2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

# Deep Learning-based Cybersecurity for Smart Grids: An Evaluation in Detecting Electricity Theft in Renewable Distributed Energy Systems

**S. Spandana Reddy[1], Kolagani Geethika[2], Nakkala Devendar Reddy[2], Nalla Bhoopal Reddy[2], Akula Kranthi Sai[2], Amarthakurthi Srinu[2]**

[1]Assistant Professor,[2]UG Scholar,[1,2]Department of Computer Science and Engineering (Cyber Security)

[1,2]Malla Reddy Engineering College and Management Sciences, Kistapur, Medchal, 501401, 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. Therefore, this project evaluating performance of various deep learning algorithms such as deep feed forward neural network (DNN), and recurrent neural network with gated recurrent unit (RNN-GRU) 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:** Internet of things, Cyber-attack, Smart energy meters, Deep neural networks, 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. 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.

## 3. PROPOSED SYSTEM

### 3.1 Overview

Smart electric meters are devices that collect data about electricity usage, such as voltage, current, power factor, and more. To detect and predict electricity theft or cyber-attacks, a deep feed-forward neural network can be used. This type of neural network is designed to process information in one direction, from the input layer to the output layer, without any feedback connections. It is called "deep" because it has multiple hidden layers, allowing it to learn complex patterns and representations. To use this neural network for electricity theft and cyber-attack detection, the first step is to collect the relevant data from smart electric meters. This data serves as the input for the neural network. Before feeding the data into the network, preprocessing steps such as normalization, feature scaling, or outlier removal may be necessary to ensure optimal performance. Next, the architecture of the neural network needs to be designed. This involves determining the number of hidden layers, the number of nodes in each layer, and the overall depth of the network. The complexity of the problem at hand and the available data will guide these design decisions.

The neural network is then trained using a labeled dataset. This dataset should include instances of normal electricity usage as well as instances where electricity theft or cyber-attacks occurred. During training, the neural network learns to associate patterns in the input data with the corresponding labels, enabling it to recognize similar patterns in the future. The hidden layers of the neural network play a crucial role in feature extraction. They automatically learn abstract representations of the input data, capturing relevant information that can help in detecting patterns associated with electricity theft or cyber-attacks. Once the neural network is trained, it can be used to predict and detect electricity theft or cyber-attacks in real-time. The data from the smart electric meters is fed into the network, and the output layer provides a prediction or detection result based on the learned patterns. To ensure ongoing security, the system continuously monitors the incoming data from smart electric meters. If the neural network detects any suspicious patterns or anomalies associated with electricity theft or cyber-attacks, it can trigger an alert for further investigation. Periodic retraining of the neural network is essential to adapt to evolving attack techniques. As new data is collected and more instances of electricity theft or cyber-attacks are detected, the neural network can be updated and improved to enhance its performance. Figure 1 shows the proposed system model. The detailed operation illustrated as follows:

**Step 1. Dataset Preprocessing:**

- **Data Collection**: Gather historical data from IoT-based smart electric meters, including electricity consumption patterns, network traffic data, and any available data related to past cyber attacks or electricity theft incidents.
- **Data Integration**: Combine data from various sources into a single dataset for analysis. Ensure that data from different sources are compatible and have a common time reference.
- **Data Cleaning**: Identify and handle missing values, outliers, and anomalies in the dataset. Clean and sanitize the data to remove noise or errors that could affect model performance.
- **Data Transformation**: Perform data transformations such as normalization or standardization to ensure that all features have similar scales. Some data may also require encoding (e.g., one-hot encoding) for machine learning models.
- **Data Splitting**: Divide the dataset into training, validation, and test sets. The training set is used for model training, the validation set for hyperparameter tuning, and the test set for model evaluation.

**Step 2. Deep Neural Network (DNN) Model Building:**

- **Architecture Selection**: Choose an appropriate DNN architecture for the task. In the context of electricity theft and cyber-attack detection, a neural network model, such as a feedforward neural network or a convolutional neural network (CNN), may be suitable.
- **Model Design**: Design the neural network architecture, including the number of layers, the number of neurons in each layer, and the activation functions. Consider incorporating techniques like dropout and batch normalization to improve model generalization.
- **Loss Function**: Define an appropriate loss function for the binary classification problem of detecting cyber-attacks (1) vs. non-attacks (0).
- **Optimization Algorithm**: Select an optimization algorithm (e.g., Adam, RMSprop) to update the neural network's weights during training.

