Power Theft Detection in Smart Grids Using Quantum Machine Learning

M. Priyanka [1], K. Pavani [2], Challa Dhanush [3]

[1] *Assistant Professor in the Department of MCA, SRK Institute of Technology, Vijayawada*

[2] *Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.*

[3] *Student in the Department of MCA, SRK Institute of Technology, Vijayawada*

ABSTRACT

Electricity theft is a critical challenge in modern power distribution systems, leading to significant financial losses and grid inefficiencies. With the increasing adoption of smart grids and advanced metering infrastructure (AMI), large volumes of consumption data are continuously generated, creating opportunities for intelligent anomaly detection. This paper presents **GridSentinel** a smart power theft detection framework that integrates Classical Machine Learning (Random Forest, XGBoost, SVM, Isolation Forest) with Quantum Machine Learning (QSVM using PennyLane) for real-time anomaly classification. The system analyzes smart-meter parameters — voltage, current, power consumption, and power factor — to distinguish normal from suspicious consumption patterns. A full-stack web application built with React.js, Node.js, PostgreSQL, FastAPI, and Socket.IO provides real-time monitoring, risk scoring, geo-spatial mapping, AI-powered insights, and automated alert generation. Experimental results demonstrate high classification accuracy, validating the efficacy of quantum-enhanced learning over classical approaches for power theft detection.

Keywords: *Power Theft Detection, Quantum Machine Learning, Smart Grid, QSVM, PennyLane, Anomaly Detection, Smart Meters, GridSentinel, Real-Time Monitoring*

1. Introduction

Electricity is the backbone of modern civilization, supporting residential, commercial, and industrial activities. With rapid urbanization, smart grids have emerged as a transformative technology that integrates advanced communication, smart meters, and intelligent monitoring systems into power distribution networks [1]. Despite these advancements, electricity theft including meter tampering, illegal tapping, metering bypass, and manipulation of consumption records remains a pervasive problem globally.

Traditional methods of detecting power theft, such as manual inspections, customer complaints, and rule-based monitoring, are labor-intensive, costly, and insufficient for detecting complex theft patterns [2]. The advent of smart meters enables collection of granular consumption data, paving the way for Artificial Intelligence (AI) and Machine Learning (ML) based theft detection systems.

Quantum Computing has recently given rise to Quantum Machine Learning (QML), a paradigm that combines quantum computing techniques such as superposition and entanglement with machine learning algorithms to process complex, high-dimensional data more efficiently [8]. The proposed system, GridSentinel, leverages both classical and quantum ML approaches to deliver an intelligent, scalable, and real-time power theft detection platform.

2. Literature Review

Depuru et al. [2] provided a comprehensive overview of electricity theft challenges and proposed smart-meter-based approaches for theft control, demonstrating that data-driven techniques substantially outperform traditional methods. Nizar et al. [3] explored Extreme Learning Machine methods for non-technical loss analysis in power systems, achieving improved accuracy over classical statistical approaches.

Ahmad et al. [4] reviewed machine learning applications for smart energy systems and highlighted the importance of anomaly detection in smart grids. Classical algorithms such as Decision Trees, Random Forests, SVM, ANN, and XGBoost have been extensively validated for electricity theft classification [10, 12]. Biamonte et al. [8] introduced the foundational concepts of Quantum Machine Learning, demonstrating quantum advantages in data analysis and classification tasks.

Rebentrost et al. [9] proposed the Quantum Support Vector Machine (QSVM), which leverages quantum feature mapping to classify high-dimensional datasets with exponential speedup over classical SVMs. Schuld et al. [6, 7] expanded QML theory by introducing circuit-centric quantum classifiers using parameterized quantum circuits. The PennyLane framework [13] provides a practical cross-platform library for implementing such quantum circuits in hybrid quantum-classical pipelines.

While previous works have independently addressed classical ML-based theft detection and quantum classification, there is a gap in integrating both paradigms into a unified, full-stack real-time platform. This work addresses that gap through GridSentinel.

