

## Smart Theft Detection Using Advance Machine Learning Using Quantum

DR.Akheel mohammed<sup>1\*</sup>, M.Sai Charan Teja<sup>2</sup>, N.Maitej<sup>2</sup>, M.Nithin <sup>2</sup>, V.Karthik<sup>2</sup>,

<sup>1</sup>Associate Professor, <sup>2</sup>UG Student, <sup>1,2</sup>Department of Artificial Intelligence and Machine Learning  
<sup>1,2</sup>J.B Institute of Engineering and Technology

\*Corresponding author:M. Sai Charan Teja ([munnurusaicharan27@gmail.com](mailto:munnurusaicharan27@gmail.com))

### ABSTRACT

Electricity theft in smart grids has become a critical challenge due to manipulation of smart meters and distributed energy generation from photovoltaic (PV) systems. Traditional machine learning algorithms often fail to detect theft on the Distribution Generation (DG) side and struggle with high-dimensional, imbalanced datasets. To address these challenges, a Quantum Machine Learning (QML) approach is employed, leveraging a hybrid Quantum Deep Learning model combining Quantum Variational Circuit (QVC) and Data Re-uploading Circuit (DRC). The QVC integrates an angle-embedding layer for encoding classical neural outputs into qubits, followed by rotational and CNOT gates with trainable parameters, ensuring noise reduction on noisy intermediate-scale quantum (NISQ) devices. The DRC layer iteratively re-uploads data to mitigate residual noise. Experiments use the “Smart Grid Theft Detection” dataset from Kaggle, with processed features split into training (80%) and testing (20%) sets. Classical algorithms such as XGBOOST and LIGHTGBM achieve accuracies of 86% and 73%, respectively, while the FH-QVC-DRC model attains 88% accuracy. Incorporating an Entanglement quantum layer further enhances performance by exploiting quantum parallelism, interference, and secure state correlations, resulting in the FH-QVC-DRC-ENT model achieving 91% accuracy. Visualization, performance metrics, and prediction outputs confirm the superior classification capability of the entanglement-enabled quantum model for distinguishing theft and non-theft instances.

**Key Words:** Smart Grid, Power Theft Detection, Quantum Machine Learning, Quantum Circuits, Hybrid Model

### 1. INTRODUCTION

Smart grids have emerged as a transformative solution for modern power systems, integrating advanced metering infrastructure (AMI), distributed energy resources, and data-driven management strategies to enhance energy efficiency, reliability, and sustainability. The increasing deployment of renewable energy sources, particularly photovoltaic (PV) systems, has enabled consumers to function as both energy users and producers, promoting decentralized energy exchange through mechanisms such as net metering and feed-in tariffs. While these advancements drive economic and environmental benefits, they also introduce new challenges associated with data integrity and secure energy transactions. Electricity theft, including manipulation of consumption and generation readings, remains a persistent global issue leading to substantial financial losses and operational disruptions for utility providers.

Despite ongoing efforts, conventional analytical and computational approaches often struggle to detect sophisticated fraud patterns, especially within high-dimensional, imbalanced, and dynamically evolving smart-grid environments. This gap underscores the need for more robust, intelligent, and scalable detection frameworks capable of leveraging complex data structures. The present study aims to address this challenge by developing an enhanced learning-based detection model designed to improve the accuracy and reliability of theft identification in smart-metered systems. The proposed framework contributes to stronger grid security, improved operational decision-making, and greater economic resilience, ultimately supporting the sustainable evolution of smart-energy infrastructures

### 2. LITERATURE SURVEY

Recent research in smart grid security has focused on leveraging advanced machine learning and quantum-based techniques to improve electricity theft detection and system reliability. A robust framework integrating Quantum Key Distribution (QKD) with Rolling Optimization Strategy (ROS), along with Extreme Gradient Boosting and Coati Optimization Algorithm, demonstrated high effectiveness in handling nonlinear and incomplete data, achieving an accuracy of **99%**, detection rate of **98.6%**, precision of **97%**, recall of **98.6%**, and F1-score of **95.15%**.

