

ELECTRICITY THEFT CYBER ATTACKS DETECTION FOR SMART ELECTRIC METERS

L. C. Usha Maheswari¹, P. Sanjana², P. Varshini², V. Akshitha², P. Ujwala²

¹Assistant Professor, ²UG Scholar, ^{1,2}Department of CSE-Cyber Security

^{1,2}Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

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.

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.

Keywords: Electricity theft, cyber-attacks, smart electric meters.

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. al [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.

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. 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. 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.

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.

Dataset description

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

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.

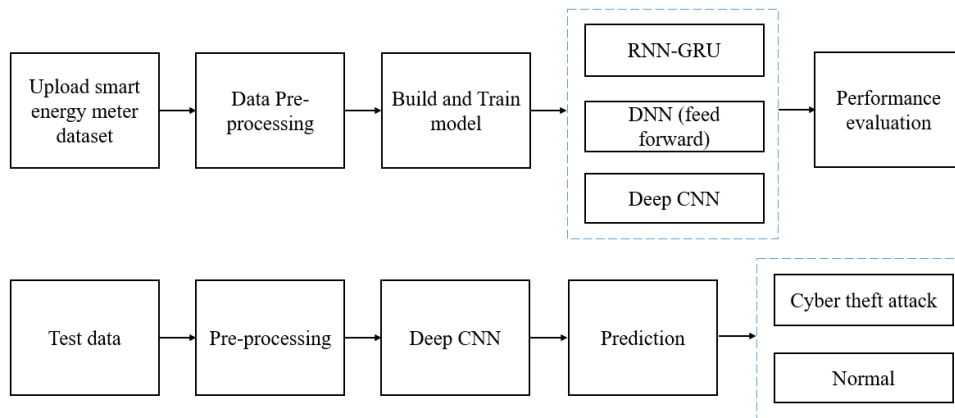


Fig. 1: Block diagram of proposed system.

Why do we need Data Pre-processing?

A real-world data generally contains noises, missing values, and maybe in an unusable format which cannot be directly used for machine learning models. Data pre-processing is required tasks for cleaning the data and making it suitable for a machine learning model which also increases the accuracy and efficiency of a machine learning model.

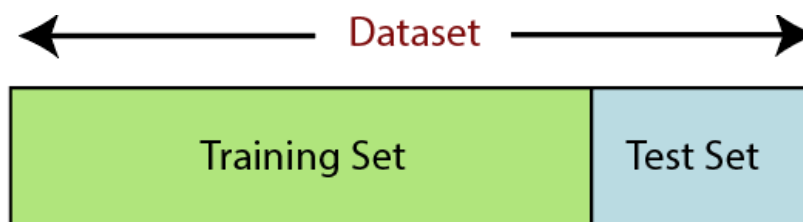
- Getting the dataset
- Importing libraries
- Importing datasets
- Finding Missing Data
- Encoding Categorical Data
- Splitting dataset into training and test set
- Feature scaling

Splitting the Dataset into the Training set and Test set

In machine learning data pre-processing, we divide our dataset into a training set and test set. This is one of the crucial steps of data pre-processing as by doing this, we can enhance the performance of our machine learning model.

Suppose if we have given training to our machine learning model by a dataset and we test it by a completely different dataset. Then, it will create difficulties for our model to understand the correlations between the models.

If we train our model very well and its training accuracy is also very high, but we provide a new dataset to it, then it will decrease the performance. So we always try to make a machine learning model which performs well with the training set and also with the test dataset. Here, we can define these datasets as:



Training Set: A subset of dataset to train the machine learning model, and we already know the output.

Test set: A subset of dataset to test the machine learning model, and by using the test set, model predicts the output.

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.

Layers Description

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 $F(k_x, k_y, d)$.

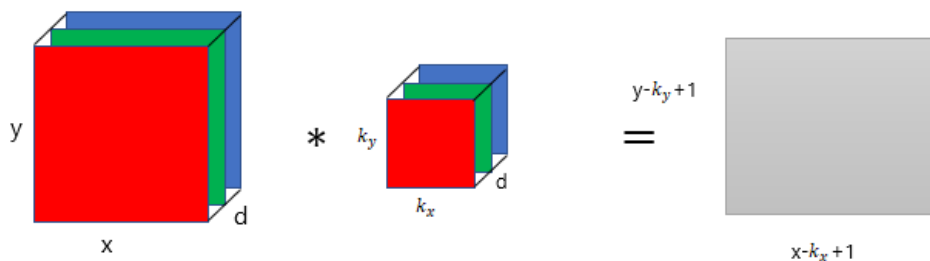


Fig. 2: Representation of convolution layer process.

