QML-IDS: Quantum Machine Learning Intrusion Detection System

1st Diego Abreu
Federal University of Pará (UFPA)

2nd Christian Esteve Rothenberg
University of Campinas (UNICAMP)

3nd Antonio Abelém
Federal University of Pará (UFPA)

***Abstract*—The emergence of quantum computing and related technologies presents opportunities for enhancing network security. The transition towards quantum computational power paves the way for creating strategies to mitigate the constantly advancing threats to network integrity. In response to this technological advancement, our research presents QML-IDS, a novel Intrusion Detection System (IDS) that combines quantum and classical computing techniques. QML-IDS employs Quantum Machine Learning (QML) methodologies to analyze network patterns and detect attack activities. Through extensive experimental tests on publicly available datasets, we show that QML-IDS is effective at attack detection and performs well in binary and multiclass classification tasks. Our findings reveal that QML-IDS outperforms classical Machine Learning methods, demonstrating the promise of quantum-enhanced cybersecurity solutions for the age of quantum utility.**

***Index Terms*—Quantum Machine Learning, Network Security, Quantum Network.**

I. Introduction

Recent advances in quantum computing signify a main shift towards the era of quantum utility, highlighting a crucial phase in the evolution of quantum technologies where quantum computers now outperform classical methods in solving complex problems efficiently and accurately [1]. Despite not yet achieving quantum supremacy—the milestone where quantum computing overtakes classical computing in solving certain tasks within practical timeframes—these developments are crucial strides toward enabling robust applications across various research domains. Within this framework, quantum technologies are poised to revolutionize network security by integrating with Intrusion Detection Systems (IDS) through Quantum Machine Learning (QML) techniques. This integration promises more precise detection of network anomalies and the capability to analyze vast datasets, addressing the dynamic challenges of cybersecurity and marking a significant advancement in safeguarding digital infrastructures in the rapidly evolving technological landscape.

A significant challenge is related to the current capabilities of quantum devices, known as Noisy Intermediate-Scale Quantum (NISQ) devices [2]. These limitations include restrictions on the number of qubits (quantum bits) available, the complexity of the quantum circuits that can be implemented (depth and available quantum logic gates), and the ability to maintain quantum coherence over time (due to noise and the inherent nature of qubits) [3]. Moreover, the lack of robust error correction mechanisms in NISQ systems also represents a significant obstacle [4]. Therefore, any proposal for a quantum IDS must take these factors into account to ensure its effective applicability in the current quantum computing landscape [2].

In this paper, we propose QML-IDS, a Quantum Machine Learning-Based Attack Detection System. The primary goal is to create an adaptable system for use with NISQ devices, overcoming the inherent limitations of current quantum computing. To achieve this goal, our approach is based on hybrid QML techniques, which leverage the capabilities of both classical and quantum computing simultaneously. To evaluate the performance of QML-IDS, a series of experiments were conducted using publicly available network security datasets. Three QML methods in our system were compared in terms of attack detection (binary classification) and identification of specific attacks (multiclass classification). Furthermore, the results obtained with QML approaches were compared with classical Machine Learning (ML) methods. The experimental results provide empirical evidence of the effectiveness of QML techniques in enhancing network attack detection capabilities and point to the feasibility of implementation in NISQ systems. The main contributions of this work are:

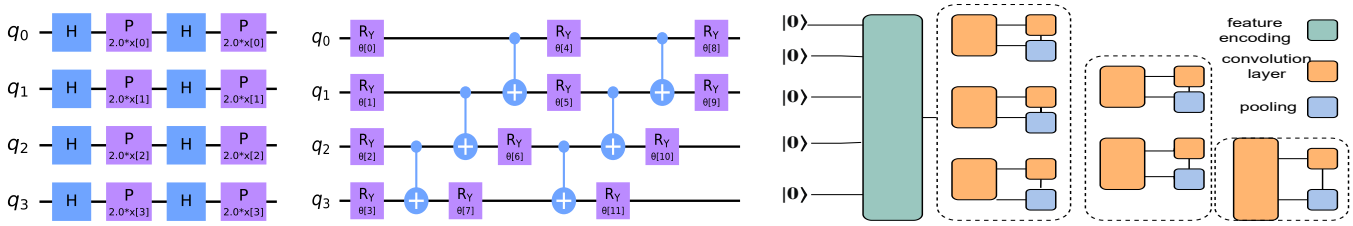
1) Development of QML-IDS, a QML-based network attack detection system that utilizes both quantum and classical computing in a hybrid manner.
2) Presentation of the operation of QML-IDS through the application of three distinct QML techniques, followed by an evaluation of the performance of each approach.
3) Implementation of QML-IDS in NISQ systems and evaluation of different quantum circuit configurations on system performance.

