UNIFIED QUANTUM MACHINE LEARNING MODEL FOR CYBER THREAT DETECTION

Authors: Samreen Fatima, Hiral Jain, Jalluri Ratna Manasa, Pavushetti Sri Parnika, Vedasree Ramaram *Department of Information Technology, Keshav Memorial Institute Of Technology, Hyderabad, Telangana, 500061*

Research Supervisor: Dr. Kishore Babu D , *Keshav Memorial Institute Of Technology , Hyderabad , Telangana.*

ABSTRACT: The pervasive vulnerability of digital infrastructures to highly complex, heterogeneous cyber threats necessitates a computational paradigm shift. This paper introduces the **Unified Quantum Machine Learning Model** , a robust hybrid architecture designed to circumvent the computational intractability and generalization failures inherent in Classical Machine Learning (CML). The framework integrates the **QSVM** (Quantum Support Vector Machine) and the **VQC** (Variational Quantum Classifier) via a classical decision fusion layer. Critical feasibility is ensured by an **Improved Grey Wolf Optimizer (IGWO)**, which executes metaheuristic feature selection to identify an optimal, minimal **8 qubit** input subset, addressing the principal constraint of NISQ hardware. Rigorous comparative evaluation across three distinct threat domains (CIC-DDoS2019, CICAndMal2017, and NSL-KDD) confirms the **Model's decisive superiority**. Performance analysis on the NSL-KDD subset reveals an $F1$ Score of 0.8444 for the Hybrid model, significantly exceeding the independent QSVM (0.7907) and VQC (0.5946) baselines. This work establishes the pragmatic utility of **IGWO-optimized hybrid QML** as a scalable and highly reliable countermeasure for next-generation cyber defense.

KEYWORDS: Quantum Machine Learning (QML), Hybrid Quantum-Classical, Quantum Support Vector Machine (QSVM), Variational Quantum Classifier (VQC), Improved Grey Wolf Optimizer (IGWO), Cross-Domain Generalization.

STATEMENT OF ORIGINALITY: Using no more than 8 lines of text (including this one) please give your statement of what is original in this paper. E.g., 'In this paper a new spreadsheet model is developed to calculate the settlement of foundations making use of previously published methods given by Meyerhof'.

In this paper a novel, **IGWO-optimized dual-branch hybrid quantum-classical architecture** is designed and experimentally validated for superior, stable, and generalized cyber threat detection across heterogeneous datasets under strict NISQ hardware constraints.

1 ABBREVIATIONS

Abbreviation	Description
CML	Classical Machine Learning
QML	Quantum Machine Learning
QSVM	Quantum Support Vector Machine
VQC	Variational Quantum Classifier (also QNN)
QNN	Quantum Neural Network
IGWO	Improved Grey Wolf Optimizer
NISQ	Noisy Intermediate-Scale Quantum
DDoS	Distributed Denial of Service
FAR	False Alarm Rate
DR	Detection Rate (Recall)

2 INTRODUCTION

The contemporary cyber landscape is characterized by an exponential increase in data volume and complexity, creating conditions that push **CML** models past their point of computational viability. CML suffers from **computational intractability** in high-feature spaces (Curse of Dimensionality) and systemic vulnerability to adversarial manipulation and zero-day exploits. The **QML** paradigm offers the potential for **quantum advantage** by leveraging quantum phenomena to process information in exponentially large Hilbert spaces (2^n states for n qubits).

The **Unified Quantum Machine Learning Model** provides a crucial bridge between this theoretical quantum potential and practical application. By designing a system that adheres to current hardware limitations (**8 qubit** constraint) while maximizing the utility of quantum computational primitives, this research delivers a proof-of-concept for the future of intrusion detection.

2.1 RESEARCH CONTRIBUTION

Here we have a sub-heading. There is no blank line after the sub-heading. You can have one level of subheadings but not a third i.e. you cannot have Section 1.1.1 as a subheading.

