International Transactions on Electrical Engineering and Computer Science
Rajeev Kumar et.al., Vol: 3, No: 2, pp: 109-119, June 2024

Electricity Theft Detection for Smart Grid Security using Smart Meter Data: A Deep Learning - CNN based Approach

Rajeev Kumar[1], Malvika Chauhan[2], Dushyant Kumar[3], Raj Kumar Verma[2]

Abstract: Not only can theft of energy result in monetary losses, but it also results in expenses that are not technical for energy providers and even for the power infrastructure. Theft of energy has a detrimental effect on both the financial viability and the quality of the electricity. Through the integration of information and energy flows, smart grids have the potential to avoid power theft. The analysis of data from smart grids makes it easier to identify instances of power theft. In contrast, previous systems fared badly when it came to detecting instances of energy theft. To help and assess energy supply businesses in decreasing the barriers of low energy, unexpected power use, and poor power management, we presented in this study a method to detect electricity theft based on consumption data from smart meters. This was done in order to assist and evaluate energy supply businesses. More specifically, the Deep CNN model is able to successfully accomplish two tasks: it differentiates between periodic and non-periodic energy while maintaining the overall features of the power consumption dataset. When it comes to detecting instances of energy theft, the results of the tests indicate that the deep CNN model displays the highest level of accuracy and exceeds prior versions.

Keywords: Electricity theft, Economic losses, Smart meter, Convolutional neural networks, Power consumption.

1. Introduction

When it comes to modern life, electricity is very necessary. Throughout the operations of power production, transmission, and distribution, there is a significant amount of energy which is lost. Technical losses (TLs) and non-technical losses (NTLs) are the two categories that are used to categorize what are known as electrical losses [1].

Article History
Received: 11-11-2023; Revised: 15-05-2024;
Accepted: 18-05-2024

✉ Dushyant Kumar
dushyant27seemar@gmail.com

[1]Department of Electrical Engineering, Dev Bhoomi Uttrakhand University, Dehradun - 248007, India
[2]Department of Electrical Engineering, Roorkee Institute of Technology, Uttarakhand - 247668, India
[3]SME at Tata Technologies Ltd, India

One of the most prevalent types of losses that are not technical is theft of electricity. The manipulation of the electrical meter, interference with the reading, and dodging it are all examples of common examples of improper behavior [2]. An increase in energy consumption, an undue demand placed on electrical systems, significant income losses for the power company, and potential threats to public safety are all potential outcomes of electricity theft. Network-oriented methodology, data-oriented approach, and hybrid strategy that combines the two techniques are the three sorts of methodologies that may be used for the purpose of detecting power theft [3]. The network architecture has to be adjusted on a regular basis in order to accommodate the implementation of network- and hybrid-oriented solutions [4-5], as well as the introduction of new devices [6]. Because of the high cost of installing new devices and the fact that security concerns restrict access to the network architecture, it is exceptionally challenging to apply these principles on a widespread scale.

https://doi.org/10.62760/iteecs.3.2.2024.87

It is possible to increase the efficiency of the identification and evaluation of suspected power theft by using data-driven solutions. These solutions focus only on the data that is supplied by smart meters and do not take into account network architecture or other devices. This has led to an increase in the number of people using data-driven tactics to identify instances of power theft [7]. A "smart grid" is a hybrid system that integrates conventional electrical networks with communication technologies that are automated. The findings of previous studies [8-11] suggest that a smart grid might potentially enhance the efficiency of electrical energy use. Both medium- and short-term storage are used by the smart grid network, in addition to the transactive power architecture [12]. Methods for predicting the demand for electricity [13] are now being developed in order to make the most efficient use of the resources that are already available. It is suggested by the authors of [14] that a multilayer power distribution system be implemented in order to reduce the negative effects of peak demand while simultaneously enabling the interchange of more power at a lower cost. Reducing the unexpected behavior of sustainable electricity is accomplished by the use of a method that is based on the information gap choice theory [15]. The transmission of data between the power grid and individual energy users is accomplished via a smart meter.

Utility companies began gathering massive volumes of data on the energy use of customers from smart meters as they introduced enhanced metering technologies in grids. This made it possible for us to spot fraudulent activities [16]. In spite of this, the AMI network has the potential to be used for a variety of different power theft schemes. There are a variety of methods that may be used to carry out attacks against AMI, including the utilization of technological tools and cyberattacks. Detecting power theft may be accomplished by human inspection in two different ways: by addressing line irregularities and by locating gear or equipment that is broken or not performing properly. In spite of the fact that these methods are necessary for doing a comprehensive inspection of each and every meter in a system, they are also time-consuming and expensive. The categorization of data using machine learning has recently captured the attention of a lot of people, despite the fact that firms that provide electrical utilities routinely collect enormous volumes of data. The privacy of customers is secured throughout the process of evaluating data on daily usage in order to identify tendencies of theft [17]. In the studies [18-19], support vector machines were used to cluster and categorize data in order to identify

