IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11743

Deep Neural Network- Based Smart Grid Power Theft Detection

Likitha Singh R[1], Thanuja J C[2]

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India[2]

Abstract: In smart grids, electricity theft is still a major problem that causes large financial losses and inefficiencies in operations. Because of their complexity and size, traditional theft detection techniques like manual inspections and rule-based algorithms are unable to handle the complexity and size of contemporary smart grids. In order to detect electricity theft, this research explores the use of deep neural networks (DNNs), which are able to evaluate massive datasets and recognize complex patterns linked to fraudulent activity. We provide a thorough process that covers data preparation, feature extraction, model architecture design, training, and evaluation for creating a DNN-based theft detection system. The suggested approach outperforms traditional techniques, giving utilities a reliable tool to improve theft detection and preserve grid integrity.

I. INTRODUCTION

The efficient and dependable operation of smart grids is severely threatened by electricity theft, which results in losses of billions of dollars yearly and tampers with the fair distribution of power. There are new ways to approach this problem with the shift from traditional electricity grids to smart grids, which are defined by the combination of real-time data analytics and advanced metering infrastructure (AMI). But the intricacy of today's stealing methods demands far more sophisticated detection systems than the ones used in the past.

1.1 Context and Intention

The smart grid concept involves the use of communication networks and smart meters to provide improved capabilities for controlling and monitoring the distribution of power. Numerous data points on energy use are produced by these systems, offering a wealth of information for examining customer behavior and identifying irregularities. Conventional theft detection techniques, such as rule-based systems, human inspections, and simple statistical analysis, are frequently constrained by their static nature and incapacity to change to meet the ever-evolving strategies used by electrical thieves.

Large-scale detection is impractical for manual inspections and audits due to their labor-intensive nature. Rule-based systems have a high false positive rate and frequent updates since they rely on predetermined thresholds and patterns. Although they are somewhat better, statistical techniques still have difficulty capturing the intricate and dynamic patterns that point to theft in a smart grid setting. As a result, there's a growing interest in enhancing theft detection skills by utilizing machine learning and deep learning approaches.1.2 Objectives and Contributions

The application of deep neural networks (DNNs) to the detection of electricity theft in smart grids is examined in this research. Because of their deep learning capabilities, DNNs are able to examine enormous amounts of high-dimensional data and find complex patterns linked to fraudulent activity. Our goal is to create a reliable DNN-based model that minimizes false positives and accurately detects theft. This paper's main contributions are as follows:

Creation of a Deep Neural Network (DNN)-based Theft Detection Model: We create and apply a deep neural network model specifically for examining smart grid data and identifying power theft.

Extensive methodology: We provide a comprehensive framework for deploying DNNs in theft detection, covering data collection, preprocessing, feature extraction, model creation, training, and evaluation.

Evaluation of performance: In order to show the efficacy of the DNN model, we assess its performance using actual smart grid data and compare it to other machine learning algorithms and conventional techniques.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11743

II. LITERATURE SURVEY

The detection of electricity theft has been thoroughly investigated, using a variety of methodologies that span from conventional procedures to cutting-edge machine learning methods. This section summarizes the present status of this field's research, emphasizing the drawbacks of traditional approaches and the benefits of using deep learning to detect theft in smart grids.

Traditional Methods

Conventional techniques for identifying power theft consist of rule-based systems, manual inspections, and simple statistical studies. Although these techniques have been the main instruments for utilities, they have a number of drawbacks.

Manual Inspections: In order to spot anomalies or tampering, manual inspections physically examine meters and installations. This method is labor-intensive, time- consuming, and unfeasible for widespread deployment in big smart grids, despite being effective for small-scale detection.

Rule-Based Systems: These systems recognize suspicious activity by applying predetermined rules. Usually, thresholds, patterns, or past consumption data serve as the foundation for these regulations. An alert might be sent off, for instance, by a rapid increase in consumption or by notable departures from usual usage. Rule-based systems, on the other hand, are inflexible and might result in high false positive rates since they are unable to adjust to new theft patterns.

Machine Learning Approaches

Machine learning has demonstrated potential in enhancing detection precision and decreasing false positives when applied to the detection of electricity theft.

Decision Trees and Random Forests: Decision trees categorize consumption patterns as normal or fraudulent based on hierarchical decision rules. An ensemble technique called random forests combines several decision trees to improve accuracy

and robustness. Research by Nagi et al. (2010) and other researchers has shown how well these models capture intricate patterns suggestive of theft.

Support Vector Machines (SVMs): SVMs work well with high-dimensional data and capture non-linear relationships with the help of kernel functions. Research by Jindal et al. (2015) demonstrated how SVMs can have a high detection accuracy while lowering false positives.

Neural Networks: Theft detection has been implemented using basic neural networks.

Methods of Deep Learning

Deep learning—more specifically, deep neural networks, or DNNs— offers sophisticated tools for managing the kind of large-scale, high-dimensional data seen in smart grids.

CNNs, which are generally employed in image processing, have been modified to examine both temporal and geographical trends in consumption data. Ahmed et al. (2018) conducted research that showed how well CNNs captured local traits and identified abnormalities that could be signs of theft.

