IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, November 2023

Electricity Theft Detection using Deep Neural Network

Prof. H. R. Agashe, Vipul Bhosale, Swarup Gite, Aishwarya Nimse, Sonali Talekar

Matoshri College of Engineering and Research Centre, Eklahare, Nashik, Maharashtra, India

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.*

Keywords: Theft Detection, Machine Learning, Artificial Neural Network (ANN), Flask Web framework, User Interface, Smart Grids, etc

I. INTRODUCTION

Deep learning techniques for electricity theft detection are studied in, where the authors present a comparison between different deep learning architectures such as convolutional neural networks (CNNs), long-short-term memory (LSTM) recurrent neural networks (RNNs), and stacked autoencoders. However, the performance of the detectors is investigated using synthetic data, which does not allow a reliable assessment of the detector's performance compared with shallow architectures. Moreover, the authors in proposed a deep neural network- (DNN-) based customer-specific detector that can efficiently thwart such cyber-attacks. In recent years, the CNN has been applied to generate useful and discriminative features from raw data and has wide applications in different areas. These applications motivate the CNN applied for feature extraction from high-resolution smart meter data in electricity theft detection. In, a wide and deep artificial neural network (ANN) model was developed and applied to analyse the electricity theft in smart grids.

In a plain CNN, the softmax classifier layer is the same as a general single hidden layer feedforward neural network (SLFN) and trained through the backpropagation algorithm. On the one hand, the SLFN is likely to be overtrained leading to degradation of its generalization performance when it performs the back-propagation algorithm. On the other hand, the back-propagation algorithm is based on empirical risk minimization, which is sensitive to local minima of training errors. As mentioned above, because of the shortcoming of the softmax classifier, the ANN is not always optimal for classification, although it has shown great advantages in the feature extraction process. Therefore, it is urgent to find a better classifier which not only owns the similar ability as the softmax classifier but also can make full use of the obtained features. In most classifiers, the random forest (RF) classifier takes advantage of two powerful

DOI: 10.48175/568

machine learning techniques including bagging and random feature selection which could overcome the limitation of the softmax classifier. Inspired by these particular works, a novel artificial neural network (ANN) model is adopted for electricity theft detection. The ANN is proposed to automatically capture various features of customers' consumption behaviours from smart meter data, which is one of the key factors in the success of the electricity theft detection model. To improve detection performance, the RF is used to replace the softmax classifier detecting the patterns of consumers based on extracted features. This model has been trained and tested with real data from all the customers of electricity utility in Ireland and London.

II. LITERATURE SURVEY

Damian O. Dike Uchechukwu A. Obiora1, Euphemia C. Nwokorie, Blessing C. Dike 2015:

The design, simulation and construction of a GSM-based prepaid meter has been achieved. It x-rayed various forms of electricity theft which include unaccountability of servicemen, irregularities of billing leading to a reduction of funds by the utility companies has also been achieved as this work prevents one on one contact between the end user and the workers.With remote monitoring of the meter reading and sending SMS whenever there is readings in the customer electricity meter, the developed system may be able to help Utilities reduce the incidences of household electricity theft.The work also revolves around the automatic disconnection and connection when the recharge is low or high respectively and extra cost due to reconnection is removed. Further improvement will be needed in including miniaturized monitoring cameras in the customer meter which will monitor physical activities around the meter in each household to check other illegal acts that were not covered in this work.

Zibin Zheng,Yatao Yang, Xiangdong Niu, Hong-Ning Dai, Yuren Zhou 2017:

They propose a Wide & Deep CNN model to detect electricity theft in smart grids. In particular, our Wide & Deep CNN model consists of the Wide component and the Deep CNN component; it gains thebenefits of memorization and generalization brought by the Wide component and the Deep CNN component, respectively. We conduct extensive experiments on realistic electricity consumption data released by State Grid Corporation of China (SGCC), the largest electricity supply company in China. The experiment results show that our proposed Wide & Deep CNN outperforms existing methods, such as linear regression, support vector machine.

Since it consumes extremely high amounts of electricity to grow marihuana, the abnormal electricity usage patterns can be captured by the proposed wide and deep CNN model.

Mubbashra Anwar,Nadeem Javaid , Adia Khalid , Muhammad Imran , Muhammad Shoaib 2020:

In this work, a pipeline is proposed to detect electricity theft in SG. The proposed pipeline is made up of SMOTE,KPCA and SVM. The imbalanced class issue is resolved using SMOTE, KPCA is used for feature extraction and SVM for the classification of electricity theft. It is the most efficient and simplest technique that is able to classify the fraudulent and non-fraudulent consumers accurately. Besides,various performance metrics are used for the evaluation of binary classification problems, such as: ROC curve, precision,recall, F1-score, MCC, and MAP are used to evaluate theperformance of the proposed model. The proposed method is general and can be applied to any field to detect the anomaly. However, our contribution is just a small step towards the goal of accurate detection of NTLs. In future, the generative adversarial networks (GANs) will be explored to tackle the issue of class imbalance by generating more realistic data for minority class and also for the anomaly detection task.

III. PROBLEM STATEMENT

The project's core challenge is to develop an effective solution for detecting electricity theft within smart grids. Conventional theft detection methods are insufficient due to the complexity of modern grids. This project aims to employ artificial neural networks (ANNs) to analyze smart meter data and identify abnormal consumption patterns indicative of theft, ultimately enhancing grid security and financial integrity.