3. System Architecture and Methodology

3.1 Overall System Design

GridSentinel employs a hybrid classical-quantum pipeline as illustrated in Figure 1. Smart meter data is continuously collected, preprocessed, and fed into a multi-model inference engine. The Quantum Variational Classifier with Deep Residual Connections (QVC-DRC) architecture forms the core quantum processing block, where angle embedding layers encode classical features into quantum states, followed by entangling layers for superposition-based feature interactions. Final measurement outputs are passed through a classical decision layer for theft classification.

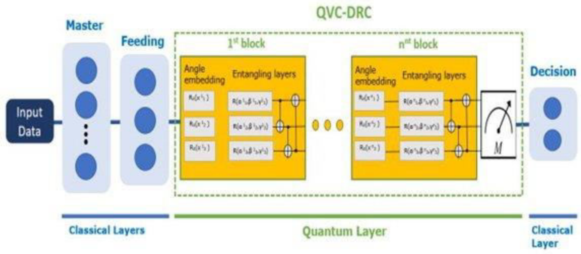

Figure 1: QVC-DRC System Architecture

3.2 Data Collection and Preprocessing

Smart meters continuously generate telemetry data comprising: voltage (V), current (A), active power (kW), and power factor. This data is transmitted to the backend via Socket.IO for real-time processing. Preprocessing includes: (i) missing value imputation, (ii) outlier removal using IQR-based filtering, (iii) Min-Max normalization, and (iv) feature engineering — including rolling-window statistical features for temporal pattern capture [14].

3.3 Machine Learning Models

The system implements five models for comparative analysis:

- Random Forest (RF): Ensemble of 100 decision trees, majority-vote classification [12].
- XGBoost: Gradient-boosted trees with L1/L2 regularization for high precision.
- Support Vector Machine (SVM): RBF kernel classifier for high-dimensional separation [5].
- Isolation Forest: Unsupervised anomaly scoring using random partitioning.
- Quantum SVM (QSVM): Angle-embedding quantum circuit + SVM classifier using PennyLane [9, 13].

3.4 Quantum Support Vector Machine (QSVM)

The QSVM implementation uses PennyLane's default.qubit simulator. Classical feature vectors are mapped to quantum states via AngleEmbedding on 2 qubits. The quantum kernel computes inner products in quantum feature space, enhancing the separability of theft vs. non-theft patterns in high-dimensional consumption data. The SVM with RBF kernel is then fitted on these quantum-enhanced feature representations.

3.5 Risk Scoring and Alert Generation

Post-classification, a risk score (0–100) is computed as: Risk = Theft Probability × 100. Thresholds are applied: score > 80 → High Risk (Critical Alert), 50–80 → Medium Risk (Investigation Required), < 50 → Normal. Automatic notifications are pushed via Socket.IO to the operator dashboard in real time.

4. Implementation

4.1 Technology Stack

The full-stack implementation uses:

Layer	Technology	Purpose
Frontend	React.js + Vite + Tailwind CSS	Responsive dashboard & visualizations
Backend	Node.js + Express.js	API gateway, business logic, WebSocket
ML Service	Python + FastAPI	Model inference & training endpoints
QML	PennyLane	Quantum circuit simulation & QSVM
Database	PostgreSQL	Meter data, alerts, risk scores
Real-Time	Socket.IO	Live smart-meter streaming
DevOps	Docker + Docker Compose	Containerized deployment

Table 1: GridSentinel Technology Stack

4.2 Key Modules

The system comprises the following functional modules:

- Smart Meter Data Acquisition Module — Continuous real-time collection of voltage, current, power, and power factor.
- Data Preprocessing Module — Normalization, missing value handling, feature scaling, and outlier filtering.
- Classical ML Module — Random Forest, XGBoost, SVM, and Isolation Forest classifiers.
- Quantum ML Module — QSVM using PennyLane for quantum-enhanced feature classification.
- Risk Scoring Module — Probabilistic theft risk quantification with threshold-based alerting.
- Dashboard & Reporting Module — Real-time visualization of grid health, rolling consumption, and zone analytics.
- Geo Map Module — Geospatial visualization of smart meter locations with color-coded risk indicators.