- **Training**: Train the DNN model on the training dataset using the selected optimization algorithm and loss function. Monitor training progress and use early stopping to prevent overfitting.
- **Hyperparameter Tuning**: Tune hyperparameters, such as learning rate, batch size, and the number of epochs, on the validation dataset to optimize model performance.

**Step 3. Prediction:**

- **Model Evaluation**: Evaluate the trained DNN model's performance on the test dataset using appropriate evaluation metrics, such as accuracy, precision, recall, F1-score, and receiver operating characteristic (ROC) curve.
- **Cyber Attack Detection**: Use the trained model to make real-time predictions on incoming data from smart electric meters. The model can classify data points as either normal or indicative of a cyber-attack.

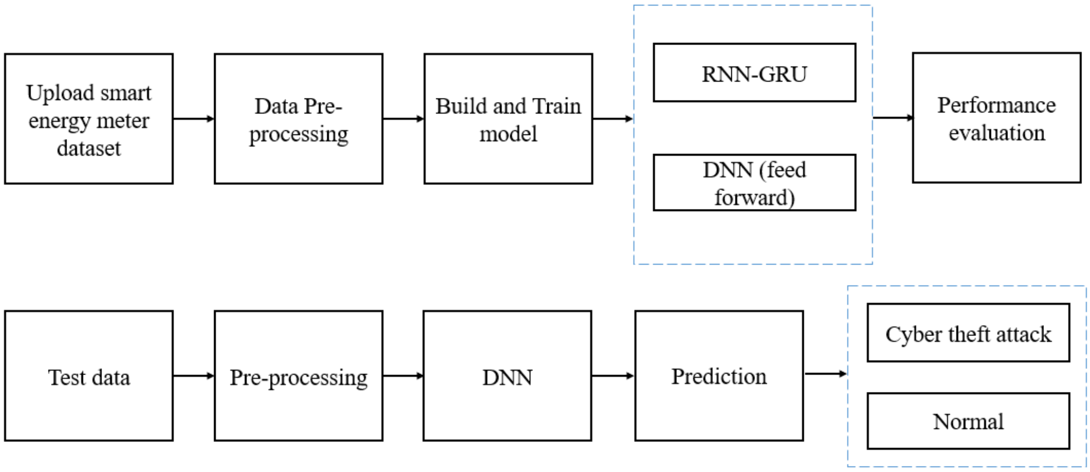


Fig. 1: Block diagram of proposed system.

### 3.2 Data Preprocessing

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.

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.

**One-Hot Encoding**: Categorical variables are one-hot encoded to convert them into a numerical format suitable for machine learning models. The code uses the pd.get_dummies() function to create binary columns for each category within categorical variables. This transformation allows machine learning algorithms to work with categorical data effectively.

**Standardization**: Standard Scaler is applied to scale numeric features, ensuring that they have a mean of 0 and a standard deviation of 1. The 'Standard Scaler' from scikit-learn is used to standardize specific numeric features. Standardization is a common preprocessing step to bring features to a similar scale, which can improve the performance of some machine learning algorithms. This transformation is important for several reasons:

- **Equal Scaling**: StandardScaler scales each feature to have the same scale. This is crucial for algorithms that are sensitive to the scale of features, such as gradient-based optimization algorithms (e.g., in neural networks) and distance-based algorithms (e.g., k-means clustering).
- **Mean Centering**: By subtracting the mean from each data point, StandardScaler centers the data around zero. This can help algorithms converge faster during training and improve their performance.
- **Normalization**: Scaling by the standard deviation normalizes the data, ensuring that features have comparable variances. This can prevent certain features from dominating others in the modeling process.
- **Interpretability**: Standardized data is more interpretable because it puts all features on a common scale, making it easier to compare the relative importance of features.

### 3.3 Dataset Splitting

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.

