ISSN: 2278-4632
Vol-13, Issue-08, August 2023

IDENTIFICATION OF THEFT FROM SMART GRIDS IN THE ELECTRICITY INDUSTRY USING NEURAL NETWORKS

[#1]VISHWANALA MURALI KRISHNA, *Department of MCA*,
[#2]Dr.V.BAPUJI, Associate Professor& HOD,
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Electricity theft is a prevalent problem that harms both customers and utilities. It stifles the economic expansion of utility companies, generates electric risks, and contributes to consumers' excessive energy expenses. The development of smart grids is critical for detecting power theft since these systems create massive amounts of data, including client usage statistics, which may be utilized in machine learning and deep learning algorithms to detect power theft. This study proposes a method for detecting theft that employs deep neural networks to classify data using broad time and frequency domain properties. To address dataset problems such as missing data and class imbalance, we employ data interpolation and synthetic data synthesis approaches. We use principal component analysis to compare and contrast the influence of characteristics in both the time and frequency domains, then run experiments in combined and reduced feature space and confirm the most significant features using the minimum redundancy maximum relevance approach. By modifying hyperparameters with a Bayesian optimizer, we can improve the performance of power theft detection. Furthermore, we use an adaptive moment estimation optimizer to run tests with different critical parameter values to discover which settings produce the best accuracy. Finally, we compare our strategy's performance to that of other approaches tried on the same dataset. We achieved 91.8% accuracy, which was second on the benchmark, and 97% area under the curve (AUC), which was 1% higher than the best AUC in previous studies.

Keywords: Deep neural network, electricity theft, machine learning, minimum redundancy maximum relevance, principal component analysis, smart grids.

I. INTRODUCTION

Utility companies have a worldwide problem with people obtaining power without paying for it. Non-technical losses (NTLs) are estimated to cost businesses some $96 billion annually [1]. According to the World Bank, over half of the energy produced in Sub-Saharan Africa is stolen. Energy hackers typically aim to reduce or eliminate their reliance on utility companies by reducing their energy consumption costs [3, 4]. Utility companies lose a significant amount of money when their electricity is stolen. Money losses in 2015 for Russia were calculated at $5.1 billion, based on data from reference [5]. Likewise, India lost $16.2 billion and Brazil lost $10.5 billion.

According to Eskom, South Africa loses $1.31 billion (R20 billion) in revenue annually due to energy theft [2]. Energy theft is costly financially and poses a severe risk to the reliability of power grids [3]. There is a risk of electric shocks and other public safety issues due to electrical surges and overloaded systems [4]. The aforementioned cause directly contributes to the universal increase in energy costs observed recently [3]. The installation of a smart grid has multiple potential benefits in the fight against electricity theft [4]. Traditional energy networks, smart meters, sensors, computer functions for monitoring and regulating the grid, and many other components are typically interconnected via a communication network to form a smart grid. Smart information regarding energy use, grid health, power prices, and other related subjects can be collected with the use of meters and sensors [6].

Several utilities examined their meters' manufacturing and installation processes. They also conducted experiments to determine whether

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

or not anyone was stealing electricity from traditional power systems by going around the lines. The aforementioned methods are costly, inefficient, and cannot detect intrusion [4, 7]. Researchers in a recent study attempted to detect power theft by sorting machine learning-based techniques into categories and using publicly available data from smart meters. Thanks to the aforementioned theft-detection techniques, prices have dropped significantly [8]. However, current classification algorithms are insufficient because they focus solely on time-domain data while ignoring frequency-domain information.

There is still an issue with electrical theft, despite the fact that much research has been done and is being done to find effective solutions. The disparity between grid deployment in rich and developing nations is a major factor in this issue's persistence, as demonstrated by reference [9]. Inadequate network infrastructure and concerns about privacy make implementation of smart grid technology challenging [10]. According to reference [10], smart meters are being considered by both developed and developing nations as a solution to the problem of non-technical losses (NTLs). It is projected by [11] that the worldwide smart grid market will expand by a factor of two between 2017 and 2023. Improvements and widespread adoption of smart grids are most likely to occur in Asia, Europe, and North America. Using a classification system based on Deep Neural Networks (DNNs), this study demonstrates how to identify electricity theft by choosing and extracting the most pertinent data. Data on China's electricity consumption is available from the State Grid Corporation of China (SGCC) at the link [12]. From January 2014 to October 2016, the data collection covers energy use. The most noteworthy ones are as follows:

In this research, we present a novel approach to detecting energy theft by employing a classification-based method based on Deep Neural Networks (DNNs) and taking advantage of broad time-domain data. Our proposed approach is grounded in a careful analysis of current literature. To further boost productivity, we recommend utilizing frequency-domain characteristics.

