

Research Paper

Advanced Power Theft Detection in Smart Grids Using Entanglement-Driven Quantum Machine Learning

D.BHANU PRIYA¹, POTTETI SURYA PRATHAP REDDY², VADDEMANU BHARGAVA KUMAR REDDY³, UMMANABOINA REDDAMMA⁴, SIRISALA SAI SUDHESHNA⁵

#1 Professor, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, SAI RAJESWARI INSTITUTE OF TECHNOLOGY

#2#3#4#5 UG Student DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, SAI RAJESWARI INSTITUTE OF TECHNOLOGY

Abstract: Electricity theft in smart grids has become a critical issue due to the manipulation of smart meters and distributed generation systems such as photovoltaic (PV) units. Traditional machine learning methods often fail to effectively handle high-dimensional, noisy, and imbalanced data, especially in distributed generation and net-metering domains. To address these limitations, this paper proposes an entanglement-enhanced Quantum Deep Learning (QDL) framework for accurate power theft detection. The model integrates a hybrid architecture combining Quantum Variational Circuit (QVC) and Data Re-uploading Circuit (DRC), along with a novel entanglement layer to exploit quantum parallelism and strong feature correlations. The dataset is preprocessed using normalization and splitting techniques, with 80% used for training and 20% for testing. Comparative analysis with classical models such as XGBoost and LightGBM demonstrates improved performance. The proposed FH-QVC-DRC-ENT model achieves superior accuracy of 91%, outperforming existing approaches. Experimental results validate that the incorporation of quantum entanglement significantly enhances classification capability, robustness, and generalization, making the model highly effective for detecting electricity theft across both consumption and distributed generation domains in smart grids.

Index terms - Smart Grid, Power Theft Detection, Quantum Machine Learning (QML), Quantum Deep Learning (QDL), Quantum Variational Circuit (QVC), Data Re-uploading Circuit (DRC), Quantum Entanglement, Distributed Generation (DG), Photovoltaic (PV) Systems, Net Metering, XGBoost, LightGBM.

1. INTRODUCTION

Smart grids have revolutionized modern power systems by integrating advanced communication technologies, renewable energy sources (RESs), and intelligent monitoring through Advanced Metering Infrastructure (AMI). With the increasing adoption of photovoltaic (PV) systems and distributed generation (DG), consumers are no longer just energy users but also energy producers. While mechanisms such as net metering and feed-in tariff (FIT) provide economic benefits, they also introduce new vulnerabilities, enabling malicious users to manipulate consumption or generation data for financial gain. These fraudulent activities lead to significant economic losses and affect grid stability, making efficient power theft detection an essential requirement in smart grid environments.

Traditional electricity theft detection methods primarily focus on consumption patterns and rely on

classical machine learning algorithms such as Support Vector Machines (SVM), Random Forest (RF), and Deep Neural Networks (DNN). However, these approaches face limitations when dealing with high-dimensional, imbalanced, and noisy datasets, especially in distributed generation scenarios. Moreover, they often fail to capture complex nonlinear correlations between consumption and generation data, reducing detection accuracy and generalization capability.

To overcome these challenges, this paper introduces an entanglement-enhanced Quantum Deep Learning (QDL) framework for power theft detection in smart grids. The proposed model combines Quantum Variational Circuits (QVC) and Data Re-uploading Circuits (DRC) with an additional entanglement layer that connects qubits to exploit quantum parallelism and interference. This enhancement enables the model to capture intricate feature relationships and improve classification performance. By leveraging the principles of quantum entanglement, the system achieves higher accuracy, robustness, and efficient pattern recognition compared to conventional methods. The proposed approach provides a scalable and advanced solution for detecting electricity theft across both consumption and distributed generation domains in next-generation smart grids.

