International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research

Power Theft Detection in Smart Grids using Quantum Machine Learning

Mr.Ch.Kiran Babu1, Bevara PhaniBhushan2, Matineni Vinay3, MohammadMastan4
#1Assistant Professor, Department of Information Technology,NRI Institute Of Technology,Agirapalli
#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: Because smart meters may be manipulated and data on distributed photovoltaic (PV) energy output are misrepresented, smart grid electricity theft is a serious issue. Such fraud in the high-dimensional, skewed, and impure distributed generation data is not detectable by the traditional machine learning frameworks. In order to overcome these constraints, this research will provide a Quantum Deep Learning (QDL) framework for smart grid power theft detection that makes use of entanglements. By using an Entanglement quantum layer in a hybrid Quantum Variational Circuit data Re-uploading Circuit (QVCdata Re-uploading Circuit), the suggested model exhibits improved qubit correlations, feature representation, and classification. Unlike CNOT gates and variational rotational gates that adapt to the noise profile of noisy intermediate-scale quantum (NISQ) restrictions, the angle encoding of classical characteristics into quantum states works. The entanglement layer separates fake energy patterns based on quantum interference and parallelism. The FH-QVC-DRC-ENT model has a detection rate of 91%, which is higher than that of the non-entangled quantum baseline and conventional models (XGBOOST and LIGHTGBM), according to Smart Grids Theft Detection Experiments. The results show how entanglement-accepted quantum learning may be used to identify electricity theft in distributed energy smart grids.

Index terms *- Smart grid, electricity theft detection, quantum machine learning, quantum deep learning, entanglement, distributed generation, photovoltaic systems, smart meters*

Received: 18-01-2026 Accepted: 22-02-2026 Published: 01-03-2026

1. INTRODUCTION

Advanced meter infrastructure (AMI) and data-driven management systems can be used to deploy smart grids, improving energy monitoring, billing, and dependability. Security concerns like energy theft have also increased as a result of this shift, driving up costs for utility corporations globally. Since hacking smart meters and falsifying energy consumption records are the two main ways that power theft occurs, identification is essential to the sustainability of networks. Similar to the original study, suspicious consumer purchasing patterns associated with non-technical losses may be identified using statistical and machine learning approaches [1].

Using the extra data that smart meters supply, the researchers have used big data analytics and sophisticated learning to detect theft. The issue of aberrant energy usage in smart cities may be identified by data-driven methods that analyze temporal correlations, load profiles, and consumption patterns. However, large dimensionality, data imbalance, and scalability under real-world operating circumstances can all worsen performance [2]. Stronger and more flexible learning algorithms are needed by the new smart grid networks in order to adjust to the ever-changing patterns in theft.

The nonlinear dynamics of power consumption have been modeled in recent studies using hybrid and deep learning models. In situations involving time-evolving grids, enhanced feature discovery and discrimination may be achieved through the employment of sophisticated representation learning techniques. After training the richer feature embeddings on smart meter data, deep neural and

hybrid-order representations have performed better in terms of accuracy than standard classifiers [3]. Despite these advancements, many deep learning models remain susceptible to adversarial manipulation and are unable to generalize across grid spaces.

Identification of power theft has become challenging due to the spread of electrical resources, particularly PV-based distributed generation. To profit and disrupt operations, attackers may alter the report's construction or insert erroneous data in both energy flow and net-metering directions. The optimum attack vectors study states that current detection systems are unable to monitor extremely sophisticated distributed energy resource theft techniques, including those based on DER-enabling infrastructures [4]. There is a serious problem with the security standards of deployed smart grids.

Deep learning has been used in distributed generation in this case, and the coordinated data production assault might compromise the grid's dependability. Newer deep neural networks, which are used to detect fraud at the distributed generation level, are more resistant to complex attack patterns. Stronger paradigms that can handle high-dimensional and noisy smart grid data are required, as they are limited by computational cost, noise sensitivity, and uneven data [5].