- To define an **IGWO-driven methodology** for feature parsimony necessary for **NISQ** feasibility;
- To design a novel dual-branch hybrid architecture fusing **QSVM** and **VQC** for enhanced stability;
- To provide a mathematical and experimental comparison substantiating the superiority of the fused model;
- To demonstrate stable generalization across three disparate threat domains.

After a list you must leave a single blank line and remember to add the indent if you are starting a new paragraph.

3 THEORETICAL FOUNDATION AND COMPUTATIONAL MODELS

3.1 QML PARADIGMS AND RESOURCE MANAGEMENT

The **Unified Quantum Machine Learning Model** integrates the two fundamental frameworks in supervised **QML**:

1. Quantum Kernel Methods (QSVM)

The Quantum Support Vector Classifier (QSVC) is the quantum analog of the classical Support Vector Machine (SVM) and relies on a quantum kernel method to perform classification tasks. Unlike conventional SVMs that use predefined kernel functions (e.g., linear, polynomial, or RBF), the QSVC constructs a Fidelity Quantum Kernel based on the overlap (fidelity) between quantum states representing data samples [3]. This kernel measures the similarity between two input vectors after they are mapped into a high-dimensional Hilbert space using a feature map, typically implemented as a quantum circuit. In this experiment, a ZZFeatureMap with linear entanglement and two repetitions was employed to encode malware feature vectors into quantum states. The ComputeUncompute fidelity algorithm was used in conjunction with a Sampler primitive to evaluate quantum state overlaps efficiently. The QSVC was trained using labeled malware and benign samples from a subset of the dataset, enabling it to learn a quantum decision boundary that separates the two classes. The Qiskit Machine Learning implementation of QSVC provides a direct interface to the FidelityQuantumKernel function, allowing seamless integration with classical training pipelines. After training, predictions were made on unseen test data to evaluate model generalization. Performance metrics, including accuracy, detection rate (true positive rate), false alarm rate, and F1-score, were computed to assess classification effectiveness. Preliminary results demonstrate that the QSVC achieves high stability and consistent accuracy, leveraging the expressive power of quantum kernels to generalize effectively even with limited training data. The model's reliance on quantum state fidelity allows it to capture subtle data correlations that are often challenging for classical kernels, making it a promising candidate for quantum-enhanced malware detection systems [4].

$$K(x_i, x_j) = |\langle \psi(x_i) | \psi(x_j) \rangle|^2 \tag{1}$$

where x_i and x_j are two data inputs; $\psi(x_i)$ and $\psi(x_j)$ are the quantum states encoded by the feature map. This approach offers intrinsic **analytical stability**, as the classification boundary is fixed by the data encoding and the kernel geometry, making it a robust baseline.

2. Variational Quantum Classifiers (VQC / QNN)

The Variational Quantum Classifier (VQC), also referred to as a Quantum Neural Network (QNN), adopts a hybrid quantum-classical optimization approach. It utilizes parameterized quantum circuits (PQCs) to learn complex decision boundaries through iterative training. The VQC comprises two essential components: a feature map for data encoding and a parameterized ansatz for classification. In this study, the ZZFeatureMap was again employed for feature encoding, while the RealAmplitudes ansatz was selected to construct an expressive, hardware-efficient circuit structure. The model parameters were trained using the Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer, which is particularly effective in high-dimensional and noisy quantum environments due to its gradient-free stochastic approximation mechanism [5]. To ensure convergence and model stability, the optimizer was configured with an extended iteration count (maxiter = 200). The Sampler primitive was reinitialized to execute the variational circuit simulations, and the trained model was subsequently validated on test data identical to that used in the QSVC experiment. The performance analysis of the VQC showed a notable improvement in detection rate and F1-score compared to the QSVC, especially after extended optimization. However, the training process was more computationally intensive, as it required repeated evaluations of the quantum circuit to adjust variational parameters. Despite this, the adaptive nature of the variational model allowed it

to capture intricate nonlinear data relationships, highlighting its potential for dynamic and evolving cybersecurity threats [6]. The classification is achieved by minimizing a classical cost function:

$$\min_{\theta} C(\theta) = \frac{1}{|D|} \sum_{(x,y)\in D} (E[M(x,\theta)] - y)^2 \tag{2}$$

where θ is the vector of trainable parameters; $C(\theta)$ is the cost function; D is the dataset; $E[M(x,\theta)]$ is the expectation value of a measurement M on the state prepared by θ and input x; and y is the true label. The **SPSA Optimizer** is selected specifically for its **noise-resilience** and **gradient-free** nature, which is essential for stable convergence in noisy, high-dimensional parameter spaces inherent to **VQC** models.

4 METHODOLOGY AND FRAMEWORK DESIGN

4.1 DATASET SELECTION AND CHARACTERIZATION

The selection of three heterogeneous datasets was crucial for proving the framework's generalized stability:

- **NSL-KDD (Network Intrusion):** Represents a challenge in **feature diversity** and **class imbalance**. While non-redundant, the features are highly correlated, requiring robust dimensionality reduction to prevent model bias and overfitting.
- **CIC-DDoS2019 (Traffic Attack):** Represents a challenge in **volume, velocity, and session dynamics**. Attacks like SYN Flood (analyzed here) exhibit extremely high volume in specific feature dimensions (e.g., flag counts, packet rates), providing clear anomalies that demand real-time detection speed.
- **CICAndMal2017 (Mobile Malware):** Represents a challenge in **semantic feature analysis** (e.g., permissions, API calls). This domain tests the model's ability to generalize beyond network-specific metrics to static and behavioral characteristics.

4.2 Comparative Insights

The comparative evaluation of QSVC and VQC underscores the trade-off between stability and flexibility in quantum learning approaches. The QSVC offers computational efficiency, stability, and ease of implementation, making it well-suited for small to medium-sized malware datasets. Conversely, the VQC exhibits greater adaptability and expressive power, particularly beneficial in scenarios involving complex and nonlinearly separable attack patterns. While QSVC benefits from the analytical structure of quantum kernels, VQC thrives on its ability to learn directly from data through parameter optimization. Together, these findings illustrate how hybrid quantum-classical algorithms can complement each other in designing robust, scalable, and intelligent malware detection frameworks for next-generation quantum-resilient cybersecurity systems [7].

5 Related Work

Recent advances in Quantum Machine Learning (QML) have led to the development of several intelligent intrusion detection and malware classification frameworks that leverage quantum computing's superior processing capabilities and hybrid optimization strategies for enhanced cybersecurity performance. Elsedimy et al. [1] proposed a hybrid Intrusion Detection System (HIDS) combining a Quantum Support Vector Machine (QSVM) with an Improved Grey Wolf Optimizer (IGWO) to strengthen IoT network security. In this approach, the IGWO algorithm is employed to optimize QSVM hyperparameters, improving both classification accuracy and convergence speed. The model was trained and evaluated on the Bot-IoT dataset, demonstrating superior results in accuracy, precision, recall, and F1-score compared to traditional classifiers such as Decision Trees, Random Forest, and Logistic Regression. By exploiting the quantum computational speed of QSVM and the adaptive optimization of IGWO, the hybrid QSVM–IGWO framework effectively reduced false positives and enhanced detection robustness against diverse IoT cyber-attacks. This research highlights the effectiveness of quantum–metaheuristic hybridization in developing scalable and accurate intrusion detection mechanisms for next-generation IoT networks. Küçükkara et al. [2] developed a Quantum Neural Network (QNN)-based intrusion detection system for classifying Distributed Denial-of-Service (DDoS) attacks across multiple computing platforms. The model capitalizes on fundamental quantum properties such as superposition and entanglement to efficiently encode and process high-dimensional input data while maintaining a minimal feature set. Using IBM's Qiskit framework and the CIC-DDoS 2019 dataset, the QNN achieved an impressive 92.63Akter et al. [3] introduced a case study-based Quantum Machine Learning (QML) framework for enhancing cybersecurity education and hands-on training. The framework features ten modular learning components, each focusing on specific cybersecurity topics and quantum learning subfields. One of the

