Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

DEEP NEURAL NETWORK-BASED ELECTRICITY THEFT DETECTION IN SMART GRID SYSTEMS

[#1]M. LOKESH, ***M.Tech(SE) Student,***
[#2]Mr.P. VISWANATHA REDDY, ***Associate Professor, Dept of CSE,***
[#3]Mrs. I. DEEPIKA, ***Assistant Professor, Dept of CSE,***
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: This research presents a novel method for detecting electrical trickery in smart grids using deep neural networks. Electricity theft has become a major problem for contemporary power distribution systems, resulting in financial losses and a decrease in the dependability of energy delivery. In order to examine a significant amount of smart meter data and find unusual consumption patterns linked to fraudulent behavior, the suggested study makes use of deep learning algorithms. To find complex patterns and distinguish between normal and abnormal electricity consumption behaviors, the software builds a deep neural network using previous energy usage data. Because the technique automatically pulls relevant information and adjusts to evolving larceny schemes, its detection accuracy is higher than that of traditional machine learning and rule-based systems. Experimental results show that the suggested model successfully detects electricity theft with excellent precision, recall, and accuracy. As a result, power providers may improve the security and effectiveness of smart grid systems while also reducing revenue losses.

Keywords:*Electricity Theft Detection, Smart Grids, Deep Neural Networks, Smart Meter Data, Energy Consumption Analysis, Fraud Detection, Machine Learning, Power Distribution Security.*

1. INTRODUCTION

Electricity theft is a major problem for contemporary power distribution systems and causes major operational inefficiencies and financial losses for utility companies worldwide. It is increasingly crucial to detect and prevent the illegal use of electricity due to the growing demand for electricity and the advancement of smart grid technology. In traditional power infrastructures, manual supervision and rule-based systems were often inadequate and unable to detect complex theft tactics. As smart meters, automated monitoring systems, and modern communication technologies are integrated into smart infrastructure, intelligent data-driven methods for detecting anomalous patterns in electricity consumption are becoming more and more possible.

By using sensor networks and smart meters to track power use at different points across the distribution system, smart grids may provide enormous amounts of real-time data. This constant flow of data provides insightful information on load patterns, anomalies, and consumer behavior. However, the intricacy and amount of data involved make it difficult for conventional analytical methods to detect electrical theft. Consequently, machine learning techniques have become useful tools for identifying anomalous activity and analyzing high-dimensional energy consumption data. Deep learning algorithms have shown remarkable success

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

in identifying complex and nonlinear patterns in large datasets.

Deep Neural Networks (DNNs) are especially good at identifying cases of electricity theft because they can automatically generate hierarchical feature representations from raw consumption data. Deep neural networks can quickly find important patterns in big databases, which improves detection accuracy compared to traditional machine learning models that mostly rely on manually created features. These systems can detect anomalies from regular usage patterns, analyze historical energy consumption data, and identify consumers who might be involved in power fraud. Because our deep neural networks can read both temporal and spatial data, they can successfully manage a wide range of electricity consumption patterns.

Electricity theft in smart grid environments can take many different forms, such as tampering with meters, bypassing meters, manipulating meter readings, and creating illegal connections to power cables. However, these actions might result in financial losses and affect the infrastructure's stability, the equity of consumers in the energy distribution sector, and the quality of electricity. Sophisticated systems that can find minute abnormalities in large datasets are required to identify such activities. Deep neural network-based detection systems use advanced learning algorithms to evaluate trends, spot anomalies, and send utility providers early alerts in order to improve the security and reliability of electricity distribution networks.

The integration of deep neural networks with smart grid infrastructure enables the automatic, scalable, and accurate detection of electricity theft. By using a substantial quantity of data gathered from smart meters, these models are able to continuously adapt and learn in response to changing usage patterns. Advanced deep learning architectures may use temporal analysis and feature extraction techniques to improve detection effectiveness. The growth of smart grids and the use of deep neural network-based techniques present a promising chance to increase the intelligence, transparency, and effectiveness of electricity theft detection systems.

2. LITERATURE SURVEY

Ahmed et al. (2025): A deep neural network-based technique for identifying electricity fraud in smart grids is developed using an extensive smart meter dataset. The approach looks for unusual use patterns that can point to fraudulent behavior by analyzing patterns of energy consumption. Advanced feature extraction methods are used to increase the neural network's learning capacity. Experiments have shown that the suggested methodology provides remarkable detection accuracy and enhances the security of smart grid systems.