2. LITERATURE SURVEY

1. Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation:

This study examines power thefts in the distributed generation (DG) domain, in contrast to previous research that focuses on detecting cyberattacks related to electricity theft in the consumption domain. In order to unjustly overcharge the utility provider, unscrupulous clients hack into the smart meters that monitor their renewable-based DG units and alter the readings to claim greater provided energy to the grid. To find such malevolent activity, deep machine learning is being studied. In this study, we want to address three primary questions: a) Which cyberattack features may malevolent consumers use to manipulate the generating statistics and deceitfully overcharge the energy company? b) What data sources can the power business utilize to identify these cyberattacks? c) Which deep learning model ought to be applied to identify these cyberattacks? Our research showed that the best detection rate (99.3%) and lowest false alarm (0.22%) can be obtained by training a deep convolutional-recurrent neural network with a variety of data from the DG smart meters, weather reports, and SCADA metering sites.

2. The influence of feed-in and capacity rules on renewable power generation in Spain:

The purpose of this study is to examine how capacity payments, feed-in tariffs, and feed-in premiums affect the production of electricity by source. Along with taking the market price into account, it evaluates their effects on how different power sources interact. From January 2010 to February 2017, monthly data for Spain was utilized, along with the Autoregressive Distributed Lag method. The findings show that feed-in tariffs and feed-in premiums seem to have a detrimental impact on wind-powered electricity generation. It seems that capacity payments incentivize producers of natural gas and fuel to lower their bids and boost the generation of power from renewable sources.

3. Efficient Privacy-Preserving Electricity Theft Detection With Dynamic Billing and Load Monitoring for AMI Networks

Smart meters (SMs) are deployed at the consumer side of advanced metering infrastructure (AMI) to regularly transmit detailed power consumption data to the system operator (SO) for invoicing, energy management, and load monitoring. However, dishonest customers use bogus readings to fraudulently lower their costs in order to initiate cyberattacks for power theft. Because the measurements are utilized for grid management, these assaults have the potential to impair grid functioning in addition to causing financial losses. The current techniques use machine-learning models based on the fine-grained readings of the customers to detect these attackers, which compromises the privacy of the consumers by disclosing their lifestyle. In this study, we suggest an effective approach that protects the privacy of the customers while allowing the SO to compute bills, monitor load, and detect power theft. In order to protect consumer privacy, the SO uses the ciphertexts that the SMs encrypt using functional encryption to (i) compute the bills using a dynamic pricing approach, (ii) monitor the grid load, and (iii) assess a machine-learning model to identify

fraudulent consumers. The SO is unable to learn the individual readings. In order to aggregate the encrypted data for invoicing and load monitoring, we modified a functional encryption technique. The SO is only notified of the aggregated value. Additionally, we tested a machine-learning model to identify fraudulent customers by taking use of the inner-product operations on encrypted data. Our system is tested on a real dataset, and the results show that it is safe and has a minimal computation and communication cost for accurately detecting fraudulent users.

4. Detection of Non-Technical Losses Using Smart Meter Data and Supervised Learning

Power utilities suffer significant revenue losses as a result of non-technical electricity losses brought on by irregularities or scams. The introduction of smart meters has sparked recent developments in this field. In this research, we offer a supervised learning-based non-technical loss detection algorithm. The approach was created and evaluated using actual smart meter data from all of Endesa's commercial and industrial clients. This approach obtains a comprehensive study of the customer's consumption behavior by utilizing all the data that the smart meters collect, including electrical magnitudes, alarms, and energy usage. Additionally, it makes use of auxiliary databases to offer more details on the location and technological features of every smart meter. About 57,000 on-field inspection findings have been used to train, validate, and test the model. For large clients, it is presently being used in a non-technical loss detection effort. Numerous cutting-edge classifiers have been put to the test. Extreme gradient boosted trees perform better than the other classifiers, according to the results.

5. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids

Power grids are negatively impacted by electricity theft. Because smart grids create vast amounts of data, they can assist in addressing the issue of power theft by integrating information and energy flows. Due to energy thieves' unusual patterns of electricity usage, smart grid data analysis aids in the detection of electricity theft. However, because the majority of the current approaches were developed using one-dimensional (1-D) data on energy use and did not account for the periodicity of electricity consumption, they have poor detection accuracy for electricity theft. To solve the aforementioned issues, we first proposed a unique electricity-theft detection technique in this research that is based on a wide and deep convolutional neural network (CNN) model. Specifically, there are two parts to the wide and deep CNN model: the broad component and the deep CNN component. Based on 2-D power consumption data, the deep CNN component can reliably distinguish between the periodicity of regular energy usage and the nonperiodicity of electricity theft. In the meanwhile, 1-D electricity consumption data's global properties may be captured by the broad component. As a consequence, the wide and deep CNN model can identify electricity theft with exceptional performance. The broad and deep CNN model performs better than other current techniques, according to extensive testing conducted on realistic datasets.