Using Principal Component Analysis (PCA), we classify using a small number of features and compare the results to classification using all input characteristics in order to improve future training and make the results more accessible.

- Finding and verifying the most crucial qualities is done with the help of the mRMR methodology, which stands for Minimum Redundancy Maximal Relevance.
- Characterized by distinct features. This can be seen in the frequency-domain properties rather than the time-domain ones.

2. RELATED WORK

The academic community is very interested in researching methods for detecting power theft in intelligent networks. The objective is to find workable solutions to the problem of energy theft. The research done so far has revealed that there are primarily three types of detecting procedures. Methods that rely solely on hardware, methods that combine hardware and data, and data-driven approaches make up these categories.

Hardware-based approaches often include the installation of additional hardware components, such as microcontrollers, sensors, and circuits, onto existing power distribution lines [13-19]. Power theft, which can involve tampering with energy meters and transmission lines, is commonly detected using these techniques. They demonstrate a poor ability to identify and deal with danger. Electricity theft known as a "power cyber-attack" occurs when hackers gain access to electricity meters and alter consumption data [7].

An example of a redesigned power meter was shown in a previous paper [13]. Electrically Erasable Programmable Read-Only Memory (EEPROM), a Global System for Mobile Communications (GSM) module, and a Central Processing Unit (CPU) were all spotted. The simulation results demonstrated that the meter can still send an SMS message by deviating from its intended behavior even when a bad load is added. To detect power theft, physical changes must be made to energy meters and power lines. In order

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

to combat electricity theft, the authors of [16] employed hardware components like as the GSM module and the ARM-cortex M3 processor. There were four observed methods of committing this form of theft: evading detection by going around the phase line, tampering with the meter, severing the neutral line, and evading detection by going around the meter. A test sample was prepared for each of the four. Prospective results. The GSM module proved that it could reliably notify the user through SMS if a theft occurred.

Smart meters based on the ADE7953 chip were developed by the authors of [17], and they are extremely vulnerable to electrical and mechanical attacks. Overvoltage, voltage drop, overcurrent, and no load were all detected with the help of the ADE7953. An interrupt was anticipated and communicated to the Microcontroller Unit (MCU). In the event of theft-reportable manipulation, the GSM module will send out SMS warnings. Mechanical tampering could be prevented with the help of a tampering switch connected to the input/output (IO) terminals of the microcontroller unit (MCU). With this set up, signals can be transmitted to the MCU in the event of tampering. By swapping the meter's input and output terminals and connecting the phase line directly to the load, we were able to verify that our hypothesis held true. There was a one in twenty-one thousand chance that the discovery would be wrong.

A voltage divider circuit, microprocessor, and other components round up the circuit designed by the cited experts [15]. The device is designed to detect power theft by contrasting the direction of current flow on the main phase line and the neutral line. The wire was already up in front of the meter. In order to see if the concept would hold up, we employed both real hardware and the Proteus software. When the meter was tampered with, an alert popped up claiming the issue had been located. The circuit layout to catch electricity thieves who bypass meters is described in the provided chapter [14]. There were a lot of different components used, including transformers, rectifiers, a computer, and a GSM module. The GSM manager immediately notified the service provider of the tampered meter through SMS (Short Message Service). Using radio-frequency identification (RFID) tags on ammeters to keep track of precise and thorough information about each ammeter was proposed in a work cited as [18]. Due to their operation, ammeters necessitated constant monitoring and management. Investigation regarding the power outage had to be done personally. Damage to, loss of, or alteration of a tag significantly increases the likelihood of energy theft.

After carefully analyzing all of the expenses involved with deployment. A return on investment (ROI) of greater than one was discovered at a Chinese energy firm. In-depth instructions on using Arduino technology to create a gadget that can detect power theft in real time are provided here. The Arduino Uno microcontroller was utilized in this investigation alongside a GSM module for wireless communication, current sensors for quantifying electrical current, and an LCD display for displaying results. The Arduino Uno microcontroller received readings from two state-of-the-art sensors located on the secondary side of the transformer and the electric service cap. If there was a significant discrepancy between the readings from the present sensors, a GSM module would notify a service provider through text message. The technology in the prototype was able to detect theft in tests. The simulation was conducted with the help of Proteus 8 program. The aforementioned strategies aren't very effective in halting invasions because they're costly and call for the usage and maintenance of specialist equipment. The solutions discussed in sources [20]-[22] for detecting energy theft involve a hybrid of physical components and data-driven techniques, such as machine learning and deep learning, to identify and locate the source of the theft. Hardware constraints make it difficult to set up and maintain these solutions.