**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.

## 4. RESULTS AND DISCUSSION

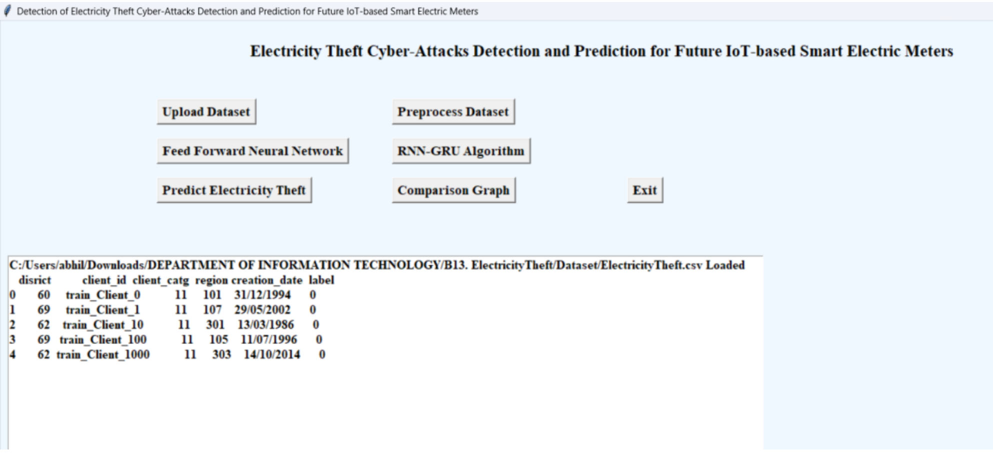
The dataset contains following columns

- district: This column represents the district where the client is located. It is a categorical variable with numerical values (e.g., 60, 69, 62, 63).
- client_id: This column is a unique identifier for each client. It is likely a string or alphanumeric value.
- client_catg: This column represents a category or classification for the client. It is a categorical variable with numerical values (e.g., 11, 12).
- region: This column indicates the region where the client is located. It is a categorical variable with numerical values (e.g., 101, 107, 301, 105, 303, 103, 309, 304, 311).
- creation_date: This column contains dates, possibly indicating when the client was registered or created. It should be treated as a date/time variable.
- label: This column a binary is a label, possibly indicating whether the client is associated with electricity theft. It takes binary values (0 for no, 1 for yes).

### Results and description

Figure 1 showcases the user interface (UI) that was integral to the research. It serves as a visual representation of the software or tool used for conducting the experiments or analysis. The UI likely includes buttons, input fields, data visualization elements, and various interactive components essential for researchers to interact with the research environment. By presenting this UI, the research aims to provide transparency in the research process, giving readers insight into how experiments were conducted, and data was analyzed within the given interface.

Figure 2 presents a sample of the electricity theft dataset after it has undergone preprocessing. The numeric values or data displayed in this figure likely represent a subset of the cleaned and transformed dataset. These values may include features or variables relevant to the research, which have been processed to a state suitable for analysis. By showing this sample data, the research offers a glimpse into the characteristics of the dataset and the initial state from which analyses were performed.


Detection of Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters
Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters
Upload Dataset
Preprocess Dataset
Feed Forward Neural Network
RNN-GRU Algorithm
Predict Electricity Theft
Comparison Graph
Exit

```
C:/Users/abhil/Downloads/DEPARTMENT OF INFORMATION TECHNOLOGY/B13. ElectricityTheft/Dataset/ElectricityTheft.csv Loaded
  disrict        client_id  client_catg  region creation_date  label
0     60    train_Client_0        11    101   31/12/1994    0
1     69    train_Client_1        11    107   29/05/2002    0
2     62   train_Client_10        11    301   13/03/1986    0
3     69  train_Client_100        11    105   11/07/1996    0
4     62 train_Client_1000        11    303   14/10/2014    0
```

Figure 2. Sample Preprocessed outcome on electricity theft dataset.