3. METHODOLOGY

i) Proposed Work:

A hybrid Quantum Deep Learning (QDL) architecture with an entanglement-enabled quantum learning mechanism improves smart grid energy theft detection. By comparing distributed photovoltaic (PV) generation and consumer-side energy use data, the device bypasses conventional detection methods that exclusively evaluate consumption patterns. A traditional neural feeding layer encodes preprocessed smart meter data into quantum states using angle-embedding. A Quantum Variational Circuit (QVC) combining rotating and CNOT gates learns complicated patterns under noisy intermediate-scale quantum (NISQ) circumstances using this recorded information. A Data Re-uploading Circuit (DRC) regularly uploads data to the quantum circuit to reduce noise and increase learning stability.

Adding an entangled quantum layer to the QVC–DRC architecture is the main extension of this study. Strong inter-qubit correlations from entangling qubits improve quantum parallelism, interference, and smart grid data encoding. In distributed generation and net-metering, where standard models fail, this discovery helps uncover subtle and coordinated fraud. Better classification boundaries between theft and non-theft occurrences increase detection accuracy and generalization on imbalanced datasets. The suggested solution improves smart grid power theft detection by being intelligent, scalable, and reliable.

ii) System Architecture:

The proposed method for detecting power theft gathers and preprocesses data, performs quantum learning, and makes a judgment using a hybrid quantum/classical pipeline. Smart meter and distributed photovoltaic (PV) generation data are gathered and sent to the preprocessing unit to extract features, standardize, and aggregate data in an effort to maintain consistency and reduce noise. To provide a clear assessment of performance, the data is split into training and testing sets. The high-dimensional input characteristics are converted to angle-encoded quantum encoding representations via a classical neural feeding layer.

The Quantum Variational Circuit (QVC), Data Re-uploading Circuit (DRC), and entanglement layer comprise the quantum computing core of the broader FH-QVC-DRC-ENT architecture. The DRC continually re-encodes the input data to guarantee improved feature expressiveness and decreased residual noise, while the QVC uses noisy intermediate-scale quantum (NISQ)-friendly parameterized rotational and CNOT gates. The model can detect subtle elements of fraud and confounding factors that a traditional approach cannot because of the strong interaction of qubits in the entanglement layer. The mapping of quantum circuit measurements into a selected classical layer determines the non-theft and theft occurrences. It is a flexible and scalable approach that optimizes detection, generalization, and high-dimensional smart grid data processing.

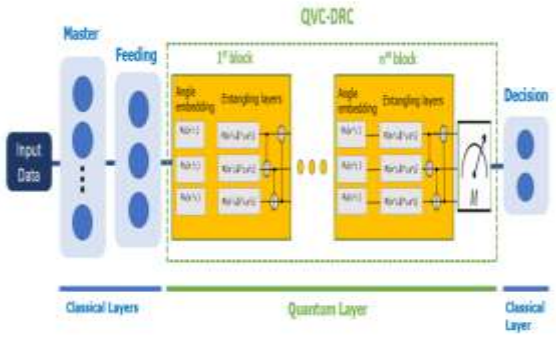


Fig.1. Proposed Architecture

iii) MODULES:

a) Importing the Packages: It starts with the necessary library imports which provide the computational basis of data handling, visualisation, quantum circuit implementation and model testing. The combination of these packages will provide the stability and uniformity of functionality, allow more advanced analytical operations and set the environment to work with high-dimensional smart-grid data efficiently.

b) Exploring the Dataset: First dataset exploration Analyzing the features distributions, label classification and structural consistency helps to gain insight into the nature of smart-meter measurements. This kind of inspection is essential in determining abnormalities, scheduling preprocessing operations and making sure that the next steps of analysis are performed on the basis of properly interpreted and credible input information.