The authors [20] of the study developed a novel method for comparing smart meter data with other sources in order to estimate the total energy use of an entire neighborhood. Dishonest customers are probably in the area if there is a significant

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

discrepancy between smart meter and transformer readings. Experts looked for clients who acted dishonestly in the targeted area. The Support Vector Machine (SVM) was proposed as a potential basis for an appropriate algorithm. Five thousand dedicated clients were used as input to the algorithm. The highest detection rate was 95%, and the lowest was 94%.

False positive rates cannot exceed 11%. The method used to anticipate TLs was developed by the authors cited in [22]. The Non-Technical Losses (NTL) are calculated by deducting the overall losses in the distribution network from the Technical Losses (TL). To model how smart meters function, we assumed that distribution transformers and smart meters would report back to the energy provider every 30 minutes. Every 30 minutes for six days, 30 different purchasers needed data in this scenario. By manipulating the simulator, dishonest individuals were able to obtain power without paying for it. The stolen energy amounted to between 1 and 10 percent of annual use. The stolen energy has a high market value.

The source [21] advises placing a "watcher meter" on a pole far from homes if there is suspicion that one or more meters have been tampered with. The purpose of this setup is to monitor the combined energy consumption of n individual residences. It is recommended that cameras be strategically placed in close proximity to the observer meter to reduce the likelihood of tampering. A mathematical approach was developed to identify instances of smart meter fraud by combining data from actual and dummy meters. A mathematical approach was evaluated by applying it to a set of real-world data on consumer spending. Energy consumption was artificially inflated on several of the meters in the research. Finding meters with shifted usage patterns was a breeze with the approach taken. Numerous researchers are engaged in the aforementioned areas due to the strong demand and consequently high salaries in those sectors. Specifically, how to use empirical evidence to combat energy theft. Using a sequence of three techniques—Support Vector Machine (SVM), Kernel function (KF), Principal Component Analysis (PCA), and Synthetic Minority Over-sampling Technique (SMOTE)—the authors of the cited article [3] devised a system for identifying power theft incidents. Researchers created fictitious data points using the Synthetic Minority Over-sampling Technique (SMOTE) to address the issue of data imbalance. Data was also mined using a technique called kernel principal component analysis (KPCA). Finally, Support Vector Machines (SVM) were utilized to classify the data. The Area Under the Curve demonstrates that after the validation procedure, the experts have created the optimal classifier.

Ninety-one percent of the information fell under the area under the receiver operating characteristic curve (AUC).

To identify incidents of electricity theft, the authors of [4] employed robust and in-depth Convolutional Neural Networks (CNN) models. Since Wide noticed that data on legitimate power use exhibits regularity while data on power theft does not, he was curious as to how many characteristics might occur simultaneously in a one-dimensional series. The data was organized in a two-dimensional structure based on weekly intervals, and the CNN technique was utilized to identify recurring trends. Area under the receiver operating characteristic curve (AUC) was optimized by varying the proportions of training and validation data. Using the same dataset as in [3] and [4], this study demonstrates that AUC scores of more than 90% may be achieved during validation and testing using the strategy given here.

Principal Component Analysis (PCA) was used to extract PCs from the raw consumption data in the study by [23]. The objective was to preserve maximal diversity. The inclusion of a new option labeled "anomaly score," which can take on a variety of values between 0 and 1. The anomaly score was calculated for each sample used in the test.

The sample would be considered flawed if the actual value fell outside the predetermined range. The procedure was evaluated based on its true positive rate (TPR), which hit a new high of

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

90.9%.

One-Class Support Vector Machines (O-SVM), Cost-Sensitive Support Vector Machines (CS-SVM), Optimal Path Forest (OPF), and C4.5 tree were employed in the research presented in [24]. Attributes were selected from consumer consumption data, and each classifier was evaluated on its own independent set of attributes. Results improved significantly when all models were used in tandem. When all of the algorithms were combined, they could only achieve an accuracy of 86.2%.