There is a high prevalence of anomalies and inconsistencies. This technique has the potential to forecast and identify any energy consumption profile. This is due to the fact that clustering is often used in algorithms as both a primary and secondary phase. Because neural networks are so efficient at identifying instances of power theft, a growing number of academics and researchers are adopting them as their primary method of investigation. The proliferation of grid assaults is a direct result of the development of the internet. According to [20], the identification of non-technical losses (NTLs) in electrical utilities is accomplished by the use of support vector machines (SVMs), which are a kind of artificial intelligence technology. Fuzzy classification, which employed the Euclidean distance to the cluster center as a criterion, was one of the unsupervised methods that were applied in [21]. A device that is used to measure distance. An artificial neural network (ANN)-based system was used in [22] to examine attributes and identify fraudulent clients via the utilization of a wavelet-based approach. Using support vector machines (SVM) and XGBoost, the authors of [23] developed a method for determining the non-technical losses that occur inside the energy system. An evaluation of consumers using information obtained from smart meters and a supporting dataset is the primary objective of the research that has been presented. Make use of the XGBoost in order to improve the accuracy of categorization. Combining an artificial neural network (ANN) with a support vector machine (SVM) to produce a hybrid algorithm was shown to be an effective way for detecting fraudulent activity in smart grid systems [24]. LSTM, which stands for long short-term memory, is used in conjunction with bat-based random under-sampling boosting in the technique described in [9]. When attempting to recognize anomalous patterns and make adjustments to parameters, the bat-based LSTM and RUSBoost are used. In order to successfully detect instances of energy theft in time-series data, the authors [8] used a CNN-LSTM combination in conjunction with the power usage pattern. It provides a description of an end-to-

end hybrid neural network that is able to evaluate sequential as well as non-sequential input, such as geographic data. Deep learning algorithms have overtaken traditional machine learning approaches in a range of applications, including image analysis, computer vision, and speech recognition, amongst others. During the development process, deep learning algorithms are applied because of their ability to handle and regulate vast amounts of data, extract features from the data, and categorize the data.

Managing data from smart meters and smart grids is a need for models. A approach that makes use of a convolutional neural network (CNN) model that is both big and deep. The deep CNN component is responsible for identifying patterns of power use, while the shallow CNN component is responsible for capturing data properties in general. Hybrid deep learning algorithms have always been the method of choice for load forecasting. Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) architectures were used in a model that was built by researchers in order to improve their ability to forecast future demand demands. It has been shown that the new models performs much better than the old strategies. In order to solve the challenge of recognizing instances of energy theft in the field, the authors of [5] constructed three classifiers that were based on gradient boosting.

The Intelligent Grid. By using the technique that has been presented, it is possible to conduct a comprehensive and objective analysis of the relative performance of numerous different classifiers in recognizing instances of theft. A threat model that is based on an attack tree was used in the study that was presented in order to explain how energy theft expresses itself in smart meters. In addition, wireless networks are used in articles in order to detect and alert on energy theft. Both of these studies provide a comprehensive description of the approaches that are now in use. Theft of electricity may be detected via AMI. There is a correlation between the quality of the data that is entered and the performance of machine learning and deep learning models. There are already available energy theft detecting technologies that provide good results. These approaches, on the other hand, have a number of shortcomings, which are detailed below.

- When using machine learning techniques in ETD, one of the most difficult challenges is the processing of unstable data. Without resorting to more conventional methods, this problem cannot be resolved.
- Incorrect values in the data that is provided often result in a decrease in classification consistency.
- Traditional energy theft detection systems are heavily dependent on human intervention, and standard machine learning algorithms struggle to comprehend massive volumes of data.
- Despite this, it will be more expensive because it will require paying people to examine massive amounts of data. The study does not take into account a wide range of non-criminal elements that may be involved.

There are a number of factors that might alter use patterns, including weather and seasonality, the installation or removal of an appliance, changes in resident status, weekends, and holidays. It is possible that normal acts that result in a sudden change in load form might be misunderstood as behaviors that are unacceptable. As a result of this accuracy flaw, there is a possibility that a significant number of false-positive findings may be obtained. In this study, a potential solution to the problem of real-time energy theft is investigated. If successful, this technology might assist both consumers and energy corporations in leading healthier lifestyles. During the course of this research, we used a preprocessing strategy on the dataset pertaining to power consumption in order to develop a deep CNN model for the purpose of handling the classification issue. Because of this, we decided to detect energy theft by using a deep convolutional neural network (CNN) structure in conjunction with data augmentation. This was accomplished by studying the irregular and anomalous consumption habits of individuals. The new technology may allow power providers to detect power outages and minimize energy usage by evaluating data about customers' actual energy use in real time. This might be accomplished via the utilization of the new technology. Anyone who intentionally takes energy might potentially gain from the strategy that has been recommended. The usefulness of the proposed solution was validated by the findings of a number of rigorous

tests that used real-time data from smart meters belonging to customers.

The other parts of the paper are arranged as follows. Section 2 provides the brief discussion about the proposed methodology, section 3 talks about the results and in section 4 the conclusion points are discussed.

