International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Deep Neural Networks are Utilized in Energy Management Systems for identifying Theft of Electricity

Ruthwik S M[1], Sridevi M[2]

[1]*Student, Department Of Masters Of Computer Application, BMS Institute Of Technology And Management, Bangalore, Karnataka, India*
[2] *Professor, Department Of Masters Of Computer Application, BMS Institute Of Technology And Management, Bangalore, Karnataka, India*

Abstract - The installation of connected systems is essential for the identification of renewable energy thieves because it generate enormous volumes of the information, include information about customer behavior, that could potentially be identify electricity theft using machine learning and deep learning techniques. This project describes a method for detecting theft that employs extensive information in the time and frequency domains in a deep neural network-based classification approach. Through data interpolation and synthetic data generation procedures, we solve dataset flaws such as missing data and class imbalance issues.

We evaluate and analyze the contribution of features from both the temporal and frequency domains, execute experiments in combined and reduced feature space using principal component analysis, and lastly add a minimal redundancy-based strategy to maximizing significance for determining what's most pertinent features. We increase the detection performance of power theft by optimizing hyper parameters with a Bayesian optimizer and using an adaptive moment estimation optimizer to run tests with varying values of critical parameters to identify the ideal settings that produce the greatest accuracy. Since we train the model with over and under sampling datasets, it provides the equal representation while training the model.

Key Words: Cyberbullying, Neural Networks Machine learning, social media.
Deep Neural Network, Natural language processing, Artificial Neural Network.

1. INTRODUCTION

Electricity Theft is a global issue that impacts utility providers. Every year, utility companies lose more than $96 billion owing to Non-Technical Losses (NTLs), with energy theft being the most significant cause. According to the World Bank, 50% of generated electricity in Sub-Saharan Africa is stolen.

The main goal of electricity thieves is to consume energy without being charged by utility providers, or to pay bills that are less than the quantity spent. As a result, utility companies face significant revenue losses as a result of power theft. According to sources, India lost $16.2 billion in 2015, Brazil lost $10.5 billion, and Russia lost $5.1 billion. Electricity theft is estimated to cost South Africa approximately $1.31 billion in revenue each year.

Aside from revenue loss, electricity theft has a direct negative impact on power grid stability and reliability. It can lead to surging electricity, electrical systems overload and public safety hazards such as electric shocks. It also has a direct impact on energy tariff increases, which affect all customers

The rising need for electricity has fueled Evolution as it occurred of smart grids, which provide several benefits such as increased energy efficiency, fewer Power cuts and improved safety. But electrical theft is an essential cause of revenue loss for utility companies and a severe worry in smart grids. Therefore, a major issue for power distribution firms is theft of energy. The objective of this investigation is to develop an effective technique towards electricity theft detection in smart electrical systems utilizing neural networks made up of computers (ANN). The suggested method would make use of a power use dataset obtained from the renowned web repository Kaggle for the purpose of only training the model. Preprocessed data will be put into the ANN, which will learn to spot patterns and abnormalities in the consumption data and finally the model is tested by providing the real-time data to predict the abnormalities or theft of electricity.

The ANN model will be trained on a dataset of lawful usage patterns before being evaluated on data including cases of energy theft even the datasets with over sampling and under - sampling is used such that the model is trained in equal representation while learning.

The model will be evaluated using test data to assess the effectiveness of the recommended course of action. Expected outcomes from our suggested technique for detecting electricity theft in smart grids utilizing ANN are favorable. Our method obtained 99% Training Accuracy and 99% Validation Accuracy. Accuracy, precision, recall, and F1-score will be employed as performance measurements. We have built the

suggested system on the Flask Web framework for ease of use and a better User Interface for forecasting results.