In another study, supervised machine learning approaches, particularly a **1D Convolutional Neural Network (CNN)**, were used to identify irregular consumption patterns in smart grid data. This model outperformed traditional algorithms such as Random Forest, XGBoost, and Logistic Regression, achieving an accuracy of **95.47%** and an F1-score of **97.42%**, highlighting the effectiveness of deep learning in fraud detection.

Furthermore, quantum computing techniques have been explored for enhancing smart grid security. A Quantum Entropy-based Q-Learning (QEQ) model was proposed for detecting Distributed Denial of Service (DDoS) attacks, demonstrating improved adaptability, faster convergence, and better performance metrics such as accuracy, precision, recall, and F1-score compared to classical reinforcement learning models.

Deep Reinforcement Learning (DRL) approaches have also been applied to electricity theft detection, utilizing models such as Deep Q Networks (DQN) and Double DQN (DDQN). These models effectively adapt to dynamic consumption patterns and detect new and evolving cyber-attacks, improving overall detection capability in smart grid environments.

Additionally, quantum machine learning has been employed for load forecasting and energy management using Quantum Controlled-NOT Neural Networks optimized with adaptive evolutionary algorithms. This approach

significantly improved prediction accuracy, reducing root-mean-square error by up to **77.02%** and **78.92%** on benchmark datasets.

Overall, existing studies demonstrate that while classical machine learning and deep learning techniques provide strong baseline performance, the integration of quantum computing methods offers enhanced efficiency, accuracy, and robustness in handling complex, high-dimensional smart grid data, thereby motivating the adoption of hybrid quantum-classical models for advanced electricity theft detection.

### 3. PROPOSED SYSTEM

The proposed system detects electricity theft in smart grids by analyzing both consumer-side and Distributed Generation (DG) data using the “Smart Grid Theft Detection” dataset, which includes smart meter readings and photovoltaic (PV) generation features labeled as theft or non-theft instances. The dataset undergoes preprocessing steps such as feature extraction, normalization, and shuffling, and is divided into training (80%) and testing (20%) sets to ensure reliable model evaluation. The detection framework is based on a hybrid Quantum Deep Learning approach that integrates a Quantum Variational Circuit (QVC) with a Data Re-uploading Circuit (DRC). The QVC employs an angle-embedding technique to encode classical data into quantum states using rotation gates, followed by trainable rotational and CNOT gates to reduce noise in NISQ devices and enhance learning capability. The DRC further improves performance by iteratively re-uploading data to refine feature representation and capture complex patterns. For performance comparison, classical machine learning algorithms such as XGBoost and LightGBM are also implemented. The proposed approach offers several advantages, including the ability to handle high-dimensional, imbalanced, and noisy datasets, improved generalization through hybrid quantum-classical architecture, automated feature encoding, and enhanced detection accuracy across multiple smart grid domains. Additionally, the model is extended by incorporating a quantum entanglement layer, enabling stronger correlations between qubits and improving classification performance. This enhancement leverages quantum parallelism and interference to increase computational efficiency, improve precision in representing complex data,

support error correction mechanisms, and strengthen the model’s ability to identify subtle patterns associated with electricity theft, resulting in a more robust and

reliable detection system.

#### 4. RESULTS DESCRIPTION

The performance of the system is evaluated using standard classification metrics, where accuracy reflects the overall correctness of predictions, precision indicates how reliably the model identifies actual theft cases among

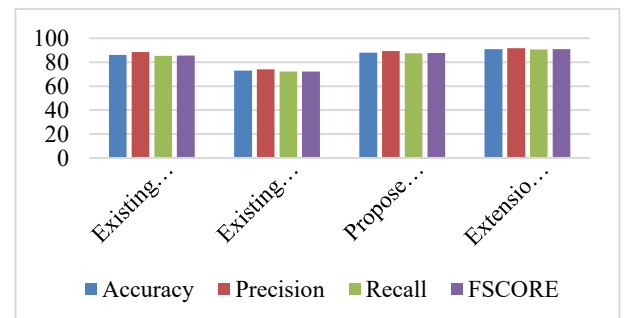
predicted positives, recall measures how effectively it captures all real theft instances, and the F1-score provides a balanced measure between precision and recall. The observed results show a clear performance gap between classical machine learning models and the proposed quantum-enhanced approaches. XGBoost achieves relatively strong performance with 86% accuracy, demonstrating its capability in handling structured data, while LightGBM shows comparatively lower performance at 73%, indicating limitations in capturing complex and irregular consumption patterns present in the dataset.