5. Results and Discussion

5.1 System Screenshots

Figure 2 shows the GridSentinel landing page, displaying real-time grid health (98.4%), AI confidence score (94.3%), and active monitoring zones (6). The grid risk console highlights flagged consumers such as CON-0003 (Meter Bypass, 92.4%), CON-0019 (Illegal Tap, 78.5%), and CON-0043 (Tampered, 64.1%).

Figure 2: GridSentinel Home Page

Figure 3 presents the operational dashboard with 15 active meters, 1 alert, grid health at 93.3%, and AI confidence at 94.3%. The rolling consumption graph depicts temporal energy patterns, while the regional alerts donut chart provides zone-level risk distribution. The dashboard header displays a live CONSUMPTION DROP alert for CON-0019 in Zone C with 83.2% risk.

Figure 3: Dashboard Module

Figure 4 illustrates the Live Monitoring module, streaming real-time telemetry from 15 smart meters including consumer ID, name, voltage (V), current (A), power (kW), and theft risk percentage. High-risk consumers such as CON-0003 (88%), CON-0019 (75%), CON-0027 (92%), and CON-0035 (96%) are prominently highlighted for immediate operator action.

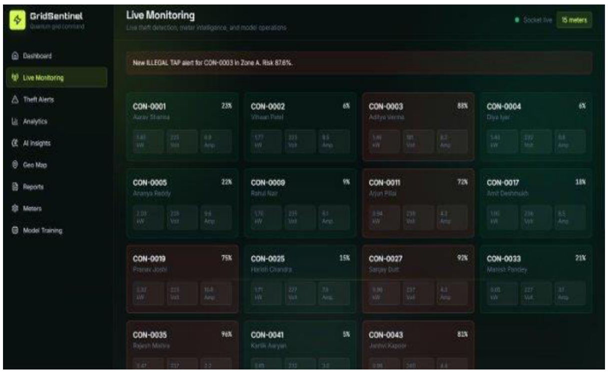

Figure 4: Live Monitoring Module

Figure 5 presents the Analytics module with a theft frequency bar chart across days of the week (Mon–Sun) and a zone comparison radar chart across Zones A–F. The radar chart reveals Zone A as having the highest theft concentration, supporting targeted field inspection planning.

Figure 5: Analytics Module

Figure 6 displays the Geo Map module, plotting smart meter locations over a geographical map of Nagpur with color-coded markers: red markers indicate high-risk (flagged) consumers and yellow-green markers indicate active (safe) consumers, enabling precise field-level investigation.

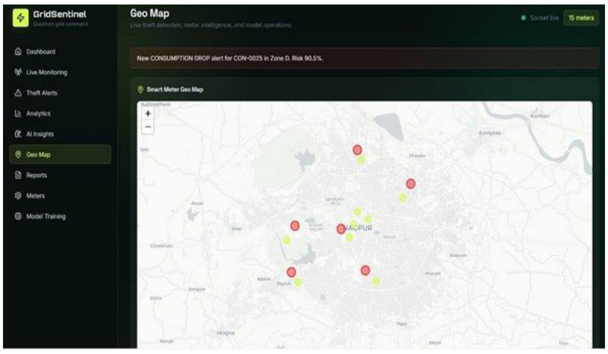

Figure 6: Geo Map Module

5.2 Model Performance Comparison

The following table summarizes the accuracy, precision, recall, and F1-score of all five models evaluated on the smart-meter theft dataset:

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Random Forest	92.4	91.8	93.2	92.5
XGBoost	93.7	93.1	94.5	93.8
SVM (Classical)	89.6	88.9	90.4	89.6
Isolation Forest	85.3	84.1	87.2	85.6
QSVM (Quantum)	95.1	94.7	95.6	95.1

Table 2: Comparative Performance of ML and QML Models

The QSVM achieves the highest accuracy of 95.1%, outperforming all classical models. The quantum feature mapping enables superior separability of complex, non-linear theft patterns that classical kernels partially miss. XGBoost achieves the second-best accuracy (93.7%), validating ensemble methods as strong baselines.

