Available online at www.sciencedirect.com
ScienceDirect
Energy Reports 9 (2023) 634–643
www.elsevier.com/locate/egyr

2022 9th International Conference on Power and Energy Systems Engineering (CPESE 2022), Doshisha University, Kyoto, Japan, 9–11 September 2022

Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach

Ejaz Ul Haq[a,b], Can Pei[b,1], Ruihong Zhang[a,*], Huang Jianjun[b,*], Fiaz Ahmad[c]

[a] *School of Mechanical Engineering and Automation, Harbin Institute of Technology, Shenzhen, China*
[b] *College of Electronic and Information Engineering, Shenzhen University, China*
[c] *Department of Electrical and Computer Engineering, Air University, Pakistan*

Received 25 October 2022; accepted 5 November 2022
Available online 16 November 2022

Abstract

Electricity theft has a considerable negative effect on energy suppliers and power infrastructure, leading to non-technical losses and business losses. Power quality deteriorates and overall profitability falls as a result of energy theft. By fusing information and energy flow, smart grids may assist solve the issue of power theft. The examination of smart grid data aids in the detection of power theft. However, the earlier techniques were not very good in detecting energy theft. In this work, we suggested an electricity theft detection approach using smart meter consumption data in order to handle the aforementioned issues and assist and assess energy supply businesses to lower the obstacles of limited energy, unexpected power usage, and bad power management. In specifically, the Deep CNN model effectively completes two tasks: it differentiates between energy that is not periodic and that is, while keeping the general features of data on power consumption. The trial's results show that the deep CNN model outperforms prior ones and has the best level of accuracy for detecting energy theft.

Peer-review under responsibility of the scientific committee of the 9th International Conference on Power and Energy Systems Engineering, CPESE, 2022.

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

1. Introduction

Our daily lives now depend on electricity. Throughout the processes of producing, transmitting, and distributing electricity, energy losses occur often. Technical losses (TLs) and non-technical losses (NTLs) are the two types of electrical losses [1]. One of the most prevalent non-technical losses is the theft of power. This improper conduct often manifests as circumventing the electrical meter, tampering with the meter reading, or meter manipulation [2]. Electricity theft may lead to energy spikes, large loads on electrical systems, significant revenue losses for the power provider, and hazards to public safety.

* Corresponding authors.
E-mail addresses: eerhzhang@hit.edu.cn (R. Zhang), huangjin@szu.edu.cn (H. Jianjun).
[1] Co-first author.

https://doi.org/10.1016/j.egyr.2022.11.072

Peer-review under responsibility of the scientific committee of the 9th International Conference on Power and Energy Systems Engineering, CPESE, 2022.

The network-oriented methodology, the data-oriented technique, and a hybrid strategy that combines the two methods are the three distinct types of power theft detection strategies [3]. When using network- and hybrid-oriented solutions [4,5], as well as the inclusion of new devices [6] the network architecture must be altered on a regular basis. Since the network architecture could not be accessed owing to security concerns and the installation of additional devices is costly, it is difficult to extensively adopt these principles. By focusing only on the data produced by smart meters and ignoring network architecture or other devices, data-oriented tactics improve the effectiveness of suspected power theft detection and evaluation. Thus, data-driven techniques for detecting power theft have grown in favor lately [7].

The term "smart grid" refers to a combination of traditional electrical networks with automated communication technologies. In accordance with past research [8–11], the smart grid may help ensure that electrical energy is used efficiently. The smart grid network uses a transactive power architecture [12] together with medium- and short-term electrical demand forecasting methods [13] to make the most of the existing resources. To decrease the effects of peak loads while enabling the trading of more power for less money, the authors of [14] suggest a multilayer power distribution architecture. To minimize the irregular behavior of sustainable power, a method based on information-gap decision theory [15] is used. Information is sent between the power grid and specific energy consumers through a smart meter.

Utility companies started collecting enormous amounts of data about customers' energy use from smart meters once they started using advanced metering infrastructure in grids, which makes it possible for us to identify fraudulent activity [16]. However, a number of novel power theft techniques may exploit the AMI network. The AMI assaults might be carried out through a variety of techniques, such technological instruments and cyber-attacks. Correct line deviations and broken or malfunctioning gear or equipment are the two main methods that human inspection is used to detect power theft. When properly checking all of the meters in a system, these procedures are, nevertheless, quite expensive in terms of both time and money.