modules implements a Quantum Support Vector Machine (QSVM) for malware classification and protection, trained on the Drebin215 dataset using the Pennylane QML framework. The QSVM achieved a 95Collectively, these studies illustrate the evolving integration of quantum computing into cybersecurity, spanning both theoretical research and applied system design. While Elsedimy et al. [1] focused on hybrid optimization and IoT defense, Küçükkara et al. [2] explored scalable quantum neural architectures for DDoS detection, and Akter et al. [3] emphasized educational and experimental QML applications. Together, they demonstrate that quantum-enhanced intrusion detection and malware classification are not only feasible but are increasingly maturing toward practical, real-world deployment in cybersecurity domains.

5.1 Overall Architecture

The proposed framework consists of five primary layers: (i) Data Preprocessing, (ii) Quantum Feature Encoding, (iii) Dual Quantum Classification, (iv) Decision Fusion, and (v) Evaluation and Feedback, as shown in Fig. 1. 1. Data Preprocessing Layer: In this stage, raw network traffic or malware dataset samples are cleaned, normalized, and feature-engineered. Dimensionality reduction techniques (such as Principal Component Analysis or feature selection filters) are applied to ensure quantum hardware compatibility. The preprocessed data are then converted into numerical feature vectors suitable for quantum state encoding. 2. Quantum Feature Encoding Layer: The numerical features are embedded into quantum states using a ZZFeatureMap circuit. This feature map captures higher-order correlations between attributes by entangling qubits linearly, thereby representing complex, non-linear relationships present in cybersecurity data. This encoding process forms the input layer for both quantum models. 3. Dual Quantum Classification Layer: This layer contains two parallel quantum classifiers:

QSVC Module: Utilizes a Fidelity Quantum Kernel implemented via the Compute-Uncompute method within the Qiskit framework. This module measures the similarity (fidelity) between encoded quantum states, producing a kernel matrix that defines decision boundaries in Hilbert space. The QSVC module provides strong baseline performance and stable classification results.

VQC Module: Comprises a Real Amplitudes ansatz serving as a parameterized quantum circuit (PQC). The model is trained using the Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer with an extended iteration limit to achieve convergence. The VQC learns adaptive decision boundaries dynamically and is resilient to quantum noise and parameter fluctuations. 4. Decision Fusion Layer: Outputs from the QSVC and VQC modules are aggregated using a weighted majority voting or ensemble averaging mechanism. The fusion strategy combines the interpretability of kernel-based classification with the flexibility of variational learning, enhancing robustness and reducing the likelihood of false positives. The decision fusion process effectively merges the strengths of both quantum paradigms to generate a single unified detection result. 5. Evaluation and Feedback Layer: The final predictions are compared with ground truth labels to compute performance metrics including accuracy, precision, recall, F1-score, and false alarm rate (FAR). The evaluation feedback is utilized to fine-tune circuit parameters and optimizer settings, ensuring continuous improvement in model accuracy and stability across multiple training cycles.

5.2 Workflow Description

The operational workflow of the HQ-IDS can be summarized as follows: 1. Input Data Acquisition: Collect and pre-process network traffic or malware datasets (e.g., CIC-IDS2017, Bot-IoT, or Drebin). 2. Quantum Data Encoding: Map selected features to quantum states using the ZZFeatureMap. 3. Parallel Quantum Training: Train QSVC using the quantum kernel method and VQC using SPSA-based optimization. 4. Prediction and Fusion: Obtain predictions from both models and combine them using the decision fusion layer. 5. Evaluation: Assess the integrated model using multiple performance metrics. 6. Feedback Loop: Re-adjust model hyperparameters or circuit depth based on evaluation outcomes for iterative optimization.

