Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

An Application of IoT-based Smart Electric Meters: Electricity Theft Cyber-Attacks Detection

A. Sneha Sree, B. Navya, G. Shreya UG Student,
B. Durga Bhavani Assistant Professor,
Department of Information Technology, Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammaguda, Secunderabad, Telangana, India

ABSTRACT
Electricity theft represents a pressing problem that has brought enormous financial losses to electric utility companies worldwide. In the United States alone, $6 billion worth of electricity is stolen annually. Traditionally, electricity theft is committed in the consumption domain via physical attacks that includes line tapping or meter tampering. The smart grid paradigm opens the door to new forms of electricity theft attacks. First, electricity theft can be committed in a cyber manner. With the advanced metering infrastructure (AMI), smart meters are installed at the customers' premises and regularly report the customers' consumption for monitoring and billing purposes. In this context, malicious customers can launch cyber-attacks on the smart meters to manipulate the readings in a way that reduces their electricity bill. Second, the smart grid paradigm enables customers to install renewable-based distributed generation (DG) units at their premises to generate energy and sell it back to the grid operator and hence make a profit. Here, CNNs can be used to detect electricity theft cyber-attacks from IoT-based smart energy meters by analyzing the time-series data collected from the meters. The CNN can learn the patterns of normal energy consumption and detect any anomalous energy consumption that may indicate electricity theft.

Keywords: Electricity theft, cyberattacks, recurrent neural network, deep neural networks, convolution neural networks.

1. INTRODUCTION

Electricity theft is defined as the consumed amount of energy that is not billed by the consumers. This incurs major revenue losses for electric utility companies. All over the world, electric utility companies lose $96 billion every year due to electricity theft. This phenomenon affects all nations, whether rich or poor. For instance, Pakistan suffers 0.89 billion rupees of loss yearly due to non-technical losses (NTLs) [1] and in India, the electricity loss exceeds 4.8 billion rupees annually. Electricity theft is also a threat to countries with strong economies; i.e., in the U.S., the loss due to electricity theft is approximately $6 billion, and in the UK, it is up to £175 million per annum. In addition, electricity theft causes a voltage imbalance and can affect power system operations by overloading the transformers [2]. Moreover, the rising electricity prices increase the burden on honest customers when the utility asks them also to pay for the theft of energy. It also increases unemployment, the inflation rate and decreases revenue and energy efficiency, which has adverse effects on a country's economic state.

Today, electric power loss has become one of the most conspicuous issues affecting both conventional power grids and smart grids. From the statistics, it has been shown that transmission and distribution losses increased from 11% to 16% between the years 1980 to 2000. The electricity losses vary from country to country. The losses in the USA, Russia, Brazil, and India were 6%, 10%, 16%, and 18%, respectively, of their total energy production [3]. The difference between the energy produced in one system and the metered energy delivered to the users is known as the power loss. To determine the amount of electricity loss, smart meters in smart grids play a prominent role. Advanced energy meters obtain information from the consumers' load devices and measure the consumption of energy in intervals of an hour. The energy meter provides additional information to

the utility company and the system operator for better monitoring and billing, and provides two-way communications between the utility companies and consumers [4]. However, it is also possible to limit the maximum amount of electricity consumption, which can terminate as well as re-connect the supply of electricity from any remote place.

2. LITERATURE SURVEY

Hasan et. a [5] implemented a novel data pre-processing algorithm to compute the missing instances in the dataset, based on the local values relative to the missing data point. Furthermore, in this dataset, the count of electricity theft users was relatively low, which could have made the model inefficient at identifying theft users. This class imbalance scenario was addressed through synthetic data generation. Finally, the results obtained indicate the proposed scheme can classify both the majority class (normal users) and the minority class (electricity theft users) with good accuracy.

Zheng et. al [6] combined two novel data mining techniques to solve the problem. One technique is the maximum information coefficient (MIC), which can find the correlations between the nontechnical loss and a certain electricity behavior of the consumer. MIC can be used to precisely detect thefts that appear normal in shapes. The other technique is the clustering technique by fast search and find of density peaks (CFSFDP). CFSFDP finds the abnormal users among thousands of load profiles, making it quite suitable for detecting electricity thefts with arbitrary shapes. Next, a framework for combining the advantages of the two techniques is proposed. Numerical experiments on the Irish smart meter dataset are conducted to show the good performance of the combined method.

