Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 35

Electricity Theft Detection in Smart Grids Using Artificial Neural Network

Jyothika J[1], Kavitha O[2], HarshaVardhan N[3], Sushmitha K[4], Bhaskar B M.Tech.[5],

[1,2,3,4] *Students, and* [5]*Faculty*
Dept. of Computer Science Engineering, Madanapalle Institute of Technology & Science, Madanapalle, India.
jyothikajyo521@gmail.com

Abstract: Smart grids, which provide several benefits like improved energy efficiency, less power outages, and enhanced security, are growing in popularity as a result of the rising need for electricity. Power theft, however, is one of the main issues with smart grids. which costs utility companies a lot of money. Therefore, electric power distribution firms are quite concerned about electricity theft. This study's objective is to provide an efficient method using artificial neural networks (ANNs) for identifying power theft in smart power networks. The suggested method will employ a dataset regarding energy usage that is taken from the well-known online resource Kaggle. Once the data has been preprocessed and inserted into the ANN, It will pick up on pattern recognition and anomalies when consuming it. After training on a dataset of acceptable consumption patterns, the Data containing instances of energy theft will be used to evaluate the ANN model. Test results will be utilized to evaluate the prototype and determine how effective the recommended course of action is. Positive results are what we expected from our proposed ANN-based technique for smart grid power theft detection of 99% Training Accuracy and 99% Validation Accuracy were attained by our method. The performance metrics that will be employed include F1- score, recall, accuracy, and precision. Additionally, the proposed framework, which makes use of Flask Web to make it easier to use and provide a better user interface for outcome prediction. The project's intended outcome is an efficient method for using artificial neural networks (ANN) to detect electricity theft in smart grids, which utility companies may employ to boost revenue collection and enhance smart grid security. This research can potentially be expanded to other domains, such as intrusion detection in computer networks and fraud detection in financial systems, that include anomaly identification in large-scale datasets.

Keywords: *F1-score, Flash, Recall, Accuracy, Precision, Kaggle and Artificial Neural Network.*

1. INTRODUCTION:

The illicit use of electricity or its tampering without the required authorization or payment is known as "electricity theft," a widespread issue that affects utility companies and jeopardizes the reliability of electrical grids across the globe. This illegal conduct can take many different forms, such as manipulating meter data, making unauthorized connections, and tampering with or circumventing meters. There are many different reasons why people steal power, such as financial difficulties, discontent with utility rates, or malicious intent. The ramifications of electricity theft are extensive and harmful. Utility firms experience significant income losses, which eventually affects their capacity to make investments in maintenance, service enhancements, and infrastructure upgrades. theft incidents, energy theft raises operating expenses Furthermore, since businesses have to spend money on manual inspections, inquiries, and court cases to deal with. Unauthorized consumption can also put undue burden the electrical grid, causing instability, safety risks for utility workers, and even dependability problems [1].Electricity theft causes significant income losses and operational inefficiencies for utility companies worldwide, making them extremely difficult to operate. Conventional approaches to identifying theft have frequently relied on consumer complaints and recurring inspections, which are reactive and laborious processes.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 35

But new paths for proactive and automatic theft detection have been made possible by the introduction of smart grid technologies, which provide real-time data analytics capabilities and advanced metering infrastructure (AMI).Artificial neural networks (ANNs) have become extremely effective tools for identifying abnormalities across a wide range of fields and evaluating intricate data patterns in recent years. By using the abundance of data produced by smart metres, artificial neural networks (ANNs) are able to recognize minute variations that may be signs of energy theft.

2. WORKING OF ELECTRICITY THEFT DETECTION:

Our paper, "**Electricity Theft Detection In Smart Grids Using Artificial Neural Network**" model will be affected by this critical stage in a cascading manner; the more and better data we gather, the more powerful our model will be. Numerous techniques, such as physical interventions and online scraping, can be used to collect data. The dataset was obtained from the well-known web repository Kaggle. You can use this URL to access the dataset. Dataset Collection from Kaggle :

https://www.kaggle.com/datasets/jayaprakashpondy/electricity-consumption-database