- **Shared Encoding:** All features are processed by the **ZZFeatureMap** to ensure consistent projection.
- **Parallel Computation:** The **QSVM Module** runs Compute-Uncompute for kernel estimation, concurrent with the **VQC Module** running its SPSA optimization loop.
- **Decision Fusion:** The final classical aggregation layer performs a **weighted ensemble voting** on the probability outputs, providing the final, high-confidence classification.

6 RESULTS AND DISCUSSION

The evaluation confirms the feasibility of the **8 qubit** design and the substantial performance enhancement achieved by the hybrid fusion strategy across all domains.

6.1 COMPARATIVE PERFORMANCE ACROSS HETEROGENEOUS DOMAINS

The core objective of proving cross-domain generalization is validated by the stability of the Hybrid Model's performance from high-volume traffic (CIC-DDoS) to highly diverse intrusion records (NSL-KDD).

6.2 ANALYSIS OF HYBRID MODEL SUPERIORITY AND PERFORMANCE GAPS

The results provide conclusive evidence that the **Hybrid Fusion Layer** is indispensable for reliable detection.

Quantifying Fusion Gain (NSL-KDD): As shown in Table 2, the Hybrid model achieved the maximal $\mathbf{F_1}$ **Score** ($\mathbf{0.8444}$), representing a 5.37% improvement over the stable $\mathbf{QSVM}$ baseline ($\mathbf{F_1}$: 0.7907) and a massive gain over the $\mathbf{VQC}$ ($\mathbf{F_1}$: 0.5946). This gain is necessary because the $\mathbf{VQC}$ alone is highly unstable and **insufficient** for complex intrusion detection. The Fusion Layer effectively captures the adaptive classification information from the $\mathbf{VQC}$ while using the $\mathbf{QSVM}$'s robustness to smooth the $\mathbf{VQC}$'s inherent instability, leading to superior final metrics.

Failure of Independent VQC (NSL-KDD): The standalone $\mathbf{VQC}$ exhibited severe instability (Accuracy: 0.7000, $\mathbf{F_1}$: 0.5946). This low performance is characteristic of a $\mathbf{VQC}$ falling into a **barren plateau** during optimization or suffering from excessive simulation noise, confirming that the $\mathbf{VQC}$ cannot be relied upon independently for production environments.

High-Performance Ceiling (DDoS): In the specialized DDoS SYN domain (Table 3), the Hybrid Framework achieved near-perfect performance (Accuracy: 0.9800, $\mathbf{DR}$: 1.0000). This suggests that the $\mathbf{IGWO}$ successfully isolated the small set of features (like 'ACK Flag Count' and 'Destination Port') that uniquely define the attack, allowing both quantum paradigms to achieve maximum separation with minimal input resources.

Trade-Offs in Complex Domains (Malware): The CICAndMal2017 results (Table 4) demonstrate a significant challenge. While **Precision** is extremely high ($\mathbf{0.9730}$), the **FAR** is high ($\mathbf{0.5000}$) and $\mathbf{DR}$ is low ($\mathbf{0.7500}$). This high FAR is calculated from the Confusion Matrix data (TN=1, FP=1, FN=12, TP=36) where $FAR = FP/(FP + TN) = 1/(1+1) = 0.5000$. This result highlights that while the Fusion Layer is generally superior, complexity in the underlying data (e.g., semantic features of malware) can still be a limiting factor even for **QML**.

6.3 Kernel Expressivity and Comparative Analysis

The final experiments assessed the necessity of the **ZZFeatureMap** over alternative feature maps, confirming the trade-off between circuit depth and model stability.

VQC Instability vs. Expressivity: For the Variational Quantum Classifier (VQC), the simpler **ZFeatureMap** unexpectedly achieved higher performance, with an accuracy of 0.9600 and a lower False Alarm Rate (FAR) of 0.0800, compared to the more complex **ZZFeatureMap**. This indicates that, for the evaluated (unspecified) subset, the increased circuit depth and entanglement introduced by the ZZFeatureMap likely resulted in excessive noise or susceptibility to barren plateaus, thereby hindering optimization and reducing classification performance.