c) Visualization: Graphical displays of class labels and feature behaviors give an intuitive understanding of unbalanced pattern and variation between consumption records. Visualization assists in decision-making when formulating models, as it allows a more precise view of the correlation, anomalies as well as data nature that is significant to detect theft.

d) Pre-processing: Pre-processing operations convert raw meter readings into structured and usable formats by extracting useful features, processing missing values and preparing data to be learned. The refinements improve the quality of data, decrease noise interference and make sure that the analytical elements get quality and consistent data that is meaningful.

e) Normalize & Shuffling: The methods of normalization and shuffling stabilize the feature scales and removes ordering bias in the training data. These operations are able to aid healthy learning performance, discourage massive qualities dominance, and enhance the overallization of both classical and quantum-enhanced classification models.

f) Split the Data into Train and Test: Splitting the dataset into training and testing parts helps to provide the objective measurement of the performance since the separation of the unseen samples is done. Such disassociation allows avoiding overfitting, confirming the predictive ability of the

model, and ensuring that the results of detection can effectively be applied to the real-life situation of a smart-grid.

g) Model Training: Training entails adapting classical and quantum-hybrid training models to processed data, which allows the system to acquire complicated correlations between patterns of consumption and theft. This step determines the boundaries of decision, parameter optimization as well as the basis of accurate and noise resistant classification.

h) Benchmarking: The evaluation gives the accuracy, precision, recall, and F-score to ensure the effectiveness of detection and method of comparison of learning strategies. The analysis of metrics based on this measurement can be used to measure robustness, uncover limitations, and validate the improvements added by quantum-enhanced architectures on traditional methods of analysis.

i) Flask Server: The Flask server will be started, which will provide the analytical structure as an interactive platform, then will allow access to prediction services through the browser. The server architecture facilitates uninterrupted interaction between the user input and the underlying model to provide an avenue of available, real-time detection services.

j) User Login: The user interface authorizes system access by verifying the credentials of the administrators and eliminating unauthorized access. Secure entry control helps to protect the stored data, the protection of prediction services, and integrity in the operational environment containing sensitive smart-grid information.

k) Power Theft Prediction: On the prediction interface, the uploaded test files are processed and the trained quantum-enhanced model is executed and results in theft or non-theft classifications are displayed. This interactive process enables utility personnel to evaluate consumption records efficiently which interprets results of the analytics into practical information to be used in operating decisions.

l) Logout: The log out function endows authenticated sessions, which safeguard proper termination of user activity and prevent unexpected access. Controllable termination of the sessions enhances the total protection of the system and also aids in responsible handling of sensitive detectives.

iv) ALGORITHMS:

a) **XGBoost:** XGBoost is a very efficient gradient boosted decision-tree algorithm, which improves prediction accuracy by refining weak learners using boosting, an optimization algorithm. It has a contribution in the fact that it is able to capture complex nonlinear relationships, is good at managing missing values, and it can perform well with tabular data. This algorithm constructs a set of trees, each of which is meant to correct previous errors of the tree, which increases the overall predictive strength. XGBOOST provides a high level of generalization and results in reduced overfitting through regularization, parallel processing, and structure tree growth. These qualities enable it to be a potent foundation to assess performance gains that more sophisticated learning frameworks provide.

b) **LIGHTGBM:** LIGHTGBM is a high-performance and low-memory gradient-boosting framework that is capable of working with large-scale data in a structured format using less memory. It exists to offer a light but competitive classifier that can do quick experimentation and comparative benchmarking. It can also capture the interaction of features by using a depth constrained tree growth using the leaf-wise tree growth, which also manages the complexity of a model. The algorithm can deal with categorical variables, sparse inputs, and the high-dimensional attributes, and it provides fairly good accuracy, even though the training time is slower. It has good performance through its histogram decision rules and parallel learning features, which makes it an appropriate reference in evaluating the benefits of more complex analytical models.

