Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

CONVOLUTIONAL NEURAL NETWORKS FOR ELECTRICITY CYBER ATTACK DETECTION: AN APPLICATION OF IOT-BASED ELECTRIC METERS

P. Hussain[1], K. Arun Kumar[2], Ch. Harish[2], B. Rajender[2]
[1,2]Department of Electronics and Communication Engineering, Kommuri Pratap Reddy Institute of Technology, Ghatkesar, Hyderabad.

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. 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.

Keywords:
Electricity theft, Cyber-attacks, IoT, deep learning, recurrent 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.

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.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

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.

3. PROPOSED SYSTEM

3.1 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.

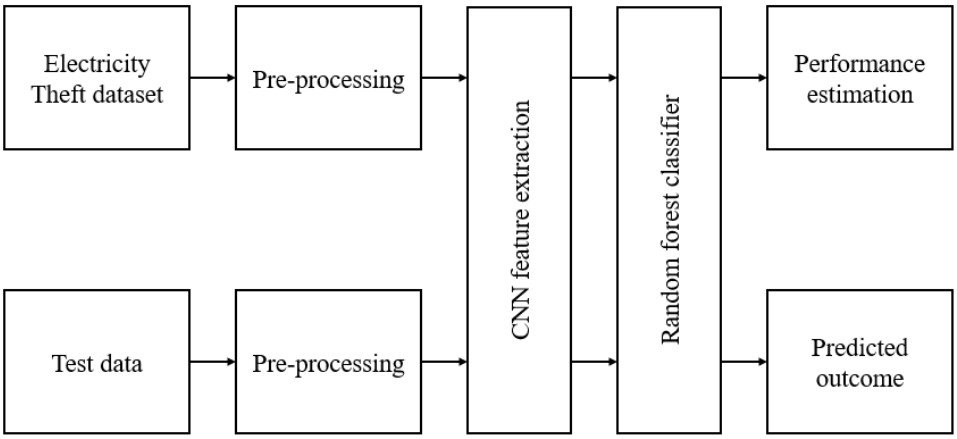


Fig. 1: Block diagram of proposed system.

3.2 CNN Classifier

According to the facts, training and testing of CNN involves in allowing every source data via a succession of convolution layers by a kernel or filter, rectified linear unit (ReLU), max pooling, fully connected layer and utilize SoftMax layer with classification layer to categorize the objects with probabilistic values ranging from.

Convolution layer is the primary layer to extract the features from a source image and maintains the relationship between pixels by learning the features of image by employing tiny blocks of source data. It's a mathematical function which considers two inputs like source image $I(x, y, d)$ where x and y denotes the spatial coordinates i.e., number of rows and columns. d is denoted as dimension of an image (here d=3 since the source image is RGB) and a filter or kernel with similar size of input image and can be denoted as $F(k_x, k_y, d)$..

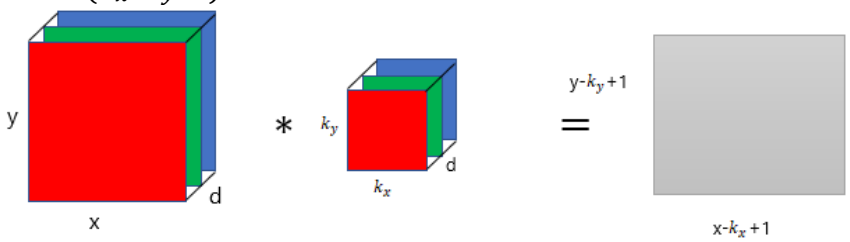
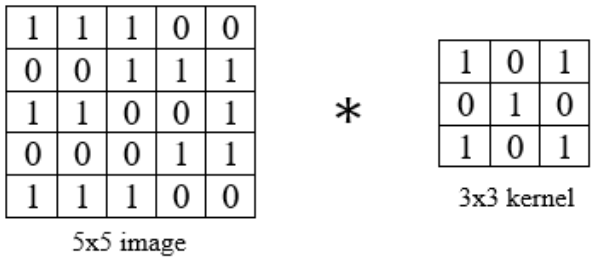


