



Electricity Theft Detection in Smart Grids Based on Artificial Neural Network

Vemuri Vasanth Kumar^{*1}, Mrs. A.Sirisha^{*2}

¹MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology (A), Beside VSEZ, Duvvada, Vadlapudi Post, Gajuwaka, Visakhapatnam-530049.

²Assistant Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Beside VSEZ, Duvvada, Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.

Abstract

Electricity theft is a pervasive issue that impacts both utility providers globally and individual electricity users. This phenomenon disrupts the economic growth of utility corporations, leading to disturbances in the power grid and resulting in increased energy costs for users. The implementation of smart grids plays a crucial role in addressing electricity theft by generating large datasets that include consumer consumption information. This data can be leveraged for effective electricity theft detection using machine learning algorithms. In this project, an artificial neural network is employed to analyze features acquired from consumer data to determine potential instances of electricity theft. The use of deep learning techniques, such as Deep Artificial Neural Network, along with evaluation metrics like accuracy score, f1 score, precision score, and recall score, enhances the efficiency and accuracy of the detection model. Real-world experiments based on actual energy consumption data are conducted to validate the proposed approach. The results of the experiments demonstrate that the suggested detection model outperforms existing methods in terms of precision and efficiency. By utilizing deep learning and advanced evaluation metrics, this project presents an efficient solution for the recovery of revenue losses in electric utilities caused by electricity theft. The application of these techniques contributes to the overall improvement of electricity grid security and economic stability for utility providers.

Keywords: Electricity Theft, Deep Artificial Neural Network, Deep Learning, Power Grid.

1. INTRODUCTION

Electricity theft poses a significant challenge for utility companies worldwide, resulting in substantial financial losses that are often transferred to paying customers. Smart grids have emerged as a promising solution to address this issue by enabling real-time monitoring of electricity usage and the detection of anomalies indicative of theft. While existing theft detection methods in smart grids have shown relative cost-effectiveness, they may be limited by their focus on time-domain features, neglecting frequency-domain features. Smart grids, characterized by their ability to gather and analyze information about electricity usage, play a crucial role in detecting unusual patterns that may signify electricity theft. This project introduces an effective electricity theft detection method based on carefully selected features in an Artificial Neural Network (ANN)-based classification approach. Machine learning algorithms, particularly Artificial Neural Networks (ANNs), enhance the accuracy of electricity theft detection by analyzing real-time energy

consumption patterns and identifying anomalies that may signal theft. These algorithms can learn from historical data, continually improving their accuracy to detect increasingly sophisticated forms of electricity theft.

The implementation of electricity theft detection using smart grids not only aids utilities in identifying and mitigating energy losses due to theft but also leads to significant cost savings. Furthermore, it improves the reliability of utility services by preventing power outages and service disruptions associated with theft incidents. The integration of smart grid technology and machine learning algorithms allows for real-time detection of electricity theft, enhancing accuracy and reducing financial losses for utilities. By enabling utilities to monitor energy consumption in real-time and promptly identify anomalies, smart grids contribute to the overall improvement of reliability and efficiency in electricity distribution networks.

2.LITERATURE SURVEY

According to new research conducted by Northeast Group, electricity theft and other so-called “non-technical losses” total a staggering \$96 billion per year globally. In a release, the Northeast Group states that the problem is “crippling utilities around the world, driving up prices for paying customers and often necessitating costly government subsidies.” The firm notes that non-technical losses including theft, fraud, billing errors and other issues are now beginning to be addressed more aggressively by utilities. “Non-technical losses are often hidden costs and have received little public attention, but have enormous costs for utilities, customers and governments,” according to Ben Gardner, president of Northeast Group. “This \$96 billion problem not only results in higher prices for paying customers and costly government subsidies but also a public safety crisis in some countries with dangerous illegal power connections. In many countries, high non-technical losses threaten the financial sustainability of the electric utilities.”