The output obtained from convolution process of input image and filter has a size of $C((x - k_x + 1), (y - k_y + 1), 1)$, 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.

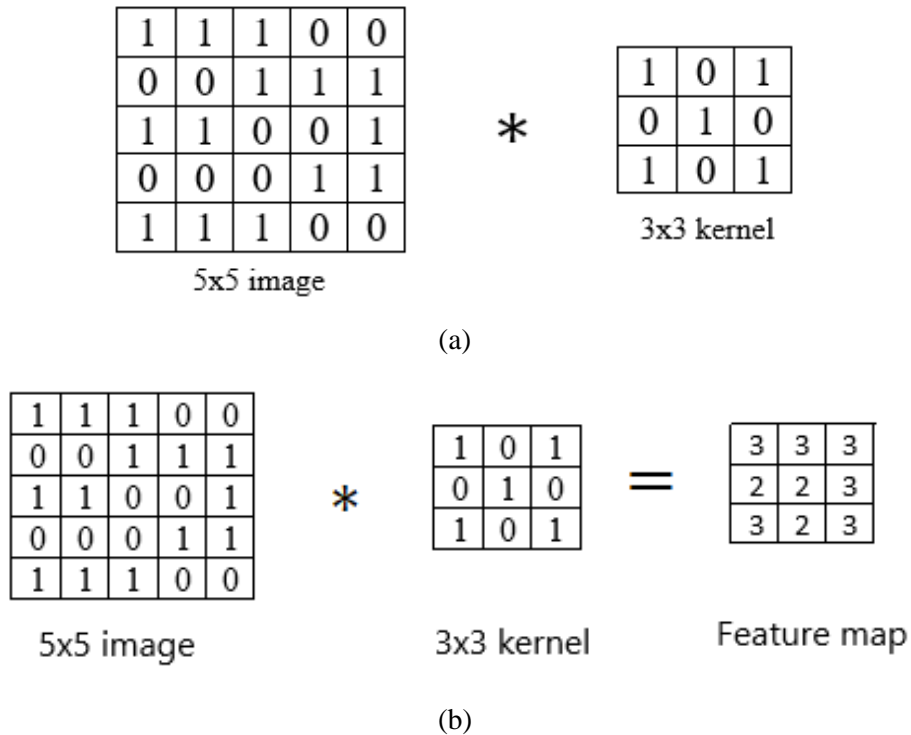


Fig. 3: Example of convolution layer process (a) an image with size 5×5 is convolving with 3×3 kernel (b) Convolved feature map.

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:

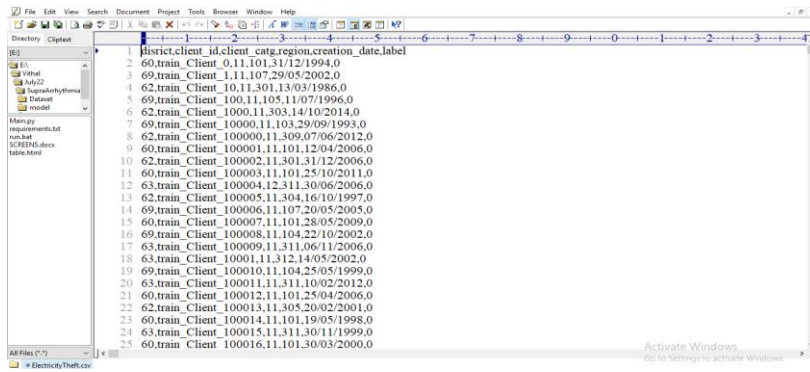
$$\mathcal{G}(x) = \max\{0, x\}$$

Max pooling 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.