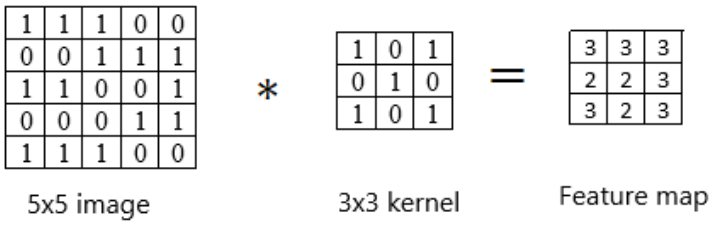
Fig. 2: Representation of convolution layer process.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

The output obtained from convolution process of input image and filter has a size of $C\left((x-k_x+1),(y-k_y+1),1\right)$, which is referred as feature map. Let us assume an input image with a size of 5×5 and the filter having the size of 3×3. The feature map of input image is obtained by multiplying the input image values with the filter values.



(a)



(b)

Fig. 3: Example of convolution layer process (a) an image with size 5×5 is convolving with 3×3 kernel (b) Convolved feature map.

ReLU layer

Networks those utilizes the rectifier operation for the hidden layers are cited as rectified linear unit (ReLU). This ReLU function $\mathcal{G}(\cdot)$ is a simple computation that returns the value given as input directly if the value of input is greater than zero else returns zero. This can be represented as mathematically using the function $max(\cdot)$ over the set of 0 and the input x as follows:

$$\mathcal{G}(x) = \max\{0, x\}$$

Max pooing layer

This layer mitigates the number of parameters when there are larger size images. This can be called as subsampling or down sampling that mitigates the dimensionality of every feature map by preserving the important information. Max pooling considers the maximum element form the rectified feature map.

3.3 Random Forest Algorithm

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining multiple classifiers to solve a complex problem and to improve the performance of the model. As the name suggests, "Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output. The greater number of trees in the forest leads to higher accuracy and prevents the problem of overfitting.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

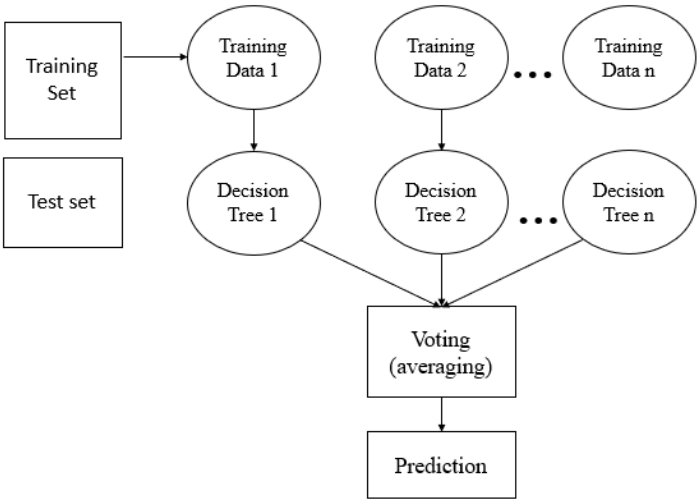


Fig. 4: Random Forest algorithm.

Random Forest algorithm

Step 1: In Random Forest n number of random records are taken from the data set having k number of records.
Step 2: Individual decision trees are constructed for each sample.
Step 3: Each decision tree will generate an output.
Step 4: Final output is considered based on Majority Voting or Averaging for Classification and regression respectively.

Types of Ensembles

Before understanding the working of the random forest, we must look into the ensemble technique. Ensemble simply means combining multiple models. Thus, a collection of models is used to make predictions rather than an individual model. Ensemble uses two types of methods:

Bagging– It creates a different training subset from sample training data with replacement & the final output is based on majority voting. For example, Random Forest. Bagging, also known as Bootstrap Aggregation is the ensemble technique used by random forest. Bagging chooses a random sample from the data set. Hence each model is generated from the samples (Bootstrap Samples) provided by the Original Data with replacement known as row sampling. This step of row sampling with replacement is called bootstrap. Now each model is trained independently which generates results. The final output is based on majority voting after combining the results of all models. This step which involves combining all the results and generating output based on majority voting is known as aggregation.