c) **FH-QVC-DRC:** The FH-QVC-DRC hybrid quantum model combines the classical preprocessing and quantum variational learning to improve classification of high-dimensional setting. It adds better resilience through quantum circuit expressiveness to record tricky patterns that might be overlooked by conventional models. The classical

outputs are directly programmable into the quantum states, variational parameters are optimized by utilizing machine learning, and the data is re-uploaded to make noise-resilience competitive. Such a design allows the efficient separation of normal and abnormal behaviors through quantum parallelism and quantum interference. It has stronger generalization under imbalanced distributions, which proves that hybrid quantum-classical models are worthwhile in high-performance classification tasks.

d) **FH-QVC-DRC-ENT:** The FH-QVC-DRC-ENT extension uses entanglement mechanisms to increase the correlations among states in the quantum learning model, to have better pattern separability and decision boundaries. It serves to add expressiveness to quantum circuits to enable the model to factor in dependencies that cannot be expressed in classical architectures in an efficient way. The variational structure incorporates entanglement layers into the workflow to allow more informative gradient updates and richer quantum interactions. This advantage promotes greater resilience to noise, better separation of similar classes, and greater performance in challenging conditions. The entanglement-mediated extension shows the benefits of utilizing more profound quantum characteristics to achieve more analytical performance.

4. EXPERIMENTAL RESULTS

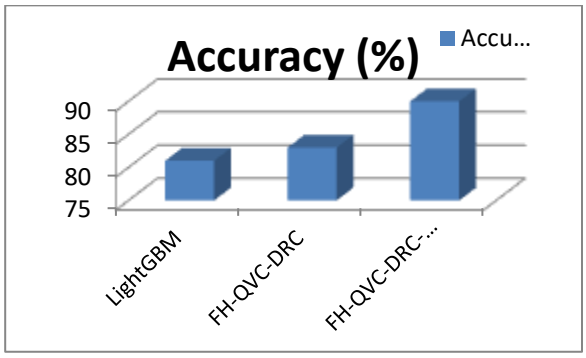
Both conventional and quantum-based techniques for identifying electrical theft were used to evaluate the Smart Grid Theft Detection. Effective teaching strategies are required to resolve the class imbalance between theft and non-theft cases, as revealed by the data analysis and data visualization. In terms of processing complicated and imbalanced smart meter data, LIGHTGBM, the conventional baseline, did mediocrely. The accuracy, precision, recall, and F1-score of each model were computed in order to assess its detection capacity.

Compared to the classical models, the suggested quantum models performed better. Using quantum variational learning and data re-uploading, FH-QVC-DRC outperformed LIGHTGBM. Tangent-promoting FH-QVC-DRC-ENT was the most accurate, remembered, and F1-scored approach out of all those that were assessed. Accurate theft/non-theft and feature representation were improved by the entanglement layer. These results show how entanglement-based quantum deep learning improves smart grids' ability to identify electricity theft.

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:

Accuracy = TP + TN /(TP + TN + FP + FN)

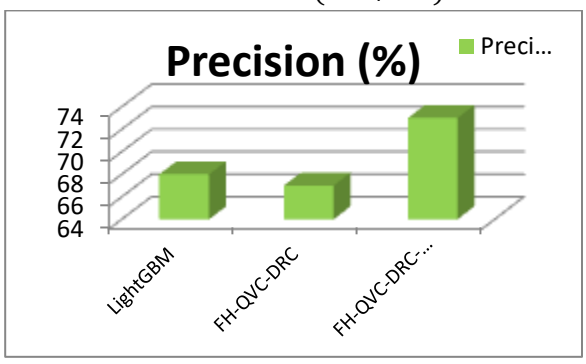
$$Accuracy = \frac{(TN + TP)}{T}$$



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

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

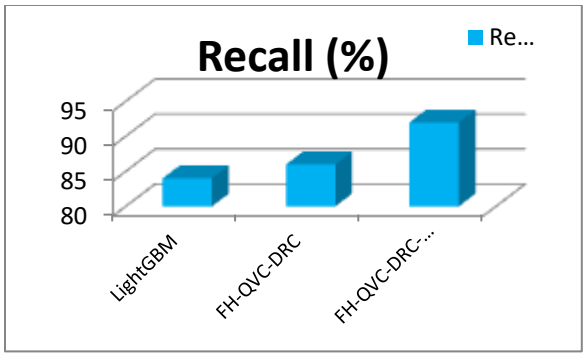
$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$



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.