IV. OBJECTIVES OF PROJECT

- To develop a customized artificial neural network (ANN) model for precise electricity theft detection in smart grids, leveraging advanced feature engineering and rigorous evaluation metrics.
- To curate a comprehensive dataset encompassing genuine consumption data and simulated theft scenarios, facilitating effective training and validation of the ANN model.
- To optimize the ANN model's parameters, layer configurations, and hyper-parameters through systematic training, ensuring accurate identification of electricity theft instances.
- To integrate the trained ANN model into a real-time monitoring system capable of efficient analysis of incoming smart meter data while minimizing processing latency.
- To assess the ANN model's performance rigorously using metrics like accuracy, precision, recall, and F1-score, showcasing its ability to discern theft instances and minimize false alarms.
- To conduct a comparative analysis, highlighting the superiority of the ANN-based approach over traditional methods in terms of electricity theft detection.
- To ensure the developed solution's scalability to handle large-scale smart grid deployments and robustness against varying consumption patterns and environmental conditions.
- To meticulously document the entire development process, from data preprocessing to model architecture, and provide actionable insights for potential deployment.
- To emphasize the positive impact of the solution on utility companies, consumers, and grid security by reducing revenue losses and promoting equitable energy distribution

V. System Design

A. System Architecture

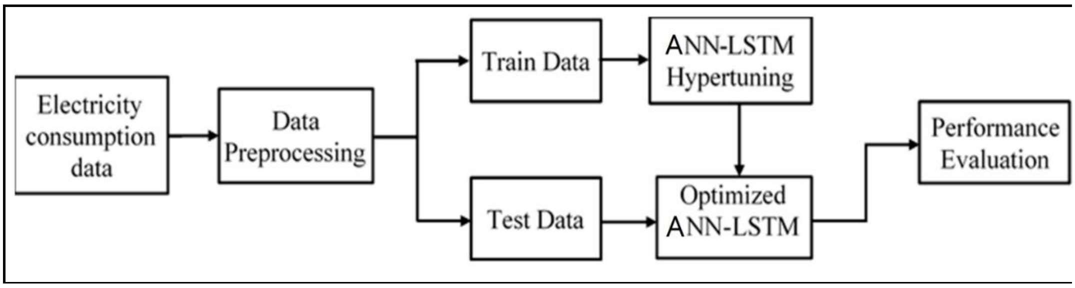

Fig. 1.System Architecture

B. Proposed System

The proposed system seeks to revolutionize electricity theft detection within smart grids by harnessing the power of advanced artificial neural networks (ANNs). This comprehensive solution encompasses data processing, model development, training, real-time monitoring, and performance evaluation. Initially, data collected from smart meters, including historical consumption patterns and real-time readings, undergoes preprocessing to ensure compatibility with the ANN model. The heart of the system lies in the ANN architecture, meticulously designed to handle complex consumption patterns and identify anomalies indicative of theft. Through iterative training and optimization, the model's parameters and hyper-parameters are fine-tuned to achieve heightened accuracy in detecting instances of electricity theft while minimizing false alarms. Integrated into a real-time monitoring system, the trained ANN continuously analyzes incoming smart meter data streams, promptly alerting utility companies upon detecting potential theft instances. The system's performance is rigorously evaluated using established metrics, including accuracy, precision, recall, and F1-score, providing quantifiable evidence of its effectiveness.

Additionally, a comparative analysis with traditional methods underlines the superiority of the ANN-based approach. Ultimately, the expected outcomes encompass improved accuracy, reduced false alarms, real-time monitoring capabilities, scalability, and a significant technological advancement in the domain of critical infrastructure security. By

DOI: 10.48175/568

contributing to enhanced grid security, financial integrity, and equitable energy distribution, the proposed system holds the potential to transform the landscape of smart grid operations.

VI. CONCLUSION

In this proposed system, a novel ANN model is presented to detect electricity theft. In this model, the ANN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Because a large number of parameters must be optimized that increase the risk of overfitting, a fully connected layer with a dropout rate of 0.4 is designed during the training phase. In addition, the SMOT algorithm is adopted to overcome the problem of data imbalance. Some machine learning and deep learning methods such as SVM, RF, GBDT, and LR are applied to the same problem as a benchmark, and all those methods have been conducted on SEAI and LCL datasets. The results indicate that the proposed CNN-RF model is quite a promising classification method in the electricity theft detection field because of two properties: The first is that features can be automatically extracted by the hybrid model, while the success of most other traditional classifiers relies largely on the retrieval of good hand-designed features which is a laborious and time-consuming task. The second lies in that the hybrid model combines the advantages of the RF and ANN, as both are the most popular and successful classifiers in the electricity theft detection field.

Since the detection of electricity theft affects the privacy of consumers, the future work will focus on investigating how the granularity and duration of smart meter data might affect this privacy. Extending the proposed hybrid CNN-RF model to other applications (e.g., load forecasting) is a task worth investigating.

VII. ACKNOWLEDGMENT

We would also like to show our gratitude to*, Prof. H. R. Agashe (Professor, department of Information Technology, Matoshri College of Engineering and Research Center, Nashik, Maharashtra, India.)* for sharing their pearls of wisdom with us during the course of this research. We are also immensely grateful to him for his comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

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-attacksin AMI networks,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.

[8]. 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]. 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]. Diahovchenko, M. Kolcun, Z. Čonka, V. Savkiv, and R. Mykhailyshyn, ‘‘Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads,’’ Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 44, no. 4, pp. 1319–1333, Dec. 2020.

[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/ ElectricityTheftDetection

[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.

DOI: 10.48175/568