2. LITERATURE SURVEY

1. Robust Electricity Theft Detection in Smart Grids Using Machine Learning and Secure Techniques

Electricity theft is a growing issue that negatively impacts both utility companies and power users. It has an impact on customers' high energy bills, generates electric dangers, and hinders the economic growth of the electric utility sector. Electricity theft is the largest problem with smart grids. Smart meters (SMs) are put at the end of customers' homes and are used to regularly communicate precise power consumption data to the provider in order to monitor loads and control energy usage. Large amounts of electricity use data are challenging for current theft detection methods to handle because of nonlinear relationships and missing values. Additionally, there is no integrated system in place to coordinate the

analysis of electricity demand data. We provide a novel framework for detecting power theft in order to overcome these restrictions and improve the system's fault tolerance and dependability. To minimize the fluctuations and decrease the computational cost, we first use the quantum key distribution (QKD) using the rolling optimization technique (ROS). The classification process then uses the coati optimization algorithm (COA) and extreme gradient boosting (EGB). Lastly, in order to increase customer confidence in the smart grid system, we suggested trade-off solutions for privacy functionality. Therefore, the simulation of the novel power theft detection framework to further improve the system dependability and fault tolerance approach in Matlab-R2023a\Simulink shows better performance than current methods. The approaches in this study to overcome the issues faced in previous technologies are tested using different metrics of authentication rate at 98(%), accuracy at 99 (%), detection rate at 98.6 (%), precision at (97%), recall at (98.6%), at F1-score (95.15%), and AUC at (0.3123).

2. Smart Grid Electricity Fraud Detection Using Machine Learning

The smart grid is a recent addition to the digitalization of every part of our life. It primarily makes it possible for customers and power companies to communicate in both directions. It guarantees that the network can use sensors and smart meters to improve safety, security, resilience, and stability. It may also track shifts in supply and demand. Globally, businesses that supply power face enormous losses each year. Power dissipation on transmitters, large equipment, and overhead power lines can result in technical loss. However, electrical thieves are mostly responsible for the non-technical losses. When data on power use is tracked over an extended period of time, it is evident that regular, honest consumers follow a particular pattern. On the other hand, power thieves have extremely erratic usage and no discernible pattern. Electricity fraud can be identified by looking for certain irregularities in use trends. In order to detect electrical fraud with much better outcomes, this research proposes an enhanced model using cutting-edge machine learning techniques. It offers a thorough framework for analyzing data gathered from smart grids using supervised learning

techniques. In order to detect unusual consumption patterns suggestive of fraudulent activities, this work use the machine learning model 1D CNN. Additionally, using a dataset gathered from the State Grid Corporation of China that contains both genuine and fraudulent consumption records, it assesses the algorithm's performance against other algorithms and literature based on accuracy, RMSE, MAE, F1-Score, and AUC. With an accuracy of 95.47% and an F1 score of 97.42%, this 1D CNN model performs better than 2D CNN, ANN, XGBoost, random forest, decision tree, and logistic regression. In order to combat power theft, this study effectively demonstrates how machine learning may be integrated with smart grids.

3. Quantum Entropy and Reinforcement Learning for Distributed Denial of Service Attack Detection in Smart Grid

One of the most damaging cyberattacks, distributed denial of service (DDoS) threats in smart grids are extremely difficult. They are creating significant financial loss and negatively impacting the electricity industry. Since classical Reinforcement Learning (RL) models learn the best mitigation strategies under various attack circumstances, they are suggested as a potential solution to the DDoS issue. However, serial processing utilizing classical computing might restrict traditional RL efficiency because the RL environment is often dynamic, which results in additional calculation capabilities. This research proposes a Quantum Entropy Q-Learning (QEQ) to combat DDoS in Smart Grids. A traditional Q-Learning (QL) model with and without the Entropy approach is contrasted with the suggested framework. To demonstrate the QEQ performance, the convergence speed and total rewards obtained under the same settings for QL and Entropy Q-Learning (EQ) are examined. Additionally, the accuracy, precision, recall, and F1 score are assessed to demonstrate our QEQ's efficacy against DDoS assaults. A comprehensive systematic simulation utilizing MATLAB, Python, the open-source Qiskit software, and the Harrow-Hassidim-Lloyd (HHL) quantum algorithm is conducted using the Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS 2019) dataset. This suggested QEQ performs better at DDoS detection because it is quick

enough, more flexible when the environment changes, and capable of enhancing the agent's decision-making in a changing state action space. Lastly, several unresolved concerns with Quantum Q-Learning are addressed along with conclusions.

4. Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids

Smart meters (SMs) are installed at customers' ends in smart power grids to provide the utility with detailed power consumption measurements on a regular basis for load monitoring and energy management. However, dishonest consumers might initiate cyberattacks to steal electricity by hacking their SMs and reporting erroneous readings in order to lower their electricity bills. Because the measurements are utilized for energy management, these assaults negatively impact the power industry by causing significant financial loss and degrading grid operation. To the best of our knowledge, the application of reinforcement learning (RL) has not yet been explored, however supervised machine learning techniques have been employed in the literature to identify the assaults. Because RL can learn via exploration and exploitation processes and choose the best course of action, it can adapt more effectively to the dynamic nature of cyberattacks and consumption patterns than the current systems. This article suggests a deep reinforcement learning (DRL) method as a potential remedy for the issue of power theft. Rewards are awarded based on detection mistakes made during training, and real dataset samples are used as an environment. Specifically, four distinct situations are described for the suggested technique. Initially, a deep Q network (DQN) and a double deep Q network (DDQN) with various deep neural network designs are used to build a global detection model. Second, in order to achieve high detection accuracy while preventing zero-day attacks, the global detector is employed to create a tailored detection model for new clients. Third, the third scenario considers altering the current customers' consumption habits. Fourth, the fourth scenario discusses the difficulties in protecting against recently started cyberattacks. Numerous tests have been carried out, and the findings show that the suggested DRL approach can improve the detection of cyberattacks involving electricity theft and

effectively learn new consumption patterns, changes in the consumption patterns of current customers, and recently launched cyberattacks.

5. A Quantum Controlled-NOT Neural Network-Based Load Forecast and Management Model for Smart Grid

The mismatch issue is brought on by the uncertainty and unpredictability of power output and resource utilization on both the supply and demand sides. As a result, managing the power supply and demand of regional smart meters has emerged as a crucial and difficult research topic in the present day. The link between predicted load and power demand supply management of smart meters, which has a significant influence on the performance of power services for regional clients, has not been sufficiently investigated by the current solutions. In this regard, a novel quantum machine learning-driven power distribution and supply management (QPD-SM) model is suggested that uses load forecasting values and effectively manages power supply to proactively anticipate the power demand of regional smart meters. To accurately predict regional load, the model uses a recently created "quantum controlled-NOT gate induced feed-forward neural network" (QCNN) that is tuned using the quantum adaptive differential evolutionary (QuADE) learning method. Additionally, a demand-supply management strategy is intended to assess and quantify the excess or shortage of power units in relation to various locations and regulate power generation and supply management appropriately. In comparison to the current state-of-the-art works, the suggested model improves root-mean-squared error by up to 77.02% and 78.92%, respectively, according to experimental data from the Australian Smart Grid Smart City and the Irish Commission for Energy Regulation.

3. METHODOLOGY

i) Proposed Work:

The proposed work introduces an advanced electricity theft detection framework using an entanglement-enhanced Quantum Deep Learning (QDL) model. The system utilizes the "Smart Grid Theft Detection" dataset, incorporating both

consumer consumption data and Distributed Generation (DG) features such as photovoltaic (PV) output. Data preprocessing involves feature extraction, normalization, shuffling, and splitting into training (80%) and testing (20%) sets. A hybrid architecture is designed by integrating a classical neural network with a Quantum Variational Circuit (QVC), where classical outputs are encoded into qubits using angle-embedding techniques. The QVC employs parameterized rotation gates and CNOT operations to learn complex feature representations while minimizing noise effects in Noisy Intermediate-Scale Quantum (NISQ) devices.

To further enhance performance, a Data Re-uploading Circuit (DRC) is incorporated to iteratively encode data into the quantum system, improving feature learning and mitigating information loss. The key novelty lies in the addition of an entanglement layer, which establishes strong correlations between qubits, enabling the model to exploit quantum parallelism and interference. This enhancement significantly improves the model's ability to detect subtle and complex fraudulent patterns in both consumption and generation domains. The proposed FH-QVC-DRC-ENT model is evaluated against classical machine learning algorithms such as XGBoost and LightGBM, demonstrating superior accuracy, robustness, and generalization capability for effective power theft detection in smart grids.

ii) System Architecture:

The system architecture consists of a hybrid classical-quantum framework designed for efficient power theft detection. Initially, the input data obtained from smart meters and distributed generation sources is passed through classical layers, including the Master layer and Feeding layer, where essential features are extracted and transformed into a suitable format. These classical layers act as preprocessing units, reducing data complexity and preparing it for quantum processing. The processed data is then forwarded to the quantum layer, ensuring a seamless transition from classical computation to quantum representation.