Despite the fact that electrical utility companies often gather an excessive amount of data, machine learning-based categorization has lately attracted a lot of interest. Consumer privacy is also protected when analyzing daily usage data to detect stealing tendencies [17]. In [18,19], SVM was used to cluster and classify data in order to look for anomalies and irregularities. This approach may be used to model and identify any energy consumption profile since clustering is often utilized as both a primary and secondary step in algorithms. Given that neural networks are so good at detecting power theft, a lot of academics and researchers are becoming more and more dependent on them. As the internet develops, attacks on the grid become more frequent. A kind of artificial intelligence technology called support vector machines (SVMs) is used in [20] to find non-technical losses (NTLs) in electrical utilities. [21] used unsupervised techniques, such as fuzzy classification utilizing the Euclidean distance to the cluster center as a distance metric. An artificial neural network (ANN)-based technology was used in [22] to examine attributes and identify fraudulent clients using a wavelet-based approach. Using SVM and XGBoost, the authors of [23] created a technique for locating non-technical losses in the energy system. The major goal of the proposed research is to assess customers using data from smart meters with the aid of a supporting dataset. To increase classification accuracy, use the XGBoost. An alternative approach [24] shown improved fraud detection efficacy in smart grid systems by merging an ANN with an SVM to create a hybrid algorithm. The approach presented in [25] is built on long short-term memory (LSTM) and bat-based random under-sampling boosting. (RUSBoost). The identification of aberrant patterns and parameter tweaking are performed using the bat-based LSTM and RUSBoost. The authors of [26] used a CNN and LSTM combo together with the power consumption pattern to discover energy theft in time-series data. The research in [27] proposes an end-to-end hybrid neural network that can assess both sequential and non-sequence input, such as geographic data.

Deep learning algorithms have exceeded traditional machine learning approaches in a variety of applications, including image analysis, computer vision, and speech recognition. Because deep learning algorithms can handle and regulate huge volumes of data, execute extraction of features, and categorize data, they are utilized to construct models to deal with smart meter data from smart grids. The authors of [28] propose a strategy based on a large and deep convolutional neural network (CNN) model. The deep CNN component can detect trends in power utilization, but the shallow CNN component can capture data features in general. Hybrid deep learning approaches have long been employed in load forecasting. Researchers at [29] developed a model that blends Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) architecture to better correctly forecast future demand. It was determined that the proposed model [29] outperformed the previous techniques substantially better. The authors of

[30] developed three classifiers based on gradient boosting to address the problem of energy theft detection in the smart grid. Using the proposed technique, the relative performance of several classifiers in recognizing incidents of theft may be completely and objectively examined. The study in [31] employed an attack tree-based threat model to explain how energy theft manifests itself in smart meters. Wireless networks are also employed in [31,32] papers for energy theft detection and alerting, and both studies give a full overview of the methodologies presently used to detect energy theft in AMI. The quality of the input data influences the performance of machine learning and deep learning models. Existing technologies for detecting energy theft provide good results. However, there are a number of shortcomings with these methods, which are listed below.

1. When using machine learning methods in ETD, processing unstable data is a big challenge. This problem remains unanswered using standard approaches.
2. Inaccurate values in the available data often lower classification accuracy.
3. Traditional energy theft detection methods mainly rely on human operations and conventional machine learning algorithms struggle when processing a significant amount of data, however it will be more expensive since it will need to pay people to review it. The study ignores a variety of non-criminal factors that may affect consumption behavior, including weather and seasonality, the installation or removal of an appliance, changes in resident status, weekends, and holidays. Normal behaviors that cause a sudden change in load shape might be mistaken for aberrant activity. This error might result in a high proportion of false-positive results, hence

In order to solve real-time energy theft and help consumers and energy companies maintain healthy lifestyles, this research looks into a potential solution.