Li et. al [7] presented a novel CNN-RF model to detect electricity theft. In this model, the CNN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Because a large number of parameters must be optimized that increase the risk of overfitting, a fully connected layer with a dropout rate of 0.4 is designed during the training phase. In addition, the SMOT algorithm is adopted to overcome the problem of data imbalance. Some machine learning and deep learning methods such as SVM, RF, GBDT, and LR are applied to the same problem as a benchmark, and all those methods have been conducted on SEAI and LCL datasets. The results indicate that the proposed CNN-RF model is quite a promising classification method in the electricity theft detection field because of two properties: The first is that features can be automatically extracted by the hybrid model, while the success of most other traditional classifiers relies largely on the retrieval of good hand-designed features which is a laborious and time-consuming task. The second lies in that the hybrid model combines the advantages of the RF and CNN, as both are the most popular and successful classifiers in the electricity theft detection field.

Nabil et. al [8] proposed an efficient and privacy-preserving electricity theft detection scheme for the AMI network and we refer to it as PPETD. Our scheme allows system operators to identify the electricity thefts, monitor the loads, and compute electricity bills efficiently using masked fine-grained meter readings without violating the consumers' privacy. The PPETD uses secret sharing to allow the consumers to send masked readings to the system operator such that these readings can be aggregated for the purpose of monitoring and billing. In addition, secure two-party protocols using arithmetic and binary circuits are executed by the system operator and each consumer to evaluate a generalized convolutional-neural network model on the reported masked fine-grained power consumption readings for the purpose of electricity theft detection. An extensive analysis of real datasets is performed to evaluate the security and the performance of the PPETD.

Khan et. al [9] presents a new model, which is based on the supervised machine learning techniques and real electricity consumption data. Initially, the electricity data are pre-processed using interpolation, three sigma rule and normalization methods. Since the distribution of labels in the electricity consumption data is imbalanced, an Adasyn algorithm is utilized to address this class imbalance problem. It is used to achieve two objectives. Firstly, it intelligently increases the minority class samples in the data. Secondly, it prevents the model from being biased towards the majority

class samples. Afterwards, the balanced data are fed into a Visual Geometry Group (VGG-16) module to detect abnormal patterns in electricity consumption. Finally, a Firefly Algorithm based Extreme Gradient Boosting (FA-XGBoost) technique is exploited for classification. The simulations are conducted to show the performance of our proposed model. Moreover, the state-of-the-art methods are also implemented for comparative analysis, i.e., Support Vector Machine (SVM), Convolution Neural Network (CNN), and Logistic Regression (LR). For validation, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), Receiving Operating Characteristics Area Under Curve (ROC-AUC), and Precision Recall Area Under Curve (PR-AUC) metrics are used. Firstly, the simulation results show that the proposed Adasyn method has improved the performance of FA-XGboost classifier, which has achieved F1-score, precision, and recall of 93.7%, 92.6%, and 97%, respectively. Secondly, the VGG-16 module achieved a higher generalized performance by securing accuracy of 87.2% and 83.5% on training and testing data, respectively. Thirdly, the proposed FA-XGBoost has correctly identified actual electricity thieves, i.e., recall of 97%. Moreover, our model is superior to the other state-of-the-art models in terms of handling the large time series data and accurate classification. These models can be efficiently applied by the utility companies using the real electricity consumption data to identify the electricity thieves and overcome the major revenue losses in power sector.

Kocaman et. al [10] developed by using deep learning methods on real daily electricity consumption data (Electricity consumption dataset of State Grid Corporation of China). Data reduction has been made by developing a new method to make the dataset more usable and to extract meaningful results. A Long Short-Term Memory (LSTM) based deep learning method has been developed for the dataset to be able to recognize the actual daily electricity consumption data of 2016. In order to evaluate the performance of the proposed method, the accuracy, prediction and recall metric was used by considering the five cross-fold technique. Performance of the proposed methods were found to be better than previously reported results.

Li et. al [11] presented a novel approach for automatic detection by using a multi-scale dense connected convolution neural network (multi-scale DenseNet) in order to capture the long-term and short-term periodic features within the sequential data. They compare the proposed approaches with the classical algorithms, and the experimental results demonstrate that the multi-scale DenseNet approach can significantly improve the accuracy of the detection. Moreover, our method is scalable, enabling larger data processing while no handcrafted feature engineering is needed.

