ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

ELECTRICITY THEFT DETECTION IN POWER GRIDS WITH DEEPLEARNING AND RANDOM FORESTS

[1]MR. RAMA BHADRA RAO MADDU, [2]CHEGONDI RAJEEV SAI

[1](Associate Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Power grids are severely damaged by energy theft, which impacts power supply quality and decreases operational profitability; this is one of the main sources of nontechnical losses (NTLs) in distribution networks. This research presents a new model for automated detection of energy theft that combines convolutional neural networks with random forests (CNN-RF). This model aims to assist utility companies in addressing the issues of wasteful electricity inspection and irregular power use. This model's first step is to train a convolutional neural network (CNN) using down sampling and convolution to learn features from large, dynamic smart meter data sets that fluctuate over time and across days. The backpropagation method is used to update the network parameters during training, and a dropout layer is introduced to reduce the danger of overfitting. Then, to determine whether the customer has committed power theft, the characteristics are used to train a random forest (RF). The hybrid model's RF is constructed using the grid search technique, which is used to find the best parameters. The results of the studies, which are based on actual data on energy use, demonstrate that the suggested detection model is more accurate and efficient than competing approaches.

1.INTRODUCTION

Companies that generate, transmit, and distribute electricity throughout the globe confront a serious challenge: energy loss. There are two common types of energy losses: technical losses (TLs) and

nontechnical losses (NTLs) [1]. A transmission loss (TL) occurs naturally during electricity transmission and is produced by internal processes in power system components like transformers and transmission lines [2]. A net transmission loss (NTL) is the difference between total losses and TLs and is almost always the result of power theft. Interestingly, the majority of electrical thefts involve physical assaults such as line tapping, meter breaking, or altering with meter readings [3]. As a result of these fraudulent practices, power firms can see a decline in their income. Theft of electrical power, for instance, is believed to cost the US economy some $4.5 billion annually [4]. More than $20 billion is lost annually by utility providers due to energy theft [5]. The security of the power grid is also compromised by acts of electrical theft. Electricity theft, for example, may put a strain on electrical infrastructure, which can create fires and endanger the public. Consequently, the security and reliability of the power system depend on reliable methods of detecting energy theft. Our ability to identify instances of energy theft has been greatly enhanced by the introduction of the advanced metering infrastructure (AMI) in smart grids. This has allowed power companies to acquire large volumes of data on electricity use from smart meters on a frequent basis [6, 7]. The AMI network does, however, provide a new vector for electrical theft assaults, thus there are two sides to every coin. Digital tools and cyber assaults are only two of the many ways that these AMI attacks may be initiated. The main ways that power theft may be detected include manually looking for unlawful line diversions, comparing malicious meter data with benign ones, and inspecting faulty gear or equipment. When checking every meter in a system, however, these approaches become prohibitively expensive and time-consuming. After all, these manual methods won't protect you against cybercriminals. Several solutions to the aforementioned issues have been proposed in recent years. Primarily, these approaches may be classified as either state-based, game-theory-based, or AI-based models.Using specialized hardware, including wireless sensors and distribution transformers, is the foundation of state-based detection [9 to 11]. Unfortunately, these approaches aren't always practical

since they need the collection of system topology and extra physical data in real-time, which isn't always possible. A game-based detection technique constructs an electrical utility vs. theft game and uses the game's equilibrium to determine distributions of normal and abnormal behaviors. Their method for decreasing energy theft is both inexpensive and reasonable, as described in [13]. Even yet, it remains difficult to formulate the utility function of all participants, including regulators, distributors, and thieves. Methods that rely on artificial intelligence include deep learning and machine learning. According to what is shown in [14–17], there are two main types of machine learning solutions: classification models and clustering models. Though the aforementioned ML detection algorithms are impressive and novel, their results are insufficient for practical use at this time. To illustrate the point, as dealing with high-dimensional data becomes more challenging, the majority of these methods resort to manual feature extraction. Statistics such as consumption maximum and minimum, as well as standard deviation and mean, are examples of classic hand-designed features. Extracting 2D characteristics from smart meter data manually is a laborious and time-consuming technique that fails to capture these properties.In [18], the authors examined the use of deep learning approaches for detecting electrical theft. They compared several deep learning architectures, including CNNs, LSTM RNNs, and stacked autoencoders. The use of synthetic data in the detector performance evaluations, however, precludes any valid comparisons to shallow systems. Not only that, but the authors of [19] suggested a customer-specific detector based on deep neural networks (DNNs) that can effectively foil these types of cyberattacks. Recent years have seen widespread usage of CNN for generating discriminative and useful features from raw data across several domains [20, 22]. These uses drive the CNN's use in power theft detection, where it is used to extract features from high-resolution smart meter data. An analysis of smart grid power theft was conducted using a broad and deep convolutional neural network (CNN) model in [23].As with any standard SLFN trained using the backpropagation technique, the softmax classifier layer in a basic CNN is identical [24]. First, when the SLFN runs the

