**Electricity Theft Detection in Smart Grids Based on Deep Neural Network**

**IEEE BASE PAPER ABSTRACT:**

Electricity theft is a global problem that negatively affects both utility companies and electricity users. It destabilizes the economic development of utility companies, causes electric hazards and impacts the high cost of energy for users. The development of smart grids plays an important role in electricity theft detection since they generate massive data that includes customer consumption data which, through machine learning and deep learning techniques, can be utilized to detect electricity theft. This paper introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach. We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features. We improve the electricity theft detection performance by optimizing hyperparameters using a Bayesian optimizer and we employ an adaptive moment estimation optimizer to carry out experiments using different values of key parameters to determine the optimal settings that achieve the best accuracy. Lastly, we show the competitiveness of our method in comparison with other methods evaluated on the same dataset. On validation, we obtained 97% area under the curve (AUC), which is 1% higher than the best AUC in existing works, and 91.8% accuracy, which is the second-best on the benchmark.

**OUR PROPOSED ABSTRACT:**

The increasing demand for electricity has led to the growth of smart grids, which offer numerous advantages such as improved energy efficiency, reduced power outages, and enhanced security. However, one of the significant challenges in smart grids is electricity theft, which is a major cause of revenue loss for utility companies. So, electricity theft is a major concern for electric power distribution companies. The aim of this project is to develop an effective approach for detecting electricity theft in smart grids based on Artificial Neural Network (ANN). The proposed approach will use electricity usage dataset which is referred from the popular web repository kaggle. The collected data will be preprocessed and fed into the ANN, which will learn to identify patterns and anomalies in the consumption data. The ANN model will be trained using a dataset of legitimate consumption patterns and then tested with data that contains instances of electricity theft. To evaluate the performance of the proposed approach, the model will be tested on a test data. The results predicted from our proposed system of electricity theft detection in smart grids using ANN is Good. Our system achieved Training Accuracy of 99% and Validation Accuracy of 99%. The performance metrics used will include accuracy, precision, recall, and F1-score. We also developed the proposed system in Flask Web framework for easy usage with better User Interface for the predicting the results. The expected outcome of this project is an effective approach for detecting electricity theft in smart grids using ANN, which can be used by utility companies to improve their revenue collection and enhance the security of the smart grid. This project can also be extended to other domains that involve anomaly detection in large-scale datasets, such as fraud detection in financial systems and intrusion detection in computer networks.

**EXISTING SYSTEM:**

* In the existing system they present an effective electricity theft detection method based on carefully extracted and selected features in Deep Neural Network (DNN)-based classification approach. We show that employing frequency-domain features as opposed to using time-domain features alone enhances classification performance. The existing system used a realistic electricity consumption dataset released by State Grid Corporation of China (SGCC).
* The existing system employed Principal Component Analysis (PCA) to perform classification with reduced feature space and compare the results with classification done with all input features to interpret the results and simplify the future training process.
* The existing system used the Minimum Redundancy Maximum Relevance (mRMR) scheme to identify the most significant features and validate the importance of frequency-domain features over time-domain features for detecting electricity theft.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Although the existing system models were able to achieve impressive results, their consideration of time-domain features alone limited their performance.
* The existing system model DNN-based methods require large amounts of labeled data for training. This can be a challenge in the case of electricity theft detection, as obtaining labeled data can be difficult and time-consuming.
* The existing system DNN models are computationally expensive to train and can take a long time, especially for large datasets. This can make it challenging to quickly adapt to new data or changes in the smart grid.
* The existing system DNN models can be prone to overfitting, which occurs when the model becomes too specialized to the training data and performs poorly on new, unseen data. This can be a problem in electricity theft detection, as it can result in missed instances of theft or false alarms.
* The existing system DNN models are often considered as black-box models, meaning that it can be difficult to interpret the decision-making process of the model. This can make it challenging to understand the factors that contribute to the detection of electricity theft, and it can be difficult to explain the results to stakeholders or regulators.
* The existing system DNN models are vulnerable to adversarial attacks, where an attacker can manipulate the input data to cause the model to make incorrect predictions. This can be a significant problem in the case of electricity theft detection, as it can allow a malicious actor to evade detection.

**PROPOSED SYSTEM:**

* Our proposed system of Electricity Theft Detection in Smart Grids Based on Artificial Neural Network (ANN) consists of the following three steps: Data Analysis and Preprocessing, Feature Extraction, and Classification. The proposed system uses the electricity consumption dataset referred from the kaggle. The collected data will undergo preprocessing, which includes data cleaning, normalization, and feature extraction. This step is critical as it ensures that the data is in a suitable format for the ANN model to learn from. The dataset doesn’t contain any label of Faithfull usage or unfaithful usage. So first we will label the dataset using Agglomerative clustering.
* The proposed system includes developing the Clustering (To find Electricity Theft (Target value)). Agglomerative clustering with cluster value = 3 as from our other analysis (base on mean energy).
* The proposed system then trained with the Artificial Neural Network (ANN). The ANN model will be trained on a large dataset of labeled electricity consumption data. The model will learn to detect patterns and anomalies in the data that indicate instances of electricity theft. The performance of the model will be evaluated using various metrics such as accuracy, precision, recall, and F1-score.

**ADVANTAGES OF PROPOSED SYSTEM:**

* High accuracy: ANN models have been shown to have high accuracy in detecting electricity theft. This is because ANN models can learn complex patterns and relationships in the consumption data, which can be difficult to identify using traditional statistical methods.
* Robustness: ANN models can handle noisy and incomplete data, which is often the case in real-world smart grid deployments. This makes ANN models more robust and less prone to errors and false positives.
* Adaptability: ANN models can adapt to changes in the smart grid, such as new types of theft or changes in consumption patterns. This makes ANN models more flexible and better suited to the dynamic nature of smart grids.
* Speed: ANN models can process large amounts of data quickly, making them suitable for real-time detection of electricity theft. This can help utility companies to respond quickly and take corrective action to minimize revenue losses.
* Automation: ANN models can be trained to automatically detect electricity theft, eliminating the need for manual inspection and reducing the workload for utility companies. This can lead to significant cost savings and increased efficiency.

**SYSTEM ARCHITECTURE:**

Predicted Results: Unfaithful and Faithfull usage prediction

Electricity Consumption Dataset

Artificial Neural Network (ANN)

Performance Analysis and Graph

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium i3 Processor.
* Hard Disk : 500 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 4 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 10 / 11.
* Coding Language : Python 3.8.
* Web Framework : Flask.
* Frontend : HTML, CSS, JavaScript.

**REFERENCE:**

LELOKO J. LEPOLESA, SHAMIN ACHARI, AND LING CHENG, (Senior Member, IEEE), “Electricity Theft Detection in Smart Grids Based on Deep Neural Network”, IEEE Access (Volume: 10), 2022.