1. To address the classification difficulty, we created a deep CNN model in this study using a preprocessing technique on the power consumption dataset. As a consequence, we made the decision to apply deep CNN structure in conjunction with data augmentation to detect energy theft by analyzing consumers' erratic and unusual use habits.
2. Companies in the power industry may be able to utilize the new method to successfully detect power outages and reduce energy use by analyzing data about customers' actual energy usage in real time. Anyone who intentionally steals energy may benefit from the proposed framework.
3. Real-time smart meter data from customer were used in a number of thorough studies, and the results confirmed the value of the suggested method

2. Proposed methodology

The deep CNN based technique is utilized in this study to identify energy theft in the smart grid. Deep CNN aims to extract significant features and classify those aspects as theft-related or non-theft-related. Fig. 1 depicts the recommended technique's framework. The recommended method for spotting power theft consisted of three basic parts. (1) Data preprocessing and analysis, (2) data is created for training and testing. (3) CNN-based deep feature extraction and classification

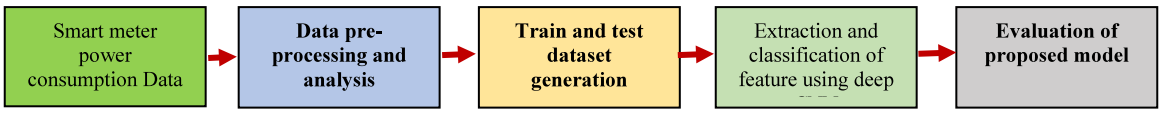


Fig. 1. Framework of the proposed electricity theft detection method.

The following aspects should be addressed in the proposed technique:

2.1. Data pre-processing and analysis

The information was compiled from 45970 industrial and residential users' records of energy usage. A smart meter was used to capture the data on electricity use during a 10-minute period. The experimental dataset was produced using data on power use from May 2018 to April 2020. A smart meter was implanted in every participant

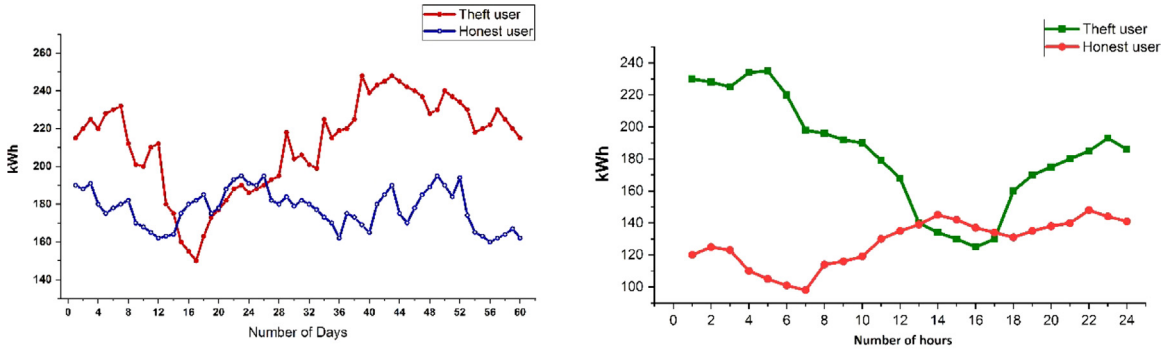


Fig. 2. A comparison of theft and honest and individuals' power usage (a) daily power consumption (b) fortnightly power consumption.

in the trial who gave their consent. Data that is currently available indicates that 17% of all consumers are power thieves. Electricity thieves' and law-abiding consumers' energy use habits are shown in Fig. 2. The first is a typical consumer, whereas the second is an electricity thief. The main finding was that there are differences in the patterns of power use between normal and atypical consumers. An atypical or electrical thief user varies more than a normal user, according to the consumption pattern. Customers who gave their permission to take part in the study and who also agreed to obtain a smart meter did so. It is reasonable to assume that all samples are obtained from reliable consumers as a consequence. On the other hand, malicious samples cannot be gathered since energy theft may never or only sometimes happen for a particular user. A sizable quantity of data from many categories must be used to train CNN so that it can deliver an appropriate categorization result. In order to increase the quantity of picture samples in image processing challenges, a variety of ways are used. Since the majority of users do not steal electricity, realistic datasets have fewer instances of power theft than conventional datasets. Poor classification accuracy or over-fitting might be produced by an unbalanced dataset, which would therefore yield low classification accuracy. As a result, in this study, we developed a data augmentation approach to generate 8765 malevolent customers in order to remedy the imbalance issue, based on Ref. [32]. This dataset is an excellent resource for smart meter research because to its large sample size, wide range of users, and extensive time span of observations. Half an hour is the new sampling pace for each customer. In order to demonstrate why a CNN should be used for feature extraction, this section looks at data from smart meters. The three fundamental methods used to pre-process the initial energy consumption data are data cleaning, missing value interpolation, and data normalization. Although they have been significantly shifted, the load files are quite comparable. In a CNN, the filter weights are constant from region to region. As a consequence, the convolutional layer's calculated features are impervious to minute variations, enabling the extraction of generally stable characteristics from variable load profiles. The effectiveness of ML and DL algorithms is affected by the consistency of the provided data. Pre-processing step improvements in data accuracy directly impact model efficiency. Consumption of loads varies in terms of amount and duration and is impacted by a wide range of uncontrollable variables, including lifestyle, the seasons, the weather, and many others. As a consequence, in addition to the weather and other external factors, consumer types and other factors also have an impact on consumer load profiles. Table 1 provides information about the dataset.