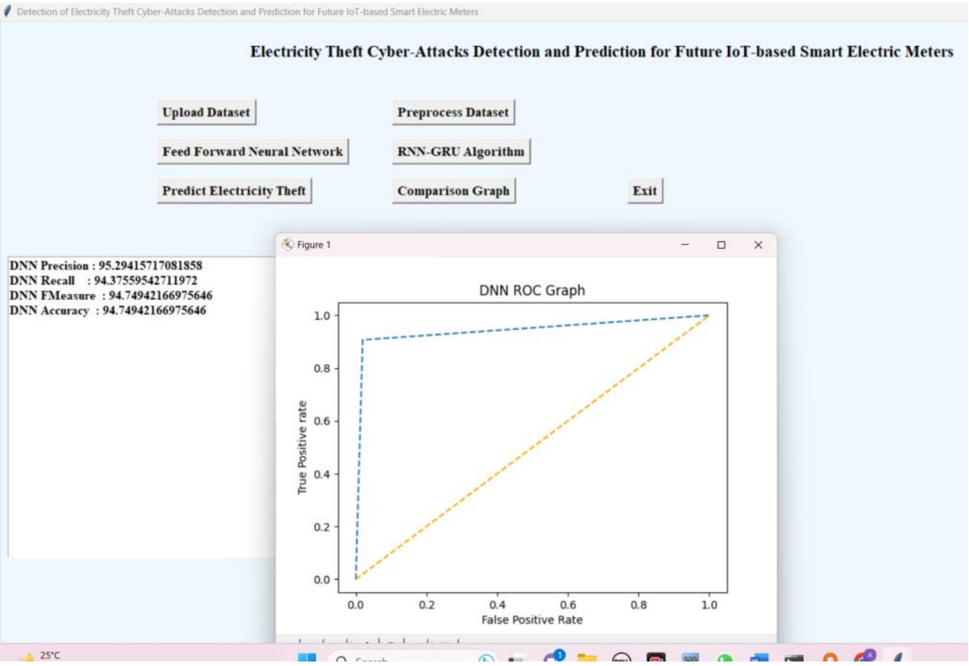
Figure 3 summarizes the performance of the proposed Deep Neural Network (DNN) model using numeric values. Precision is 95.29%, which indicates the accuracy of the positive predictions made by the DNN model. Recall is 94.37%, which reflects the model's ability to capture the actual positive instances. F1 Score is 94.74%, which is a balanced measure of precision and recall. Accuracy is 94.74%, which represents the overall correctness of the DNN model's predictions.

Figure 4 displays the Receiver Operating Characteristic (ROC) curve for the proposed Deep Neural Network (DNN) model. While not providing numeric values directly, the ROC curve visualizes how the model performs across various threshold values, illustrating the trade-off between true positive rate and false positive rate.

Figure 5 presents the performance metrics for an existing Gated Recurrent Unit (GRU) model, using numeric values in parentheses. Precision is 68.86% measures the accuracy of positive predictions made by the GRU model. Recall is 51.58% indicates the model's ability to capture actual positive instances. F1 Score is 40.34% is a balanced measure of precision and recall. Accuracy is 40.34% represents the overall correctness of the GRU model's predictions.

Similar to Figure 4, this figure likely displays the Receiver Operating Characteristic (ROC) curve for the existing Gated Recurrent Unit (GRU) model, providing a visual representation of the model's performance in distinguishing between positive and negative instances.

Figure 6 exhibit the results of predictions made by one or both of the models (DNN and GRU) on a test dataset, though specific numeric values are not mentioned. It could include a comparison of predicted outcomes against actual outcomes, visually illustrating how well the models perform in practical scenarios. This visual representation allows readers to assess the real-world applicability of the models.



Detection of Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters

Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters

```
DNN Precision : 95.29415717081858
DNN Recall    : 94.37559542711972
DNN FMeasure  : 94.74942166975646
DNN Accuracy  : 94.74942166975646
```

Figure 3. Proposed DNN performance.

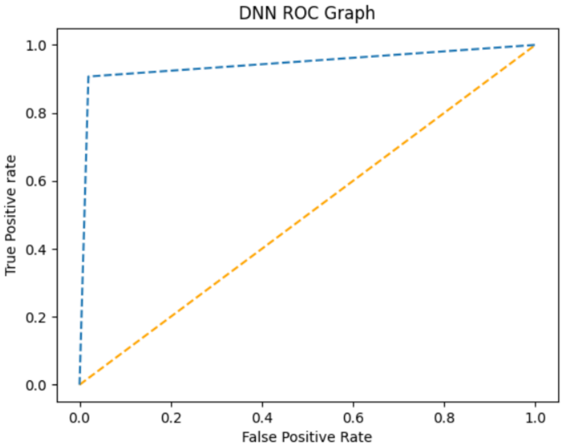


Figure 4. Proposed DNN-RoC Curve.