Recurrent neural networks, Long Short-Term Memory (LSTM), and convolutional neural networks (CNNs) were all brought together by scientists in [25]. Four convolutional neural network (CNN) layers and three long short-term memory (LSTM) layers were used as hidden layers in our investigation. The strategy was only effective to the extent that the convolutional neural network could effectively extract features from a given set. The characteristics were extracted from the one-dimensional time series data used by the researchers. The highest level of accuracy achieved during model validation was 89%. The authors of the cited article [26] used the Local Outlier Factor (LOF) algorithm in conjunction with the k-means clustering technique to identify instances of energy theft. The fluctuating demands placed on our consumers were analyzed with k-means clustering. The Local Outlier Factor (LOF) technique was also utilized to identify consumers with load profiles significantly different from the cluster nodes. The method's efficacy may be assessed because its AUC is 81.5%. When the validation score is 97% and the precision score is 91.8%, our model performs optimally.

Two incidents of energy theft prompted the development of mitigation models. In the first stage, an advanced technique known as Light Gradient Boosting (LGB) is utilized. The data set was balanced using the techniques of Synthetic Minority Over-sampling (SMOTE) and Edited Nearest Neighbor (ENN). Classification was handled by the LGB model, while feature extraction was handled by the Alex Net model. SALM, which stands for SMOTEENN-Alex Net-LGB, was the proposed model; the alternative, more complex model makes use of adaptive boosting. To address the issue of unequally sized classes, the team turned to the Conditional Wasserstein Generating Adversarial Network with Gradient Penalty (CWGAN-GP) technique. To create a more balanced data set, we had to make up numbers that were quite similar to the minority group's numbers. AdaBoost was used for classification after features were extracted via Google Net. The proposed model was called GAN-NET Boost. The models were tested using the SGCC data presented here. The area under the curve (AUC) values for the SALM and GAN-Net Boost models were 90.6% and 96% during the evaluation process, respectively. Although these models had the potential to generate impressive outcomes, they were hindered by their reliance on time-only data. Our approach demonstrates that incorporating frequency-domain features into time-domain variables enhances categorisation performance.

3. PRELIMINARIES

Here, we take a deep dive into three powerful approaches: recurrent neural networks (RNNs), PCA, and MLMR.

A. Deep neural networks

Machine learning technologies such as artificial neural networks (ANNs) attempt to simulate the way the human brain learns. Long-standing approaches to machine learning may lack the sensitivity required to spot emerging patterns and trends, necessitating heavy reliance on alternative approaches [30].

Many interconnected layers of nodes or neurons make up the structure [29]. In a neural network, the neuron serves as the backbone. The concept originates with the McCulloch-Pitts neuron, a simplified model of a neuron in the brain.

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

The brain (commonly written as 31) is the most critical component of the nervous system. Figure 1 is an image depicting a neuron model. The problematic layer is relatively close to the point at which the ANN acquires data.

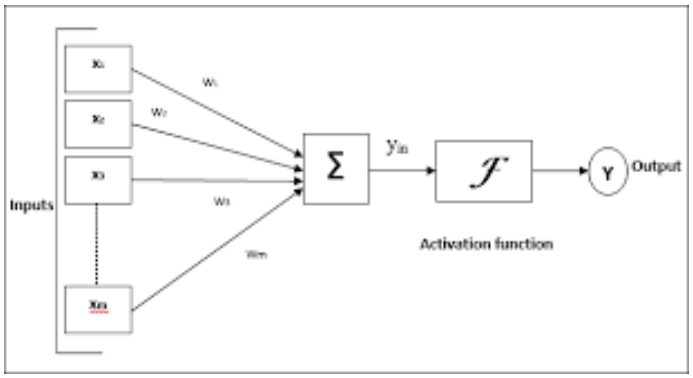
FIGURE 1. First hidden layer neuron model.

The advancement of ANNs has led to the development of Deep Neural Networks (DNNs) [32]. DNNs differ from traditional networks in that they conceal two or more processing layers. Deeper artificial neural networks (ANNs) are better at learning complicated and abstract features than their shallower counterparts. This finding is supported by prior studies [33]. It is usual practice to assign a single neuron to represent each class in the output layer when solving classification problems [29].