2. Proposed methodology

In this study, a deep convolutional neural network (CNN)-based technique is used to detect instances of energy theft in smart grids. The goal of Deep CNN is to identify fundamental characteristics and categorize them as either theft-related or non-theft-related. Fig. 1 illustrates the methodology that is being offered in its structure. The suggested method for determining whether or not power theft had occurred comprised of three primary stages. (1) Creating data for training and testing; (2) Preprocessing and evaluating the data that has been collected. Using CNN for deep feature extraction and classification comes in third. The following aspects should be addressed in the proposed technique:

2.1 Data pre-processing and analysis

It was the records of energy use of 45970 residential and industrial clients that provided the source of the data. During a period of ten minutes, data on the amount of electricity that was used was collected by a smart meter. For the purpose of developing the experimental dataset, data on electricity consumption from May 2018 to April 2020 were blended together. An implantable smart meter was placed in each and every participant in the trial who gave their consent. There are now 17% of all customers that are considered to be power thieves, according to the data. Both law-abiding residents and those who steal electricity have different patterns of energy usage. When compared to the second, the first is a typical consumer, while the second is a power thief. The most important finding was that the patterns of power use differed between typical and non-typical customers. In comparison to the consumption patterns of a typical user, the conduct of an atypical user, often known as an electrical thief, is drastically different. For their participation in the project, customers were given a smart meter in exchange for their consent. Because of this, it is safe to conclude that all of the samples were obtained from consumers who can be relied upon. However, malicious samples cannot be collected since an individual user may never or only sometimes suffer energy theft. This makes it impossible to collect malicious samples. In order to train, it is necessary to utilize a substantial amount of data from a variety of categories.

CNN so that it may provide a classification result that is acceptable. In order to increase the number of picture samples, activities that include image processing make use of a range of different ways. In comparison to traditional datasets, realistic datasets have a lower number of instances of power theft since the majority of users do not steal energy. There is a possibility that an unequal dataset could result in poor classification accuracy or overfitting, which will ultimately lead to low prediction accuracy.

The creation of 8765 hostile consumers was accomplished via the use of data augmentation in this project. According authors, in order to solve the problem of imbalance between the two. This dataset is a very significant resource for smart meter research due to the fact that it has a big sample size, a diverse user base, and a lengthy period of observation. A new sample period of half an hour is provided to each individual customer. In order to demonstrate why a CNN should be used for feature extraction, this part undertakes an analysis of data obtained from smart meters. Data cleaning, missing value interpolation, and data normalization are the three fundamental approaches that are used in the pre-processing of raw energy consumption data.

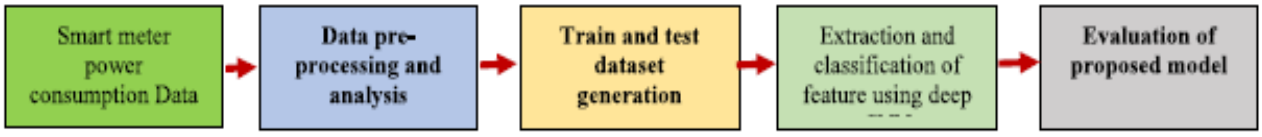

Fig. 1: Framework of the proposed electricity theft detection method.

Although there have been significant changes made to them, the load files are relatively comparable to one another. This means that the filter weights in a CNN remain the same from one area to the next. As a direct result of this, the anticipated traits associated with the convolutional layer are resistant to minute modifications. The use of variations makes it possible to obtain generally stable characteristics from a wide variety of load patterns. The performance of machine learning and deep learning algorithms is affected by the consistency of the data that is supplied. The effectiveness of the model is directly impacted by the degree of precision of the data that is obtained during the pre-processing step. Variations in load consumption may be attributed to a variety of uncontrollable variables, including lifestyle, seasons, and weather. The load profiles of consumers are affected by a number of different elements, such as the weather and the kind of consumer. Detailed information on the dataset can be found in Table. 1.

2.2 *Training and testing dataset generation*

After doing preliminary research, it has been shown that demographics and other variables, in addition to the weather, have a substantial impact. These modifications are made to the electrical load profiles of individual users. As a result of the large daily swings in energy consumption, it may be challenging to derive features just from data pertaining to one-dimensional power use. To determine whether or not the previously described technique is successful, the cross-validation method divides the pre-processed dataset into two distinct datasets: the train dataset, which contains 75% of the train set, and the test set, which contains 25% of the train set. On a dataset that has a large number of power thieves in comparison to lawful consumers, it is possible that deep learning and machine learning algorithms will have difficulty performing well. Although the train dataset is used for the purpose of training the parameters of the model, the test dataset is utilized to assess the model's capacity to generalize to fresh customer samples.

2.3 *Extraction and classification of feature using deep convolutional neural network*

Through the use of convolution and pooling methods, the deep CNN model was able to acquire features from a vast and diverse dataset consisting of smart meter readings collected at various times throughout the day. Deep convolutional neural networks (CNNs), such as the one seen in Fig. 2, are constructed by combining convolutional and pooling layers. The CNN is a sophisticated neural network that learns by the use of the Adam optimizer. An architecture for supervised learning that include a number of levels. For the purpose of generating feature descriptions and mitigating the impacts of external distortion, convolutional layers are effectively used. In order to generate a wide range of feature maps, the convolutional layer makes use of a number of different feature filters. The proliferative capacity of neurons in normal brain networks is limited due to the fact that these neurons are linked. As a result of the fact that it connects each neuron to its neighbors, CNN has the potential to transcend the limitations of conventional neural networks. Periodic patterns are generated by a 2-D convolution layer using the 2-D power usage data that is supplied into the layer. The notion of pooling is the primary foundation around which CNNs are built. CNNs are often applied in the middle of two convolutional layers. Because there are fewer factors to take into consideration, the data becomes easier to interpret and handle.