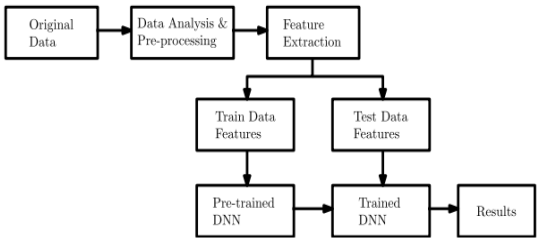

Fig -1: Proposed Architecture

2. Related Work

Theft of electricity and illicit ground surface conductor connections are a widespread problem in South Africa, according to SAIEE researchers. This phenomenon not only causes income loss and equipment damage, but it also poses a life-threatening concern. Despite decades of research into non-technical losses, no general solution has been given due to the problem's complexity. The project studies the use of zero-sequence current-based detection as a mitigation approach for dealing with unauthorized ground surface conductor connections. The validity of this approach, as well as its influence on seasonal changes in soil resistivity, is demonstrated by simulation and experimental data.

In this research, Zibin Zheng and I intend to progress a unique power theft detection approach to overcome the aforementioned difficulties. We first propose a Wide & Deep Convolutional Neural Networks (CNN) model to learn power usage data and identify electricity thieves. Our Deep & Wide CNN model is made up of two parts: a Wide component with a fully-connected layer of neural networks and a Deep CNN component with numerous a fully-connected layer is a pooling layer, and a layer that uses convolution. In nature, the Deep CNN component can learn the periodicity of power use data while the Pan counterpart may gather worldwide statistics. The advantages of the Wide and Deep CNN are combined in this way. components, resulting in high performance in power theft detection.

Some publications investigated ETD approaches, which utilize smart meter consumption data to identify deceptive users. Academics are concerned about the observation of customer load profiles for signs of electricity loss in traditional electric systems. Maximum consumption, mean consumption, inspection remarks summation, standard deviance, and average deviation were the six metrics employed by Angelo's et al. neighborhood mean consumption, to provide a typical form of power consumption for each user. For gathering consumers with similar characteristics, K-means fuzzy clustering was obtained. Customers with plenty of parking near the cluster centers were deemed to be potential cheaters.

Quentin Low spoke about it. Electricity theft through unauthorized connections is a substantial source of non-technical loss contribution. These connections are often connected to South African supply networks' low voltage networks. Socioeconomic conditions are the primary cause of these occurrences, and a collective strategy involving political, economic, and engineering interaction is required to develop solutions that address all stakeholder needs while also addressing the safety of the population living in these communities where these illegal connections occur.

3. Existing System

They describe an effective technology for detecting theft of power in use today system that is based on carefully collected and chosen characteristics in a Deep Neural Network (DNN)-based classification methodology. We demonstrate that utilizing frequency-domain features rather than time-domain features alone improves classification performance. The previous approach relied on a realistic power usage dataset made the State Grid Corporation of China (SGCC) makes online.

To understand the findings and ease future training, the current system used Principal Component Analysis (PCA) to conduct classification with reduced feature space and compare What happened from classification done with all input characteristics. The old approach relied on Utilizing the Minimum Redundancy Maximum Relevance (MRMR) approach, being most crucial characteristics and justify the importance of frequency-domain data over time-domain features in identifying electricity theft.

Whereas prior system models produced outstanding results, their reliance on time-domain properties alone restricted their efficacy. For training, conventional system model DNN-based approaches require enormous volumes of labelled data. These is a useful tool for stealing electricity prevention. difficulty since acquiring labelled data can be difficult and time-consuming. The present system DNN models are computationally costly to train and can take a long time, especially for big datasets. This might make it difficult to adjust fast to new data or changes in the smart grid.

The current systems Overfitting may arise in DNN models when the model gets overly specialized to the training data and performs badly on fresh, unknown data. This can be a concern in identifying robbery of power since it might lead to missed thefts or false alarms. Existing system DNN models are frequently regarded as black-box models, implying that the model's decision-making process might be difficult to explain. This can make understanding the aspects that lead to the detection of energy theft difficult, as well as explaining the results to stakeholders or authorities.

4.Proposed System

The current system Adversarial attacks on DNN models are possible, in which an attacker manipulates the input data to cause the model to generate inaccurate predictions. This can be a serious issue in discovering theft of electricity since it allows a bad actor to avoid detection.

Our suggested following procedures make up the neural network modelling (ANN) method used in discovering energy theft in virtual grids: data analysis and preprocessing, feature extraction, and classification. The suggested approach makes advantage of the Kaggle-referenced power usage dataset for only training purpose and testing or the model is evaluated by feeding the real-time data for predicting electricity theft. Preprocessing of the obtained data will involve data cleansing, normalization, and feature extraction. This step is crucial because it guarantees that the data is in a format that the ANN model can learn from. The dataset contains no labels for loyal or unfaithful usage. So, we'll start by labelling the dataset via Agglomerative clustering.