In a neural network, complicated properties are filtered and trained at every layer except the output layer. In contrast, the output layer's job is to make classifications using the features it has acquired through training [29, 34]. Shallow structural topologies with a single layer for non-linear transformation were the primary focus of machine learning approaches prior to the development of Deep Neural Networks (DNNs) [32]. Included in this group are models such as the Support Vector Machine (SVM), the Logistic Regression (LR), and the Single-Layer Artificial Neural Network (S-ANN). To accomplish their many computational tasks, deep neural networks (DNNs) employ several architectures. There are three distinct designs that make up deep neural networks (DNNs): convolutional, recurrent, and feed-forward.

FIGURE 2. Fully connected feed-forward DNN general architecture.

full-linking feed-forward model was used in this investigation. Company was called DNN. All connections between nodes in a typical feed-forward deep neural network (DNN) are pre-established, as shown in Figure 2.



- The image depicts the core components of a deep neural network (DNN).
- The x in the neural network architecture stands for the attributes or representations of the input data.
- The input weights (wi) in a Deep Neural Network are the connection weights between the input layer and the first hidden layer.
- Between the input and output layers of a neural network are the "hidden layers." The goal of employing it is to establish a connection between input and output [30].
- Neuronal weights are a closely guarded secret. The difficult-to-reach levels under the surface need better communication.
- There is a weight layer between the output layer and the final hidden layer.
- The output layer, denoted by the symbol y, is the DNN's final and most significant layer. Included in the paper are the findings from
- For the calculation in a feed-forward architecture, the output of the preceding layer is fed into a sequence of inputs. The last processes are what produce the final product. The network always produces the same output for any given input, regardless of the inputs that came before it. This sort of conduct is known as "stable." Nobody provided us with any editable text.

4. DNNs' HISTORY OF DEVELOPMENT

While the earliest ANNs were created in the 1940s, research on DNNs is credited with

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

beginning in the 1960s. Construction on the LeNet system began in 1989. To interpret the handwritten digits, it used a network of digital neurons. There was a lot of development after 2010; for example, Alex Net and Microsoft developed picture recognition algorithms.

Academically, Neuron and DianNao's investigation into and discovery of the DNN accelerator is intriguing.

Improvements in computer design and semiconductor technology are highlighted as crucial to the development of deep neural networks (DNNs) in the cited studies [30], [32], and [33]. These developments have simplified parallel processing and reduced the overall cost of the system.

The massive amounts of data collected by cloud services and other enterprises streamline the process of assembling massive databases. This is due to the fact that training deep neural networks (DNNs) effectively is the primary focus.

Improvements in signal/information processing and machine learning have led to new techniques for making deep neural networks (DNNs) more accurate and applicable in a wider range of settings.

Research from the past [33] demonstrates that DNNs may have many layers if the technology allowed for them.

DNN TRAINING

Since weight adjustments must be done repeatedly [33], a large dataset and sufficient computing power are required for training a deep neural network (DNN). Synaptic weights between neurons in a Deep Neural Network (DNN) are adjusted during training [30].

During training, a Deep Neural Network (DNN) takes in information and adapts accordingly. Supervised learning, semi-supervised learning, unsupervised learning, and reinforcement learning are the other four ways to learn [33, 36].

In this research, we adopted a guided-learning approach. According to references [28] and [34], the conventional method for deep neural networks (DNNs) to learn with supervision is as follows:

- W D [wi; wh1; wo] are the initial weights given.
- The input layer receives the incoming signal x.
- Once the output error has been calculated, the weights are adjusted accordingly.
- Every every training set needs to go through steps 2 and 3.

BACK PROPAGATION

The user's text contains no grammatical or stylistic errors that necessitate rewriting. In a multi-layer artificial neural network (ANN), the loss function is determined by the link weights between the input and output layers. The back propagation technique uses the chain rule to calculate the loss function's gradient. This gradient is computed by summing the products of local gradients that propagate from input to output nodes in a neural network [28, 29, 36]. It is common practice in back propagation methods to make adjustments to neural network settings on a layer-by-layer basis. In many cases, optimization methods based on gradients are used for this purpose [37].

ACTIVATION FUNCTION

It's possible to program an activation function so that it behaves like a real neuron. It receives a signal as input and generates an output that serves as the input for the following neuron [38, 39]. Activation functions come in a wide variety of forms, but they can be roughly classified as either linear or nonlinear. Organizational make-up

$$g = f(z) \quad (2)$$

FUNCTIONS FOR LINEAR ACTIVATION

The result of a linear activation function is proportional to its input. The expression (3) in the preceding sentence can be used as a synonym for the relevant elements.

$$f(z) = c(z) \quad (3)$$

C is a constant

The derivative of the linear activation function is f 0(z) D C, and its output falls within the range (1;1). The application of a gradient cannot reduce an error since it is unrelated to the input [40]. Regression issues often employ this activation function [41].