backpropagation method, its generalization performance will suffer due to overtraining. The backpropagation method, in contrast, is hypersensitive to training error minima since it relies on empirical risk reduction. Despite CNN's impressive performance in feature extraction, it is not always the best choice for classification due to the softmax classifier's shortcomings, as shown above. In light of this, the search for a superior classifier that can fully use the information acquired and has capabilities comparable to the softmax classifier is essential. The random forest (RF) classifier is able to circumvent the softmax classifier's shortcomings by using two robust machine learning techniques: bagging and random feature selection. Our new convolutional neural network-random forest (CNN-RF) model for detecting power theft is inspired by these specific efforts.

Electricity theft detection models rely on convolutional neural networks (CNNs) to automatically extract certain characteristics of consumers' consumption behaviors from smart meter data. Swapping out the softmax classifier that uses extracted features to identify consumer trends with the RF improves detection performance. Actual data from all of Ireland's and London's power utility consumers was used to train and test this model.

2.LITERATURE SURVEY

The research paper focuses on addressing the issue of electricity theft in power grids, which results in significant financial losses and disruptions in power supply. To tackle this problem effectively, the author proposes a novel approach that combines Convolutional Neural Networks (CNN) and Random Forest algorithms. By leveraging the power of CNNs, the model can learn and extract relevant features from the power consumption data. These features capture patterns and abnormalities that indicate potential instances of theft. The CNN is trained to distinguish between periods of normal energy usage and those associated with theft, assigning a label of 0 or 1 accordingly.To further improve the location precision, the creator incorporates the CNN with Irregular Woods, a flexible and hearty AI calculation. The Arbitrary Backwoods calculation uses a group of choice trees, which collectively make predictions based on the extracted features from the CNN. This combination improves the overall

prediction accuracy compared to using either algorithm individually.The proposed model goes through a training phase using labeled data, where patterns of energy theft and normal energy usage are learned. The model is then evaluated and tested on real-world energy consumption data to assess its effectiveness. The results demonstrate that the combined CNN-Random Forest model outperforms traditional algorithms in accurately identifying instances of electricity theft. This innovative approach offers a more efficient and reliable method for utility companies to detect and mitigate energy theft, thereby minimizing financial losses and ensuring a stable power supply

3. EXISTING SYSTEM

Traditional methods rely on manual inspection and periodic audits to detect electricity theft. Lack of real-time monitoring leads to delayed detection and response to theft incidents.Limited effectiveness in identifying sophisticated theft techniques, leading to revenue loss for utility companies. High relianceon human expertise andresourceintensive processes. Inefficient use of resources due to false alarms and inaccurate detection.

DISADVANTAGES:

Existing systems for detecting electricity theft suffer from several disadvantages. These include reliance on manual inspection and periodic audits, lack of real-time monitoring leading to delayed detection, limited effectiveness in identifying sophisticated theft techniques, high reliance on human expertise, resource-intensive processes, and inefficient use of resources due to false alarms and inaccurate detection. These drawbacks contribute to revenue loss for utility companies and hinder efforts to combat electricity theft effectively.

3.1 PROPOED SYSTEM:

Enhancing energy theft detection in power grids, the suggested method employs state-of-the-art machine learning techniques, particularly deep learning and random forests. The system's goal is to enhance the efficacy and precision of theft detection by using these algorithms to circumvent the shortcomings of conventional approaches.