The suggested system comprises the development of Clustering (to detect Electricity Theft (Target value)). As in our previous study (base), we used agglomerative clustering with a cluster value of 3.

After that, the suggested system was trained using the Artificial Neural Network (ANN). A big dataset of labelled power use Statistics is going to be employed to train the ANN model. The programme will learn to recognize patterns and abnormalities in data that suggest cases of electricity theft. The model's performance will be measured using several metrics like as accuracy, precision, recall, and F1-score.

great accuracy: ANN models have been demonstrated to identify power theft with great accuracy. This is due to the fact that ANN models may learn complicated patterns and correlations in consumption data that are difficult to detect using standard statistical approaches.

Robustness: ANN models can deal with noisy and missing data, which is frequently encountered in real-world smart grid deployments. This increases the robustness of ANN models and reduces the likelihood of mistakes and false positives.

Adaptability: ANN models are capable of adapting to changes in the smart grid, such as new forms of theft or shifts in consumption patterns. This makes ANN models more adaptable to the dynamic nature of smart grids.

Speed: Because ANN models can handle huge volumes of data fast, they are ideal for detecting energy theft in real time. This can assist utility firms in responding fast and taking corrective measures to reduce revenue losses.

Automation: ANN models may be taught to identify energy theft automatically, removing the need for physical inspection and lowering utility companies' burden. This can result in substantial cost reductions and enhanced efficiency.

This project makes use of univariate time-series data on electricity use. A univariate measurement is a single measurement that is conducted regularly across time. Data can be represented by its features (properties) for classification issues, which can then be provided as input to the classifier, as shown in the Fig.1. Given a collection of distinct samples, data is categorized depending on how alike characteristics. Time-domain and frequency-domain information were retrieved and utilized as input to a deep neural network for classification like this article. The classification performance of time-domain, frequency-domain, and integrated characteristics from both domains was compared. The confusion matrix shows how many predictions are correct and incorrect per class.

5.Result

The classification of electrical signals, which has a wide range of practical uses, presents one of the most significant difficulties in all of humanity. The suggested system is put into test in the following paragraphs, and the results are gathered and discussed to show how effective it really is. Numerous studies have made references to the energy usage statistics. The measurements involve running the most optimal set up (of two chosen layers) on the bike theory, analyzing an electrical commands classification system setting up, measuring accuracy and loss using the deep CNN and BM models, and at last contrasting the success and failure leads obtained by the CNN and BM models to the ones from the CNN system independently.

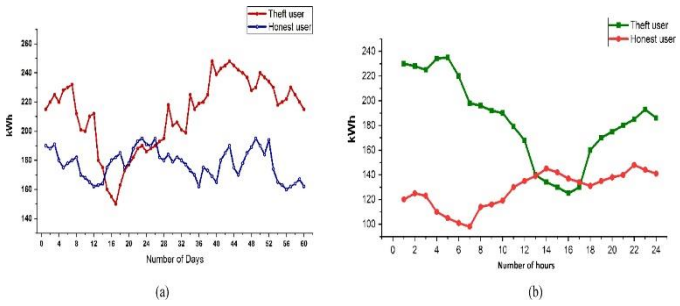

Fig -2: Graphical representation of electricity theft

The designed model will predict the theft by analyzing certain quantities of real-time data fed into the system, the system will predict as faithful if there is no theft in electricity from smart grids and predicts unfaithful is there are any abnormalities or theft occurred from the smart electric grids the pie chart representation shows the amount of faithful and unfaithful electricity consumptions in easy and understandable manner.

