Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, No.4, November : 2024

A DEEP LEARNING METHOD FOR RECOGNIZING DISTRIBUTED GENERATION FRAUD AND ELECTRICITY THEFT IN SMART GRIDS

Dr. T. Venkata Ramana Associate Professor, Department of CSE – AIML, CVR College of Engineering, Hyderabad, India : meetramana1204@gmail.com
Dr.Banoth Samya, Associate Professor, Department of CSE, CVR College of Engineering, Hyderabad, India : samyabanoth@gmail.com
Dr. Srikanth Lakumarapu, Associate Professor, Department of CSE, CVR College of Engineering, Hyderabad, India : dr.srikanthcse@gmail.com

ABSTRACT
The act of stealing electricity poses a significant and urgent issue, resulting in substantial financial damages for electric utility providers on a global scale. Annually, electricity theft in the United States amounts to a staggering $6 billion. Historically, instances of electricity theft have occurred in the realm of consumption through physical methods such as tapping into power lines or interfering with meters. The smart grid paradigm enables the emergence of novel methods for perpetrating electricity theft assaults. Electricity theft can be perpetrated through cyber means. The advanced metering infrastructure (AMI) involves the installation of smart meters at customers' locations, which consistently report their usage data for the purpose of monitoring and billing. In this scenario, malevolent consumers have the ability to initiate cyber assaults on the intelligent meters with the intention of manipulating the recorded data in a manner that decreases their electricity expenses. Furthermore, the smart grid paradigm allows customers to install distributed generation (DG) units that rely on renewable sources of energy at their premises. This enables them to create electricity and sell it back to the grid operator, so generating a profit. This study aims to assess the effectiveness of different deep learning algorithms, including deep feed forward neural network (DNN) and recurrent neural network with gated recurrent unit (RNN-GRU), in detecting cyber-attacks on energy systems. In modern developed nations, solar panels are utilized to produce power. customers have the option tosell any surplus energy to other customers in need. To accurately track consumption and production, separate meters are installed. Some malevolent users may manipulate smart meters in order to increase their electricity bills and gain additional revenue from renewable distributed energy sources. This assault has the potential to result in significant financial damages for the organizations involved. This study use deep learning models to identify potential modifications and anticipate theft in order to detect such attacks.

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]. Thedifference between the energy produced in one system and the metered energy delivered to the usersis 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 asre-connect the supply of electricity from any remote place.

2. 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 firststep 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 correspondinglabels, 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.

3. RESULTS AND DISCUSSION

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 performin terms of key metrics.

- Precision (%): Precision is a metric that measures the accuracy of positive predictions madeby 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

4. 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