3.EXISTING SYSTEM

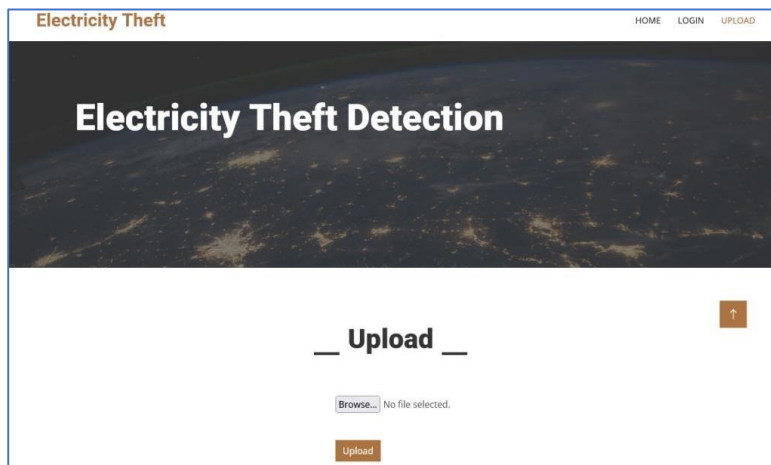
In the existing system, an effective electricity theft detection method is presented, utilizing a carefully extracted and selected set of features within a Deep Neural Network (DNN)-based classification approach. The system employs Principal Component Analysis (PCA) to perform classification with a reduced feature space. This approach is then compared with classification done using all input features to interpret the results and simplify the future training process. The existing methodology focuses on enhancing the efficiency of the electricity theft detection system by strategically selecting features that contribute most significantly to the classification process. The utilization of a Deep Neural Network underscores the system's capacity to learn complex patterns and relationships within the data, providing a robust framework for accurate classification. To further streamline the classification process, Principal Component Analysis is employed to reduce the dimensionality of the feature space. This reduction aims to retain the most informative aspects of the data while minimizing redundancy, ultimately optimizing the efficiency of the classification model. Comparisons are made between the classification results obtained with the reduced feature space through PCA and the results achieved using all input features. This analysis helps in interpreting the impact of feature reduction on the overall classification accuracy and performance. The integration of PCA not only aids in achieving computational efficiency but also simplifies the future training process. By focusing on the most relevant features, the system can potentially reduce the computational burden during training while maintaining or even enhancing its ability to accurately detect instances of electricity theft.

4. PROPOSED SYSTEM

The proposed system for electricity theft detection in smart grids is based on Artificial Neural Networks (ANN), specifically the Multi-Layer Perceptron (MLP) model. The proposed system uses historical data on energy consumption, voltage, and current to train the ANN model to detect abnormal patterns that may indicate electricity theft. 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.