NON-LINEAR FUNCTIONS FOR ACTIVATION

The derivative of the linear activation function,

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

denoted by f'(z), is a constant. When the activation function is linear, the result is between 1 and 1. Because they are not dependent on the input, gradients cannot be utilized to mitigate mistakes [40]. The decrease is a common application of the activation function under discussion here (Ref. 41).

Sigmoid / Logistic

$$f(x) = \frac{1}{1 + e^{-x}}$$

1)

Principle component Analysis

Nonlinear activation functions are frequently used in deep neural networks (DNNs) due to their responsiveness to input changes and ability to discriminate between distinct outputs (Reference 40). The Sigmoid activation function is one of the most widely employed functions in the area due to its usefulness as a nonlinear activation function.

Mathematical symbol best describes the sigmoid activation function.

_ **Q** D **E**1

Principal component analysis (PCA) is a statistical technique for reducing the number of dimensions in a dataset without losing any useful information. In principal component analysis, the original variables are transformed into a new collection of independent variables.

In data analysis, principal component analysis (PCA) is a technique used to extract meaningful insights from a system of interconnected features or variables standing in for observations [42]. Principal components (PCs) are a fresh set of variables used to characterize the received information. Singular Value Decomposition (SVD) was used for analysis in this investigation [43]. The Singular Value Decomposition (SVD) is a statistical technique for decomposing a feature matrix X into its component elements, P, D, and Q by using the formula X = P D Q RT. Here, P represents the normalized eigenvectors of the matrix XXT, Q represents the transpose of X, and R represents the original matrix X.

- The rows and columns of E demonstrate the eigenvalues of the matrix XXT.
- However, after normalization, the eigenvectors of XTX are represented by the matrix R.

So that V D1 are produced and are sorted in decreasing order of variance [23]. A PC is given by for position p.

5. DNN-BASED ELECTRICITY THEFT DETECTIONMETHOD

This section describes the methodology's three stages—feature extraction, data analysis, and preprocessing—for detecting electricity theft.

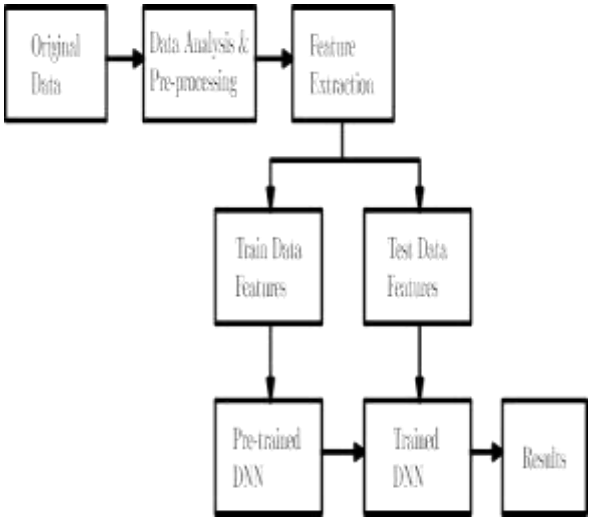


FIGURE 3. Electricity theft detection workflow diagram.

Broken smart meters, insufficient storage space, sluggish data transfers, and unanticipated system repairs are just some of the issues plaguing the dataset [4]. The dataset used in this study is not unique, but it is shared with other studies. The components of the composition are not numbers and have no numerical value. Data analysis techniques revealed that over a period of 1034 days, 5.45% of the entries in this dataset included either zero values or null values, or a combination of the two. People didn't give a hoot about the aforementioned concepts because they didn't consider them to be relevant. An "unoccupied observation" is one in which for each ai in the set an, either ai = 0 or ai / R. These measurements are useless for reporting electricity consumption over 0 kWh because they lack class-identifying

