U. Haq, C. Pei, R. Zhang, H. Jianjun, and F. Ahmad, "Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach," *Energy Reports*, Vol.9, pp.634-643, 2023.
- [5] S. Fanifosi, S. Ike, E. Buraimoh, and I. E. Davidson, "33kV Distribution Feeder Line Sag and Swell Mitigation using Customized DVR," in *Proceedings of the 5th International Conference on Information Technology for Education and Development: Changing the Narratives Through Building a Secure Society with Disruptive Technologies*, ITED 2022, Institute of Electrical and Electronics Engineers Inc., 2022.
- [6] R. Din and P. B. Prabadevi, "Data Analyzing using Big Data (Hadoop) in Billing System," *International Journal of Computer Sciences and Engineering*, Vol.5, No.5, pp.84-88, 2017.
- [7] S. Abbas et al., "Improving Smart Grids Security: An Active Learning Approach for Smart Grid-Based Energy Theft Detection," *IEEE Access*, Vol.12, pp.1706-1717, 2024.
- [8] R. Yadav and Y. Kumar, "Detection of non-technical losses in electric distribution network by applying machine learning and feature engineering," *J. Eur. des Syst. Autom.*, Vol.54, No.3, pp.487-493, 2021.
- [9] L. D. Soares, A. de S. Queiroz, G. P. López, E. M. Carreño-Franco, J. M. López-Lezama, and N. Muñoz-Galeano, "BiGRU-CNN Neural Network Applied to Electric Energy Theft Detection," *Electron.* 2022, Vol.11, pp.693, 2022.
- [10] M. Adil, N. Javaid, U. Qasim, I. Ullah, M. Shafiq, and J. G. Choi, "LSTM and bat-based rusboost approach for electricity theft detection," *Appl. Sci.*, Vol.10, No.12, 2020.
- [11] H. Gul, N. Javaid, I. Ullah, A. M. Qamar, M. K. Afzal, and G. P. Joshi, "Detection of non-technical losses using SOSTLink and Bidirectional Gated Recurrent Unit to Secure Smart Meters," *Appl. Sci.*, Vol.10, No.9, 2020.
- [12] 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 Trans. Ind. Informatics*, Vol.14, No.4, pp.1606-1615, 2018.
- [13] G. Lin et al., "Electricity Theft Detection in Power Consumption Data Based on Adaptive Tuning Recurrent Neural Network," *Front. Energy Res.*, Vol.9, pp.673, 2021.
- [14] Petrlik, P. Lezama, C. Rodriguez, R. Inquilla, J. E. Reyna-González, and R. Esparza, "Electricity Theft Detection using Machine Learning," *Int. J. Adv. Comput. Sci. Appl.*, Vol.13, No.12, pp.420-425, 2022.
- [15] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J. G. Choi, "Electricity theft detection using supervised learning techniques on smart meter data," *Sustain.*, Vol.12, No.19, pp.1-25, 2020.
- [16] X. Lu, Y. Zhou, Z. Wang, Y. Yi, L. Feng, and F. Wang, "Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid," *Energies (Basel)*, Vol.12, No.18, 2019.

- [17] R. Akram et al., "Towards big data electricity theft detection based on improved rusboost classifiers in smart grid," *Energies* (Basel), Vol.14, No.23, 2021.
- [18] A. Ullah, N. Javaid, A. S. Yahaya, T. Sultana, F. A. Al-Zahrani, and F. Zaman, "A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters," *Wirel Commun Mob Comput*, Vol.2021, 2021.
- [19] I. Kawoosa, D. Prashar, M. Faheem, N. Jha, and A. A. Khan, "Using machine learning ensemble method for detection of energy theft in smart meters," *IET Generation, Transmission and Distribution*, 2023.
- [20] 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," *J. Electr. Comput. Eng.*, Vol.2019, 2019.

## AUTHORS PROFILE

**Babawale Bunmi Folajinmi** obtained a B.Eng. in Electrical and Electronics Engineering from the University of Agriculture, Makurdi, Benue, Nigeria, in 2010. He is a registered engineer specializing in electrical power and machine engineering, with over 12 years of experience in power distribution and expertise in energy auditing. He is a member of the Council for the Regulation of Engineering in Nigeria (COREN) and currently works as an energy auditor at an electricity distribution company in Nigeria. His research interests include Power System Optimization, Machine Learning, and Deep Learning.



**Emmanuel Majiyebo Eronu** earned his B.Eng. in Electrical & Computer Engineering and a Ph.D. in Computer Engineering from the Federal University of Technology, Minna, as well as an M.Sc. in Electrical and Electronic Engineering from the University of Lagos. He is a Senior Lecturer in the Department of Electrical/Electronic Engineering at the University of Abuja. He is an accomplished academic and an experienced lead software developer with expertise in embedded systems, the Internet of Things (IoT) with cybersecurity, and backend software development. His research focuses on embedded systems, IoT, wireless communication, and software engineering. He is a member of NSE, IEEE, and a registered engineer with COREN.



**Seyi Josiah Fanifosi** earned his B.Tech. in Electrical and Electronic Engineering from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2012 and an M.Eng. in Electrical and Electronic Engineering from the University of Benin, Nigeria, in 2019. He is currently pursuing a Ph.D. in Electrical and Computer Engineering at the Klipsch School of Electrical and Computer Engineering, New Mexico State University, USA. His research interests include power systems, machine learning, and renewable energy. He is a member of Nigerian Society of Engineers and a registered engineer with COREN.