Aldegheishem et. al [12] developed two novel ETD models. A hybrid sampling approach, i.e., synthetic minority oversampling technique with edited nearest neighbor, is introduced in the first model. Furthermore, AlexNet is used for dimensionality reduction and extracting useful information from electricity consumption data. Finally, a light gradient boosting model is used for classification purpose. In the second model, conditional wasserstein generative adversarial network with gradient penalty is used to capture the real distribution of the electricity consumption data. It is constructed by adding auxiliary provisional information to generate more realistic data for the minority class. Moreover, GoogLeNet architecture is employed to reduce the dataset's dimensionality. Finally, adaptive boosting is used for classification of honest and suspicious consumers. Both models are trained and tested using real power consumption data provided by state grid corporation of China. The proposed models' performance is evaluated using different performance metrics like precision, recall, accuracy, F1-score, etc. The simulation results prove that the proposed models outperform the existing techniques, such as support vector machine, extreme gradient boosting, convolution neural network, etc., in terms of efficient ETD.

3. EXISTING SYSTEM

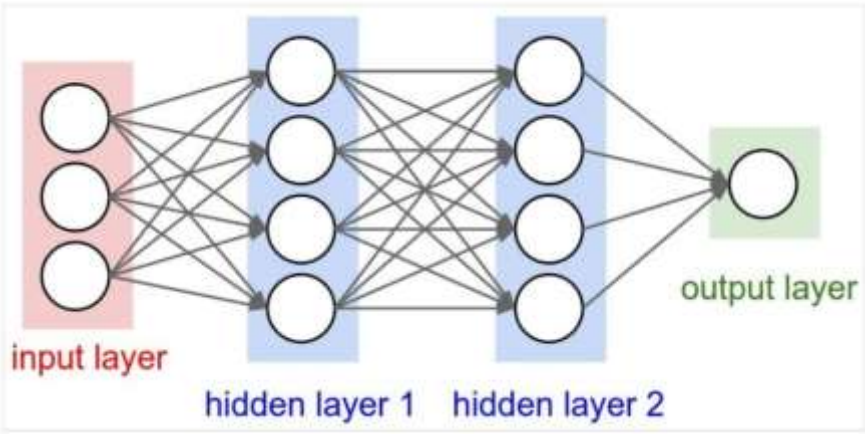
3.1 RNN-GRU

Recurrent Neural Networks (RNNs) are a type of artificial neural network that is designed to work with sequential data. RNNs are particularly useful in modeling time series data, natural language

processing, speech recognition, and many other tasks that involve sequential inputs. One of the variants of RNNs is the Gated Recurrent Unit (GRU) algorithm. GRU is a variant of RNN that was introduced in 2014. GRU is a simpler and more efficient version of the Long Short-Term Memory (LSTM) algorithm, which is another popular variant of RNN. The GRU algorithm has a gating mechanism that allows it to selectively update and reset the hidden state of the network at each time step. The gating mechanism consists of two gates: the reset gate and the update gate. The reset gate determines how much of the previous hidden state to forget, while the update gate determines how much of the new information to add to the current hidden state. The GRU algorithm has fewer parameters than the LSTM algorithm, which makes it faster and easier to train. GRU has been shown to perform as well as LSTM on a wide range of tasks, including machine translation, speech recognition, and image captioning.

3.2 Deep Neural Networks

Deep Neural Networks (DNNs), also known as Multi-Layer Perceptrons (MLPs), are a type of artificial neural network that is widely used for a variety of applications such as image classification, speech recognition, natural language processing, and many others. In DNN, the information flows only in one direction, from input to output, without any feedback loops. DNNs consist of several layers of interconnected neurons, where each neuron is connected to all the neurons in the previous and next layer. The input layer receives the input data, which is then passed through one or more hidden layers before reaching the output layer, where the final prediction is made. The weights and biases of the neurons in each layer are updated during the training phase, using a backpropagation algorithm, to minimize the error between the predicted output and the actual output.



Advantages of DNN:

- DNNs are simple and easy to implement compared to other deep learning models such as CNN and RNN.
- DNNs can handle a wide range of input data types such as numerical, categorical, and textual data.
- DNNs are highly customizable, and their architectures can be modified to suit specific applications.

Drawbacks of DNN compared to CNN:

- DNNs are not suitable for processing data that has a spatial structure such as images, videos, and audio signals.
- DNNs require a large number of parameters to achieve high accuracy on complex tasks, which can lead to overfitting and slow training.
- DNNs do not take into account the local spatial correlation between neighboring pixels in images, which is important for tasks such as image classification and object detection.
- Compared to DNNs, Convolutional Neural Networks (CNNs) are designed specifically for processing data with a spatial structure such as images and videos. CNNs use convolutional

layers to extract local features from the input data, which are then passed through one or more fully connected layers to make the final prediction. CNNs have been shown to achieve state-of-the-art performance on a wide range of image and video-related tasks.