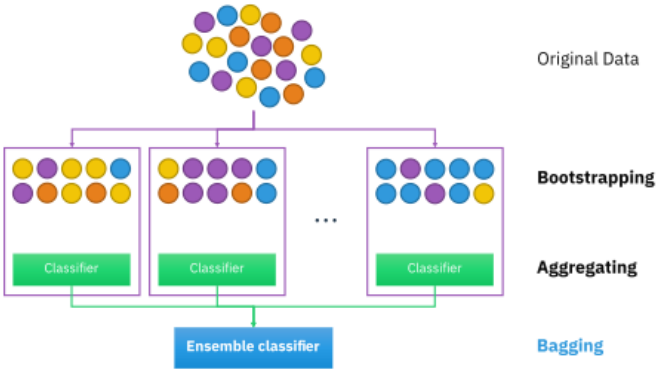


Fig. 5: RF Classifier analysis.

Boosting– It combines weak learners into strong learners by creating sequential models such that the final model has the highest accuracy. For example, ADA BOOST, XG BOOST.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

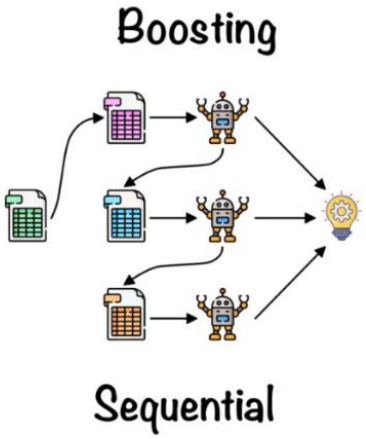
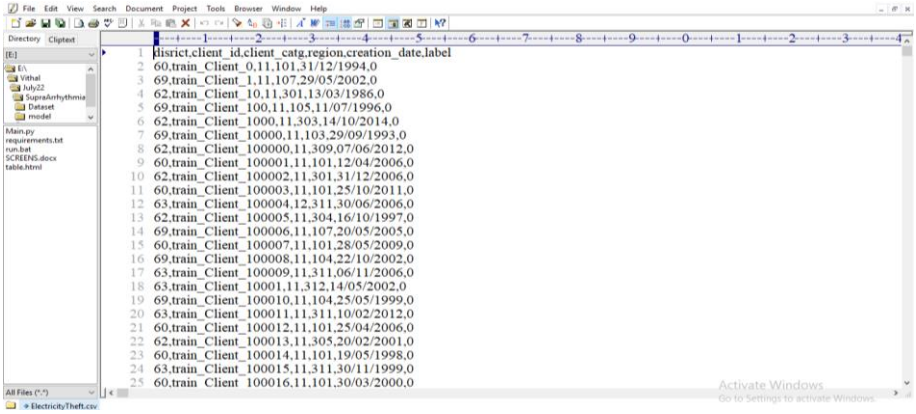


Fig. 6: Boosting RF Classifier.

4. RESULTS AND DISCUSSION

To implement this project, we have used Smart Meter electricity recording dataset and below are the details of that dataset

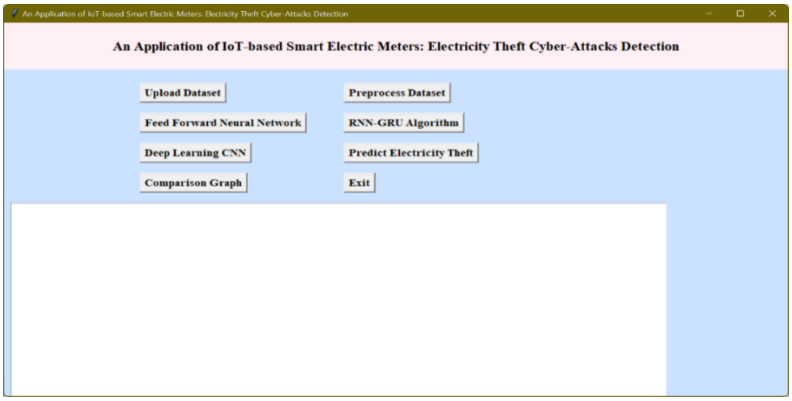


In above screen first row represents dataset column names and remaining rows contains dataset values which contains electricity details and last column contains class label as 0 or 1 where 0 means No Attack and 1 means Attack.