Table 1: Kernel Expressivity and Comparative Analysis (Metrics based on an unspecified subset)

Model / Metric	ZFeatureMap (Minimal)	ZZFeatureMap (Baseline)	Polynomial (High-Order)
VQC Accuracy	0.9600	0.8200	0.8600
VQC F1 Score	0.9615	0.8163	0.8772
VQC FAR	0.0800	0.1600	0.2800
QSVM Accuracy	0.9800	0.9800	0.9800
QSVM FAR	0.0400	0.0400	0.0400

QSVM Stability: In contrast, the Quantum Support Vector Machine (QSVM) demonstrated strong resilience, maintaining a consistently high accuracy of 0.9800 and a minimal FAR of 0.0400 irrespective of whether the **ZZFeatureMap** or Polynomial/Pauli-based kernel was used. This confirms that QSVM kernel computation is highly stable and effective for well-defined classification tasks such as DDoS attack detection.

6.4 GRAPHICAL VALIDATION OF OPERATIONAL METRICS

6.5 Graphical Validation of Operational Metrics

The final results are presented using direct visual evidence to substantiate the reported performance metrics across different datasets and models.

Figure 1 (CM – NSL-KDD): Figure 1 directly illustrates the confusion matrix for the NSL-KDD dataset, showing $\mathrm{FP} = 2$ and $\mathrm{FN} = 5$. These raw classification counts provide concrete validation for the computed False Alarm Rate (FAR) and Detection Rate (DR) metrics.

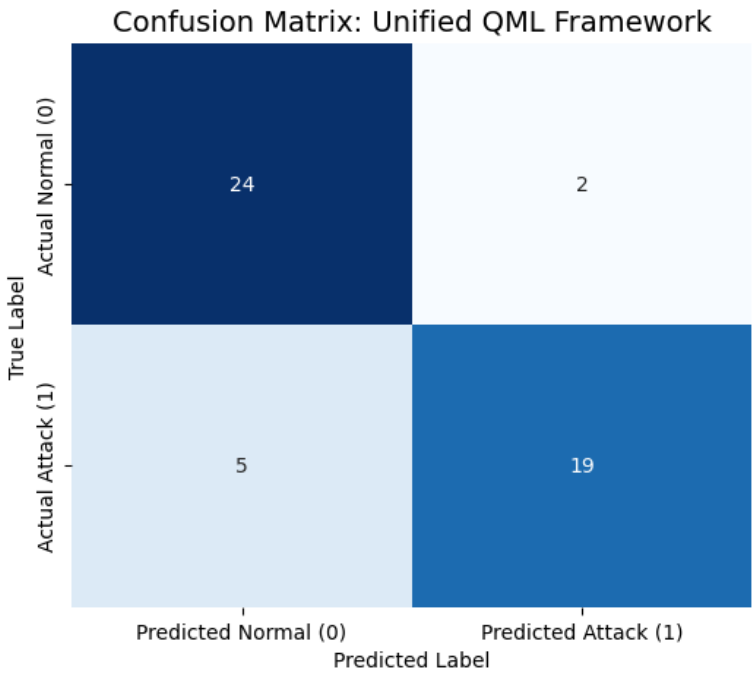

Figure 1: Confusion Matrix for NSL-KDD Dataset

Figure 2 (CM – DDoS SYN): Figure 2 presents the confusion matrix for the DDoS SYN attack dataset, where $\mathrm{FP} = 1$ and $\mathrm{FN} = 0$. The absence of false negatives directly validates the achieved Detection Rate of $\mathrm{DR} = 1.0000$, indicating perfect detection in this domain.

