DEEP LEARNING APPROACHES FOR CYBER-ATTACK DETECTION IN ELECTRICITY DISTRIBUTION NETWORKS FOR SAFEGUARDING AGAINST TAMPERING AND THEFT

[1]Chenreddy Gouthami, [2]Balaswamy V, [3]Ramesh Mocherla

[1,3]Assistance Professor, Department of CSE, Sree Dattha Institute of Engineering and Science

[2]Associate Professor, Department of CSE, Sree Dattha Institute of Engineering and Science

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.

Keywords: Advanced metering infrastructure (AMI), DNN, Solar plates, Electricity theft, RNN.

1. INTRODUCTION

Electricity theft has long plagued utility companies globally, posing significant financial challenges. Traditional methods of theft involve physical tampering with meters or lines, leading to substantial revenue losses. In the United States, for instance, the annual toll of stolen electricity amounts to a staggering $6 billion. With the advent of the smart grid, new avenues for theft have emerged, compounding the challenge. The smart grid integrates advanced metering infrastructure (AMI), employing smart meters that monitor and report consumption data for billing purposes. However, this also introduces vulnerabilities, as malicious actors can exploit these systems through cyber-attacks to manipulate readings and reduce their electricity bills. Additionally, the smart grid facilitates the installation of renewable energy sources like solar panels, allowing consumers to sell excess energy back to the grid. This introduces further complexity, as malicious users may tamper with smart meters to inflate their production readings, leading to significant financial losses for utility agencies.

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. heng 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.

3. PROPOSED SYSTEM

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:

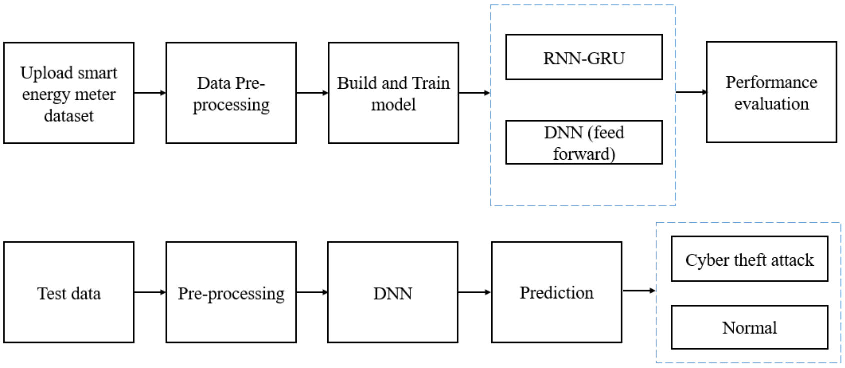

Fig. 1: Block diagram of proposed system.

At its simplest, a neural network with some level of complexity, usually at least two layers, qualifies as a deep neural network (DNN), or deep net for short. Deep nets process data in complex ways by employing sophisticated math modeling. To truly understand deep neural networks, however, it's best to see it as an evolution. A few items had to be built before deep nets existed. First, machine learning had to get developed. ML is a framework to automate (through algorithms) statistical models, like a linear regression model, to get better at making predictions. A model is a single model that makes predictions about something. Those predictions are made with some accuracy. A model that learns—machine learning—takes all its bad predictions and tweaks the weights inside the model to create a model that makes fewer mistakes. The learning portion of creating models spawned the development of artificial neural networks. ANNs utilize the hidden layer as a place to store and evaluate how significant one of the inputs is to the output. The hidden layer stores information regarding the input's importance, and it also makes associations between the importance of combinations of inputs.

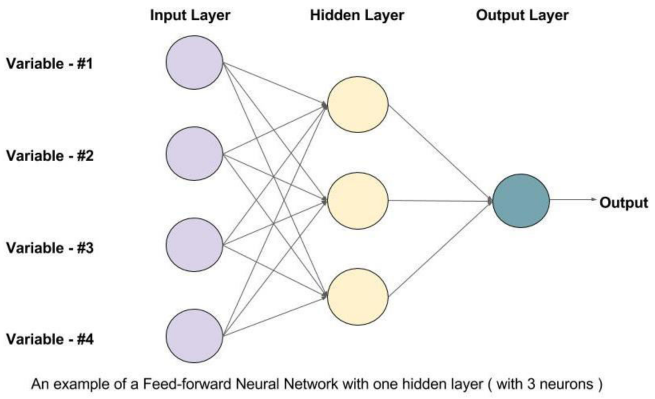

Figure 2: ANN

Deep neural nets, then, capitalize on the ANN component. They say, if that works so well at improving a model—because each node in the hidden layer makes both associations and grades importance of the input to determining the output—then why not stack more and more of these upon each other and benefit even more from the hidden layer? So, the deep net has multiple hidden layers. 'Deep' refers to a model's layers being multiple layers deep.