Algorithm Name	Accuracy	Precision	Recall	F-SCORE
Existing XGBoost	86.0	88.5	85.2	85.5
Existing LightGBM	73.0	74.04	72.2	72.1
Propose FH-QVC-DRC	88.0	89.2	87.4	87.7
Extension FH-QVC-DRC-ENT	91.0	91.5	90.6	90.8

The proposed hybrid quantum model (FH-QVC-DRC) improves the performance to 88% accuracy, along with higher precision, recall, and F1-score, which indicates better learning of nonlinear relationships and improved handling

of high-dimensional and imbalanced data. This improvement can be attributed to the quantum variational circuit’s ability to encode data into a higher-dimensional Hilbert space and the data re-uploading mechanism that enhances feature representation iteratively. The extension of this model with an entanglement layer (FH-QVC-DRC-ENT) further boosts the accuracy to 91% and improves all other evaluation metrics, showing the highest overall performance among all models.

This enhancement is primarily due to the role of quantum entanglement, which enables strong correlations between qubits and allows the model to capture subtle dependencies and hidden patterns in the data that classical methods cannot efficiently represent. The higher precision value indicates a reduction in false positives, meaning fewer normal cases are incorrectly classified as theft, while the increased recall demonstrates improved detection of actual theft instances. The improved F1-score confirms that the model maintains a



good balance between precision and recall, making it reliable for real-world applications.

Graph.9.2 Comparison Graph

Overall, the results demonstrate that quantum-enhanced learning models provide superior performance in electricity theft detection by effectively handling complex, noisy, and high-dimensional smart grid data. The consistent improvement across all metrics highlights the robustness, efficiency, and scalability of the proposed approach, making it more suitable for practical deployment compared to traditional machine learning techniques.

#### 5. CONCLUSION

Electricity theft detection in smart grids can be significantly enhanced through the application of quantum machine learning techniques, particularly in addressing challenges associated with high-dimensional, imbalanced, and noisy datasets. The system utilizes the “Smart Grid Theft Detection” dataset, which includes features derived from smart meter readings and photovoltaic (PV) distributed generation, ensuring comprehensive coverage of both consumption and generation behaviors. The data is systematically preprocessed through feature extraction, shuffling, normalization, and splitting into training (80%) and testing (20%) sets to ensure reliable and unbiased model evaluation.

trainable rotational and CNOT gates that improve learning efficiency while reducing noise effects in NISQ devices. The DRC further enhances the model by iteratively re-uploading data, enabling better feature representation and improved capture of complex patterns. Experimental results demonstrate that classical models such as XGBoost and LightGBM achieve accuracies of 86% and 73%, respectively, while the proposed FH-QVC-DRC model improves performance to 88%. The extended FH-QVC-DRC-ENT model, incorporating a quantum entanglement layer, achieves the highest accuracy of 91%, confirming its superior capability in capturing subtle relationships and improving classification reliability.

The system not only provides improved numerical performance but also delivers results through a structured interface that presents total records, categorized theft and non-theft instances, and attention-required indicators. Detailed outputs include instance-level predictions along with model-generated recommendations, enabling effective interpretation and decision-making. This integration of accurate prediction with clear result presentation enhances the practical applicability of the system in real-world smart grid environments.

Furthermore, the framework demonstrates strong potential for scalability and future enhancements, including integration with real-time smart meter data, deployment on cloud platforms for large-scale processing, and incorporation of IoT-based sensing devices for automated monitoring. The development of advanced hybrid quantum-classical architectures and user-centric dashboards can further improve visualization, adaptability, and operational efficiency. Overall, the proposed approach establishes a robust, efficient, and scalable solution for electricity theft detection, highlighting the transformative potential of quantum deep learning in modern energy management systems.