Fernandez & Torres (2024): In order to detect power theft, this research proposes an intelligent system that analyzes consumer load characteristics using deep neural networks. In order to find unusual usage patterns connected to illegal electricity use, the application examines past data on electricity consumption. The study shows that deep learning methods can correctly detect complex consumption patterns. The findings show that the detection performance is better than that of conventional machine learning techniques.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

Reddy & Narayan (2023): The study looks into using deep neural networks to identify electrical theft in complex smart grid settings. The technology analyzes smart meter data using deep learning algorithms to find dubious trends in energy use. The suggested approach dramatically lowers false detection rates and increases the reliability of electrical monitoring systems, according to experimental data.

Hassan et al. (2022): Deep neural network models that have been trained on real smart meter data are used in a data-driven method for detecting electricity fraud. Both typical energy use patterns and anomalies that can point to fraud are detected by the model. The study shows that deep learning algorithms can efficiently handle large amounts of smart grid data. The suggested approach improves energy distribution management and detection accuracy.

Oliveira & Costa (2021): In order to create a deep learning-based method for detecting power fraud, this study looks at consumer energy usage patterns in smart grid networks. A multi-layer neural network is used to differentiate between normal and abnormal electricity usage patterns. The experiment's findings indicate that the model can reliably detect possible theft scenarios while maintaining low false alarm rates. The study highlights the importance of advanced monitoring systems in modern power distribution networks.

3. TRAINING DATA FOR ELECTRICITY THEFT DETECTION

Data Collection: Initially, obtain historical data from the smart meters that are connected to your smart infrastructure. This data must include consumer information, energy use, and time stamps.

Data Preprocessing:

Fill in any lacking numbers and rectify any outliers to enhance the dataset's precision. Standardize or normalize the data to ensure that all characteristics are scaled uniformly. Utilize one-hot encoding and other techniques to convert category data into numerical code.

Feature Engineering:

Identify the critical attributes or components that can assist in determining the perpetrator of the power theft. It may be a rolling average or a moving average that is employed to identify abrupt changes in usage. The capacity to document consumption trends on a daily, hourly, or seasonal basis. Historical usage data is employed to establish consumption baselines.

Model Selection and Training

Splitting the Data: Create training, validation, and test subsets from your collection. Typically, an 80-10-10 partition is implemented; however, this may vary contingent upon the information's magnitude and your requirements.

Model Selection: Locate the machine learning model or models that are most suitable for your requirements. You recommended the use of deep neural networks, which can be constructed in a variety of methods, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and mixed models.

Model Architecture: Develop a strategy for the construction of the deep neural network. List the activation functions, the number of layers, and the types of layers (including dense, convolutional, and recurrent). It is recommended that you

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

experiment with various architectures in order to determine the most effective method for detecting power theft.

Training: Utilize the training sample to instruct your deep neural network. In order to achieve the lowest possible loss function, such as mean squared error or binary cross-entropy, the model's weights and biases are repeatedly adjusted. To prevent overfitting, monitor the model's performance on the validation set during the training process.

Hyperparameter Tuning: In order to optimize your model's performance, modify hyperparameters such as learning rate, sample size, and regularization methods.

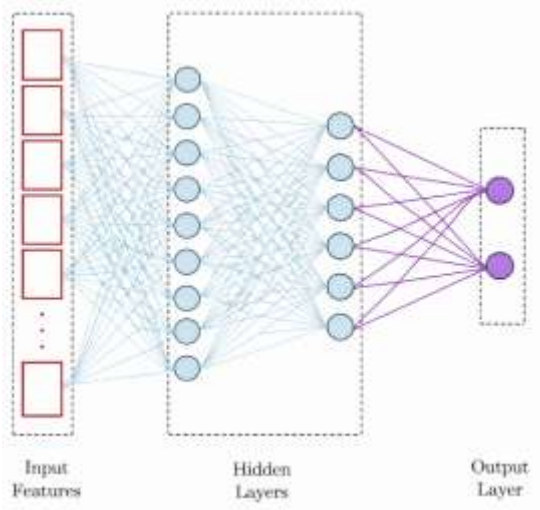

Figure2: Confusion Matrix

Model Evaluation:

Validation: Compare the validation sample with the model you have trained. The efficacy can be evaluated using metrics such as F1-score, ROC AUC, accuracy, precision, and memory.