In summary, DNNs are a simple and easy-to-implement type of neural network that can handle a wide range of input data types, while CNNs are specifically designed for processing data with a spatial structure such as images and videos. The main drawback of DNNs compared to CNNs is their limited ability to capture spatial information, which is important for many image and video-related tasks.

4. PROPOSED SYSTEM

Detecting electricity theft is a critical problem in the power distribution industry, as it leads to significant revenue losses and poses a threat to the stability of the power grid. With the increasing deployment of IoT-based smart energy meters, it is possible to detect electricity theft through data analytics and machine learning.

In this context, two approaches are adopted when renewable DG units are integrated in the power grid, namely, the net metering system and the feed-in tariffs (FITs) policy. In the net metering system, the excess generation from the DG can be stored as future credit for customers. On the other hand, in the FIT policy, which is referred to as clean energy cashback, customers sell all their generated energy to the grid and get paid in exchange. The incentives offered by the FIT programs are more effective compared with net metering for promoting renewable energy. Hence, FIT requires two meters to be installed in the customer premises, one meter is a selling meter that monitors the energy generated from the DG unit, which is directly injected (sold) to the grid, and the other meter is a buying meter that monitors the consumption. Thus, consumption and generation can be charged independently. In this two-metering system, malicious customers can manipulate the integrity of the reported energy generation data to claim higher supplied energy to the grid and hence falsely overcharge the electric utility company. Such a malicious act is possible due to the weak authentication firmware that is installed in most smart meters deployed worldwide. While several research works have investigated electricity theft cyber-attacks at the consumption domain, such a research problem is not well investigated in the DG domain and requires a better attention.

Therefore, this project evaluating performance of various deep learning algorithms such as deep feed forward neural network (DNN), recurrent neural network with gated recurrent unit (RNN-GRU) and convolutional neural network (CNN) for electricity cyber-attack detection. Now-a-days in advance countries solar plates are used to generate electricity and these users can sale excess energy to other needy users and they will be maintained two different meters which will record consumption and production details. While producing some malicious users may tamper smart meter to get more bill which can be collected from electricity renewable distributed energy. This attack may cause huge losses to agencies. To detect such attack, this project is employing deep learning models which can detect all possible alterations to predict theft.

The CNN architecture for this task would have an input layer that takes in the time-series data from the smart energy meter. The input data is then passed through multiple convolutional layers, which extract the relevant features from the input data. The features extracted by the convolutional layers are then fed into a fully connected layer, which performs the final classification task, i.e., detecting whether there is electricity theft or not. The training data for the CNN would consist of time-series data collected from smart energy meters, along with labels indicating whether or not there was electricity theft during that period. During training, the CNN learns to distinguish between normal and anomalous energy consumption patterns, which enables it to detect electricity theft cyber-attacks in real-time. One advantage of using CNNs for this task is that they can learn complex patterns and

relationships in the time-series data, which may be difficult to capture with traditional statistical methods. Additionally, CNNs can be trained using large amounts of data, which can help improve their accuracy and robustness. Overall, CNNs can be an effective tool for detecting electricity theft cyber-attacks from IoT-based smart energy meters, which can help reduce revenue losses and improve the stability of the power grid.

4.1 Dataset description

This dataset contains information of the amount of electricity each consumers used. Columns contains the dates and Rows refers to the consumers. This dataset contains the electricity consumption for a year 2015.

4.2 Data Preprocessing in Machine learning

Data pre-processing is a process of preparing the raw data and making it suitable for a machine learning model. It is the first and crucial step while creating a machine learning model. When creating a machine learning project, it is not always a case that we come across the clean and formatted data. And while doing any operation with data, it is mandatory to clean it and put in a formatted way. So, for this, we use data pre-processing task.