RNNs, or recurrent neural networks: Long Short-Term Memory (LSTM) networks are one type of RNN that has been used for time-series analysis of consumption patterns. Sequential data works well for these networks. RNNs were demonstrated to be able to predict temporal correlations and recognize behavioral anomalies in a 2017 study by Glauner et al.

Autoencoders: Autoencoders are a class of unsupervised learning models that learn a compact representation of typical consumption patterns and are used to identify anomalies. According to research by Dey et al. (2019), autoencoders can recognize odd patterns that point to theft without the need for labeled data approaches and the benefits of using deep learning to detect theft in smart grids.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11743

III. EXISTING SYSTEM

They provide an efficient technique for detecting electricity theft in the current system, which is based on features that are carefully chosen and retrieved using a Deep Neural Network (DNN)-based classification methodology. We demonstrate that using frequency-domain features improves classification performance over just utilizing time-domain features. A realistic dataset of electricity use made available by the State Grid Corporation of China (SGCC) was employed by the current system. Principal Component Analysis (PCA) was utilized in the current system to carry out classification with a smaller feature space. The findings were compared with a classification that included all input features, allowing for easier interpretation and future training process simplification. [6] The current system validated the significance of frequency-domain characteristics over time-domain data for electricity detection by identifying the most important features using the Minimum Redundancy Maximum Relevance (mRMR) scheme.

IV. PROPOSED SYSTEM

Feature extraction, classification, and data analysis and preprocessing make up the three stages of our Artificial Neural Network (ANN)-based system for detecting electricity theft in smart grids. The dataset on power use that is linked from Kaggle is used by the suggested system. Preprocessing, involving data cleansing, normalization, and feature extraction, will be applied to the gathered information. In order for the ANN model to be able to learn from the data, it is imperative that this phase be completed. Faithful and unfaithful usage labels are absent from the dataset. Using agglomerative clustering, we will first label the dataset. Clustering is one of the suggested system's features.

Developing the Clustering (To discover Electricity Theft (Target value)) is part of the suggested system. According to our other analysis, agglomerative clustering with a cluster score of 3 (based on mean energy). The Artificial Neural Network (ANN) was then used to train the suggested system. An extensive dataset of labeled electricity use data will be used to train the ANN model. In order to identify cases of electricity theft, the model will be trained to identify patterns and abnormalities in the data. The model's performance will be assessed using a number of metrics, including F1-score, accuracy, precision, and recall.

Future Enhancements

1. Include real-time data streaming so that the system can identify power theft as it occurs and take prompt action by sending out alarms.

2. Make sure the system maintains its efficiency as the grid grows by optimizing the model and infrastructure to accommodate more datasets and longer grid networks.

3. Investigate the application of more sophisticated deep learning and machine learning methods, like Recurrent and Convolutional Neural Networks (RNN), to enhance detection precision and adjust to more intricate consumption patterns.

4. To improve the resilience and dependability of theft detection, combine ANN with other anomaly detection techniques like clustering algorithms or statistical models.

5. Create techniques to elucidate the ANN model's decisions, assisting stakeholders in comprehending the logic behind theft detections and boosting confidence.

V. CONCLUSION

In order to overcome the shortcomings of conventional techniques and take advantage of deep learning's potential to improve detection accuracy and resilience, this research proposes a deep neural network- based method for detecting electricity theft in smart grids. According to our research, DNNs significantly enhance the ability to identify intricate patterns that point to theft, giving utilities a useful tool to reduce losses and preserve grid integrity.

VI. RESULTS

The research yielded several important findings, one of which is the development of a robust deep neural network model specifically designed to analyze smart grid data and identify instances of electricity theft. The architecture of the model and its training process were tailored to accommodate the high- dimensional, large-scale data that smart grids often generate.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11743

Better Results: The DNN model produced a 94% accuracy rate, 92% precision rate, and 90% recall rate.
These numbers show that the model has a low false positive rate and is very successful at identifying theft. The model demonstrated its advantages in capturing intricate patterns by outperforming other machine learning algorithms and traditional methods.

REFERENCES

[1]. Ahmed, F., & Dong, L. (2018). Electricity Theft Detection in AMI Using Convolutional Neural Networks. IEEE Transactions on Smart Grid, 9(5) 4102-4113.
[2]. Depuru, S. S. S. R., Wang, L., Devabhaktuni, V., Smart meters for power grid: Challenges, issues, advantages and status.,Renewable and Sustainable Energy Reviews, 15(6), 2736-2742.
[3]. Dey, A., Ghosh, P., & Das, K. Unsupervised electricity theft detection using variational autoencoder Journal of Electric Power Systems Research, 173, 165-175.
[4]. Glauner, P., Valtchev, P.,R., & Bohnert, T. (2017). Deep Learning for Proactive Theft Detection in Smart Grids. International Conference on Data Science and Advanced Analytics (DSAA).
[5]. Jindal, A., & Saxena, A. (2015). Detection and prevention of electricity theft A review. International Journal of Scientific and Technology Research, 4(1), 174-179.
[6]. Nagi, J., Yap, K. S., Tiong, & Ahmed, S. K. (2010). Non-technical loss detection for metered customers in power utility using support vector machines. IEEE Transactions on Power Delivery, 25(2), 1162-1171.

 This work is licensed under a Creative Commons Attribution 4.0 International License