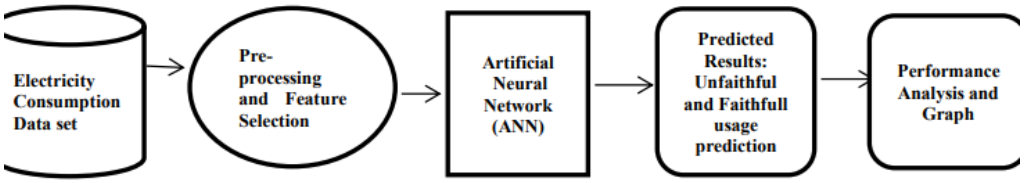
First, data is transferred toward the layer of input, which subsequently forwards it to the concealed levels. Every input initially has a random weight assigned to it by the links between these two levels. and each input neuron thereafter receives bias. Subsequently, the weighted sum—a mixture of weights and bias—is processed by the activation function. The output is computed after the activation function selects the node that fires for feature extraction. We refer to the entire method as forward propagation. The output model is obtained, and the error is calculated by comparing it with the original output. The weights are then modified in order to minimise the error during the backward propagation phase[2]. For a predetermined number of epochs, this iterative procedure is carried out. In the end, the modified model weights and predictions are made.

Artificial neural networks have a wide range of applications, including predictive modeling, adaptive control, and problem-solving in artificial intelligence. These networks can be trained using datasets, allowing them to learn from experience and draw conclusions from complex and seemingly unrelated information. In the context of electricity theft detection in smart grids, a proposed system utilizes Artificial Neural Networks (ANN). This system leverages historical data on energy consumption, voltage, and current to train the ANN model[3]. By analyzing this data, the model can identify abnormal patterns that may indicate instances of electricity theft. A sizable dataset of labelled electricity use data will be utilised to train the ANN model. The programme will be able to identify possible instances of electricity theft by learning to recognise patterns and abnormalities in the data. The model's performance will be assessed using a number of measures, such as accuracy, precision, recall, and Fl-score.

3. ARCHITECTURE:

A neural network is called a multi-layer perceptron because it includes several layers, each of which carries out a distinct function. The number of layers in the network grows in tandem with the model's complexity. In its most basic form, An input layer, a hidden layer, and an output layer make up a neural network. These neural networks must be taught using some training data and machine learning techniques before they can be applied to a particular problem. After receiving the input signals, the input layer forwards them to the subsequent layer, which generates the final forecast[5].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 35



Fig(i) System Architecture

In the multi-layered perceptron that was previously explained, they are essentially the dense or buried layers. They consist primarily of neurons, which are the building blocks that combine to form perceptrons. To put it simply, perceptrons, or dense layers, are represented by a vertical combination of neurons, which you can see in the accompanying image. Each circle in the image represents a neuron. You can now see a detailed view of every neuron in the image above. Here, each neuron has a set of weights (in the example picture, w1, w2, and w3) as well as biases. The activation function is applied based on these calculations, and the output is equal to activation(combination). The sample image shows sigmoid activation, which is denoted by 1/(1 + e-F)[4].Other activation functions include tanh, Leaky ReLU, ReLU, and many others.

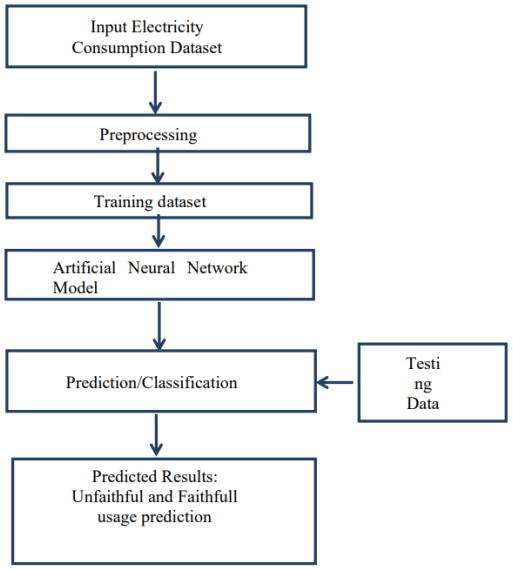
By building the first layer with the input_dims argument, we can define the input features of the Keras Model. The input will be 8 in this instance. The challenge now becomes, how can we count The quantity of neurons in each layer and how many layers there are overall? Exactly how many layers to utilise is a difficult decision. Usually, a variety of layers, a variety of neurons, and a few activation functions are used with the Keras tuner. It looks for the optimal arrangement through permutation and combination. This method can be time-consuming, though, which is a disadvantage[1]. To obtain additional information, please consult the Keras tuner documentation. In this example, a fully connected three layer network is defined using a Dense Class. The activation argument receives the activation function as input, whereas the first argument defines The quantity of neurons in each layer.