The quantum layer is built using a QVC-DRC architecture with entanglement blocks, where each

block includes angle embedding and entangling layers. In the angle embedding stage, classical data is encoded into qubits using rotation gates, followed by entangling operations (such as CNOT gates) to establish correlations between qubits. Multiple such blocks are stacked with data re-uploading to enhance feature learning and reduce noise effects. The inclusion of the entanglement layer enables better interaction among qubits, improving pattern recognition capability. Finally, measurement operations convert quantum states back into classical outputs, which are passed to the final decision layer for classification of theft and non-theft instances with improved accuracy and robustness.

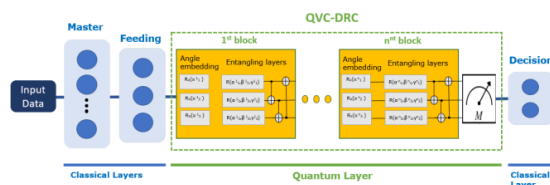


Fig.1. Proposed Architecture

iii) MODULES:

1. Importing the Packages: Beginning with essential library imports establishes the computational foundation required for data handling, visualization, quantum circuit execution, and model evaluation. Integrating these packages ensures consistent functionality, enables advanced analytical operations, and prepares the environment for efficient processing of high-dimensional smart-grid data.

2. Exploring the Dataset: Initial dataset exploration examines feature distributions, class labels, and structural consistency to understand the nature of smart-meter readings. Such inspection is vital for identifying irregularities, planning preprocessing tasks, and ensuring that subsequent analytical stages operate on well-interpreted and reliable input data.

3. Visualization: Graphical representations of class labels and feature behaviors provide intuitive insight into imbalanced patterns and variation across consumption records. Visualization supports informed decision-making during model development, enabling better understanding of correlations, anomalies, and data characteristics critical for theft detection accuracy.

4. Pre-processing: Pre-processing operations transform raw meter readings into structured, usable formats by extracting relevant features, handling missing values, and organizing data for learning. These refinements enhance data quality, reduce noise

interference, and ensure that analytical components receive clean, consistent, and meaningful inputs.

5. Normalize & Shuffling: Normalization and shuffling techniques stabilize feature scales and eliminate ordering bias in training data. These operations support robust learning performance, prevent dominance of large-scale attributes, and improve the generalization capability of both classical and quantum-enhanced classification models.

6. Split the Data into Train & Test: Dividing the dataset into training and testing portions ensures objective performance measurement by isolating unseen samples for evaluation. This separation prevents overfitting, validates the model's predictive strength, and confirms that detection outcomes reliably generalize to real-world smart-grid scenarios.

7. Model Training: Training involves fitting classical and quantum-hybrid learning frameworks to processed data, enabling the system to learn complex relationships between consumption patterns and theft behavior. This phase develops decision boundaries, optimizes parameters, and establishes the foundations for accurate and noise-resistant classification.

8. Evaluation: Performance evaluation calculates accuracy, precision, recall, and F-score to verify detection effectiveness and compare learning strategies. Metrics derived from this analysis measure robustness, expose limitations, and validate improvements contributed by quantum-enhanced architectures over traditional analytical approaches.

9. Flask Server: Launching the Flask server deploys the analytical framework into an interactive environment, enabling browser-based access to prediction services. The server infrastructure supports seamless communication between user inputs and the backend model, ensuring accessible, real-time detection functionality.

10. User Login: The login interface authenticates system access by validating administrator credentials and preventing unauthorized use. Secure entry control safeguards stored data, protects prediction services, and maintains integrity within the operational environment handling sensitive smart-grid information.

11. Power Theft Prediction: The prediction interface processes uploaded test files, executes the trained quantum-enhanced model, and displays theft or non-theft classifications. This interactive mechanism allows utility personnel to assess consumption records effectively, translating analytical outcomes into actionable insights for operational decision-making.