Table 1. Dataset information.

Description	Value
Data collecting time slot	1 May 2018–30 April 2020
Type of data	Time series
Resolution of data	Smart meter data in high resolution
Number of customers in total	45970
Number of ordinary users	38155
Number of power thieves	7815

2.2. Training and testing dataset generation

Preliminary studies illustrate that demographics and other variables, in addition to the weather, have a significant influence on the electrical load profiles of individual consumers. However, it may be difficult to infer features based on experience alone from 1D power consumption data due to the large daily fluctuations in energy usage. To evaluate the efficacy of the strategy outlined above, the cross-validation methodology divides the pre-processed dataset into train and test datasets, with 75% of the train set and 25% of the test set. It is feasible that DL and ML techniques will struggle to perform well on a dataset where power thieves greatly outnumber legitimate consumers. The parameters of the model are learned from the train dataset, and its ability to generalize to new customer samples is tested in the test dataset.

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

Utilizing convolution and pooling methods, the deep CNN model designed learns features from a large and varied dataset of smart meter readings gathered throughout the day. Convolutional and pooling layers are combined to create deep-CNNs, like the one in Fig. 3. The CNN is trained using the Adam optimizer and is a sophisticated multi-layered supervised learning architecture. To build feature descriptions and lessen the impacts of outside distortion, convolutional layers are utilized. The convolutional layer uses a variety of feature filters to produce various feature maps. Because neurons in normal brain networks are coupled, their capacity to expand is limited. Due to the fact that CNN connects every neuron to its neighbors, it is able to transcend the constraints of traditional neural networks. Periodic patterns are produced from the input 2-D power usage data using a 2-D convolution layer. CNNs, which are often utilized between two convolutional layers, are fundamentally based on the concept of pooling. The data becomes easier to understand and handle with fewer factors to take into account. Each feature map from the preceding convolutional layer correlates to a feature vector in the pooling layer. Even as the size of the output feature maps shrinks, the quantity of output feature vectors in the pooling layer remains constant. To reduce the amount of training weights and filters, as well as the number of parameters and characteristics that are not necessary for the job at hand, the pooling layer in CNN is often utilized. Another method for preventing over fitting is the use of a pool layer. A popular technique for gathering resources is the maximal operation (max). The pooling layer must first gather data from each domain before determining which domain the greatest value of the pooling filter covers. In this research, the maximum pooling approach is also used. Due to its sparseness and ability to minimize gradient, LReLU is used in this work as an activation function in the deep CNN model. The stack created by the output of the pooling layer enters this fully linked layer. The classification result, which is a two-probability value utilized for two-class classification, is then obtained using the softmax activation function. The input is marked as such when there is a greater possibility of engaging in energy theft than there is that the data is normal.

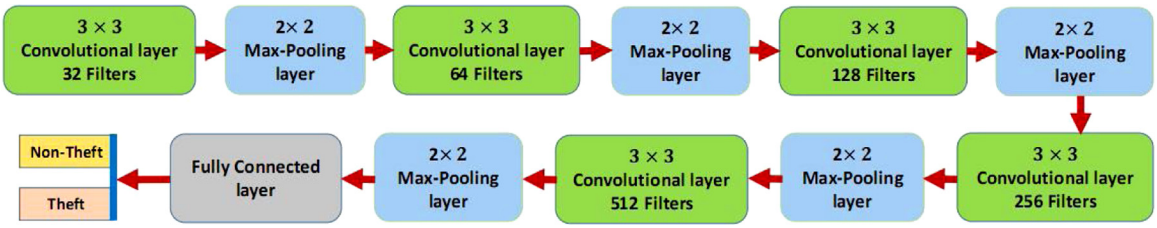


Fig. 3. Framework of Deep CNN model.