4. RESULTS AND DISCUSSION

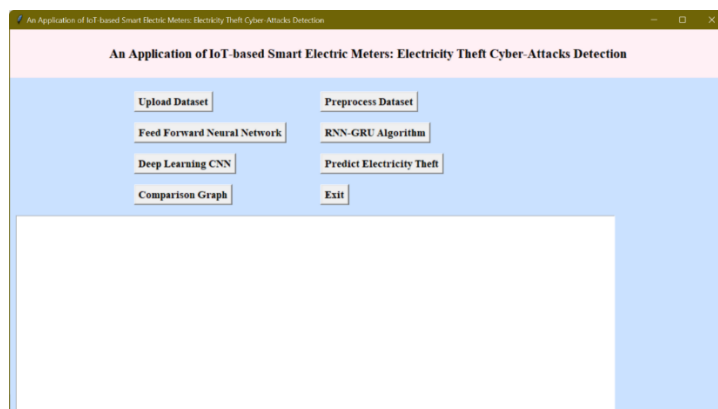
To implement this project, we have used Smart Meter electricity recording dataset and below are the details of that dataset



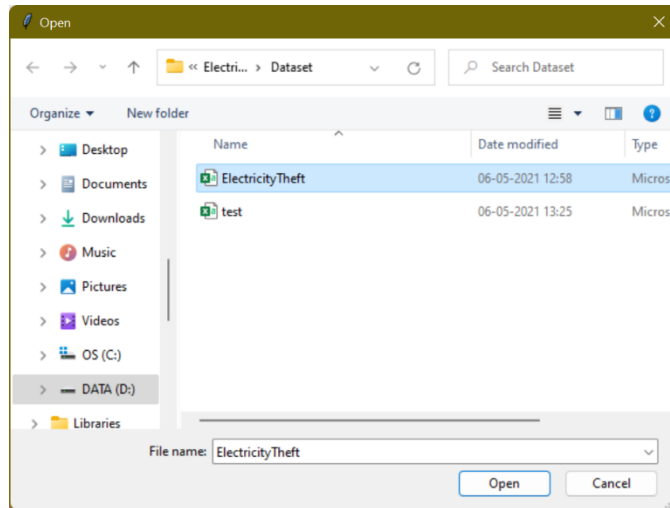
In above screen first row represents dataset column names and remaining rows contains dataset values which contains electricity details and last column contains class label as 0 or 1 where 0 means No Attack and 1 means Attack.

To implement this project, we have designed following modules

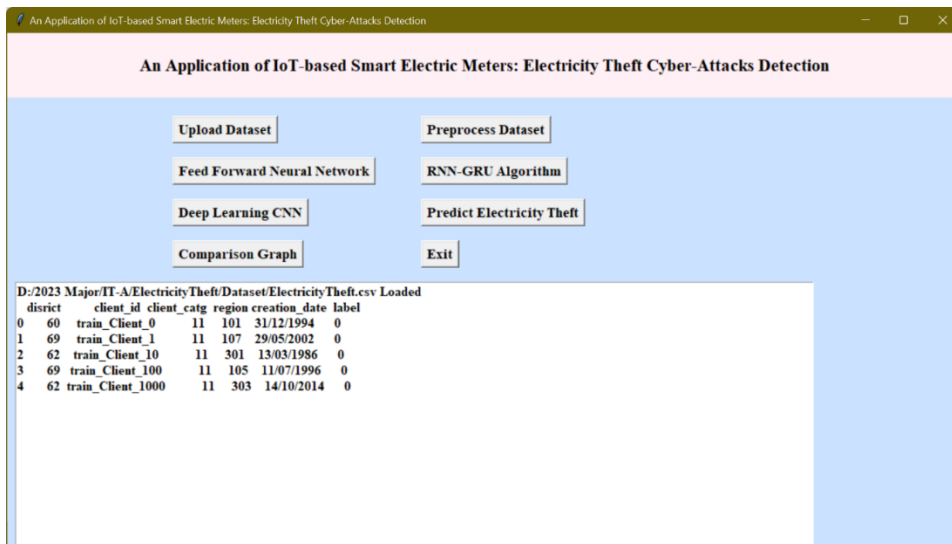
- 1) Upload Electricity Theft Dataset: using this module we will upload dataset to application
- 2) Preprocess Dataset: using this module we will read dataset and then remove missing values and then convert all non-numeric data into numeric as deep learning accept only numeric data. Processed dataset 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