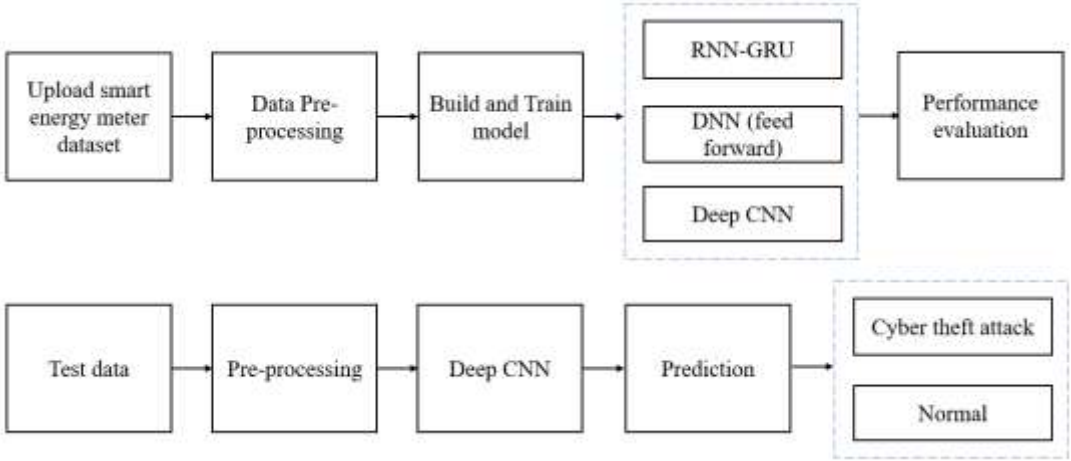


Fig. 1: Block diagram of proposed system.

4.3 CNN Classifier

CNN (Convolutional Neural Network) is a type of neural network that is particularly well-suited for visual recognition tasks, such as image classification, object detection, and segmentation. CNNs are designed to automatically learn spatial hierarchies of features from raw input data, such as images or videos, without the need for manual feature extraction. A typical CNN consists of multiple layers, including convolutional layers, pooling layers, and fully connected layers. In the convolutional layers, the network applies a set of learnable filters to the input image to extract features at different spatial locations. The filters are learned through backpropagation during training, and they enable the network to detect patterns such as edges, corners, and textures. The pooling layers reduce the spatial resolution of the feature maps and make them more robust to small translations.

The fully connected layers perform the final classification or regression task based on the features extracted from the previous layers. During training, the network learns to adjust the parameters of the filters and the fully connected layers to minimize the difference between the predicted outputs and the true labels of the training data. CNNs have been shown to achieve state-of-the-art performance on a wide range of visual recognition tasks, such as image classification, object detection, and segmentation. They have revolutionized the field of computer vision and have enabled breakthroughs in areas such as autonomous driving, facial recognition, and medical image analysis.

4.4 Advantages of proposed system

- Ability to learn complex representations: Deep CNNs can learn increasingly complex representations of input data as the depth of the network increases. This allows the network to

capture high-level features and patterns that are important for accurate classification, detection, segmentation, and other visual recognition tasks.

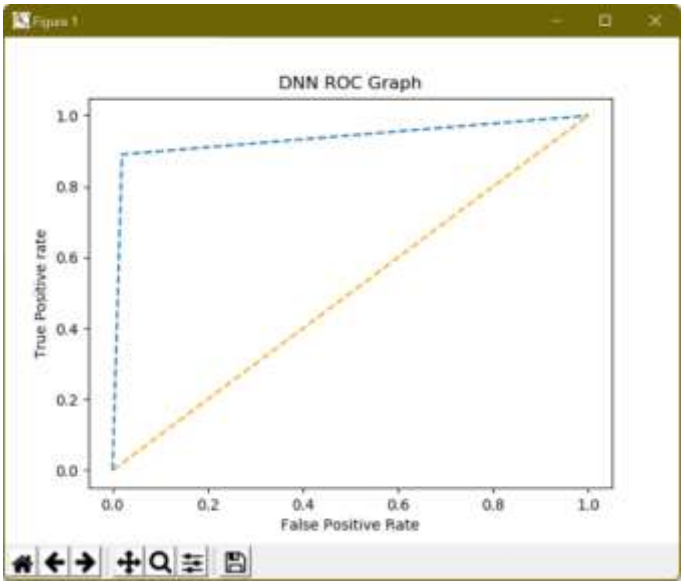
- Parameter sharing: The convolutional layers of deep CNNs use parameter sharing to reduce the number of parameters in the network. This makes the model more efficient and reduces the risk of overfitting, especially for large-scale datasets.
- Hierarchical feature extraction: Deep CNNs can extract features at multiple levels of abstraction, which enables the network to learn hierarchical representations of the input data. This is particularly useful for visual recognition tasks, where objects and scenes can be represented as a hierarchy of features.
- Translation invariance: Deep CNNs can achieve translation invariance, which means that the network can recognize objects in an image regardless of their position. This is achieved through the use of pooling layers, which reduce the spatial resolution of the feature maps and make them more robust to small translations.
- Transfer learning: Deep CNNs can be used for transfer learning, where a pre-trained model is fine-tuned on a new dataset with limited labeled examples. This is particularly useful for tasks with limited labeled data, as the pre-trained model can serve as a good starting point for learning new features and patterns.