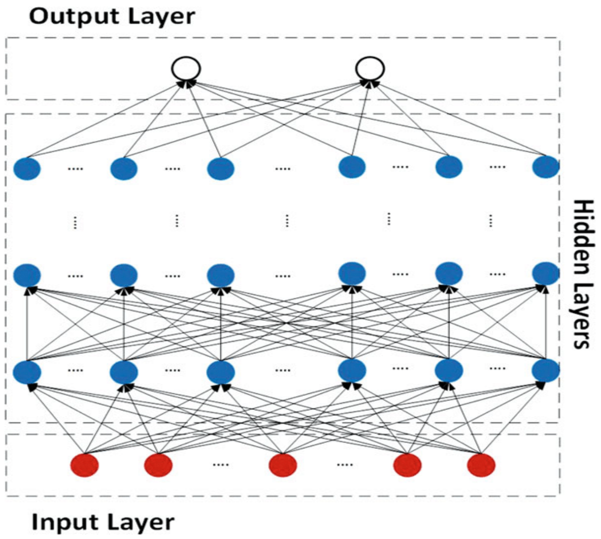

Figure 3. Hidden layer architecture.

In the context of detecting and predicting electricity theft cyber-attacks in IoT-based smart electric meters, a deep feedforward neural network can be employed to analyze data collected from these devices. The objective is to identify abnormal usage patterns or potential instances of electricity theft, indicating a possible cyber-attack. Below is the architecture of the neural network:

- Sequential Layer: The sequential layer serves as the foundation of the neural network model. It allows us to organize and stack other layers in a specific order, determining how data flows through the network.
- Dense Layers with ReLU Activation Function: The dense layers are fully connected layers where each neuron is connected to all neurons in the previous and following layers. ReLU (Rectified Linear Unit) activation function is commonly used to introduce non-linearity into the network. It helps the network learn complex

relationships between input features and output labels. ReLU is defined as f(x) = max(0, x), where x represents the input.

- Dense Layer with Softmax Activation Function: The final dense layer in the network is typically used for classification tasks. The softmax activation function is applied to this layer, which produces a probability distribution across the different classes in the problem. In the context of electricity theft cyber-attack detection, this layer can be utilized to predict the likelihood of an attack or classify instances as normal or abnormal.
- Adam Optimizer: The Adam optimizer is a popular choice for training neural networks. It is an enhanced version of stochastic gradient descent (SGD) that adjusts the learning rate dynamically based on gradient characteristics. The Adam optimizer facilitates faster convergence during training and often delivers good results.

To train a deep feedforward neural network for electricity theft cyber-attack detection and prediction, we follow these steps:

- Data Preparation: Gather data from IoT-based smart electric meters, including information such as energy consumption, usage patterns, timestamps, and any other relevant data. Label the data as normal or potentially indicative of electricity theft.
- Data Preprocessing: Clean the data by handling missing values, normalize the features, and encode categorical variables if necessary. Split the data into training and testing sets.
- Model Architecture: Define the architecture of the deep feedforward neural network with the sequential layer, dense layers with ReLU activation, and the final dense layer with softmax activation. Determine the number of neurons and layers based on the complexity of the problem and available computational resources.
- Compile the Model: Configure the model with the Adam optimizer by an appropriate loss function as categorical cross-entropy.
- Training: Feed the training data into the model and optimize the network's weights using the Adam optimizer. Monitor the loss function and evaluation metrics to assess the model's performance.
- Evaluation: Evaluate the trained model on the testing data to assess its ability to generalize and perform on unseen instances. Adjust the model architecture or hyperparameters if necessary.
- Prediction: Once the model is trained and evaluated, it can be used to predict electricity theft or detect abnormal usage patterns in real-time data from smart electric meters.