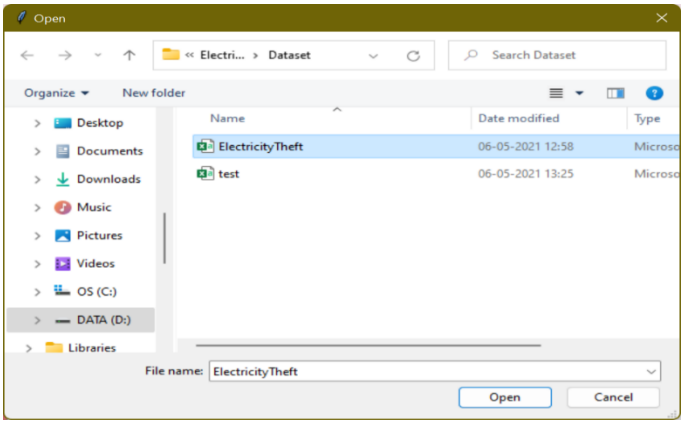
To implement this project, we have designed following modules

1) Upload Electricity Theft Dataset: using this module we will upload dataset to application
2) Pre-process 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

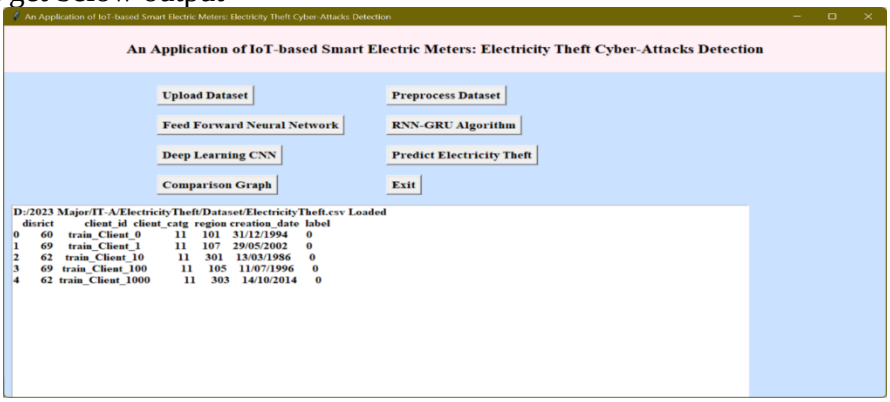
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023



In above screen click on 'Upload Electricity Theft Dataset' button to upload dataset and get below output

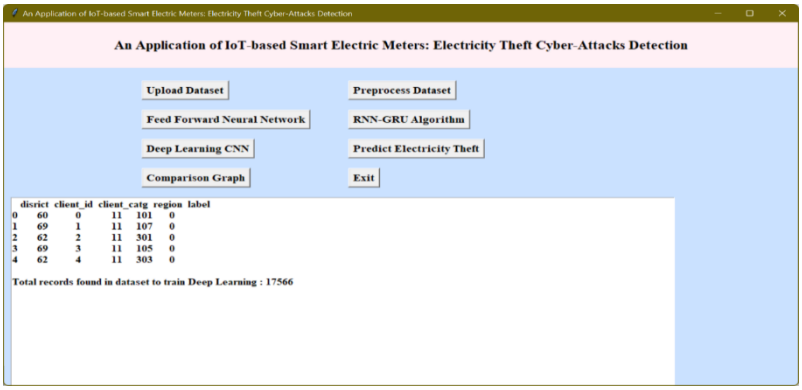


In above screen selecting and uploading 'electricity theft' dataset and then click on 'Open' button to load dataset and get below output