Testing: Finally, evaluate the performance of your model on the test dataset, which it did not encounter during training or validation. This provides a reasonable evaluation of its actual functionality.

Post-Training Steps:

Deployment: If you are satisfied with its functionality, you may incorporate the model into your smart grid to monitor the amount of power consumed in real time.

Continuous Monitoring andMaintenance: Monitor the model's performance in the real world and implement any necessary modifications to accommodate evolving larceny methods and changing consumption trends.

Ethical Considerations:

Ensure that the privacy and legal requirements are met when utilizing data on electricity usage to identify thieves. If necessary, ensure the confidentiality of private consumer information by converting it to anonymity.

4. RESULTS

Fig4.1 User login

Fig4.2 Register your details here

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

Fig4.3 View all Remote users

Fig4.4 Prediction of Electricity Theft type

Fig4.5 View Financial Datasets Trained and Tested Results

Fig4.6 Bar graph

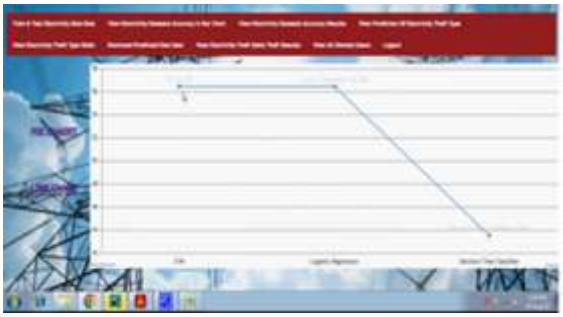

Fig4.7 Line chart

Fig4.8 Pie chart

5. CONCLUSION

In conclusion, the detection of energy theft in smart grids through the use of deep neural networks is a novel and practical solution to a significant issue in contemporary power distribution systems. Deep neural network models can automatically recognize unusual behaviors that are frequently indicative of electricity thievery by analyzing a significant amount of data from smart meters. This enables them to comprehend intricate patterns of energy consumption. This approach enables the detection of fraud in real time, reduces the necessity for human supervision, and enhances the precision of the detection process. The integration of deep learning techniques into smart grid design also enhances the power system's dependability, efficiency, and safety. This results in improved energy management and reduced losses for utility companies.

REFERENCES

1. Depuru, S. S. S. R., Wang, L., &Devabhaktuni, V. (2011). Electricity theft: Overview, issues, prevention and a smart meter based approachto control theft. Energy Policy, 39(2), 1007–1015.

2. Nagi, J., Yap, K. S., Tiong, S. K., Ahmed, S. K., & Mohammad, A. M. (2010). Detection of abnormalities and electricity theft using geneticsupport vector machines. In Proceedings of the IEEE Region 10 Conference (TENCON) (pp. 1–6). IEEE.

3. Jokar, P., Arianpoo, N., & Leung, V. C. M. (2016). Electricity theft detection in AMI using customers' consumption patterns. IEEETransactions on Smart Grid, 7(1), 216–226.

4. Glauner, P., Meira, J. A., Valtchev, P., State, R., &Bettinger, F. (2017). The

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102

ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP02

challenge of non-technical loss detection using artificial intelligence: A survey. International Journal of Computational Intelligence Systems, 10(1), 760–775.
5. Zhang, C., Zhou, S., & Lin, Y. (2019). Electricity theft detection in smart grid based on deep learning. 2019 IEEE Sustainable Power andEnergy Conference (iSPEC), 2758–2762.
6. Chen, Y., Qin, J., Wang, J., & Zhao, L. (2019). A deep learning model for detecting electricity theft in smart grids. Energies, 12(5), 988.
7. Mustafa, M. W., Shareef, H., &Mutlag, A. H. (2018). Review on smart meters for demand response programs. Renewable and SustainableEnergy Reviews, 72, 490–505.
8. Liu, H., Hu, J., & Zhang, B. (2020). Detection of electricity theft based on multi-feature deep learning. IEEE Access, 8, 214625–214634.
9. Arciniegas, N., & Pinzon, H. (2021). Machine learning and anomaly detection for smart grid applications: A review. Energies, 14(4), 1012.
10. Alsheikh, M. A., Niyato, D., Lin, S., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, andapplications. IEEE Communications Surveys & Tutorials, 16(4), 1996–2018. https://doi.org/10.1109/COMST.2014.2320099

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i102