ADVANTAGES:

Systematic analysis ensures fine-tuning for optimal detection accuracy and efficiency.Careful feature engineering

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

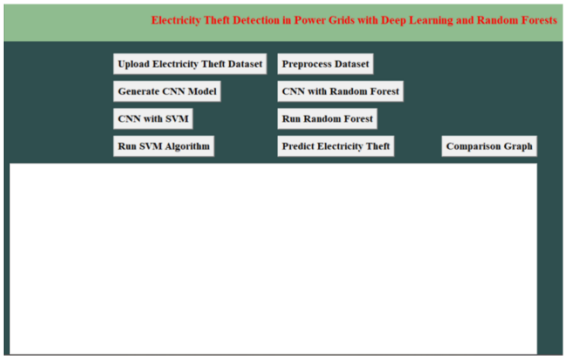
www.ijasem.org

Vol 18, Issue 2, 2024

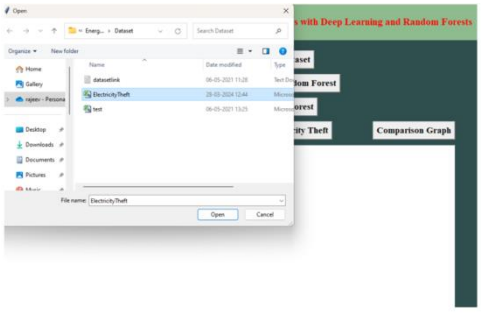
focuses on relevant indicators, reducing false alarms. Integration of diverse algorithms enhances detection capabilities.Designed for real-time data handling, enabling prompt response to theft incidents.

4. OUTPUT SCREENS

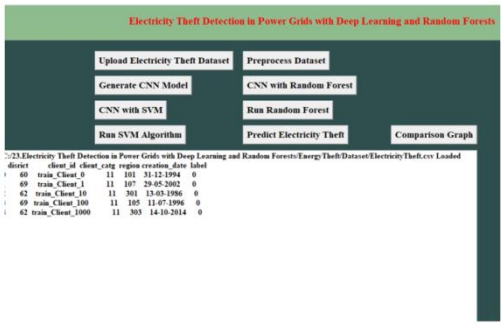
Home Page:



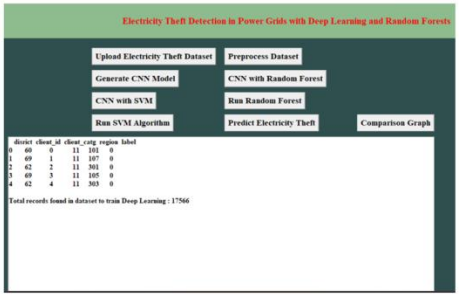
Upload Data Set:



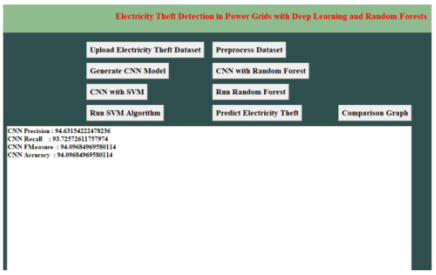
Data Extracted From Dataset:



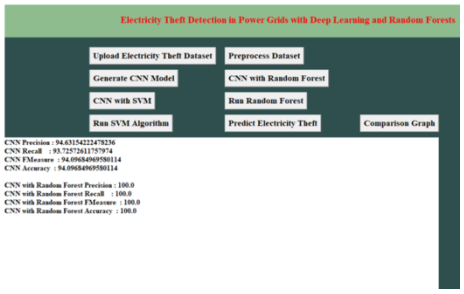
Preprocessing:



CNN Model:



CNN With Random Forest:



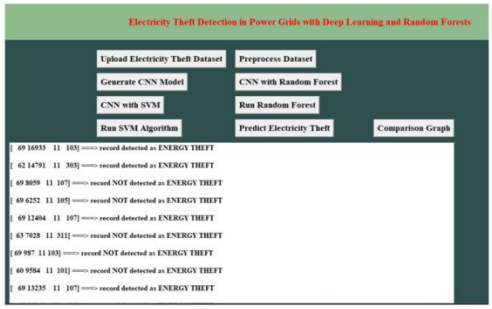
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