3. Results and experiments

To evaluate the proposed method, a real dataset of 45970 consumers' daily consumption over a two-year period was employed (May 1, 2018–April 30, 2020). There is a clear imbalance in the statistics since just 17% of the customers in the data are predators and 83% are regular users. Python 3.7.4 is set up on a typical PC with an Intel Core i7 processor operating at 3.40 GHz and 16.0 GB of RAM. TensorFlow is used to organize the model's architecture.

The success of the devised strategy is evaluated using the confusion matrix. Precision, recall, AUC, F1-score, ROC curves, and MCC are just a few of the crucial performance measures that may be extracted from confusion matrix data. The confusion matrix for the proposed model is shown in Table 2. As shown in Table 2, the proposed technique has a very low false-positive rate, which is critical for ETD. The proposed approach is compared with relevant prior research and basis classifiers for further study. The results demonstrate that the suggested strategy outperforms existing solutions across the board.

Table 2. Confusion matrix of the proposed model.

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

True Negative Rate is a measure of accuracy that indicates the percentage of really trustworthy clients that the classifier identified. One measure of a classifier's efficacy is its True Positive Rate (TPR), sometimes called Recall. In and of itself, measures of accuracy like recall and accuracy are not enough to provide a whole picture of how well a model performs. Due to the F1-score being produced, enhancements to accuracy and recall are favored. A skewed distribution of classes in a binary classification issue is well-suited to the F1-score statistic. The F1-score is derived from the weighted harmonic mean of recall and accuracy. The ROC-AUC is a useful metric for identifying cases of energy theft. The model for determining how well it can be detected is graphically shown. An efficient classifier has a ROC-AUC very near to 1. If all of the criteria used to rank MCC are reliable and provide accurate predictions, then the algorithm will get a high overall score. A value that is near to 1, a score of 0, and a score of 1 all indicate accurate model categorization, lack of class separation abilities, and faulty model classification, respectively. The MCC score is between -1 and 1.

The CNN classifier begins to be impacted by the unequal data, resulting in a high FPR. Fig. 4 illustrates the comparison we made to demonstrate the importance of balanced data. The proposed model has low classification performance on imbalance data. The CNN model displays inaccuracies on the imbalance dataset because it makes the assumption that actual power thieves are honorable customers. The suggested CNN model's classification performance improves once the data have been balanced.

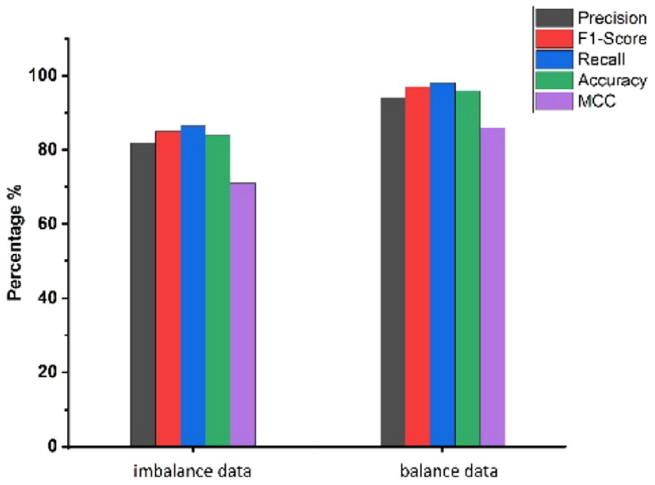


Fig. 4. Efficiency of proposed model using imbalance data and balance data.

The chosen hyper-parameter values are mostly responsible for the proposed model's performance. In order to improve classification accuracy, CNN is first run at random before the best hyper-parameter values are selected. Fig. 5 shows the proposed model's ROC-AUC representation with and without a modification in the value of the hyper-parameter. Fig. 6 presents the receiver operating characteristic area under the curve (ROC-AUC) for the