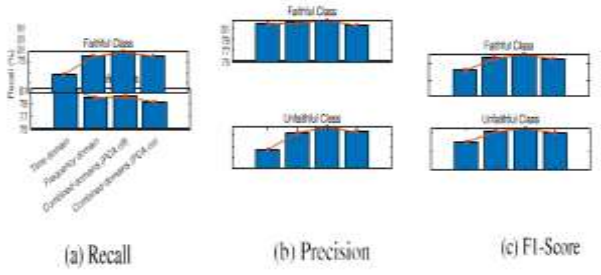
ISSN: 2278-4632
Vol-13, Issue-08, August 2023

properties. The data set was cleaned up by eliminating the aforementioned observations so that it would be more representative of reality. They were disqualified from the competition for being ineligible to compete in either class. The third column of Table 1 reveals that a

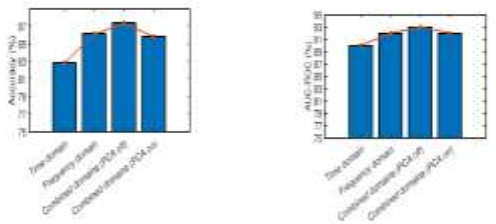
When applied to datasets with several categories, Principal Component Analysis (PCA) has not previously improved validation results. Despite their being less than a one percent difference between the comparable statistics, the committed consumers showed significant improvement in recall, accuracy, and F1-score. However, the untrustworthy institution

Parameter	Class	Before synthetic data generation	After synthetic data generation							
			Time-domain		Frequency-domain		Combined Domains			
							PCA Not Used		PCA Used	
			Valt(%)	Test (%)	Valt(%)	Test (%)	Valt(%)	Test (%)	Valt(%)	Test (%)
Recall	Faithful	94.6	85.8	84.1	92.8	92.3	94.2	94.5	93.0	92.5
	Unfaithful	4.3	89.2	81.4	90.4	79.9	90.0	80.0	89.0	79.2
Precision	Faithful	91.4	88.8	81.9	90.6	82.1	90.4	82.6	89.4	81.6
	Unfaithful	6.9	86.3	83.7	92.7	91.2	93.9	93.5	92.7	91.4
F1-Score	Faithful	93.0	87.3	83.0	91.7	86.9	92.3	88.2	91.2	86.7
	Unfaithful	5.3	87.7	82.5	91.5	85.2	91.9	86.2	90.8	84.9
Accuracy		86.9	87.5	82.8	89.9	86.1	91.1	87.3	90.5	85.8
AUC-ROC		66	94	90	96	92	97	93	96	92

MCC = 0.84 (on validation) and 0.75 (on test).



(a) Recall (b) Precision (c) F1-Score



(d) Accuracy (e) AUC-ROC

6. CONCLUSION

This research examined the effectiveness of a deep neural network (DNN) based classification technique for detecting power theft in smart grids using time-domain and frequency-domain data. Several classification tasks were examined in the study, all of which took input from either the time domain, the frequency domain, or both. The model's effectiveness was evaluated using standard metrics such as recall, precision, F1-score, accuracy, AUC-ROC, and MCC. Classification using frequency domain features outperforms time domain feature-based classification, which outperforms both frequency domain and time domain feature-based classification.

The classifier achieved an AUC-ROC (area under the receiver operating characteristic curve) of 93.03% during testing. To reduce the amount of characteristics, Principal Component Analysis (PCA) was utilized. Seven of the twenty potential components were used to achieve an AUC-ROC of 92% and an accuracy rate of 85.8% during testing of the classifier. After that, we conducted an experiment to determine which factors impacted hyperparameter optimization the most. After the validation process, accuracy improved by 1% as a result of this. The Adam optimizer was used to determine the optimal values for key parameters.

Our research revealed an AUC of 97%, which is the area under the curve. The highest AUC found in those studies was 1% lower than this. In addition, with an accuracy of 91.8%, our system ranked as the second most accurate of the data-driven algorithms evaluated on the gold-standard dataset. This method involves investigating financial transactions. The electricity industry isn't the only place where anomaly detection can be useful. It has numerous possible applications. Due to our detection threshold, we can only confirm instances of relatively little energy theft. One of our long-term objectives is to refine our processes to make the detection of power theft in real time easier. A new strategy is currently being developed to address the issue of preventing power theft in real time. Since the study relied heavily on data from SGCC shoppers, this technique might be retested with data from other regions to determine how well it performs in those settings.