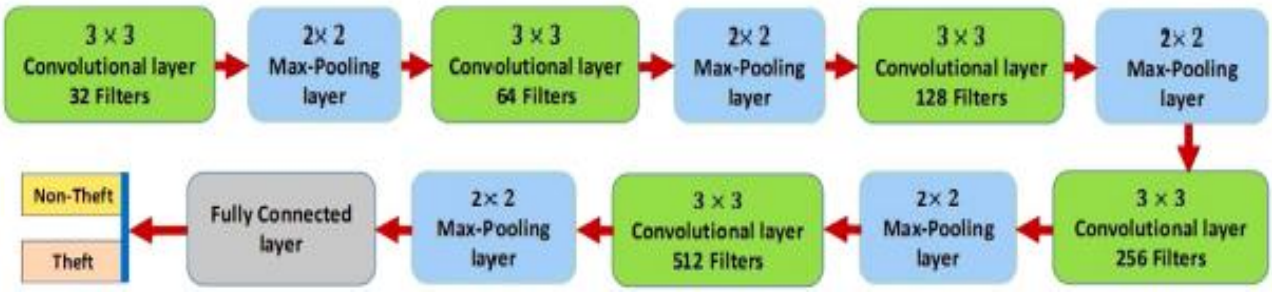

Fig. 2: CNN architecture used in the proposed method

A feature vector in the pooling layer is correlated to the map that was generated by the convolutional layer that came before it. Since the size of the output feature map is decreasing, the number of output feature vectors that are included inside the pooling layer remains unchanged. In convolutional neural networks (CNN), the pooling layer is often used to reduce the quantity of training weights and filters, as well as the number of parameters and features that are not required for the job at hand. Another strategy that may be used to prevent overfitting is the pool layer. Utilizing the maximum operation, sometimes known as max, is a common approach to acquiring resources. It is necessary for the pooling layer to collect input from each domain before it can determine which domain currently has the highest value. Those that cover the pooling filter. Additionally, the maximum pooling method is used in the course of this inquiry. As a result of its sparsity and its capacity to lower gradient, LReLU is used as an activation function in the deep CNN model that is being considered in this study. The stack that is formed by the output of the pooling layer is the one that is introduced into this fully linked layer. Following this, the classification result is generated by using the softmax activation function, which, when applied to two-class classification, yields a number that represents the likelihood of two classes. In situations when there is a greater likelihood of involvement in energy theft compared to situations in which the data is normal, the input is given the appropriate marking.

Table. 1: Data set preparation

Description	Value
Collecting data time slot	1 May 2018 - 30 April 2020
Data type	Time series data
Data resolution	Smart meter data in high resolution
Total customers	45970
Ordinary users	38155
Power thieves	7815

3. Experimental results

In order to assess the suggested method, a real dataset consisting of the daily consumption of 45970 consumers was employed during a period of two years, beginning on May 1, 2018, and ending on April 30, 2020. The findings unequivocally demonstrate that there is a disparity, since just 17% of the Eighty-three percent of the clients who utilize the data are regular users, while the remaining customers are predators. Python 3.7.4 is installed on a standard personal computer that has a 3.40 GHz Intel Core i7 processor and 16.0 GB of random access memory (RAM). TensorFlow is used in order to establish the architecture of the model. An evaluation of the effectiveness of the suggested method is carried out with the help of the confusion matrix. The area under the curve (AUC), F1 scores, ROC curves, mean squared error (MCC), accuracy, recall, and other critical performance metrics may all be computed with the use of confusion matrix data. With regard to the suggested model, the confusion matrix is shown in Table. 2. It describes the proposed solutions. Technique is essential for ETD due to the fact that it has a very low percentage of false-positive results. Comparative analysis is performed between the proposed approach and relevant past research and base classifiers for the purpose of further exploration. Based on the results, it is clear that the strategy that was suggested is superior to the ones that are currently being used in every respect.

Table. 2: Proposed model confusion matrix

Detected/Actual	Honest user	Theft user
Honest user	9384	155
Theft user	97	1856

An accuracy indicator known as the True Negative Rate is a measurement that indicates the number of customers who are very reliable that the classifier detected. A metric that is used to evaluate the effectiveness of a classifier is called recall, which is also often referred to as True Positive Rate (TPR). Some measurements of accuracy, such as recall and accuracy, may not be sufficient to offer a good picture of how something works. What kind of performance a model has. Because of the F1-score that was obtained, it is desirable to achieve improvements in both recall and accuracy. When dealing with a binary classification problem that has a skewed class distribution, the F1-score statistic is an excellent choice. The F1-score is calculated by taking the weighted harmonic mean of the memory and accuracy scores. For the purpose of detecting instances of energy theft, the ROC-AUC is an effective indicator. For the purpose of evaluating the model's detection performance, a graphical representation of the model is shown below. In a successful classifier, the ROC-AUC is very close to being equal to one. If all of the factors that are used to