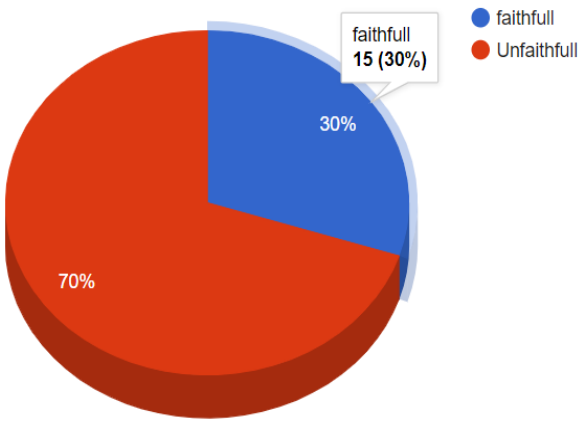

Fig -3: Pie chart representation

6.CONCLUSION

In this research, we examined the way sophisticated circuits can identify electricity theft. utilizing time-domain and frequency-domain characteristics in a DNN-based classification technique. Similar to DNN network, isolated classification tasks based on time-domain, frequency-domain, and mixed domain features were examined. The model's performance was measured using widely known performance metrics such as recall, precision, F1-score, accuracy, AUCROC, and MCC.

We discovered that classification using frequency-domain features outperforms classification using time-domain features, which in turn outperforms classification using both domains. When tested, the classifier achieved 87.3% accuracy and 93% AUC-ROC. For feature reduction, we employed PCA. When evaluated, the classifier achieved 85.8% accuracy and 92% AUC-ROC using 7 out of 20 components.

We next examined individual features' contributions to the classification job and validated the relevance of frequency-domain features over time-domain features in a successful classification task using the MRMR method. Finally, the model will predict the theft of electricity from the smart grids when the model is tested with real-time data.

7.Future Enhancement

When compared to other data-driven algorithms assessed on the same dataset, we got 97% AUC, which is 1% better than the best AUC in previous research, and 91.8% accuracy, which is the second-highest on the benchmark.

The strategy employed here makes advantage of consumption data trends. Aside from electricity distribution networks, it may be employed in anomaly detection applications in any sector. Our approach makes a minor contribution to accurately detecting energy theft since we detect theft that occurred over time.

In the future, we hope to expand our approach to identify real-time electricity theft. Because this strategy was tested based on SGCC consumers' usage habits, it may be checked against datasets from diverse places to assure its applicability elsewhere.

Despite decades of research into the problem of electricity theft and non-technical losses, no comprehensive answer has been discovered as a universal mitigating ingredient. Various strategies have been proposed and implemented with great success, one of which is the implementation of SMART meter technology.

This deployment approach is only applicable to genuine installations and is often applied at the paying client end. The problem that requires more serious attention is the region where unlawful connections are made to the source transformers on declared networks where no billing is placed, and where the community's safety risk is increased.

Future research is now being conducted to discover a potential approach to reduce these types of incidents by identification and isolation of the afflicted source.

REFERENCES

[1] Bhattacharyya, R., & Basu, S. (2018). India Inc looks to deal with rising
stress in employees. Retrieved from ‘The Economic Times’

[2] OSMI Mental Health in Tech Survey Dataset, 2017 from Kaggle

[3] Van den Broeck, J., Cunningham, S. A., Eeckels, R., & Herbst, K.
(2005). Data cleaning: detecting, diagnosing, and editing data abnormalities. PLoS medicine, 2(10), e267.

[4] Shwetha, S, Sahil, A, Anant Ku mar J, (2017) Predictive analysi s using
classification techniques in healthcare domain, International Journal of
Linguistics & Computing Research, ISSN: 2456-8848, Vol. I, Issue. I,
June-2017

[5] Tomar, D., & Agarwal, S. (2013). A survey on Data Mining approaches
for Healthcare. International Journal of Bio-Science and Bio-Technology,
5(5), 241-266.

[6] S. Foster. (Nov. 2, 2021). Non-Technical Losses: A $96 Billion Global Opportunity for Electrical Utilities. [Online]. Available: https://energycentral.com/c/pip/ non-technical-losses-96-billion-globalopportunity-electrical-utilities

[7] 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.

[8] 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. (IWCMC), Jun. 2020, pp. 2138–2142.

[9] 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.

[10] S. Foster. (Nov. 2, 2021). Non-Technical Losses: A $96 Billion Global Opportunity for Electrical Utilities. [Online]. Available: https://energycentral.com/c/pip/ non-technical-losses-96-billion-globalopportunity-electrical-utilities