5. RESULTS AND DISCUSSION

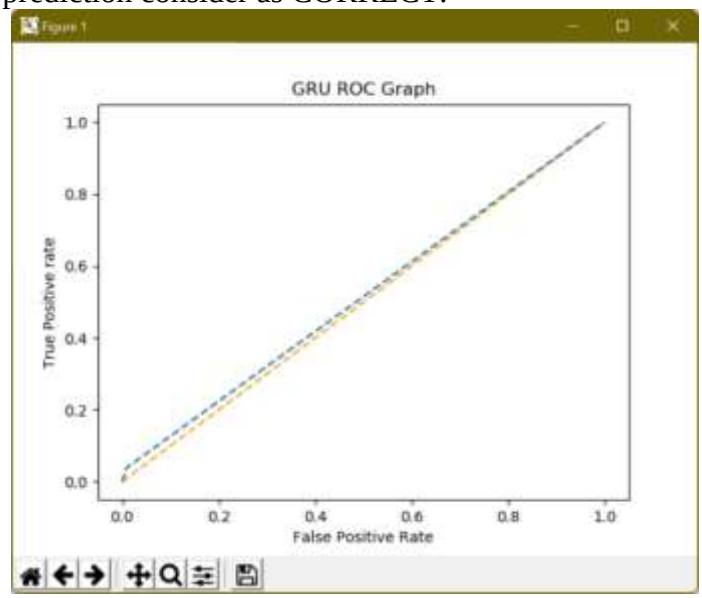
To implement this project, we have designed following modules:

1) Upload Electricity Theft Dataset: using this module we will upload dataset to application.
2) Preprocess Dataset: using this module we will read dataset and then remove missing values and then convert all non-numeric data into numeric as deep learning accept only numeric data. Processed dataset will be split into train and test where 80% dataset used for training and 20% for testing.
3) Feed Forward Neural Network: processed train data will be input to DNN algorithm to train theft detection model and this model will be applied on test data to calculate prediction accuracy.
4) RNN-GRU Algorithm: processed train data will be input to GRU algorithm to train theft detection model and this model will be applied on test data to calculate prediction accuracy.
5) Deep Learning CNN Algorithm: processed train data will be input to CNN algorithm to train theft detection model and this model will be applied on test data to calculate prediction accuracy.
6) Predict Electricity Theft: using this module we will upload test data and then Extension algorithm will predict weather test data is normal or contains theft signatures.
7) Comparison Graph: using this module we will plot comparison graph of all algorithms.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

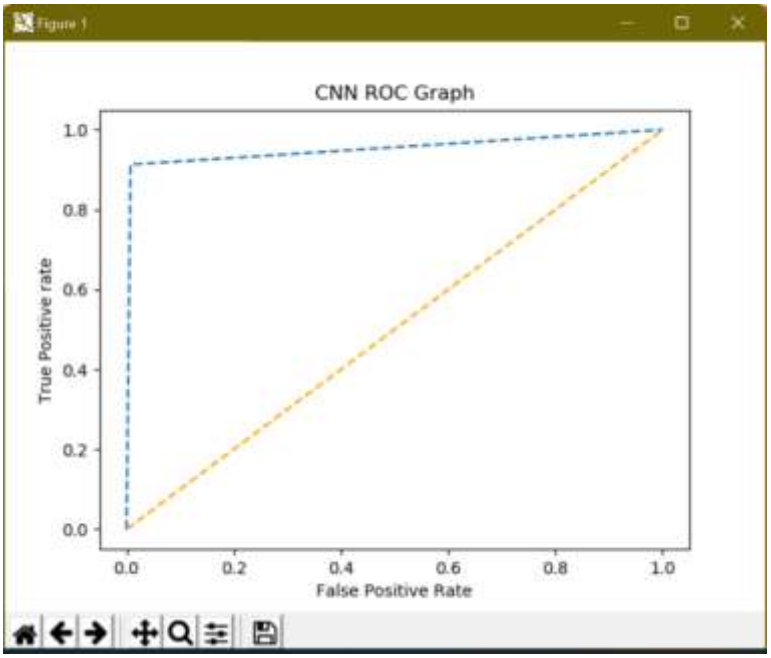


In above ROC graph x-graph represents False Positive Rate and y-axis represents True Positive Rate and if blue line comes below orange line then we can say prediction is false and if blue line comes on top of orange line then prediction consider as CORRECT.