12. Logout: The logout operation terminates authenticated sessions, ensuring secure closure of user activity and preventing unintended access. Controlled

session termination strengthens overall system protection and supports responsible management of sensitive detection functionalities.

iv) ALGORITHMS:

XGBOOST:

XGBoost is a powerful gradient boosting algorithm that builds an ensemble of decision trees by iteratively correcting the errors of previous models. It effectively captures complex nonlinear relationships in smart grid data while handling missing values and high-dimensional features. With built-in regularization and parallel processing, it reduces overfitting and improves generalization. Due to its strong predictive performance on structured data, it serves as a reliable baseline for comparing advanced quantum-based models.

LIGHTGBM:

LightGBM is a fast and memory-efficient gradient boosting framework designed for large-scale data processing. It uses a leaf-wise tree growth strategy to capture feature interactions while maintaining computational efficiency. The algorithm handles high-dimensional, sparse, and categorical data effectively, making it suitable for smart grid datasets. Its faster training speed and competitive accuracy make it an ideal model for benchmarking against more complex learning approaches.

FH-QVC-DRC:

The FH-QVC-DRC model is a hybrid quantum-classical approach that combines classical preprocessing with quantum variational learning. It encodes classical features into quantum states using angle embedding and applies parameterized quantum circuits to learn complex data patterns. The data re-uploading mechanism enhances feature representation and reduces the impact of noise in quantum systems. This model improves classification performance by leveraging quantum parallelism and interference, enabling better detection of power theft patterns.

FH-QVC-DRC-ENT:

The FH-QVC-DRC-ENT model extends the hybrid quantum framework by incorporating an entanglement layer to strengthen correlations between qubits. This enhancement allows the model

to capture deeper relationships in data, improving pattern separability and classification accuracy. By exploiting quantum entanglement, the model achieves better robustness, noise resistance, and generalization. As a result, it provides superior performance in detecting complex and subtle power theft behaviors in smart grid systems.

v) Dataset Description

The dataset used in this study is the “Smart Grid Theft Detection” dataset obtained from Kaggle, which contains electricity consumption and distributed generation data collected from smart meters. It includes features representing household energy usage patterns along with photovoltaic (PV) generation values, enabling analysis across both consumption and distributed generation domains. Each data instance is labeled as either theft or non-theft, allowing the problem to be formulated as a binary classification task.

The dataset consists of high-dimensional and time-dependent attributes that reflect variations in energy usage behavior over time. Preprocessing steps such as feature selection, normalization, and shuffling are applied to improve data quality and model performance. The dataset is divided into 80% training and 20% testing sets to ensure unbiased evaluation. Its diversity and complexity make it suitable for evaluating both classical machine learning models and advanced quantum deep learning approaches for accurate power theft detection in smart grid environments.

4. EXPERIMENTAL RESULTS

The experimental evaluation compares classical machine learning models (XGBoost and LightGBM) with the proposed quantum-based models (FH-QVC-DRC and FH-QVC-DRC-ENT) using performance metrics such as accuracy, precision, recall, and F1-score. From the results, XGBoost achieves around 86% accuracy, while LightGBM shows relatively lower performance at approximately 73% accuracy, indicating limitations in handling complex and high-dimensional smart grid data. The proposed FH-QVC-DRC model improves the performance to nearly 88% accuracy, demonstrating the effectiveness of hybrid quantum-classical learning in capturing nonlinear patterns and reducing noise through quantum circuits.

Further enhancement using the entanglement layer in the FH-QVC-DRC-ENT model results in the best performance, achieving approximately 91% accuracy, along with improved precision, recall, and F1-score. The entanglement mechanism strengthens feature correlations and enables better discrimination between theft and non-theft instances. Additionally, the prediction interface demonstrates practical applicability by accurately classifying uploaded test data through a web-based system. Overall, the results confirm that the entanglement-enhanced quantum model significantly outperforms classical approaches, providing a more robust and reliable solution for power theft detection in smart grids.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

$$\text{Accuracy} = \frac{TP + TN}{(TP + TN + FP + FN)}$$

$$\text{Accuracy} = \frac{(TN + TP)}{T}$$

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

$$\text{Precision} = \frac{\text{True positives}}{(\text{True positives} + \text{False positives})} = \frac{TP}{(TP + FP)}$$

$$\text{Precision} = \frac{TP}{(TP + FP)}$$

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

$$\text{Recall} = \frac{TP}{(FN + TP)}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model

accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

$$F1 = 2 \cdot \frac{(\text{Recall} \cdot \text{Precision})}{(\text{Recall} + \text{Precision})}$$