In this instance, as the challenge is binary classification, ReLU is utilised as the mechanism for activation function in the initial two layers and the sigmoid in the last layer. The loss function, optimizer, and any metrics must be specified in order to build the Keras model. We shall employ "binary_crossentropy" as the loss function for this binary classification issue. The optimizer will be configured to "adam" since it self-tunes and works well for a variety of issues. Additionally, we will use the metrics argument to report the categorization accuracy. Preprocessing Training dataset Artificial Neural Network Model Predicted Results: Unfaithful and Faithfull usage prediction Input Electricity Consumption Dataset Prediction/Classification Testi ng Data The fit() function will then be used in order to fit our model on the loaded data. The training procedure will consist of 64 batches and 100 epochs.

Every epoch will see an update to the amount of rows in the dataset. The evaluate() function can be used to assess the model on the dataset. It creates predictions for every input and output pair given input and output arguments. It gathers metrics like accuracy and average loss to generate scores. We disregard the lost value because we are just concerned with. Finally, by using the model's predict() method, we may make predictions. The output layer makes use of the reporting the accuracy. sigmoid activation function, therefore probabilities between 0 and 1 will be predicted.

1.Often referred to as An ascending chart, the DFD is a straightforward graphic depiction that shows the input data, the data processing and the output data that is produced.
2. The most important tools for demonstrating system components is a diagram of data flow (DFD), which may be used to represent system operations, the data These procedures need, external parties interacting with the system, as well as information moving through it.
3. DFD provides a visual representation of the movement and transformation of information within a system. It is a graphical technique that illustrates how data flows and changes as it goes from input to output.
4. A system can be represented using the DFD, also called a bubble chart, at different levels of abstraction

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
Volume7-Issue2, January 2024
Paper: 35



Fig(ii) Data Flow Diagram

1. ADVANTAGES :

1.Artificial neural network (ANN) models have proven to be highly accurate in identifying instances of electricity theft. This is because they can recognise complex patterns and relationships in consumption information that are difficult to find with conventional statistical techniques.
2. ANN models exhibit robustness by effectively handling noisy and incomplete data, which is commonly encountered in real-world smart grid deployments. This enhances their reliability and reduces the likelihood of errors and false positives[3].
3. The adaptability of ANN models allows them to adjust to changes in the smart grid, such as new types of theft or alterations in consumption patterns. This flexibility makes them well-suited for the dynamic nature of smart grids.
4. With their ability to process large volumes of data rapidly, ANN models are ideal for real-time detection of electricity theft. This enables utility companies to promptly respond and implement corrective measures to minimize revenue losses.
5. By training ANN models to automatically detect electricity theft, the need for manual inspection is eliminated.

2. SAMPLE OUTPUT:

Fig (iii) Prediction of Theft Detection

3. CONCLUSION:

In this paper, we looked into how Artificial Neural Networks (ANNs) might be used to identify cases of smart grid electricity theft. Our results showed that ANNs performed better in categorization than current systems. The suggested solution performed admirably, achieving 99% training and 99% validation accuracy. This approach demonstrates its versatility beyond electrical distribution networks by utilising consumption data patterns, and it may be implemented in a range of anomaly detection applications. This project's methodology is centred on long-term theft detection, which is a major help in precisely identifying cases of energy theft. The revenue loss caused by energy theft in smart grids could be greatly decreased by the suggested ANN-based approach. The system's goal is to reduce the impact of electricity theft by quickly identifying theft in real-time and notifying power providers. This will ultimately improve the overall security and efficiency of the smart grid infrastructure.

4. 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. 209216, 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. 21382142.

[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. 16061615, 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 gridThe new and improved power grid: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944980, 4th Quart., 2012.