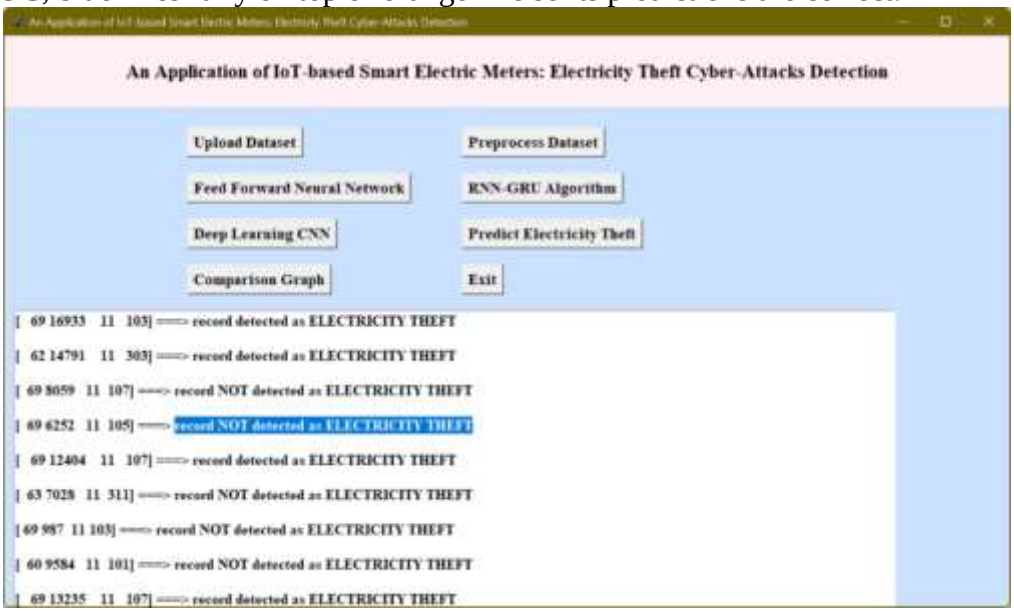


In above ROC, blue line coming little below to orange line so its predictions are not correct.

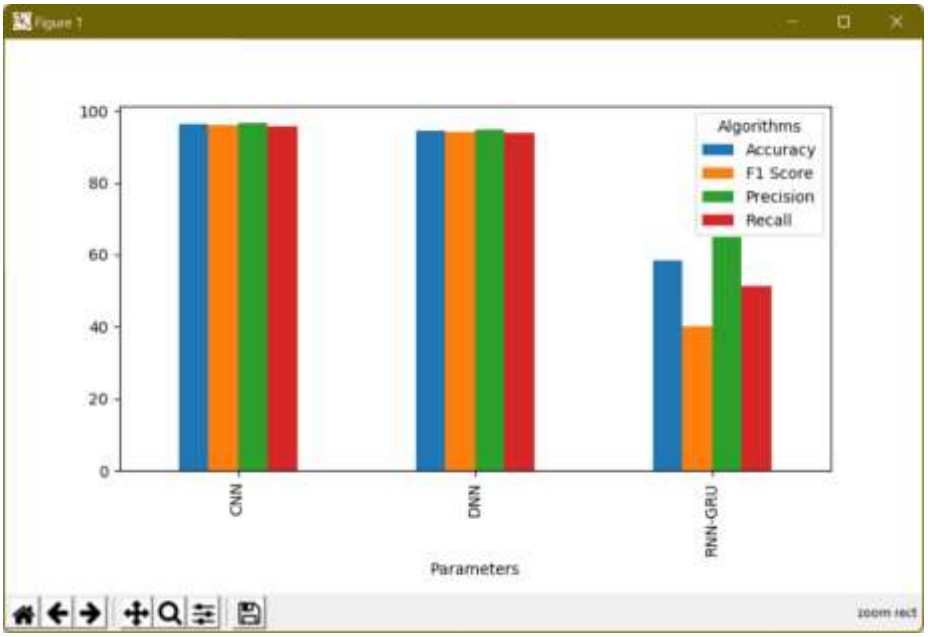
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023



In above ROC, blue lines fully on top of orange line so its predictions are correct.