rank MCC are dependable and generate accurate estimates, then MCC will get a high grade to its overall performance. Having a score of zero, a number that is close to one, and a score of one all suggest that the model classification is incorrect, that the class separation skills are inadequate, and that the model categorization is accurate, in that order. These scores range from -1 to 1 on the MCC scale. The CNN classifier starts to be affected by the unequal data, which resulted in a significant false positive rate. We constructed a comparison to illustrate the importance of having balanced data, and Fig. 3 displays that comparison. When the suggested model is applied to data that is skewed, it performs particularly poorly in classification. When applied to the dataset that is not balanced, the CNN model makes errors since it presumes that consumers who are really power thieves are loyal to the company. It has been hypothesized that the classification performance of the CNN model may be improved if the data is consistent.

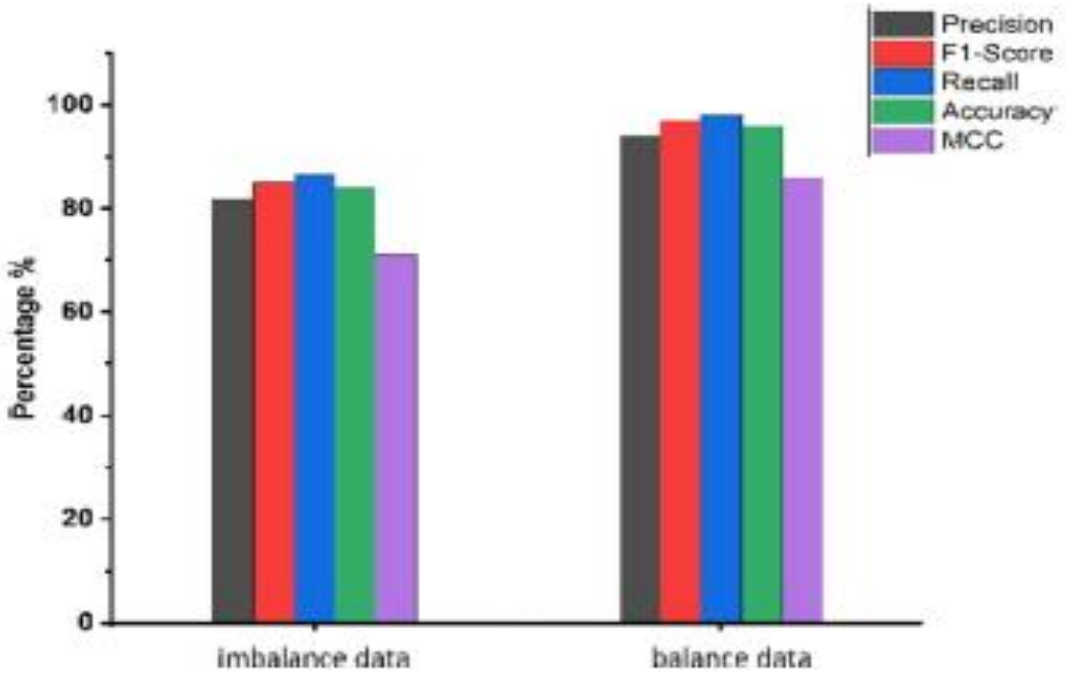

Fig. 3: Efficiency of proposed method using imbalance and balanced data

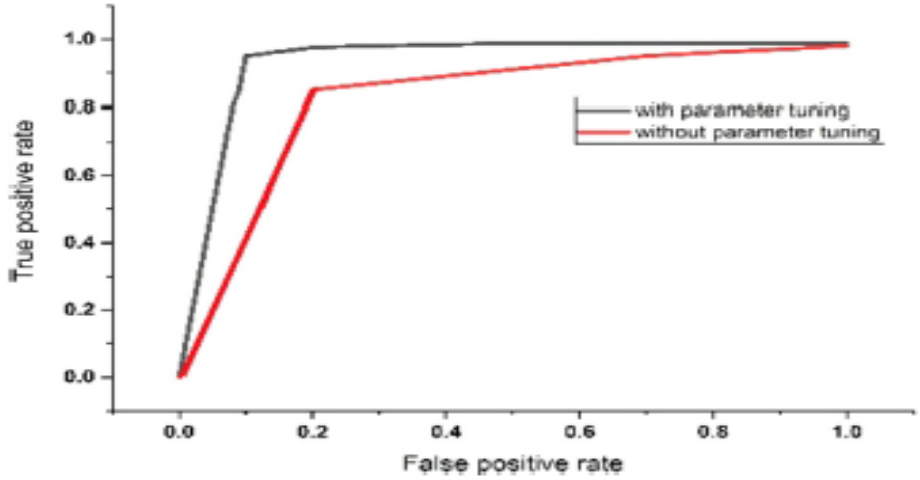

Fig. 4: Analyzing ROC-AUE with and without adjusting parameters

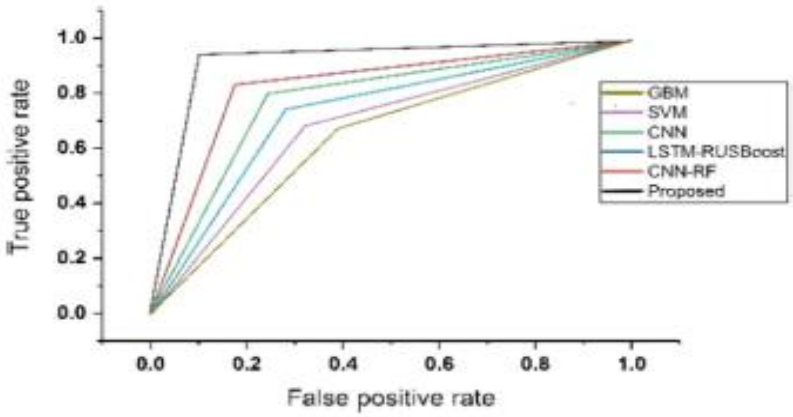

Fig. 5: ROC-AUC based comparison of the state of the art and proposed methods

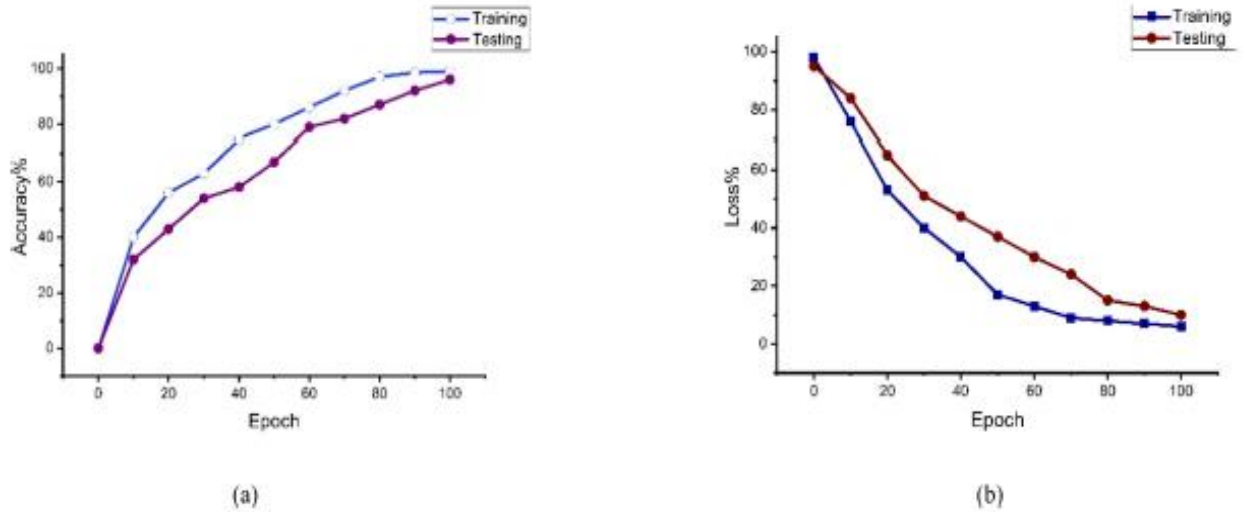

Fig. 6: Evaluation of the developed deep learning based CNN (a) accuracy and (b) Loss