The proposed framework is based on a hybrid Quantum Deep Learning approach that combines a Quantum Variational Circuit (QVC) with a Data Re-uploading Circuit (DRC). The QVC employs angle embedding to encode classical data into quantum states, followed by

## 6. REFERENCES

- [1] Abdulqadder, I. H., Aziz, I. T., & Flaih, F. M. (2025). Robust Electricity Theft Detection in Smart Grids Using Machine Learning and Secure Techniques. *International Journal of Intelligent Engineering & Systems*, 18(1).
- [2] Parvin, F., & Tabassum, T. (2025, July). Smart Grid Electricity Fraud Detection Using Machine Learning. In *2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)* (pp. 1-6). IEEE.
- [3] Said, D., Bagaa, M., Oukaira, A., & Lakhssassi, A. (2024). Quantum entropy and reinforcement learning for distributed denial of service attack detection in smart grid. *IEEE Access*.
- [4] El-Toukhy, A. T., Badr, M. M., Mahmoud, M. M., Srivastava, G., Fouda, M. M., & Alsabaan, M. (2023). Electricity theft detection using deep reinforcement learning in smart power grids. *IEEE Access*, 11, 59558-59574.
- [5] Kumar, J., Saxena, D., Singh, A. K., & Vasilakos, A. V. (2023). A quantum controlled-not neural network-based load forecast and management model for smart grid. *IEEE Systems Journal*, 17(4), 5714-5725.
- [6] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.
- [7] A. Arif, T. A. Alghamdi, Z. A. Khan, and N. Javaid, "Towards efficient energy utilization using big data analytics in smart cities for electricity theft detection," *Big Data Res.*, vol. 27, Feb. 2022, Art. no. 100285.
- [8] Y. Zhu, Y. Zhang, L. Liu, Y. Liu, G. Li, M. Mao, and L. Lin, "Hybrid-order representation learning for electricity theft detection," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1248–1259, Feb. 2023.
- [9] V. B. Krishna, C. A. Gunter, and W. H. Sanders, "Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 790–805, Aug. 2018.
- [10] N. Bhusal, M. Gautam, R. M. Shukla, M. Benidris, and S. Sengupta, "Coordinated data falsification attack detection in the domain of distributed generation using deep learning," *Int. J. Electr. Power Energy Syst.*, vol. 134, Jan. 2022, Art. no. 107345.
- [11] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.
- [12] A. C. Marques, J. A. Fuinhas, and D. P. Macedo, "The impact of feed-in and capacity policies on electricity generation from renewable energy sources in Spain," *Utilities Policy*, vol. 56, pp. 159–168, Feb. 2019.
- [13] M. I. Ibrahim, M. Mahmoud, M. M. Fouda, F. Alsolami, W. Alasmay, and X. Shen, "Privacy preserving and efficient data collection scheme for AMI networks using deep learning," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 17131–17146, Dec. 2021.
- [14] PR Newswire, "96 Billion is Lost Every Year to Electricity Theft." Accessed: Jan. 2023. [Online]. Available: <https://www.prnewswire.com/news-releases/96-billion-is-lost-every-year-to-electricity-theft-300453411.html>
- [15] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Detection of non-technical losses using smart meter data and supervised learning," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2661–2670, May 2019.
- [16] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.
- [17] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent

mechanism,” IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[18] S. Zidi, A. Mihoub, S. M. Qaisar, M. Krichen, and Q. A. Al-Haija, “Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment,” J. King Saud Univ.-Comput. Inf. Sci., vol. 35, no. 1, pp. 13–25, Jan. 2023.

[19] M. Shaaban, U. Tariq, M. Ismail, N. A. Almadani, and M. Mokhtar, “Data-driven detection of electricity theft cyberattacks in PV generation,” IEEE Syst. J., vol. 16, no. 2, pp. 3349–3359, Jun. 2022.

[20] M. Ezeddin, A. Albaseer, M. Abdallah, S. Bayhan, M. Qaraqe, and S. Al-Kuwari, “Efficient deep learning based detector for electricity theft generation system attacks in smart grid,” in Proc. 3rd Int. Conf. Smart Grid Renew. Energy (SGRE), Mar. 2022, pp. 1–6.