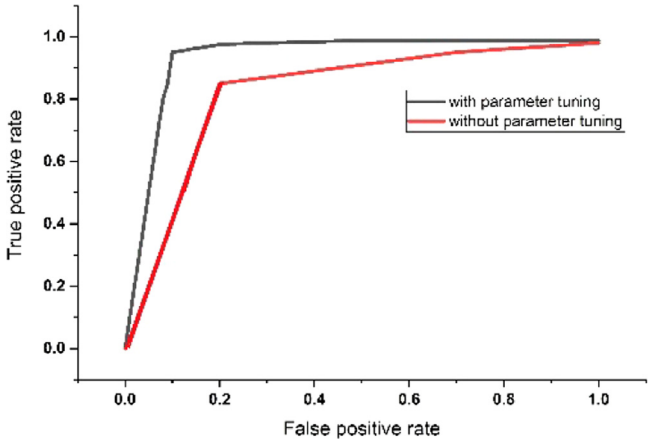


Fig. 5. Analyzing ROC-AUC with and without Adjusting Parameters.

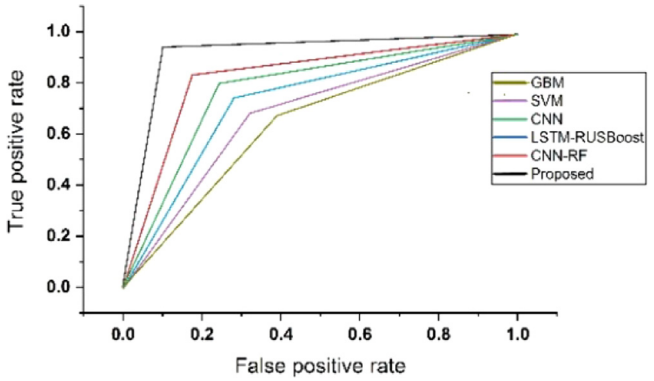


Fig. 6. ROC-AUC based comparison of the state-of-the-art and the proposed technique.

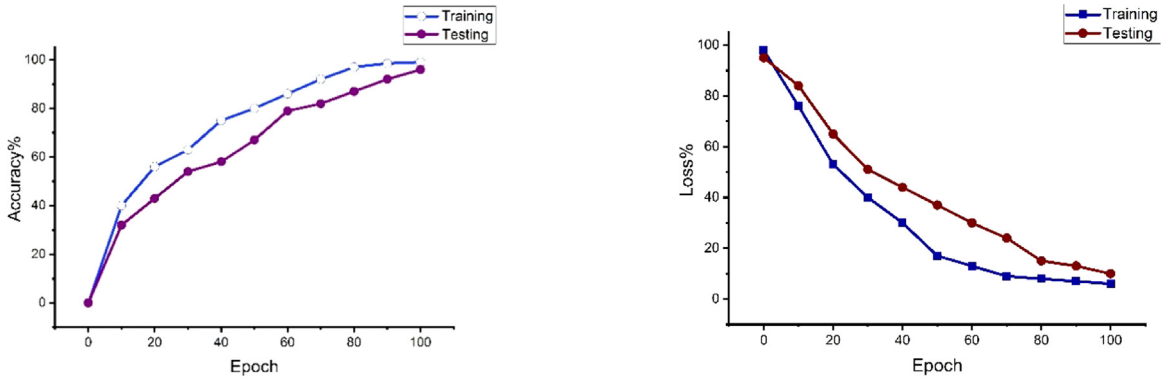
state-of-the-art and our proposed method from this analysis. The ROC-AUC results demonstrate that our suggested technique exceeds the most recent cutting-edge methods.

Fig. 7(a) and (b) show the proposed model's accuracy (left) and loss (right) (b). Our suggested technique effectively adapts from high-dimensional datasets by using smaller epoch values, but this comes at the expense of over-fitting. The accuracy improves with the number of epochs because the training and test losses get less. These results demonstrate the model's enhanced sensitivity.

Precision, recall, ROC, F1-score, MCC, and accuracy are compared between our suggested technique and the previous methods in Fig. 8. CNN-based DL approaches outperform ML methods such as logistic regression, support vector machines, and random forests when comparing several algorithms for detecting electric theft. As a result of the convolutional neural network's ability to extract features from a wide range of power consumption patterns, we have been able to improve the accuracy with which energy theft can be detected. The suggested approach also outperforms any competing models. Energy theft detection is, at its core, an anomaly-based activity, since it relies on spotting suspicious clients' out-of-the-ordinary energy use. It would be interesting to see how well Deep CNN generalizes to different datasets, since it performs well on the dataset used in this research.