To a large extent, the performance of the suggested model is determined by the values of the hyper-parameters that are used. To achieve a higher level of accuracy in classification, the optimal hyper-parameter values are chosen during the first CNN operation, which is carried out at random. The ROC-AUC representation of the proposed model is shown in Fig. 4, both with and without a change in the value of the hyper-parameter. As a result of our investigation, Fig. 5 illustrates the receiver operating characteristic area under the curve (ROC-AUC) for both our suggested method and the current state of the art. The results of the ROC-AUC indicate that our suggested strategy is superior to the methods that are already in use. Using the findings of this investigation, we came up with an innovative method. The ROC-AUC findings demonstrate that our proposed approach is superior to the most cutting-edge methodologies currently available. A representation of the accuracy (left) and loss (right) of the proposed model can be seen in Fig. 6 (a) and 6 (b). The approach that we have developed makes use of smaller epoch values in order to effectively adapt from high-dimensional datasets; however, this comes at the risk of overfitting. When the number of epochs increases, the accuracy also increases since the amount of test and training losses decreases. These findings highlight the degree of sensitivity that the model presently has. With regard to accuracy, precision, recall, ROC, F1-score, and MCC, Fig. 7 presents a comparison between our suggested technique and the methods that are already in use. CNN-based deep learning methods beat other machine learning techniques such as random forests, logistic regression, and support vector machines when it came to identifying electrical theft. This was the case when compared to other algorithms.