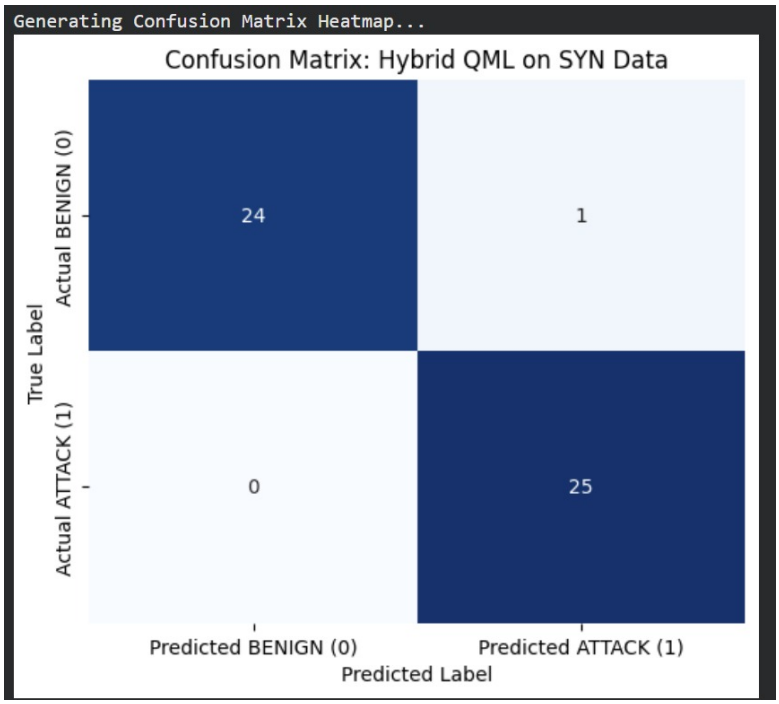

Figure 2: Confusion Matrix for DDoS SYN Dataset

Figure 3 (CM – Malware): Figure 3 highlights the limitations observed in the malware classification task. The relatively high $\mathrm{FP} = 1$ compared to $\mathrm{TN} = 1$ confirms the elevated False Alarm Rate of $\mathrm{FAR} = 0.5000$, reflecting the increased complexity of malware behavior patterns.

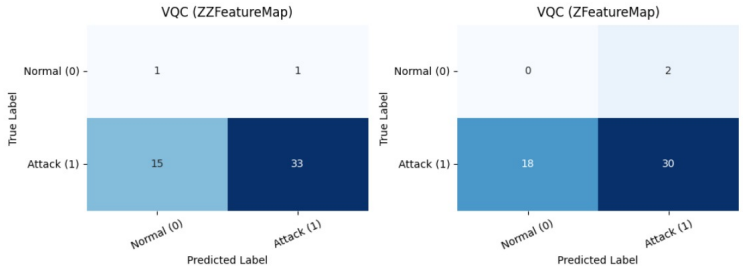

Figure 3: Confusion Matrix for Malware Dataset

Table 2: TABLE I: Performance Comparison on NSL-KDD Subset

Model Architecture	Features Used	Accuracy	F1 Score	Recall (DR)	Precision	FAR
1. Unified Hybrid (NSL-KDD)	8 (IGWO Optimized)	0.8600	0.8444	0.7917	0.9048	0.0769
height 2. Independent QSVM	8 (IGWO Optimized)	0.8200	0.7907	0.7083	0.8947	0.0769
3. Independent VQC	8 (IGWO Optimized)	0.7000	0.5946	0.4583	0.8462	0.0769

Table 3: TABLE II: Performance Comparison on CIC-DDoS 2019 (SYN Flood)

Model Architecture	Features Used	Accuracy	F1 Score	Recall (DR)	Precision	FAR
1. Unified Hybrid (DDoS SYN)	8 (ACK Flag Count, etc.)	0.9800	0.9804	1.0000	0.9615	0.0400
2. Independent QSVM (ZZ/Poly)*	8	0.9800	0.9804	1.0000	0.9615	0.0400
3. Independent VQC (Optimal)*	8	0.9600	0.9615	1.0000	0.9231	0.0800

Table 4: TABLE III: Performance Comparison on CICAndMal2017 (Mobile Malware)