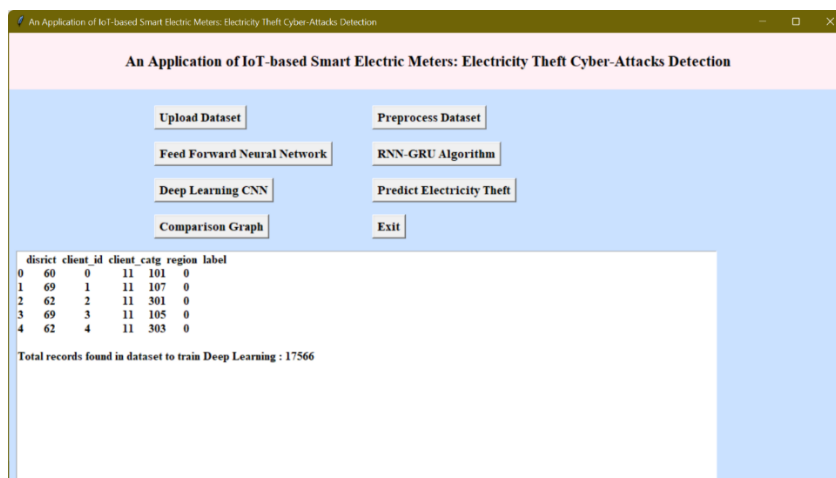
In above screen click on ‘Upload Electricity Theft Dataset’ button to upload dataset and get below output



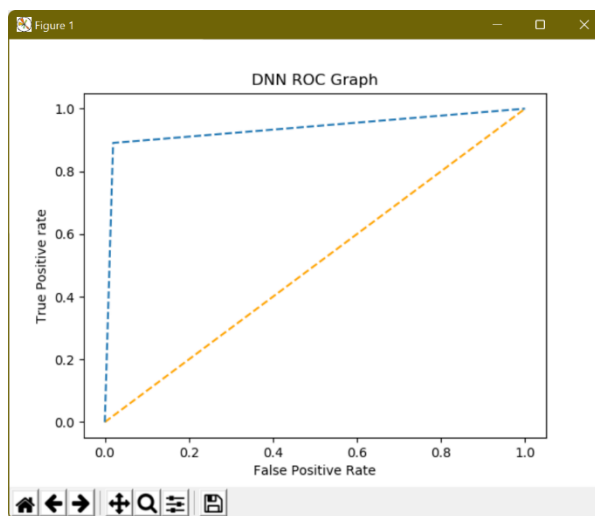
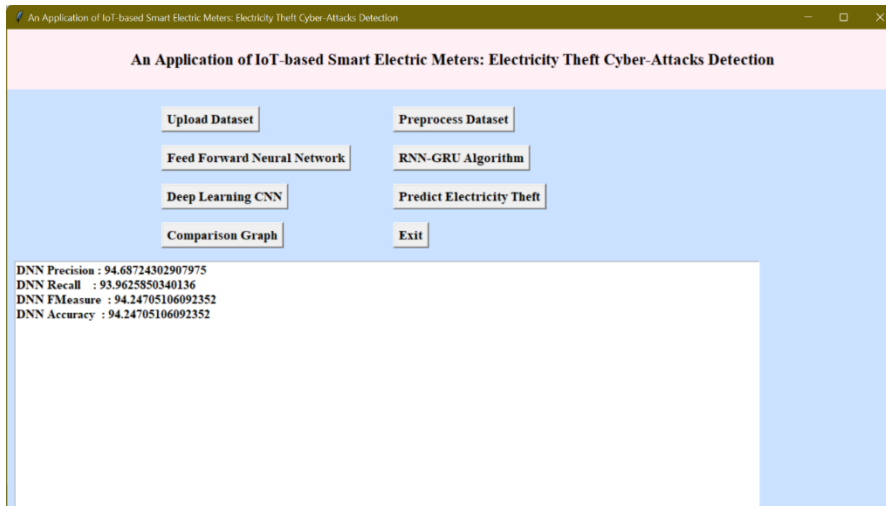
In above screen selecting and uploading ‘electricity theft’ dataset and then click on ‘Open’ button to load dataset and get below output