To run web prediction double click on 'runFlask.bat' file to start flask server and then will get below page

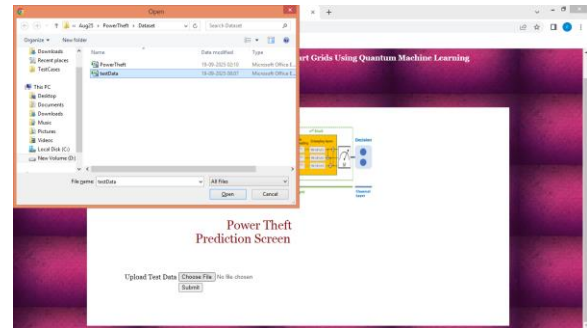


Fig6 uploading test data file

In above screen selecting and uploading test data file and then click on buttons to get below page

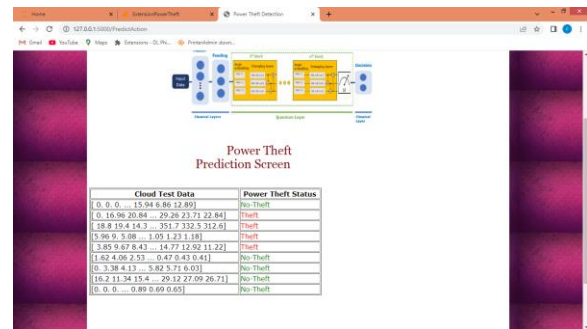
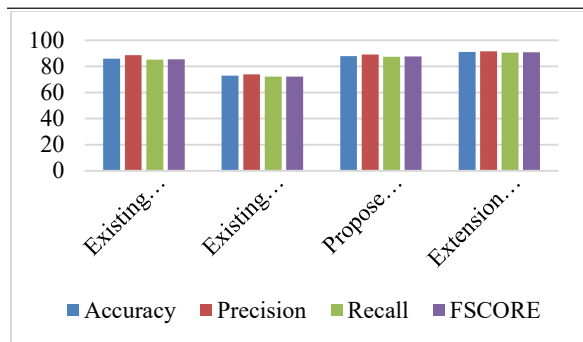


Fig7 results

In above screen in first column showing test data values and in second column can see predicted results.



Graph.1 Comparison Graph

Algorithm Name	Accuracy	Precision	Recall	FSCORE
Existing XGBoost	86.0	88.571429	85.226817	85.531211
Existing LightGBM	73.0	74.045139	72.240064	72.196478
Propose FH-QVC-DRC	88.0	89.239176	87.474910	87.760098
Extension FH-QVC-DRC-ENT	91.0	91.584565	90.666399	90.889766

Table.1 Performance Evaluation Table

5. CONCLUSION

This paper presents an entanglement-enhanced Quantum Deep Learning framework for effective power theft detection in smart grids. By integrating Quantum Variational Circuits (QVC), Data Re-uploading Circuits (DRC), and an entanglement layer, the proposed model successfully overcomes limitations of classical machine learning approaches in handling high-dimensional, noisy, and imbalanced data. The system effectively analyzes both consumption and distributed generation (DG) patterns, providing a comprehensive detection mechanism across smart grid domains.

Experimental results demonstrate that the proposed FH-QVC-DRC-ENT model achieves superior

performance compared to traditional models such as XGBoost and LightGBM, with improved accuracy, robustness, and generalization capability. The incorporation of quantum entanglement enhances feature representation and classification precision, enabling better identification of complex theft patterns. Overall, the proposed approach offers a reliable, scalable, and advanced solution for securing modern smart grids against electricity theft.

6. FUTURE SCOPE

The proposed work can be further extended by implementing the quantum model on real quantum hardware instead of simulators to evaluate performance under practical quantum constraints. Future research can explore advanced quantum architectures and optimization techniques to further improve accuracy and scalability for large-scale smart grid datasets. Integration with real-time streaming data from IoT-enabled smart meters can enhance the system's capability for continuous monitoring and instant theft detection.