REFERENCES

[1] S. Foster. (Nov. 2, 2021). Non-Technical

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

Losses: A $96 Billion Global Opportunity for Electrical Utilities. [Online]. Available: https://energycentral.com/c/pip/ non-technical-losses-96-billion-global- opportunity-electrical-utilities

[2] Q. Louw and P. Bokoro, ''An alternative technique for the detection and mitigation of electricity theft in South Africa,'' SAIEE Afr. Res. J., vol. 110, no. 4, pp. 209–216, Dec. 2019.

[3] M. Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib, ''Electricity theft detection using pipeline in machine learning,'' in Proc. Int. Wireless
Commun. Mobile Comput. (IWCM), Jun. 2020, pp. 2138–2142.

[4] 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. Informat., vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[5] P. Pickering. (Nov. 1, 2021). E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering. [Online]. Available: https://www.electronicdesign.com/technologies/meters

[6] X. Fang, S. Misra, G. Xue, and D. Yang, ''Smart grid—The new and improved power grid: A survey,'' IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[7] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin, and K. Qaraqe, ''Effi- cient detection of electricity theft cyber-attacks in AMI networks,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.

[8] A. Maamar and K. Benahmed, ''Machine learning techniques for energy theft detection in AMI,'' in Proc. Int. Conf. Softw. Eng. Inf. Manage. (ICSIM), 2018, pp. 57–62.

[9] A. Jindal, A. Schaeffer-Filho, A. K. Marnerides, P. Smith, A. Mauthe, and
L. Granville, ''Tackling energy theft in smart grids through data-driven analysis,'' in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2020, pp. 410–414.

[10] I. Diahovchenko, M. Kolcun, Z. Čonka, V. Savkiv, and R. Mykhailyshyn, ''Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads,'' Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 44, no. 4, pp. 1319–1333, Dec. 2020.

[11] M. Jaganmohan. (Mar. 3, 2022). Global Smart Grid Market Size by Region 2017–2023. [Online]. Available: https://www.statista.com/statistics/246154/global-smart-grid-market-
size-by-region/

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou. (Sep. 30, 2021). Electricity Theft Detection, [Online]. Available: https://github.com/henryRDlab/
ElectricityTheftDetection

[13] D. O. Dike, U. A. Obiora, E. C. Nwokorie, and B. C. Dike, ''Minimizing household electricity theft in Nigeria using GSM based prepaid meter,'' Amer. J. Eng. Res., vol. 4, no. 1, pp. 59–69, 2015.

[14] P. Dhokane, M. Sanap, P. Anpat, J. Ghuge, and P. Talole, ''Power theft detection & initimate energy meter information through SMS with auto power cut off,'' Int. J. Current Res. Embedded Syst. VLSI Technol., vol. 2, no. 1, pp. 1–8, 2017.

[15] S. B. Yousaf, M. Jamil, M. Z. U. Rehman, A. Hassan, and S. O. G. Syed, ''Prototype development to detect electric theft using PIC18F452 micro- controller,'' Indian J. Sci. Technol., vol. 9, no. 46, pp. 1–5, Dec. 2016.

[16] K. Dineshkumar, P. Ramanathan, and S. Ramasamy, ''Development of ARM processor based electricity theft control system using GSM net- work,'' in Proc. Int. Conf. Circuits, Power Comput. Technol. (ICCPCT), Mar. 2015, pp. 1–6.

[17] S. Ngamchuen and C. Pirak, ''Smart anti-tampering algorithm design for single phase smart meter applied to AMI systems,'' in Proc. 10th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol., May 2013,
pp. 1–6.

[18] B. Khoo and Y. Cheng, ''Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis,'' in Proc. Wireless Telecommun. Symp. (WTS), Apr. 2011, pp. 1–6.

[19] J. Astronomo, M. D. Dayrit, C. Edjic, and E. R. T. Regidor, ''Development of electricity theft detector with GSM module and alarm system,'' in

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

Proc. IEEE 12th Int. Conf. Humanoid, Nanotechnol., Inf. Technol., Commun. Control, Environ., Manage. (HNICEM), Dec. 2020, pp. 1–5.

[20] P. Jokar, N. Arianpoo, and V. C. M. Leung, ‘‘Electricity theft detection in AMI using customers’ consumption patterns,’’ IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 216–226, Jan. 2015.

[21] W. Han and Y. Xiao, ‘‘A novel detector to detect colluded non-technical loss frauds in smart grid,’’ Comput. Netw., vol. 117, pp. 19–31, Apr. 2017.

[22] S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, ‘‘Electricity theft detection using smart meter data,’’ in Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT), Feb. 2015, pp. 1–5.