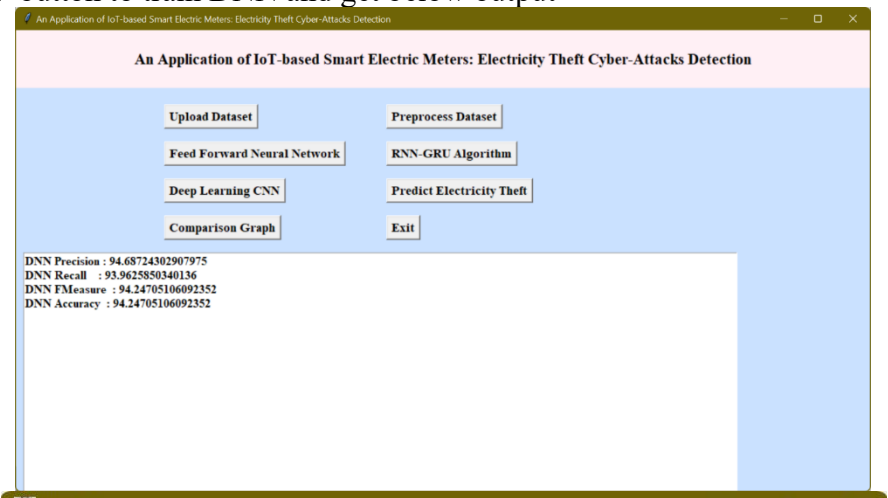


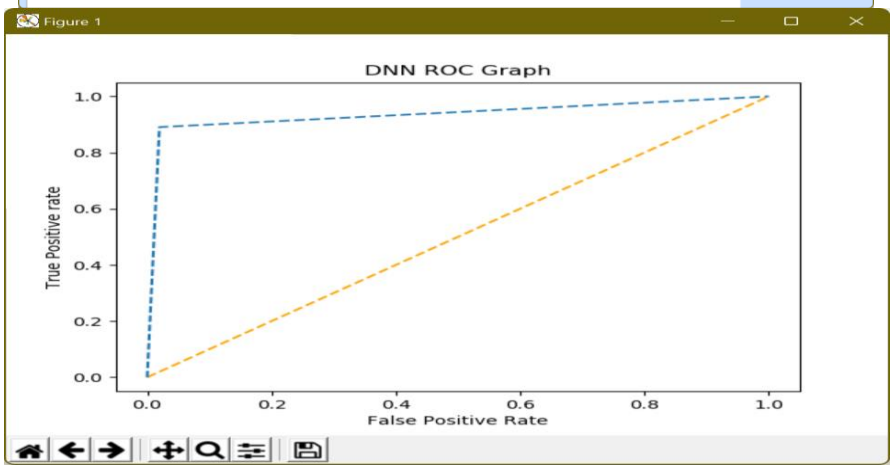
In above screen dataset loaded and now click on 'Preprocess Dataset' button to clean dataset and get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023



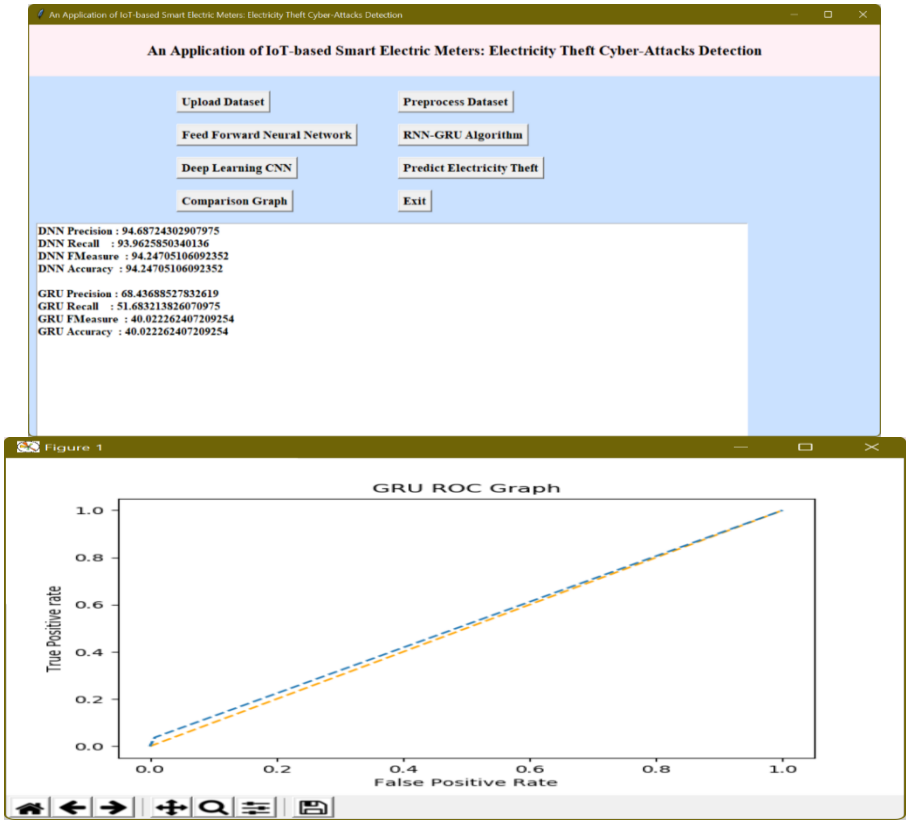
In above screen all non-numeric data converted to numeric format and now click on 'Feed Forward Neural Network' button to train DNN and get below output