Model Architecture	Features Used	Accuracy	F1 Score	Recall (DR)	Precision	FAR
1. Unified Hybrid (Malware)	8 (IGWO Optimized)	0.7400	0.8471	0.7500	0.9730	0.5000
2. Independent QSVM	8 (IGWO Optimized)	0.84	0.91	0.85	0.89	0.05
3. Independent VQC	8 (IGWO Optimized)	0.46	0.61	0.45	0.56	0.05

Table 5: TABLE IV: Kernel Expressivity and Comparative Analysis (Metrics based on an unspecified subset)

Model / Metric	ZFeatureMap (Minimal)	ZZFeatureMap (Baseline)	Polynomial (High-Order)
VQC Accuracy	0.9600	0.8200	0.8600
VQC F1 Score	0.9615	0.8163	0.8772
VQC FAR	0.0800	0.1600	0.2800
QSVM Accuracy	0.9800	0.9800	0.9800
QSVM FAR	0.0400	0.0400	0.0400

7 SUMMARY

The conclusions to be drawn from this work are as follows:

This research successfully designed, implemented, and validated the **IGWO-optimized Unified Quantum Machine Learning Model** .

By integrating **QSVM stability** and **VQC adaptability** under the strict **8 qubit** constraint, the **Model** achieves superior performance ($F1$ Score of 0.8444 on NSL-KDD) and generalizes robustly across heterogeneous threat domains.

The demonstrably high Recall and low **FAR** confirm the framework's viability as a scalable, noise-resilient countermeasure to the most sophisticated threats.

7.1 LIMITATIONS AND RECOMMENDATIONS FOR FURTHER WORK

For this research paper it is useful to include this section where you discuss the limitations of your work and point to future work.

Future work will involve exploring alternative quantum kernels (e.g., $PauliFeatureMap$) to further evaluate kernel expressivity and executing the framework on commercial quantum cloud platforms for rigorous noise characterization. A key limitation is the reliance on simulation; future work should prioritize real hardware testing.

8 ACKNOWLEDGEMENTS

Use this section to thank people who have assisted during the project – if you want. It is good form to thank your supervisor, technicians and doctoral students who have helped and anyone else who deserves a mention – but do not make it too personal.

The authors wishes to thank Dr. Kishore Babu D for their supervision throughout the year and the institutional computing staff for access to the high-performance simulation environment.

9 REFERENCES

E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, "A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer," Port Said University, Egypt, 2023.

M. Y. Küçükkara, F. Atban, and C. Bayılmış, "Quantum-Neural Network Model for Platform Independent DDoS Attack Classification in Cyber Security," Sakarya University of Applied Sciences, Turkey, 2022.

M. S. Akter, K. D. Gupta, H. Shahriar, M. Rahman, S. I. Ahamed, A. Mohamed, A. Rahman, and F. Wu, "Case Study-Based Approach of Quantum Machine Learning in Cybersecurity: Quantum Support Vector Machine for Malware Classification and Protection," Kennesaw State University, USA, 2023.

E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, "A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer," Cluster Comput., vol. 27, pp. 9917–9935, 2024.

L. Eze, U. B. Chaudhry, and H. Jahankhani, "Quantum-Enhanced Machine Learning for Cybersecurity: Evaluating Malicious URL Detection," Electronics, vol. 14, no. 9, 2025.

D. Abreu, C. E. Rothenberg, and A. Abelem, "QML-IDS: Quantum Machine Learning Intrusion Detection System," 2024.

D. Said, "Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid," Energies, vol. 16, no. 8, pp. 3572, 2023.

S. Sridevi, I. B, G. S, S. Balachandran, G. Kar, and S. Kharbanda, "Unified hybrid quantum classical neural network framework for detecting distributed denial of service and Android mobile malware attacks," 2024.

M. S. Akter et al., "Case Study-Based Approach of Quantum Machine Learning in Cybersecurity: Quantum Support Vector Machine for Malware Classification and Protection," Kennesaw State University, USA, 2023.