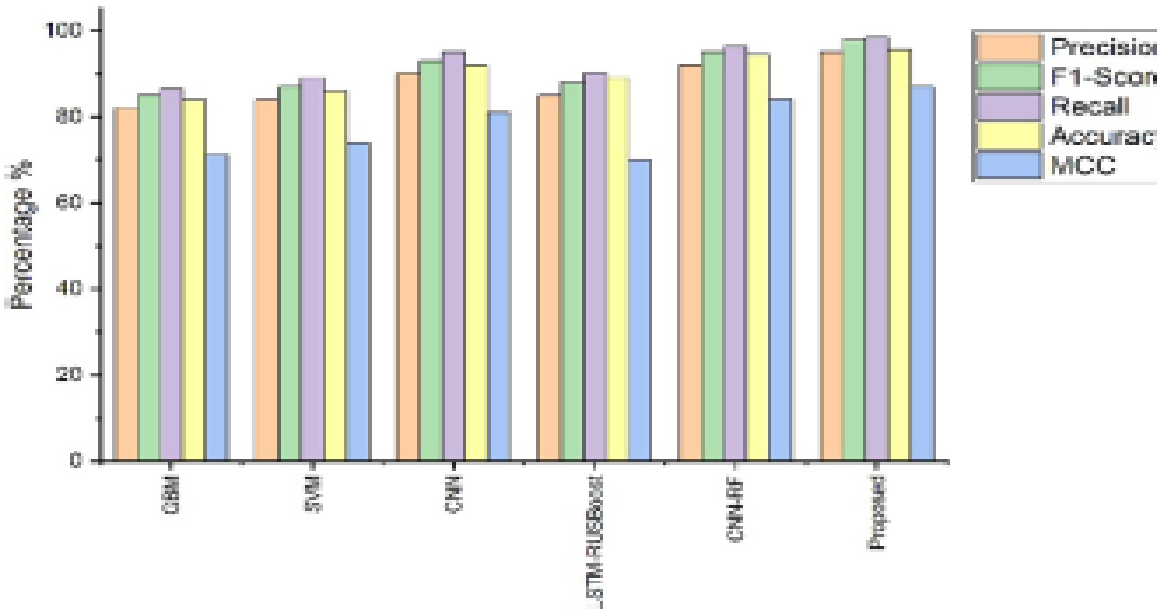

Fig. 7. Performance comparison of Deep-CNN and state-of-the-art.

Through the use of a convolutional neural network, we were able to enhance the accuracy of energy theft detection by collecting information from a variety of power consumption patterns. In addition, the overall performance of the suggested method is superior to that of any other competing models. The technique is essentially anomaly-driven due to the fact that identifying suspicious customers' unusual energy use is necessary for the detection of energy theft. Witnessing Deep CNN's performance would be an incredible experience. It has a high level of performance on the dataset that was used in this inquiry, which suggests that it can be applied to other datasets.

4. Conclusion

For the purpose of identifying instances of power theft, this article presents a deep convolutional neural network model. When it comes to classifying recoverable qualities as either thieves or non-thieves, CNN is applied as an automated feature extractor via its use. In the original, authentic data from the smart meter, there are a number of errors and data points that are missing. In order to solve this issue, we carried out an exhaustive investigation and preliminary data processing, which comprised activities such as normalization and accusation. Overfitting is a potential outcome of several data components; however, the CNN employs a dropout layer to prevent this from occurring. It's possible that machine learning and deep learning algorithms, when applied to the same data, might detect instances of unlawful energy theft. The proposed method, in contrast to the majority of other widely used classifiers, has the potential to automatically extract features, therefore saving both time and effort. A comprehensive testing procedure was carried out on a large number of valid datasets so that we could demonstrate the utility of the proposed application. According to the results of the tests, the proposed technique performs better than other strategies that are available. Based on the statistics, it seems that the ETD model that was suggested is accurate and has a low risk of false-positive diagnosis. We are going to investigate. A method for predicting the possibility of power theft based on short-term use that makes use of unique customer practices. Given the lack of attention that has been paid to this topic, we want to develop a model that is capable of identifying threats that originate from inside the system.

Conflict of Interest

The authors declared "No conflict of interest".

References

[1] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen "Energy-theft detection issues for advanced metering infrastructure in smart grid", *Tsinghua Science and Technology*, Vol. 19, No. 2, pp.105-120, 2014. https://doi.org/10.1109/TST.2014.6787363

[2] 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. https://doi.org/10.1109/JSAC.2013.130714

[3] G. M. Messinis and N. D. Hatziargyriou "Review of non-technical loss detection methods", *Electric Power Systems Research*, Vol. 158, pp. 250-266, 2018. https://doi.org/10.1016/j.epsr.2018.01.005

[4] T. A. Short "Advanced metering for phase identification, transformer identification, and secondary modeling", *IEEE Transactions on Smart Grid*, Vol. 4, No. 2, pp.651-658, 2013. https://doi.org/10.1109/TSG.2012.2219081

[5] 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, 2016. https://doi.org/10.1109/TSG.2016.2574714

[6] M. Z. Gunduz, and R. Das "Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns. *Sensors*, Vol. 24, No. 4, art. no. 1148, 2024. https://doi.org/10.3390/s24041148

[7] P. Glauner, N. Dahringer, O. Puhachov, J. A. Meira, P. Valtchev, R. State and D. Duarte "Identifying irregular power usage by turning predictions into holographic spatial visualizations", *2017 IEEE International Conference on Data Mining Workshops*, pp. 258-265, 2017. https://doi.org/10.1109/ICDMW.2017.40