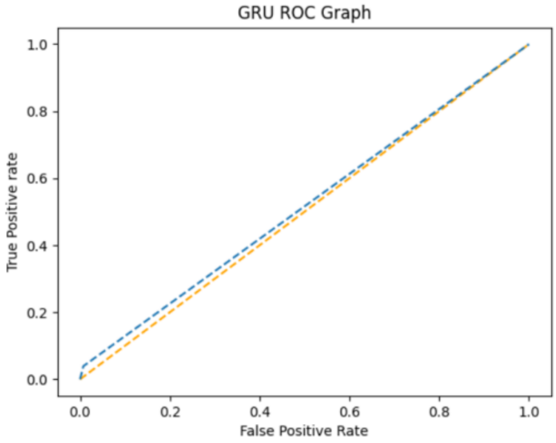
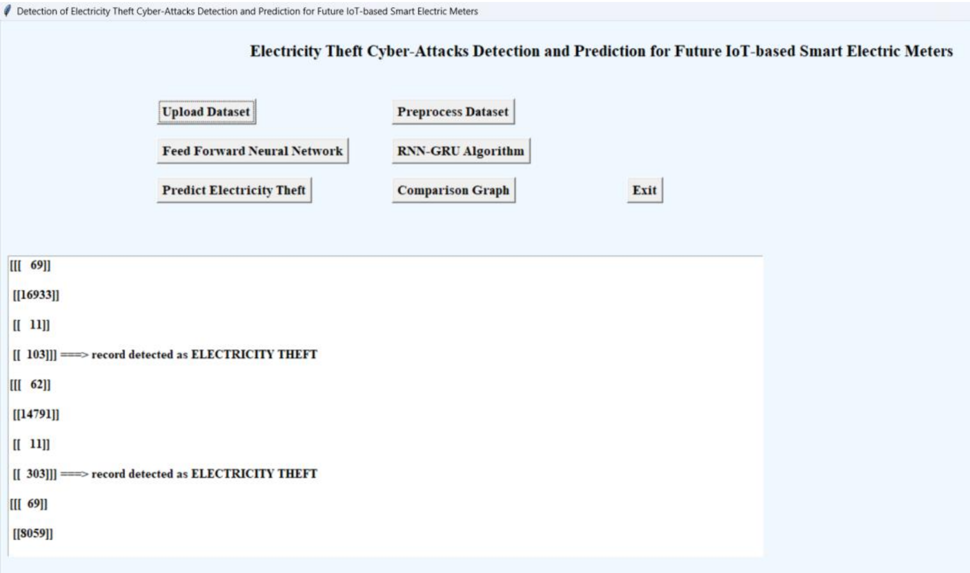


Figure 5. Existing GRU-RoC Curve.


Detection of Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters
Electricity Theft Cyber-Attacks Detection and Prediction for Future IoT-based Smart Electric Meters
Upload Dataset
Preprocess Dataset
Feed Forward Neural Network
RNN-GRU Algorithm
Predict Electricity Theft
Comparison Graph
Exit

```
[[[  69]]
 [[16933]]
 [[  11]]
 [[ 103]]] ==> record detected as ELECTRICITY THEFT
[[[  62]]
 [[14791]]
 [[  11]]
 [[ 303]]] ==> record detected as ELECTRICITY THEFT
[[[ 69]]
 [[8059]]
```

Figure 6. Prediction results from test data.

Table 1 serves as a concise summary of the performance of two different models, the "Proposed DNN" (Deep Neural Network) and the "Existing GRU" (Gated Recurrent Unit), with regard to electricity dataset. The table is designed to help readers quickly understand how these models perform in terms of key metrics.

- Precision (%): Precision is a metric that measures the accuracy of positive predictions made by a model. In the context of this table, "Precision (%)" represents the percentage of positive predictions made by each model that were actually correct. A higher precision indicates that the model makes fewer false positive errors.
- Recall (%): Recall, also known as sensitivity or true positive rate, measures the model's ability to capture actual positive instances. It represents the percentage of actual positive instances that the model correctly identifies. A higher recall value indicates that the model captures more of the true positive cases.
- F1 Score (%): The F1 score is a balanced metric that combines both precision and recall into a single value. It is the harmonic mean of precision and recall and provides an overall assessment of the model's performance. A higher F1 score suggests that the model achieves a good balance between precision and recall.
- Accuracy (%): Accuracy represents the overall correctness of the model's predictions, including both true positives and true negatives. It is the percentage of all predictions (both positive and negative) that were correct. However, accuracy can be misleading in imbalanced datasets where one class is significantly more prevalent than the other.

Table 1. Performance comparison.

| Model | Precision (%) | Recall (%) | F1 Score (%) | Accuracy (%) |
|---|---|---|---|---|
| Proposed DNN | 95.29 | 94.37 | 94.74 | 94.74 |
| Existing GRU | 68.86 | 51.58 | 40.34 | 40.34 |

## 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) 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