In above screen in square bracket, we can see TEST data and after arrow =➔ symbol we can see THEFT detection and 'THEFT NOT DETECTTED'.



In above graph x-axis represents algorithm names with each different colour bar represents different metric such as 'accuracy, precision, recall and FSCORE' and Y-axis represents score values. In all algorithms CNN got high performance.

6. CONCLUSION

Global energy crises are increasing every moment. Everyone has the attention towards more and more energy production and also trying to save it. Electricity can be produced through many ways which is then synchronized on a main grid for usage. Weather losses are technical or non-technical. Technical losses can abstract be calculated easily, as we discussed in section of mathematical modeling that how to calculate technical losses. Whereas nontechnical losses can be evaluated if technical losses are known. Theft in electricity produce non-technical losses. To reduce or control theft one can save his economic resources. Smart meter can be the best option to minimize electricity theft, because of its high security, best efficiency, and excellent resistance towards many of theft ideas in electromechanical meters. So, in this paper we have mostly concentrated on theft issues. Therefore, this project evaluated performance of various deep learning algorithms such as deep feed forward neural network (DNN), recurrent neural network with gated recurrent unit (RNN-GRU) and convolutional neural network (CNN) for electricity cyber-attack detection.

REFERENCES

[1] Das, A.; McFarlane, A. Non-linear dynamics of electric power losses, electricity consumption, and GDP in Jamaica. Energy Econ. 2019, 84, 104530.
[2] Bashkari, S.; Sami, A.; Rastegar, M. Outage Cause Detection in Power Distribution Systems based on Data Mining. IEEE Trans. Ind. Inf. 2020.
[3] Bank, T.W. Electric Power Transmission and Distribution Losses (% of output); IEA: Paris, France, 2016.
[4] 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. Inform. 2018, 14, 1606–1615.
[5] Hasan, M.N., Toma, R.N., Nahid, A.A., Islam, M.M. and Kim, J.M., 2019. Electricity theft detection in smart grid systems: A CNN-LSTM based approach. Energies, 12(17), p.3310.
[6] K. Zheng, Q. Chen, Y. Wang, C. Kang and Q. Xia, "A Novel Combined Data-Driven Approach for Electricity Theft Detection," in IEEE Transactions on Industrial Informatics, vol. 15, no. 3, pp. 1809-1819, March 2019, doi: 10.1109/TII.2018.2873814.

[7] Li, S., Han, Y., Yao, X., Yingchen, S., Wang, J. and Zhao, Q., 2019. Electricity theft detection in power grids with deep learning and random forests. Journal of Electrical and Computer Engineering, 2019.

[8] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary and E. Serpedin, "PPETD: Privacy-Preserving Electricity Theft Detection Scheme with Load Monitoring and Billing for AMI Networks," in IEEE Access, vol. 7, pp. 96334-96348, 2019, doi: 10.1109/ACCESS.2019.2925322.

[9] Khan, Z.A., Adil, M., Javaid, N., Saqib, M.N., Shafiq, M. and Choi, J.G., 2020. Electricity theft detection using supervised learning techniques on smart meter data. Sustainability, 12(19), p.8023.

[10] Kocaman, B., Tümen, V. Detection of electricity theft using data processing and LSTM method in distribution systems. Sādhanā 45, 286 (2020). https://doi.org/10.1007/s12046-020-01512-0

[11] Li, B., Xu, K., Cui, X., Wang, Y., Ai, X., Wang, Y. (2018). Multi-scale DenseNet-Based Electricity Theft Detection. In: Huang, DS., Bevilacqua, V., Premaratne, P., Gupta, P. (eds) Intelligent Computing Theories and Application. ICIC 2018. Lecture Notes in Computer Science (), vol 10954. Springer, Cham. https://doi.org/10.1007/978-3-319-95930-6_17

[12] A. Aldegheishem, M. Anwar, N. Javaid, N. Alrajeh, M. Shafiq and H. Ahmed, "Towards Sustainable Energy Efficiency with Intelligent Electricity Theft Detection in Smart Grids Emphasising Enhanced Neural Networks," in IEEE Access, vol. 9, pp. 25036-25061, 2021, doi: 10.1109/ACCESS.2021.3056566.