Deep Neural Networks are used to identify theft of energy in systems for managing energy.

Shubha R, Bhavani R

The National Institute of Engineering

ABSTRACT

The prevalence of electricity theft, which is a serious concern, has an bang on equally service company and power consumers. It has a negative impact on the financial health of utility companies, raises electrical safety concerns, and significantly raises energy costs for consumers. The creation of smart grids is essential for preventing electricity theft because these systems produce a vast amount of data, offers user usage data that may be used to detect energy theft via device wisdom or deep learning approaches.

Smart grids will offer a no of benefits, including increased energy efficiency, fewer power outages, and improved security, as the demand for electricity rises. One of the main sources of income for utility companies is electricity theft.
The goal of this research is to demonstrate how a synthetic neural network may be used to identify energy theft in smart grids.
We'll start by pre-processing the collected data, which we'll call the Kaggle electricity usage dataset.
Then, the Kaggle dataset will be fed into the ANN, which will learn to identify patterns and variations in the consumption data. The ANN will then be trained on the dataset's valid consumption patterns. Finally, the dataset will be tested against a group of instances of theft

INTRODUCTION

Utility providers are impacted by the global phenomenon known as electricity theft.

Value concern lose more than $96 billion annually as a effect of NTLs, with the main cause being electricity theft.

World Bank estimates that 50% of electricity production in Sub-Sahara Africa is subject to theft.

The main objective of electricity theft, which is illegal, is to obtain power without paying any fees to the value company or to receive bills for less than the sum of power actually consumed. Utility companies lose a significant amount of money as a result of power theft. India lost USD 16,2 billion, Brazil lost USD 10,5 billion, and Russia lost USD 5,1 billion in 2015, for instance. The annual revenue lost to electricity theft in South Africa is estimated to be $1,31 billion.

power thievery has a direct and detrimental effect on the stability and dependability of the power grid in addition to its detrimental economic effects.

Electrical surges, overloads of electrical systems, and risks to public safety like electric shocks can all result from it.

It also directly influences energy tariff increases, which have an effect on all customers.

Smart grids are being created to supply the growing demand for electricity. They provide a number of advantages, including increased security, decreased power outages, and improved energy efficiency. The goal is to find a reliable AI-based technique for detecting power theft in smart grids. The proposed methodology will use a power use dataset obtained from the well-known web platform Kaggle. With the help of this dataset, the ANN will be taught to spot trends and outliers in the consumption data.

The ANN model will be trained using a dataset of permitted usage patterns before being assessed using data containing instances of energy theft. The proposed strategy's model performance will be evaluated using test data. An artificial neural network is used in our suggested method for detecting power theft in smart grids. (ANN) is expected to yield promising results. Our method produced training accuracy and rationale precision of 99% each. As performance indicators, accuracy, precision, recall, and F1-score will be used. For ease of use and a better User Interface for predicting results, we built the suggested system using the Flask Web framework.

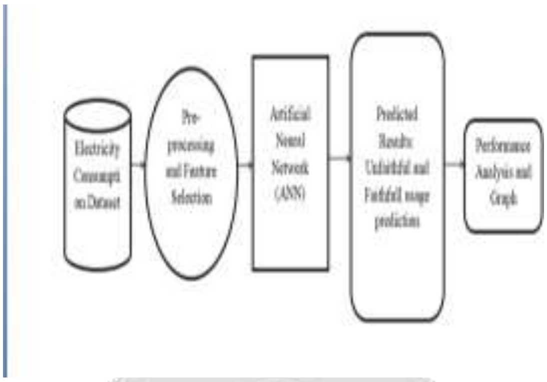

Electricity Consumpti on Dataset
Pre-processing and Feature Selection
Artificial Neural Network (ANN)
Predicted Results: Unfaithful and Faithful usage predictions
Performance Analysis and Graph

Fig. 1. Proposed Architecture

LITERATURE SURVEY:

According to SAIEE researchers, illegal ground surface conductor connections and electricity theft are major issues in South Africa. This phenomenon poses a serious threat to human life in addition to causing income loss and equipment damage. Despite decades of research into non-technical losses, the issue's complexity has prevented any broad solutions from being provided.In this examine, unauthorized ground surface conductor connections are dealt with using a mitigation strategy called zero-sequence current-based detection. Both simulated and real-world data explain that this way is efficient and has an impact on seasonal variations in soil resistivity.

In bid to circumvent the problems mentioned above, Zibin Zheng's research aims to develop a new method of detecting power theft.