The development of an electricity theft cyber-attack detection and prediction system for future IoT-based smart electric meters offers several significant advantages:

- **Enhanced Grid Security**: One of the primary advantages is the bolstering of grid security. By proactively detecting and predicting cyber-attacks and electricity theft, the system can prevent unauthorized access and manipulation of electric meters and associated infrastructure. This safeguarding of the grid's integrity ensures a stable and reliable power supply for consumers.

- **Cost Savings**: Detecting and preventing electricity theft has a direct financial impact. Electricity theft is a significant concern for utility providers, as it leads to revenue losses. By identifying and addressing theft incidents promptly, utilities can recover lost revenue and potentially lower electricity rates for law-abiding consumers.
- **Improved Billing Accuracy**: The system contributes to more accurate billing. By monitoring electricity consumption patterns and identifying anomalies associated with theft, utilities can ensure that consumers are billed accurately for their usage. This fairness in billing builds trust with customers and reduces disputes.
- **Early Threat Detection**: Early detection of cyber attacks on smart electric meters is crucial for preventing potential widespread disruptions. The system's ability to recognize suspicious network behavior and anomalous patterns allows utilities to respond swiftly and implement security measures to mitigate threats, safeguarding the stability of the electric grid.
- **Data-Driven Insights**: The system generates valuable data-driven insights. By analyzing historical data and cyber attack patterns, utilities can gain a deeper understanding of attack vectors and vulnerabilities. This information informs the development of more robust security strategies and policies.
- **Operational Efficiency**: Improved efficiency is another advantage. The system's automation of cyber attack detection and prediction processes reduces the manual effort required for monitoring and responding to incidents. This frees up resources for more strategic tasks and reduces operational costs.
- **Scalability**: IoT-based smart electric meters are scalable, making it feasible to deploy the system across a wide geographic area. As the grid expands and incorporates more smart meters, the system can adapt and scale accordingly to ensure consistent protection.

4. RESULTS

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 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.

.

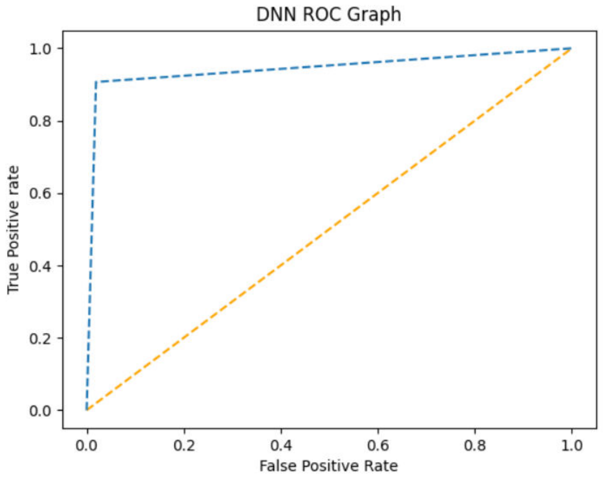

Figure 4: Proposed DNN-ROC Curve.

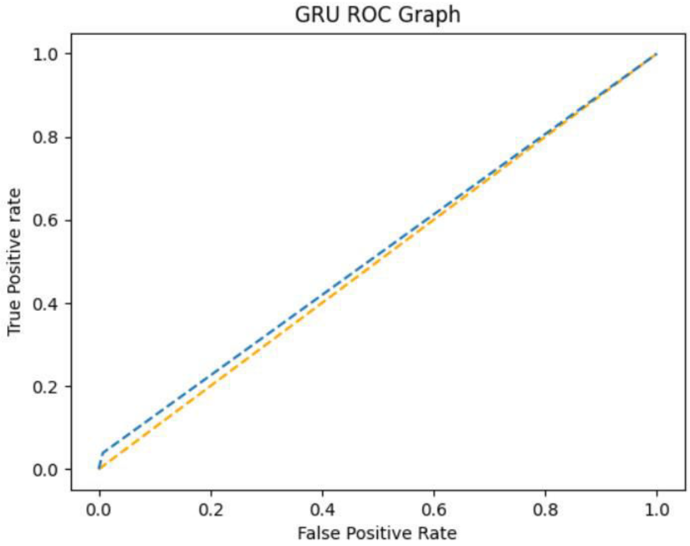

Figure 5: Existing GRU-RoC Curve.

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.