4. Conclusion

This research details a deep convolutional neural network model that can detect electricity theft. CNN is used as an automatic feature extractor to classify the retrieved characteristics into thieves and non-thieves. The genuine, first smart meter data was missing certain information and had various errors. To fix this, we performed a full study and pre-processing of the data, which included normalization and accusation. When there are several data



(a) (b)

Fig. 7. Evaluation of the developed Deep Learning –CNN (a) Accuracy (b) Loss.

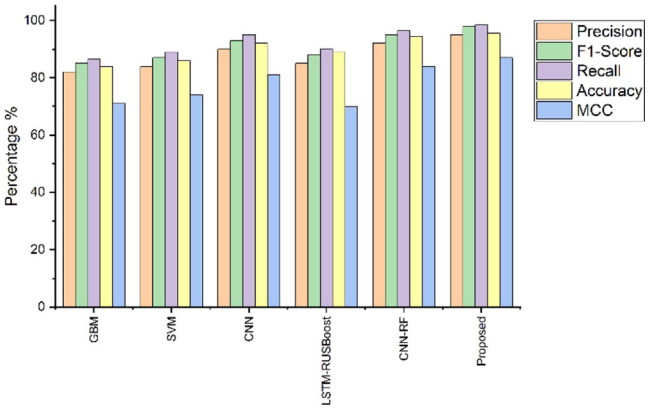


Fig. 8. Performance comparison of Deep-CNN and state-of-the-art.

components, over-fitting may occur, but the CNN adds a dropout layer to prevent this. Using the same dataset, machine learning and deep learning tools may detect energy theft. The suggested model can automatically extract features, whereas most other traditional classifiers need tedious and time-consuming feature extraction from human input. To demonstrate the efficiency of the suggested strategy, we carried out extensive testing on a number of actual datasets. The results of the testing show that the suggested method performs more effectively than competing ones. The results show that the suggested model for ETD is accurate and has a low false-positive rate. We will examine unusual customer behavior based on their short-term usage in the future to identify power theft. Since this problem has not been fully addressed, we want to create a model that can detect insider system attacks.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work was supported by Stable Support Plan for Shenzhen Universities, China, through Project GXWD20201230155427003-20200823171314001. This work was also supported in part by the Shenzhen Science and Technology Project, China (No. 20200821152629001).