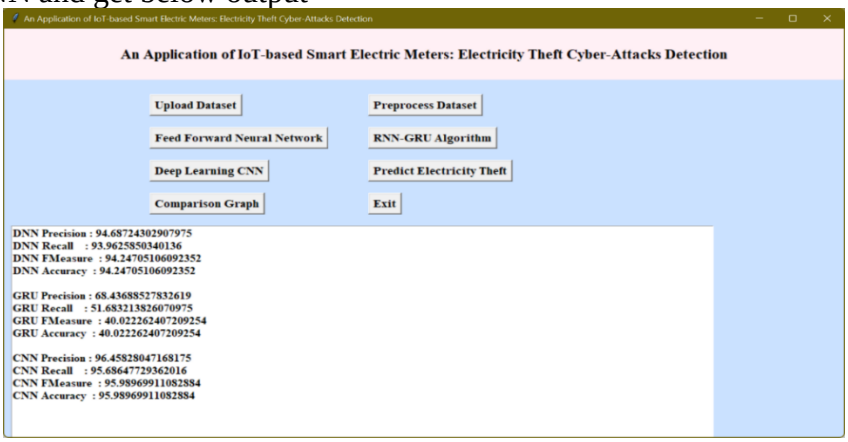


In above screen with DNN feed forward algorithm we got 94.24% accuracy and in ROC graph x-graph represents False Positive Rate and y-axis represents True Positive Rate and if blue line comes below orange line then we can say prediction is false and if blue line comes on top of orange line then prediction consider as CORRECT. Now close above graph and then click on 'RNN-GRU Algorithm' button to train GRU and get below output

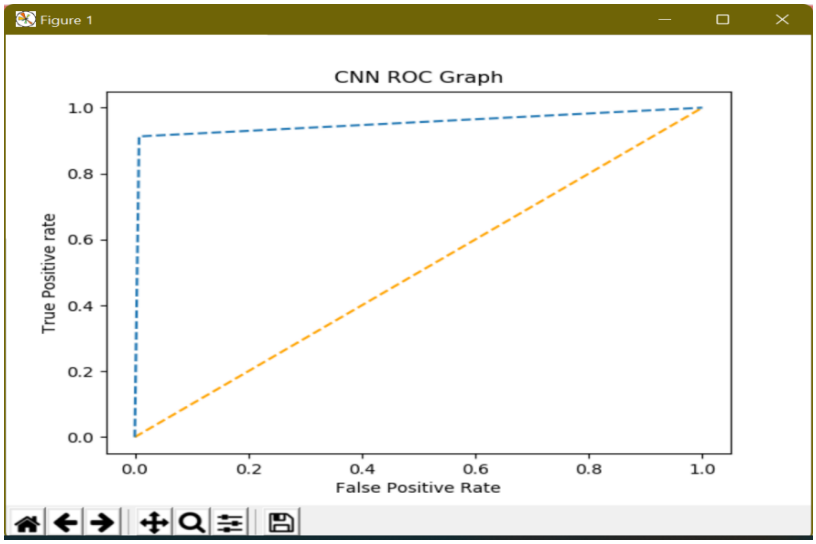
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023