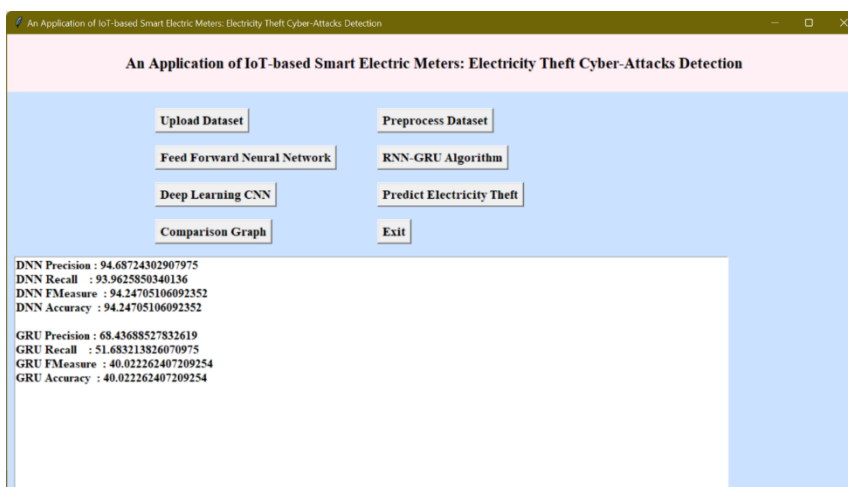
In above screen dataset loaded and now click on ‘Preprocess Dataset’ button to clean dataset and get below output

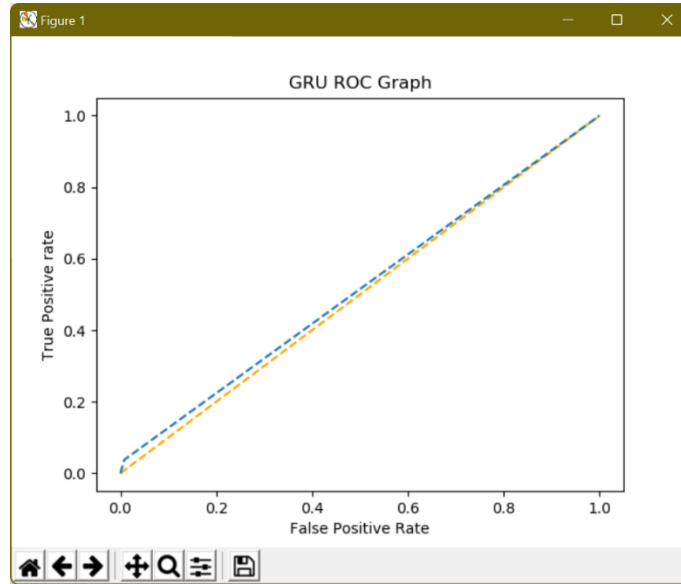


In above screen all non-numeric data converted to numeric format and now click on ‘Feed Forward Neural Network’ button to train DNN and get below output



In above screen with DNN feed forward algorithm we got 94.24% accuracy and in ROC graph x-axis 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