To classify current thieves and learn about power usage data, we first suggest a Wide & Deep Convolutional Neural Networks (CNN) model. The Deep CNN component of our Deep & Wide CNN model has many convolutional layers, a pooling layer, and a fully-connected layer. A layer of neural networks that is fully connected exists in our model's Wide component. This model combines the benefits of the Wide and Deep CNN components to achieve high performance in clout larceny exposure.

Research has been conducted on End-to-End (ETD) methods, which detect fraudulent users by utilizing consumption information from smart metres. Concerns have been raise among academics regarding the examination of customer load patterns for indications of electricity theft in conventional power systems. Angelos et al. used five parameters: maximum consumption, mean consumption, inspection remarks summation, standard deviance, and neighbourhood mean consumption to provide an average form of power consumption for each user. Using K-means fuzzy clustering, consumers with similar traits were grouped. Customers who could easily find parking close to the cluster centres were suspected of being swindlers.

Quentin Louw talked about it. Electricity theft resulting from unauthorized connections is a large non-technical loss factor. It is customary to connect these to the South African supply networks' low voltage networks. Since socioeconomic factors are the primary factor for these occurrences, a coordinated strategy involving political, economic, and engineering interaction is required to come up with solutions that satisfy the needs of all parties while also guaranteeing the safety of the citizens of the communities where these illegal connections occur.

PROPOSED SYSTEM:

The current system's DNN models are vulnerable to adversarial attacks, in which a perpetrator tampers with the effort data to produce false predictions. This, united with its skill to evade detection, can make it a major issue in the investigation of power theft.

 Our proposed method for detecting electricity theft in smart grids using artificial neural networks (ANN) consists of three steps: feature extraction, data analysis, and preprocessing. The suggested approach uses the Kaggle-referenced dataset for power usage. Data cleaning, quality origin, and data normalization are the steps that make up the preprocessing of the acquired data. The data must be presented so that the ANN model can understand it, and this crucial step makes sure of that. The dataset lacks labels for either faithful or unfaithful usage. We will first employ agglomerative clustering to label the dataset.

To sense power larceny and achieve the target value, the proposed system develops clustering. We employed agglomerative clustering with a cluster value of three, just like in the base study.

After that, an artificial neural network was used to train the suggested system.

The ANN model will be trained using a substantial dataset of labelled power consumption data. Participants will gain the ability to identify patterns and discrepancies in data that indicate instances of power theft. Accuracy, precision, recall, and F1-score are the metrics that will be used to gauge how well the model performs.

Great accuracy: Power theft detection using ANN models has been demonstrated to be effective. This results from the potential for ANN models to detect intricate correlations and patterns in consumption data that are challenging to detect using conventional statistical methods.

Robustness: In real-world smart grid deployments, noisy and missing data are frequently present. These situations can be handled by ANN models. The probability of errors and false positives is consequently decreased, and the robustness of ANN models is increased.

Adaptability: One of the advantages of ANN models is their capacity to adapt to the ever-evolving smart grid landscape, including novel types of theft and changes in consumption patterns. As a result, ANN models can better accommodate the dynamic nature of smart grids.

Speed: The best models for detecting real-time energy theft are artificial neural networks (ANNs), which can process massive amounts of data quickly. Utility providers may be in a position to respond quickly and take the necessary steps as a consequence of minimizing revenue losses.

Automation: Energy theft can be detected automatically by ANN models, eliminating the need for physical inspection and lessening the burden on utility companies. This can result in substantial cost reductions and enhanced efficiency.

Data on uniform electricity use is utilized for this project. A single univariate measure is a single, repeating measure. Property representations of data are used to organize it, and these representation are then altered into classifier input.The proximity of features provided by a collection of independent samples guides the classification of data.

METHODOLODY:

- Importing Libraries**:** The code commences with the import of the required libraries, like NumPy library, pandas library, Matplotlib library, seaborn library, and machine learning modules are RandomForestClassifier and AdaBoostClassifier.
- Loading Data: The data is converted from the CSV file "daily_dataset.csv" to a DataFrame named "daily".
- Data Analysis and Preprocessing: Print out the total count of customers and the total days. Make sure there's nothing wrong with the data. A boxplot will show you how the daily energy counts change by half an hour. It will show you how frequently you used various daily energy counts.
- Data Filtering: Instances with less than 48 daily energy counts are flagged and eliminated from the data set.
- ID Analysis Based on Total Days Count: A boxplot shows how many energy counts each individual ID has. A plot visualizes the energy counts of individual IDs per day.
- Choosing a Data Period: The dataset is sorted by identification number (ID) to identify the period (usually one year) that has the maximal number of records for the common of IDs.
- Data Manipulation: An identification is used to order the data, and the weighted average of the different values of each attribute is calculated. The “LCLid” column is omitted. The three sets of data—thefts1, thefts2, and thefts3—are created by combining the two sets of data. Random transformation is used to simulate manipulation or anomaly for these data subsets. A new column “label” is added to denote whether an instance is tampered or not (lab = 1) and whether an instance is not tampered (lab = 0).The manipulated data subsets are merged with the primary data sets to create the final dataset for model compilation.
- Model Building: The dataset is classified as X-dimensional segment (X) or Y-dimensional segment (Y).The characteristics are scaled using pattern scaling. The data is divided into training and testing datasets. The Keras library is used to define a neural network model.
  The model is then further optimized with the help of Adama Optimizer, as well as the binary CEPL (Cross- Entropy Loss function).The model is retrained on the original training data set,