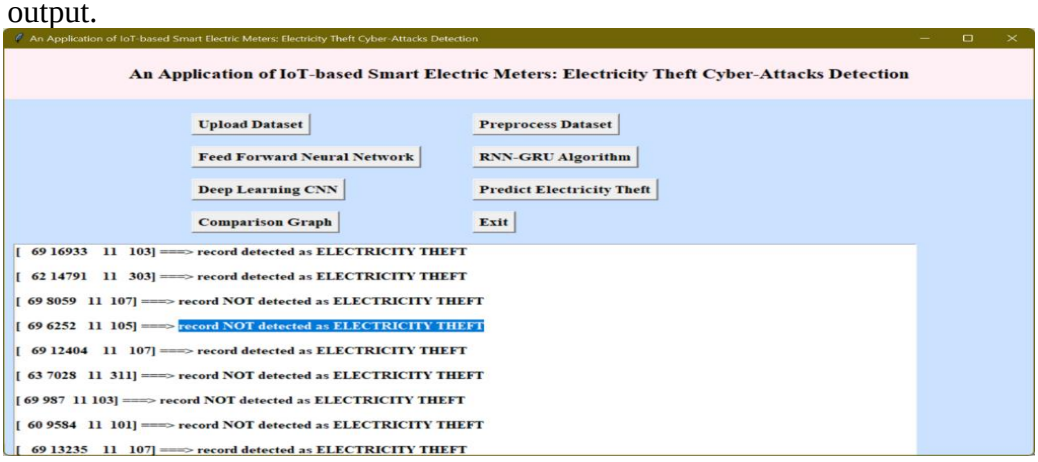
In above screen with GRU we got 40.02% accuracy and blue line coming little below to orange line, so its predictions are not correct and now close above graph and then click on 'Deep Learning CNN' button to train CNN and get below output



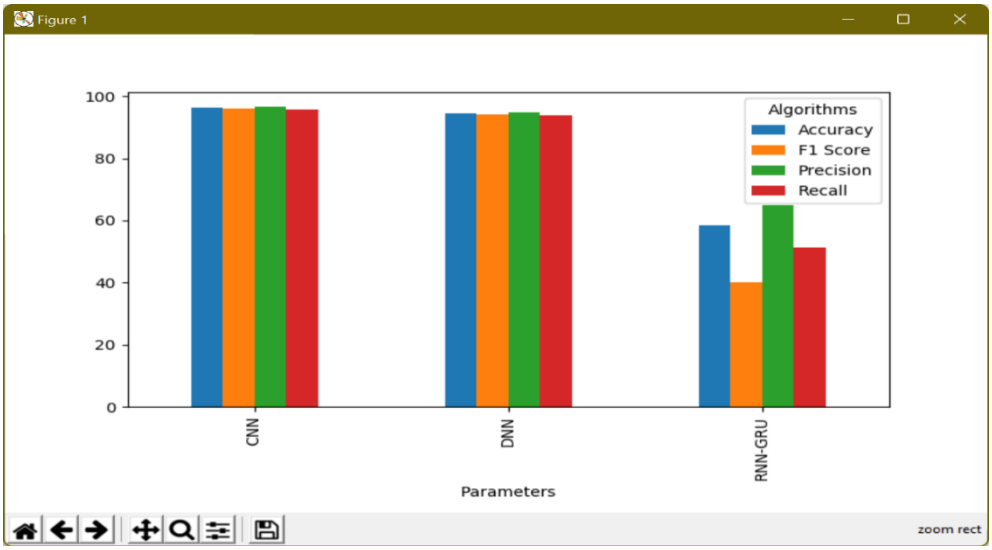
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023



In above screen with CNN, we got 95.98% accuracy and blue lines fully on top of orange line so its predictions are correct. Now click on 'Predict Electricity Theft' button to upload test data and get prediction output.



In above screen in square bracket, we can see TEST data and after arrow =➔ symbol we can see THEFT detection and 'THEFT NOT DETECTTED'. Now click on 'Comparison Graph' button to get below graph



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.

5. 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