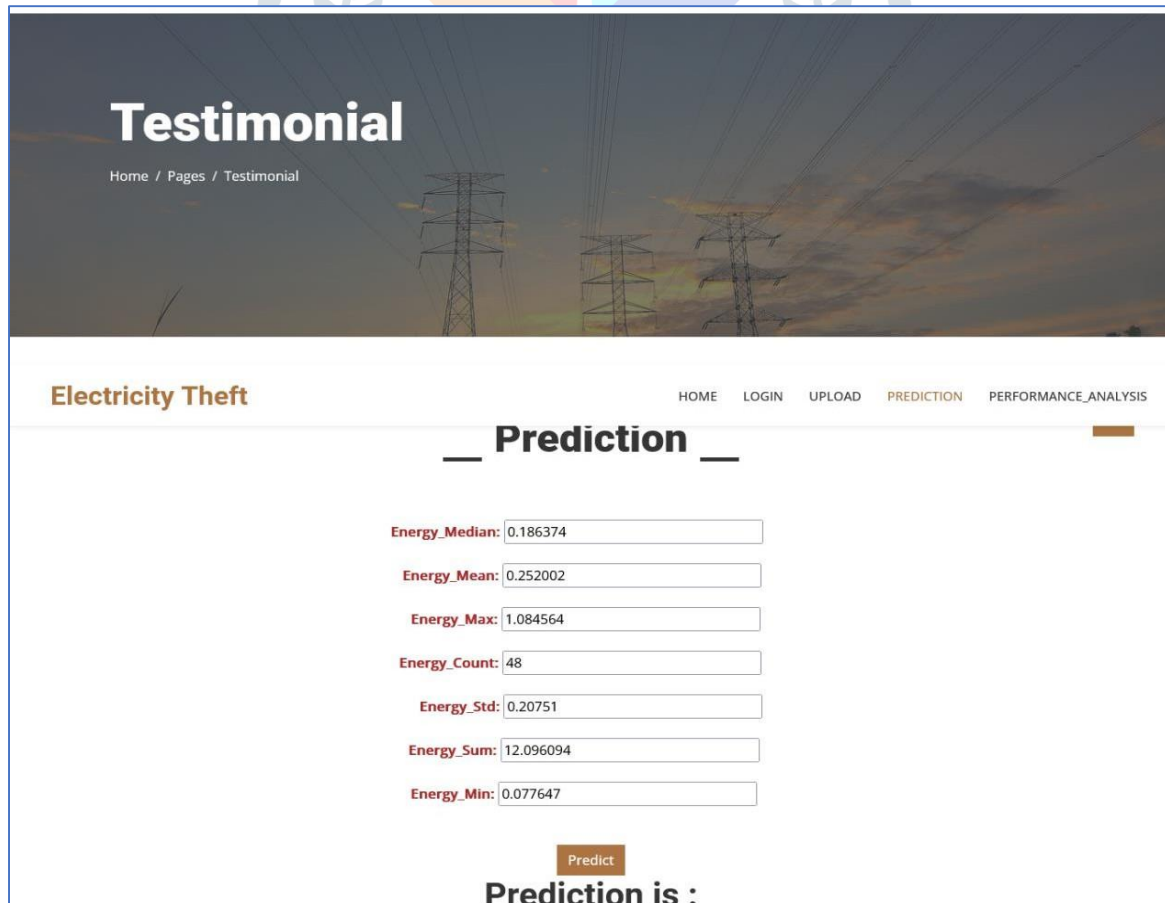
5. EXPERIMENTAL RESULTS

Home Page:



The screenshot shows the home page of the 'Electricity Theft Detection' application. The page has a dark header with the title 'Electricity Theft' and navigation links for 'HOME', 'LOGIN', and 'UPLOAD'. Below the header is a large banner image with the text 'Electricity Theft Detection'. Underneath the banner is a white box containing an 'Upload' button, a file selection area with a 'Browse...' button and the text 'No file selected.', and another 'Upload' button.

Theft Prediction:



The screenshot shows the 'Prediction' page of the 'Electricity Theft Detection' application. The page has a dark header with the title 'Electricity Theft' and navigation links for 'HOME', 'LOGIN', 'UPLOAD', 'PREDICTION', and 'PERFORMANCE_ANALYSIS'. Below the header is a large banner image with the text 'Testimonial'. Underneath the banner is a white box containing a 'Prediction' button, a list of input fields for energy statistics, and a 'Predict' button. The input fields are:

Energy_Median:	0.186374
Energy_Mean:	0.252002
Energy_Max:	1.084564
Energy_Count:	48
Energy_Std:	0.20751
Energy_Sum:	12.096094
Energy_Min:	0.077647

Below the input fields is a 'Predict' button and the text 'Prediction is :'. The background of the page features a large image of power lines and towers.

6. CONCLUSION

In this project, we explored the application of Artificial Neural Networks (ANNs) for the detection of electricity theft in smart grids. The investigation revealed that the classification performed by ANNs surpassed the performance of existing systems. The proposed system achieved remarkable results with a training accuracy of 99% and a validation accuracy of 99%. The approach leveraged consumption data patterns, showcasing its adaptability beyond electrical distribution networks for deployment in various anomaly detection applications. The method employed in this project focuses on the detection of theft occurring over time, contributing significantly to the accurate identification of energy theft. The proposed Artificial Neural Network (ANN)-based system exhibits the potential to substantially reduce revenue loss attributed to electricity theft in smart grids. By detecting theft in real-time and promptly alerting power companies, the system aims to minimize the impact of electricity theft, ultimately enhancing the overall efficiency and security of the smart grid infrastructure.

7. REFERENCES

- [1] S. Foster, "Non-Technical Losses: A \$96 Billion Global Opportunity for Electrical Utilities," Nov. 2, 2021. [Online]. Available: <https://energycentral.com/c/pip/non-technical-losses-96-billion-globalopportunity-electrical-utilities>
- [2] Q. Lou 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 Communication Mobile Computer (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. Information, vol. 14, no. 4, pp. 1606-1615, Apr. 2018.
- [5] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin, and K. Qaraqe, "Efficient detection of electricity theft cyberattacks in AMI networks," in Proc. IEEE Wireless Communication Networks Conf. (WCNC), Apr. 2018, pp. 1-6.
- [6] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid: The new and improved power grid: A survey," IEEE Communication Surveys Tuts., vol. 14, no. 4, pp. 944-980, 4th Quart., 2012.