[8] H. Gul, N. Javaid, I. Ullah, A. M. Qamar, M. K. Afzal, and G. P. Joshi "Detection of non-technical losses using SOSTLink and bidirectional gated recurrent unit to secure smart meters", *Applied Sciences*, Vol. 10, No. 9, art. no. 3151, 2020. https://doi.org/10.3390/app10093151

[9] M. Adil, N. Javaid, U. Qasim, I. Ullah, M. Shafiq and J. G. Choi "LSTM and bat-based RUSBoost approach for electricity theft detection", *Applied Sciences*, Vol. 10, No. 12, art. no. 4378, 2020. https://doi.org/10.3390/app10124378

[10] S. Mujeeb, and N. Javaid "ESAENARX and DE-RELM: Novel schemes for big data predictive analytics of electricity load and price", *Sustainable Cities and Society*, Vol. 51, art. no. 101642, 2019. https://doi.org/10.1016/j.scs.2019.101642

[11] M. Nazari-Heris, M. A. Mirzaei, B. Mohammadi-Ivatloo, M. Marzband, and S. Asadi "Economic-environmental effect of power to gas technology in coupled electricity and gas systems with price-responsive shiftable loads", *Journal of Cleaner Production*, Vol. 244, art. no. 118769, 2020. https://doi.org/10.1016/j.jclepro.2019.118769

[12] M. Marzband, F. Azarinejadian, M. Savaghebi, E. Pouresmaeil, J. M. Guerrero, and G. Lightbody "Smart transactive energy framework in grid-connected multiple home microgrids under independent and coalition operations", *Renewable energy*, Vol. 126, pp.95-106, 2018. https://doi.org/10.1016/j.renene.2018.03.021

[13] M. Jadidbonab, B. Mohammadi-Ivatloo, M. Marzband, and P. Siano "Short-term self-scheduling of virtual energy hub plant within thermal energy market. *IEEE Transactions on industrial electronics*, Vol. 68, No. 4, pp.3124-3136, 2020. https://doi.org/10.1109/TIE.2020.2978707

[14] H. R. Gholinejad, A. Loni, J. Adabi and M. Marzband "A hierarchical energy management system for multiple home energy hubs in neighborhood grids", *Journal of Building Engineering*, Vol. 28, art. no.101028, 2020. https://doi.org/10.1016/j.jobe.2019.101028

[15] M. A. Mirzaei, A. Sadeghi-Yazdankhah, B. Mohammadi-Ivatloo, M. Marzband, M. Shafie-khah, and J. P. Catalão "Integration of emerging resources in IGDT-based robust scheduling of combined power and natural gas systems

considering flexible ramping products", *Energy*, Vol 189, art. no. 116195, 2019. https://doi.org/10.1016/j.energy.2019.116195

[16] 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, pp.376-388, 2014. https://doi.org/10.1016/j.knosys.2014.08.014

[17] B. Li, K. Xu, X. Cui, Y. Wang, X. Ai, and Y. Wang "Multi-scale DenseNet-based electricity theft detection. In *Intelligent Computing Theories and Application: 14th International Conference, ICIC 2018, Wuhan, China, August 15-18, 2018, Proceedings, Part I,* Vol. 14, pp. 172-182, 2018. https://doi.org/10.1007/978-3-319-95930-6_17

[18] P. Jokar, N. Arianpoo, and V. C. Leung "Electricity theft detection in AMI using customers' consumption patterns", *IEEE Transactions on Smart Grid*, Vol. 7, No. 1, pp.216-226, 2015. https://doi.org/10.1109/TSG.2015.2425222

[19] J. Nagi, A. M. Mohammad, K. S. Yap, S. K. Tiong, and S. K. Ahmed "Non-technical loss analysis for detection of electricity theft using support vector machines", *2008 IEEE 2nd International Power and Energy Conference*, pp. 907-912, 2008. https://doi.org/10.1109/PECON.2008.4762604

[20] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad "Nontechnical loss detection for metered customers in power utility using support vector machines", *IEEE transactions on Power Delivery*, Vol. 25, No. 2, pp.1162-1171, 2009. https://doi.org/10.1109/TPWRD.2009.2030890

[21] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés and A. N. De Souza "Detection and identification of abnormalities in customer consumptions in power distribution systems", *IEEE Transactions on Power Delivery*, Vol. 26, No. 4, pp.2436-2442, 2011. https://doi.org/10.1109/TPWRD.2011.2161621

[22] R. Jiang, H. Tagaris, A. Lachsz, and M. Jeffrey "Wavelet based feature extraction and multiple classifiers for electricity fraud detection. In *IEEE/PES Transmission and Distribution Conference and Exhibition*, Vol. 3, pp. 2251-2256, 2002. https://doi.org/10.1109/TDC.2002.1177814

[23] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero and A. Gómez-Expósito "Detection of non-technical losses using smart meter data and supervised learning", *IEEE Transactions on Smart Grid*, Vol. 10, No. 3, pp.2661-2670, 2019. https://doi.org/10.1109/TSG.2018.2807925

[24] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and P. Nelapati "A hybrid neural network model and encoding technique for enhanced classification of energy consumption data", In *2011 IEEE power and energy society general meeting*, pp. 1-8, 2011. https://doi.org/10.1109/PES.2011.6039050

Copyright: © 2024 by the authors, Licensee ITEECS, India. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

***