and then retrained again on the original testing data set. Each training dataset iteration shall be documented and loss values shall be printed.

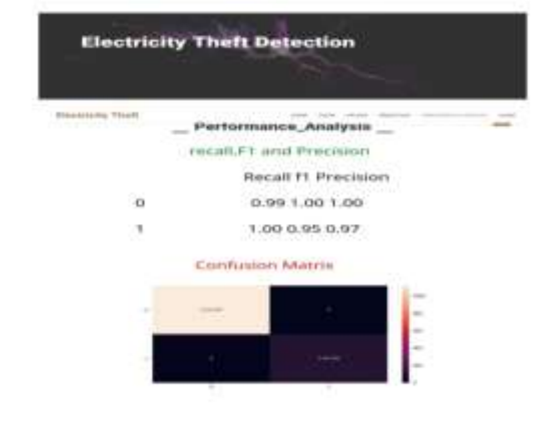
- Model Evaluation and Performance: Model accuracy and loss values are determined over various training and testing period. The model's performance is measured and can be determined by looking at its accuracy and loss curve over different training cycles.
- Results and Interpretation: Data from the training process indicates the model's change in model precision and loss over the training time. The model can then be employed in anomaly detection or classification operations, where it is anticipated to be capable of distinguishing a conditioned event from a normal event based on the patterns generated during training.

RESULT:

Artificial Neural Networks (ANN) are being employed in this project to develop an intelligent grid-based solution to identify power theft.

The suggested method would use data on power use that collected from well-known web repository kaggle. The pre-processed data will be fed to the ANN, which will then train to spot patterns and anomalies in the consumption data.

The ANN model will be tested initially using data containing examples after being trained on a dataset of approved use patterns. The test data will be used to examine the model's adequacy of the suggested method. The use of ANN to our suggested technique for detecting stolen energy in intelligent grids is likely to provide favorable outcomes.



Electricity Theft Detection

Electricity Theft

__ Performance_Analysis __

recall,F1 and Precision

	Recall	f1	Precision
0	0.99	1.00	1.00
1	1.00	0.95	0.97

Confusion Matrix

CONCLUSION

An artificial neural network (ANN) was used in the study to examine how electricity theft could be detected in smart grids. We observed that the classification performance was improved when an ANN was used in place of the current system. In our proposed system, we achieved 99% Training Accuracy and 99% Validation Accuracy. This method employs data on consumption trends. Our work only has a small impact on accurately identifying energy theft because we only find gradual theft.

In conclusion, the proposed artificial neural network (ANN) system holds the promise of significantly reducing the financial losses caused by electricity theft in smart grids. By detecting theft in real-time and alerting utility companies, the system can help lessen the effects of electricity theft and improve the smart grid's overall efficiency and security.

Future Enhancement:

Add time-series analysis, supervised anomaly detection, and external data sources to the theft detection strategy to make it more effective. For more dependable outcomes, use ensemble models and perceptible artificial intelligence (AI). To find subtle anomalies, use collaboration-based filtering, continuous assessment, and real-time implementation. Concentrate on compliance and privacy. To improve the model, adjust it for different locations and establish a feedback loop. When combined, these improvements improve the reliability, adaptability, and usability of intelligent meter data-driven theft detection.

REFERENCES

[1] 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

[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. (IWCMC), 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, ‘‘Efficient 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] "Progress and challenges in smart grids: Regional generation, smart metering, energy storage, and smart loads," I. Diahovchenko, M. Kolcun, Z. onka, V. Savkiv, and R. Mykhailyshyn, Trans. Electr. Eng., vol. 44, no. 4, pp. 1319-1333, Dec. 2020, Iranian J. Sci. Technol.

[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-marketsize-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/ Electricity Theft Detection

[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 microcontroller,’’ Indian J. Sci. Technol., vol. 9, no. 46, pp. 1–5, Dec. 2016.