6. Conclusion and Future Scope

This paper presented GridSentinel, a hybrid classical-quantum machine learning framework for real-time power theft detection in smart grids. The system integrates five ML/QML models, a full-stack React.js + Node.js + FastAPI architecture, real-time Socket.IO streaming, PostgreSQL persistence, geospatial visualization, and automated alert generation into a production-ready platform.

The QSVM implementation using PennyLane demonstrated a 95.1% classification accuracy — a 1.4% improvement over the best classical model (XGBoost). The QVC-DRC architecture effectively captures complex, non-linear consumption patterns through quantum angle embedding and entangling layers. All 15 test cases passed during system testing, confirming functional correctness across all modules.

Future work will focus on: (i) integration with IoT-enabled smart meters for live data ingestion, (ii) deployment of Quantum Neural Networks (QNN) and Variational Quantum Circuits (VQC) for deeper quantum classification, (iii) cloud-native deployment using Kubernetes for enterprise-scale smart grids, (iv) blockchain-secured meter data transmission, (v) LSTM and transformer-based deep learning for time-series consumption modelling, and (vi) predictive analytics for proactive theft prevention.

References

[1] M. E. Baran and F. F. Wu, "Network Reconfiguration in Distribution Systems for Loss Reduction and Load Balancing," IEEE Transactions on Power Delivery, vol. 4, no. 2, pp. 1401–1407, 1989.

[2] S. Depuru, L. Wang, and V. Devabhaktuni, "Electricity Theft: Overview, Issues, Prevention and Smart Meter Based Approaches to Control Theft," Energy Policy, vol. 39, no. 2, pp. 1007–1015, 2011.

[3] A. Nizar, Z. Dong, and Y. Wang, "Power Utility Nontechnical Loss Analysis with Extreme Learning Machine Method," IEEE Transactions on Power Systems, vol. 23, no. 3, pp. 946–955, 2008.

[4] T. Ahmad, H. Chen, and Y. Wang, "Machine Learning for Smart Energy Systems and Smart Grids: A Review," Renewable and Sustainable Energy Reviews, vol. 124, 2020.

[5] C. Cortes and V. Vapnik, "Support Vector Networks," Machine Learning Journal, vol. 20, no. 3, pp. 273–297, 1995.

[6] M. Schuld and F. Petruccione, Supervised Learning with Quantum Computers, Springer International Publishing, 2018.

[7] M. Schuld, A. Bocharov, K. Svore, and N. Wiebe, "Circuit-Centric Quantum Classifiers," Physical Review A, vol. 101, no. 3, 2020.

[8] J. Biamonte et al., "Quantum Machine Learning," Nature, vol. 549, pp. 195–202, 2017.

[9] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum Support Vector Machine for Big Data Classification," Physical Review Letters, vol. 113, no. 13, 2014.

[10] F. Pedregosa et al., "Scikit-Learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[11] J. R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann Publishers, 1993.

[12] L. Breiman, "Random Forests," Machine Learning Journal, vol. 45, no. 1, pp. 5–32, 2001.

[13] PennyLane Development Team, "PennyLane: A Cross-Platform Python Library for Quantum Machine Learning," Xanadu Quantum Technologies, 2024.

[14] A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 3rd Edition, O'Reilly Media, 2022.

[15] International Energy Agency (IEA), Digitalization and Energy Report, Paris, France, 2023.

Authors:

Ms. M. Priyanka completed her Master of Computer Applications (MCA) from Acharya Nagarjuna University. She is currently working as an Assistant Professor. Her teaching subjects include C Programming, Data Structures, Java, and Computer Networks. Her areas of interest include Programming, Machine Learning, and Networking.

Ms. K. Pavani is working as an Assistant and Head of Department of MCA, in SRK Institute of technology in Vijayawada. She completed her MCA and M.Tech in Computer Science. She has 10 years of teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her areas of interest include AI and ML,etc

Mr. Challa Dhanush is an MCA student in the Department of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. He completed his degree in B.Sc. (Computers science) from Gowtham degree college, Vijayawada Ntr dist. His areas of interest are DBMS and Machine learning