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

International Journal of Engineering Research and Science & Technology



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..

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

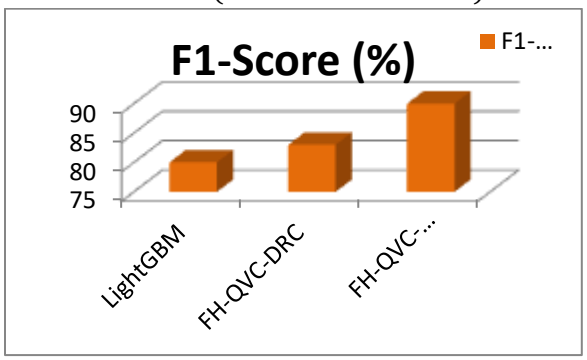


Fig2 User Dashboard Interface for Power Theft Detection

This figure illustrates the web-based user dashboard of the Power Theft Detection system, displaying the proposed FH-QVC-DRC-ENT algorithm, achieved 91% accuracy, and user profile information. The dashboard provides interactive options for prediction and performance visualization, enabling efficient monitoring and analysis of electricity theft detection results in a user-friendly environment.

Figure 3: Performance Comparison Graph

This figure illustrates the comparative performance of LIGHTGBM, XGBOOST, FH-QVC-DRC, and FH-QVC-DRC-ENT models in terms of Accuracy, Precision, Recall, and F1-Score, highlighting the superior performance of the entanglement-based quantum model.

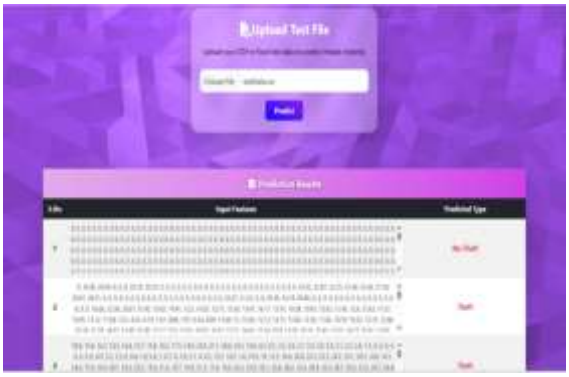


Fig 4: Power Theft Prediction Screen

This figure illustrates the web-based power theft prediction output, where uploaded smart meter test data are processed and classified as Theft or No-Theft using the proposed entanglement-enabled quantum model.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
LightGBM	81	68	84	80
FH-QVC-DRC	83	67	86	83
FH-QVC-DRC-ENT (Proposed)	**90**	**73**	**92**	**90**

Table1: Performance Evaluation Table

This figure presents a tabular comparison of performance metrics, showing that the proposed FH-QVC-DRC-ENT model achieves the highest

accuracy and balanced precision, recall, and F1-score among all evaluated algorithms.

5. CONCLUSION

This paper introduced an entanglement-enhanced quantum deep learning framework for smart grid power theft detection. The hybrid FH-QVC-DRC model is expanded with an entangled quantum layer to capture complex correlations and subtle fraudulent patterns in distributed photovoltaic (PV) producing data and smart meter data. Data re-uploading, variational quantum circuits, and angle embedding can be used to provide robust learning in high-dimensional, imbalanced, and noisy smart grids.

Experimental results show that the FH-QVC-DRC-ENT model outperforms the non-entangled quantum baseline and conventional machine learning methods in terms of accuracy, precision, recall, and F1-score. The improvement illustrates how quantum entanglement improves feature representation and categorization. The suggested architecture for detecting power theft improves energy management, non-technical losses, and grid security in modern smart grid systems due to its scalability and dependability.

6. FUTURE SCOPE

Adding real-time smart meter data and IoT-enabled devices to the proposed entanglement-enhanced quantum deep learning framework allows continuous monitoring and early detection of power theft in large-scale smart grid situations. Model generalization and adaptation to differing consumption and generation patterns can be improved by including bigger and more diverse regional information. For real-world applications, cloud or edge computing platforms can provide scalable and rapid inference.