References

[1] Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen XS. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19(2):105–20.
[2] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J Sel Areas Commun 2013;31(7):1319–30.
[3] Messinis GM, Hatziargyriou ND. Review of non-technical loss detection methods. Electr Power Syst Res. 2018;158:250–66.
[4] Short TA. Advanced metering for phase identification, transformer identification, and secondary modeling. IEEE Trans Smart Grid 2013;4:651–8.
[5] Leite JB, Mantovani JRS. Detecting and locating non-technical losses in modern distribution networks. IEEE Trans Smart Grid 2018;9:1023–32.
[6] Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen X. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19:105–20.
[7] Glauner P, Dahringer N, Puhachov O, Meira JA, Valtchev P, State R, et al. Identifying irregular power usage by turning predictions into holographic spatial visualizations. In: Proceedings of the 2017 IEEE international conference on data mining workshops. 2017, p. 258–65.
[8] Gul H, Javaid N, Ullah I, Qamar AM, Afzal MK, Joshi GP. Detection of non-technical lossesusing SOSTLink and bidirectional gated recurrent unit to secure smart meters. Appl Sci 2020;10:3151.
[9] Adil M, Javaid N, Qasim U, Ullah I, Shafiq M, Choi J-G. LSTM and bat-based RUSBoost approach for electricity theft detection. Appl Sci 2020;10:1–21.
[10] Mujeeb S, Javaid N. ESAENARX and DE-RELM: Novel schemes for big data predictive analytics ofelectricity load and price. Sustain Cities Soc 2019;51:101642.
[11] Nazari-Heris M, Mirzaei MA, Mohammadi-Ivatloo B, Marzb M, Asadi S. Economic-environmentaleffect of power to gas technology in coupled electricity and gas systems with price-responsive shiftableloads. J Clean Prod 2020;244:118769.
[12] Marzb M, Azarinejadian F, Savaghebi M, Pouresmaeil E, Guerrero JM, Lightbody G. Smart transactiveenergy framework in grid-connected multiple home microgrids under independent and coalition operations. Renew Energy 2018;126:95–106.
[13] Jadidbonab M, Mohammadi-Ivatloo B, Marzb M, Siano P. Short-term self-scheduling of virtual EnergyHub plant within thermal energy market. IEEE Trans Ind Electron 2020.
[14] Gholinejad HR, Loni A, Adabi J, Marzb M. A hierarchical energy management system for multiplehome energy hubs in neighborhood grids. J Build Eng 2020;28:101028.
[15] Mirzaei MA, Sadeghi-Yazdankhah A, Mohammadi-Ivatloo B, Marzb M, Shafie-khah M, Catalão JP. Integration of emerging resources in IGDT-based robust scheduling of combined power and natural gassystems considering flexible ramping products. Energy 2019;189:116195.
[16] Guerrero JI, Le'on C, Monedero I, Biscarri F, Biscarri J. Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection. Knowl-Based Syst 2014;71(4):376–88.
[17] Li B, Xu K, Cui X, Wang Y, Ai X, Wang Y. Multi-scale DenseNet-based electricity theft detection. In: Proceedings of the international conference on intelligent computing, vol. 6. 2018, p. 172–82.
[18] Jokar P, Arianpoo N, Leung VC. Electricity theft detection in AMI using customers' consumption patterns. IEEE Trans Smart Grid 2015;7:216–26.
[19] Nagi J, Mohammad A, Yap KS, Tiong SK, Ahmed SK. Non-technical loss analysis for detection of electricity theft using support vector machines. In: Proceedings of the 2008 IEEE 2nd international power and energy conference. Piscataway, NJ, USA: IEEE; 2008, p. 907–12.
[20] Nagi J, Yap KS, Tiong SK, Ahmed SK, Mohamad M. Nontechnical loss detection formetered customers in power utility using support vector machines. IEEE Trans Power Deliv 2009;25:1162–71.
[21] Angelos EWS, Saavedra OR, Cortés OAC, de Souza AN. Detection and identification of abnormalities in customer consumptions in power distribution systems. IEEE Trans Power Deliv 2011;26:2436–42.
[22] Jiang R, Tagaris H, Lachsz A, Jerey M. Wavelet based feature extraction and multiple classifiers for electricity fraud detection. In: Proceedings of the IEEE/PES transmission and distribution conference and exhibition, Vol. 3. Piscataway, NJ, USA: IEEE; 2002, p. 2251–6.
[23] Buzau MM, Tejedor-Aguilera J, Cruz-Romero P, Gómez-Expósito A. Detection of non-technical losses using smart meter data and supervised learning. IEEE Trans Smart Grid 2018;10:2661–70.
[24] Depuru SSSR, Wang L, Devabhaktuni V, Nelapati P. A hybrid neural network model and encoding technique for enhanced classification of energy consumption data. In: Proceedings of the 2011 IEEE power and energy society general meeting. Piscataway, NJ, USA: IEEE; 2011, p. 1–8.
[25] Adil M, Javaid N, Qasim U, Ullah I, Shafiq M, Choi J-G. LSTM and bat-based RUSBoost approach forelectricity theft detection. Appl Sci 2020;10:4378.

[26] Hasan MN, Toma RN, Nahid A-A, Islam MMM, Kim J-M. Electricity theft detection in smart grid systems: A CNN-LSTM based approach. Energies 2019;12:3310.
[27] Buzau M-M, Tejedor-Aguilera J, Cruz-Romero P, Gomez-Exposito A. Hybrid deep neural networks for detection of non-technical losses in electricity smart meters. IEEE Trans Power Syst 2020;35:1254–63.
[28] Zheng Z, Yang Y, Niu X, Dai H-N, Zhou Y. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Trans Ind Inf 2018;14:1606–15.
[29] Hasan M, Toma RN, Nahid AA, Islam MM, Kim JM. Electricity theft detection in smart GridSystems: A CNN-LSTM based approach. Energies 2019;12:3310.
[30] Punmiya R, Choe S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. IEEE Trans Smart Grid 2019;10(2):2326–9. http://dx.doi.org/10.1109/TSG.2019.2892595.
[31] Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen X. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19(2):105–20. http://dx.doi.org/10.1109/TST.2014.6787363.
[32] Lin G. Feng H, Feng X, Wen H, Li Y, Hong S, Ni Z. Electricity theft detection in power consumption data based on adaptive tuning recurrent neural network. Front Energy Res 2021;9:773805. http://dx.doi.org/10.3389/fenrg.2021.773805.