Additionally, the model can be expanded to handle multi-class classification for identifying different types of fraud such as cyberattacks, meter tampering, and energy manipulation. Incorporating explainable AI (XAI) techniques can improve transparency and trust in decision-making. Future work may also focus on hybrid edge-cloud deployment and federated learning to ensure data privacy, reduce latency, and enable secure, distributed power theft detection in next-generation smart grid environments.

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] Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.
- [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] Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.
- [9] Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835.
<https://doi.org/10.56025/ijaresm.2025.1304254828>.
- [10] Doragacharla, V. R. (2026). Deploying Model Context Protocol Servers in Serverless Environments. Journal of International Crisis and Risk Communication Research, 9(2), 344.
- [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] Prodduturi, S. M. K. (2024). Legal challenges in regulating AI-powered cybersecurity tools. International Journal of Engineering & Science Research, 14(4), 316-323.
- [13] Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
- [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] Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50.
<https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50>.
- [16] Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew Management Systems. International Journal of Enhanced Research in Management & Computer Applications, 13(11), 50–55.
<https://doi.org/10.55948/ijermca.2024.0116>.
- [17] Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
- [18] Henry Cyril. (2025). AI-DRIVEN ANOMALY DETECTION, OUTAGE PREDICTION, AND SELF-HEALING IN TELECOM PROVISIONING SYSTEMS. International Journal of Applied Mathematics, 38(12s), 2817–2832.
<https://doi.org/10.12732/ijam.v38i12s.1589>.
- [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] Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s),

1270–1285.

<https://doi.org/10.12732/ijam.v38i4s.685>.

[21] M. M. Badr, M. I. Ibrahim, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmay, “Detection of false-reading attacks in smart grid net-metering system,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1386–1401, Jan. 2022.

[22] L. Xue, L. Cheng, Y. Li, and Y. Mao, “Quantum machine learning for electricity theft detection: An initial investigation,” in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber. Phys. Social Comput. (CPSCoM) IEEE Smart Data (SmartData) IEEE Congr. Cybermatics (Cybermatics)*, Dec. 2021, pp. 204–208.

[23] W. Qi, A. I. Zenchuk, A. Kumar, and J. Wu, “Quantum algorithms for matrix operations and linear systems of equations,” *Commun. Theor. Phys.*, vol. 76, no. 3, Mar. 2024, Art. no. 035103.

[24] Y. Du, X. Wang, N. Guo, Z. Yu, Y. Qian, K. Zhang, M.-H. Hsieh, P. Rebentrost, and D. Tao, “Quantum machine learning: A hands-on tutorial for machine learning practitioners and researchers,” 2025, arXiv:2502.01146.

[25] P. Rebentrost, A. Steffens, I. Marvian, and S. Lloyd, “Quantum singular-value decomposition of nonsparse low-rank matrices,” *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, Jan. 2018, Art. no. 012327.

[26] S. Stein, Y. Mao, J. Ang, and A. Li, “QuCNN: A quantum convolutional neural network with entanglement based backpropagation,” in *Proc. IEEE/ACM 7th Symp. Edge Comput. (SEC)*, Dec. 2022, pp. 368–374.

[27] S. A. Stein, B. Baheri, D. Chen, Y. Mao, Q. Guan, A. Li, S. Xu, and C. Ding, “QuClass: A hybrid deep neural network architecture based on quantum state fidelity,” in *Proc. Mach. Learn. Syst.*, 2022, pp. 251–264.

[28] N. Schetakis, D. Aghamalyan, M. Boguslavsky, A. Rees, M. Rakotomalala, and P. R. Griffin, “Quantum machine learning for credit scoring,” *Mathematics*, vol. 12, no. 9, p. 1391, May 2024.

[29] K. Blazakis, Y. Katsigiannis, N. Schetakis, and G. Stavrakakis, “One day ahead wind speed forecasting based on advanced deep and hybrid quantum machine learning,” in *Proc. 1st Int. Conf. Frontiers Artif. Intell., Ethics Multidisciplinary Appl.*, Athens, Greece, Sep. 2023, pp. 155–168.

[30] M. Schuld and N. Killoran, “Quantum machine learning in feature Hilbert spaces,” *Phys. Rev. Lett.*, vol. 122, no. 4, Feb. 2019, Art. no. 040504.