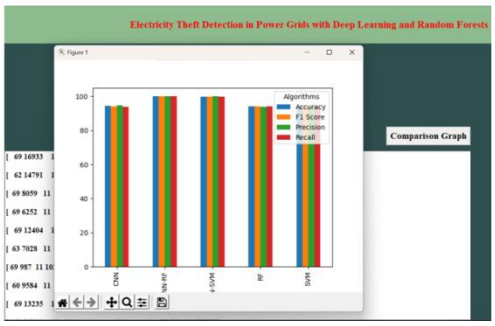
www.ijasem.org

Vol 18, Issue 2, 2024

Predict The Output:



Visulaization Bars:



5. CONCLUSION

To identify power theft, this research introduces a new CNN-RF model. Within this framework, the convolutional neural network (CNN) functions as an automated feature extractor when delving into smart meter data, while the RF serves as the output classifier. We create a fully connected layer with a dropout rate of 0.4 during training since optimizing a large number of parameters increases the danger of overfitting. Additionally, the issue of data imbalance is addressed by using the SMOT algorithm. For the sake of comparison, the same issue has been tested on the SEAI and LCL datasets using a variety of ML and DL techniques, including support vector machines (SVMs), radial basis functions (RFs), gradient descent techniques (GBDTs), and linear regression (LR). According to the findings, the suggested CNN-RF model has two qualities that make it a potentially useful classification approach for detecting energy theft: The first is that, unlike most other conventional classifiers, the hybrid model can automatically extract features. This is in contrast to the tedious and time-consuming process of retrieving well-designed features by hand. Second, as RF and CNN are two of the most widely used and effective classifiers for detecting power theft, the hybrid model takes advantage of both of their strengths.Since customers' privacy is at stake in the fight against power theft, researchers will soon be looking at the effects of smart meter data granularity and duration on consumers' privacy. It might be wise to look at ways to adapt the suggested hybrid CNN-RF model for use in other contexts, such as load forecasting.

6.REFERENCES

[1] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: overview, issues, prevention and a smart meter based approach to control theft," Energy Policy, vol. 39, no. 2, pp. 1007–1015, 2011.View at: Publisher Site | Google Scholar

[2] J. P. Navani, N. K. Sharma, and S. Sapra, "Technical and non-technical losses in power system and its economic consequence in Indian economy," International Journal of Electronics and Computer Science Engineering, vol. 1, no. 2, pp. 757–761, 2012.View at: Google Scholar

[3] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1319–1330, 2013.View at: Publisher Site | Google Scholar

[4] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security & Privacy Magazine, vol. 7, no. 3, pp. 75–77, 2009.View at: Publisher Site | Google Scholar

[5] T. B. Smith, "Electricity theft: a comparative analysis," Energy Policy, vol. 32, no. 1, pp. 2067–2076, 2004.View at: Publisher Site | Google Scholar

[6] J. I. Guerrero, C. León, I. Monedero, F. Biscarri, and J. Biscarri, "Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection," Knowledge-Based Systems, vol. 71, no. 4, pp. 376–388, 2014.View at: Publisher Site | Google Scholar

[7] C. C. O. Ramos, A. N. Souza, G. Chiachia, A. X. Falcão, and J. P. Papa, "A novel algorithm for feature selection using harmony search and its application for non-technical losses detection," Computers & Electrical Engineering, vol. 37, no. 6, pp. 886–894, 2011.View at: Publisher Site | Google Scholar

[8] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: a surveyficial intelligence: a survey," International Journal of

Computational Intelligence Systems, vol. 10, no. 1, pp. 760–775, 2017.View at: Publisher Site | Google Scholar

[9] S.-C. Huang, Y.-L. Lo, and C.-N. Lu, "Non-technical loss detection using state estimation and analysis of variance," IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 2959–2966, 2013.View at: Publisher Site | Google Scholar

[10] Rahmati, H. R. Pourghasemi, and A. M. Melesse, "Application of GIS-based data driven random forest and maximum entropy models for groundwater potential mapping: a case study at Mehran region, Iran," CATENA, vol. 137, pp. 360–372, 2016.View at: Publisher Site | Google Scholar

[11] N. Edison, A. C. Aranha, and J. Coelho, "Probabilistic methodology for technical and non-technical losses estimation in distribution system," Electric Power Systems Research, vol. 97, no. 11, pp. 93–99, 2013.View at: Publisher Site | Google Scholar

[12] J. B. Leite and J. R. S. Mantovani, "Detecting and locating non-technical losses in modern distribution networks," IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1023–1032, 2018.View at: Publisher Site | Google Scholar