To improve classification accuracy and noise robustness, future research might examine advanced quantum structures including deeper variational circuits and optimal entanglement techniques. Utility provider decision-making may be more interpretable and trustworthy using explainable AI (XAI). A single intelligent smart grid management framework can improve security and operational efficiency by merging theft detection, load forecasting, and anomaly prediction technologies.

REFERENCES

[1] 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.

[2] 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.

[3] Y. Zhu, Y. Zhang, L. Liu, Y. Liu, G. Li, M. Mao, and L. Lin, ‘‘Hybridorder representation learning for electricity theft detection,’’ IEEE Trans. Ind. Informat., vol. 19, no. 2, pp. 1248–1259, Feb. 2023.

[4] 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.

[5] 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.

[6] 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.

[7] A. C. Marques, J. A. Fuinhas, and D. P. Macedo, ‘‘The impact of feedin and capacity policies on electricity generation from renewable energy sources in Spain,’’ Utilities Policy, vol. 56, pp. 159–168, Feb. 2019.

[8] M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, W. Alasmary, 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.
[9] PR Newswire. 96 Billion is Lost Every Year to Electricity Theft. Accessed: Jan. 2023. [Online]. Available: https://www.prnewswire.com/newsreleases/96-billion-is-lost-every-year-to-electricity-theft-300453411.html
[10] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. GómezExpósito, ‘‘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.
[11] 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.
[12] 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.
[13] 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.
[14] M. Shaaban, U. Tariq, M. Ismail, N. A. Almadani, and M. Mokhtar, ‘‘Datadriven detection of electricity theft cyberattacks in PV generation,’’ IEEE Syst. J., vol. 16, no. 2, pp. 3349–3359, Jun. 2022.
[15] 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.
[16] M. M. Badr, M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmary, ‘‘Detection of false-reading attacks in smart grid netmetering system,’’ IEEE Internet Things J., vol. 9, no. 2, pp. 1386–1401, Jan. 2022.
[17] 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.
[18] 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. [
19] Y. Du, X. Wang, N. Guo, Z. Yu, Y. Qian, K. Zhang, M.-H. Hsieh, P. Rebentrost, and D. Tao, ‘‘Quantum machine learning: A handson tutorial for machine learning practitioners and researchers,’’ 2025, arXiv:2502.01146.
[20] P. Rebentrost, A. Steffens, I. Marvian, and S. Lloyd, ‘‘Quantum singularvalue decomposition of nonsparse low-rank matrices,’’ Phys. Rev. A, Gen. Phys., vol. 97, no. 1, Jan. 2018, Art. no. 012327.

[21] 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.
[22] S. A. Stein, B. Baheri, D. Chen, Y. Mao, Q. Guan, A. Li, S. Xu, and C. Ding, ‘‘QuClassi: A hybrid deep neural network architecture based on quantum state fidelity,’’ in Proc. Mach. Learn. Syst., 2022, pp. 251–264.
[23] 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.
[24] 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.
[25] M. Schuld and N. Killoran, ‘‘Quantum machine learning in feature Hilbert spaces,’’ Phys. Rev. Lett., vol. 122, no. 4, Feb. 2019, Art. no. 040504.
[26] A. Pérez-Salinas, A. Cervera-Lierta, E. Gil-Fuster, and J. I. Latorre, ‘‘Data re-uploading for a universal quantum classifier,’’ Quantum, vol. 4, p. 226, Feb. 2020.
[27] A. Pérez-Salinas, D. López-Núñez, A. García-Sáez, P. Forn-Díaz, and J. I. Latorre, ‘‘One qubit as a universal approximant,’’ 2021, arXiv:2102.04032. [28] S. Lloyd, M. Schuld, A. Ijaz, J. Izaac, and N. Killoran, ‘‘Quantum embeddings for machine learning,’’ 2020, arXiv:2001.03622.
[29] Z. Li, J. Peng, Y. Mei, S. Lin, Y. Wu, O. Padon, and Z. Jia, ‘‘Quarl: A learning-based quantum circuit optimizer,’’ in Proc. ACM Program. Lang., vol. 8, Apr. 2024, pp. 555–582.
[30] F. Phillipson, ‘‘Quantum machine learning: Benefits and practical examples,’’ in Proc. QANSWER, Jan. 2020, pp. 51–56.