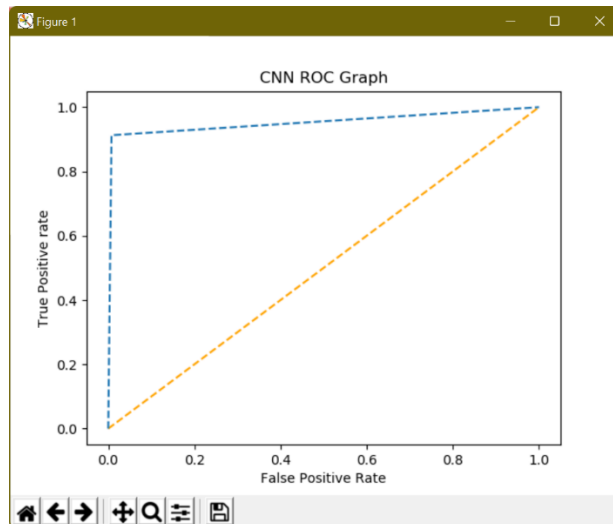




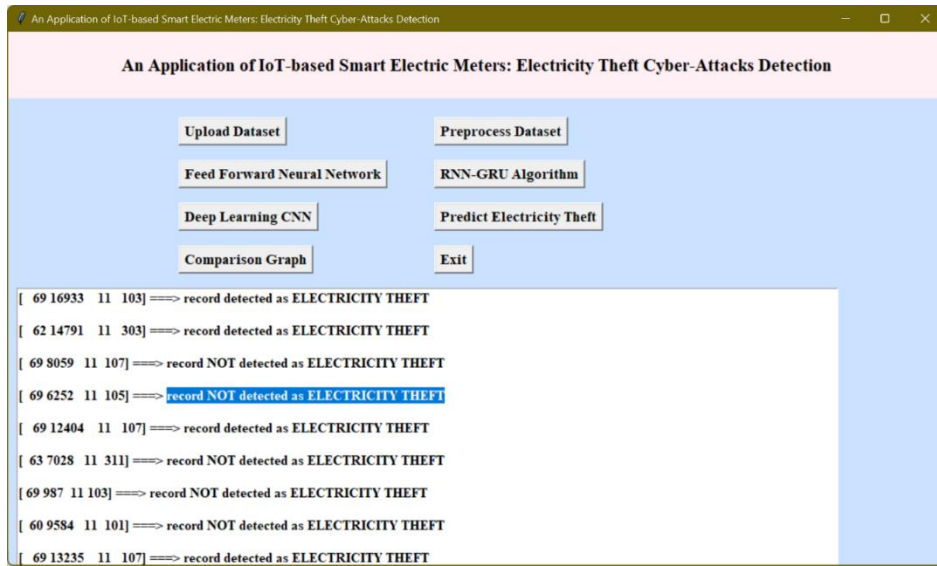
In above screen with GRU we got 40.02% accuracy and blue line coming little below to orange line so its predictions are not correct and now close above graph and then click on 'Deep Learning CNN' button to train CNN and get below output

The screenshot shows a web application window titled 'An Application of IoT-based Smart Electric Meters: Electricity Theft Cyber-Attacks Detection'. The interface includes several buttons: 'Upload Dataset', 'Preprocess Dataset', 'Feed Forward Neural Network', 'RNN-GRU Algorithm', 'Deep Learning CNN', 'Predict Electricity Theft', 'Comparison Graph', and 'Exit'. Below the buttons, a text area displays performance metrics for three models:

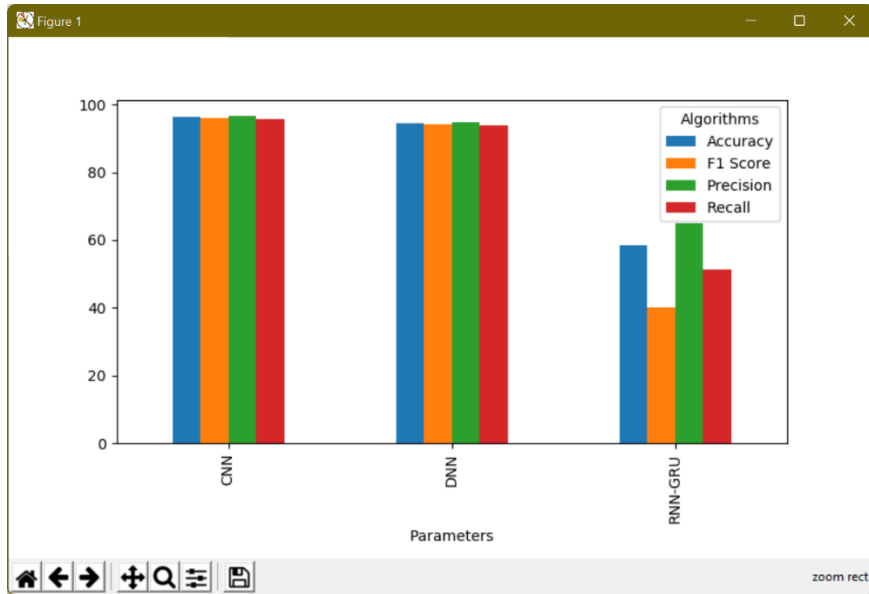
Model	Precision	Recall	FMeasure	Accuracy
DNN	94.68724302907975	93.9625850340136	94.24705106092352	94.24705106092352
GRU	68.43688527832619	51.683213826070975	40.022262407209254	40.022262407209254
CNN	96.45828047168175	95.68647729362016	95.98969911082884	95.98969911082884



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 DETECTED’. 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. Alasmay 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.