II. Hybrid Quantum Machine Learning

Quantum Machine Learning can be understood as a set of techniques that combine principles of quantum computing (such as superposition, interference, and entanglement) with Machine Learning techniques to perform tasks like classification, regression, and clustering of data [5]. In this work, our focus is on hybrid QML approaches, which use both quantum and classical computing to create learning models.

A. Variational Quantum Classifier (VQC)

The Variational Quantum Classifier (VQC) [6] is a hybrid Quantum Machine Learning algorithm that leverages parameterized quantum circuits combined with classical optimization techniques for classification tasks. It operates by encoding



(a) Feature Map Circuit. (b) Variational Circuit (Ansatz). (c) QCNN.

Fig. 1: Examples of Quantum Circuits used in QML.

classical input data into quantum states through a process known as a feature map (Fig 1.a), transforming these states within a quantum circuit whose parameters are iteratively adjusted based on training data to delineate the optimal decision boundary between classes. This encoding and manipulation of quantum states allow the VQC to exploit the quantum mechanical properties of superposition and entanglement, aiming to achieve superior classification performance over classical algorithms in certain scenarios. Thus, the specific choice of the feature map influences the VQC's ability to represent the important features of the input data, directly impacting the performance of the generated model.

The core of the VQC involves three main steps: encoding the input data into quantum states, processing these states through a variational quantum circuit (or Ansatz, Fig 1.b), and optimizing the circuit parameters using classical optimization techniques. Initially, input data are mapped onto a high-dimensional quantum space using a feature map, which is a unitary operation that prepares the quantum states representing the data. The variational circuit then applies a series of quantum gates, controlled by adjustable parameters, to these states, effectively learning the underlying data patterns.

The final stage involves refining the model through a classical optimization process, where a classical optimizer fine-tunes the *Ansatz* parameters to minimize a cost function. This iterative adjustment aims to identify the optimal circuit configuration that best delineates the target classes. Through this process, the VQC seeks to harness the computational advantages of quantum computing, potentially offering new capabilities in the field of machine learning and data classification.

B. Quantum Support Vector Machines (QSVM)

The Quantum Kernel Support Vector Machine (QSVM) [7] represents a quantum-enhanced version of the classical Support Vector Machine (SVM) algorithm, leveraging the principles of quantum computing to map input data into a high-dimensional quantum feature space. This quantum feature space potentially allows for more effective separation of data that are not linearly separable in their original space. The process involves the construction of a quantum kernel, which is a measure of similarity between pairs of data points in this quantum space. This kernel is generated through quantum transformations applied to the quantum states representing the input data, enabling the QSVM to exploit the computational advantages of quantum mechanics for complex classification tasks.

During the training phase, QSVM utilizes a quantum circuit to project the training examples into the quantum feature space, where it computes the kernel matrix that captures the intricate relationships between these examples. The algorithm then identifies support vectors, which are key data points that define the optimal separation hyperplane in the quantum feature space. These support vectors and the kernel matrix guide the construction of a hyperplane that maximizes the margin between different classes, mirroring the objective of classical SVM but within a quantum computational framework.

In the testing phase, new, unlabeled examples are similarly mapped into the quantum space, and their classification is determined based on their position relative to the quantum hyperplane. This approach allows QSVM to classify data by effectively utilizing quantum operations to handle datasets that challenge traditional classification methods. The effectiveness of QSVM heavily relies on the choice of the feature map and the design of the quantum kernel, which are critical for capturing the essential characteristics of the data in the quantum feature space, thereby enabling the algorithm to achieve high classification accuracy.

C. Quantum Convolutional Neural Network (QCNN)

The Quantum Convolutional Neural Network (QCNN) [8] is an adaptation of classical convolutional neural networks (CNNs). The architecture of QCNNs (Fig 1.c) mirrors that of their classical counterparts, consisting of convolutional layers, pooling layers, and fully connected layers, albeit implemented with quantum operations. The convolutional layers in a QCNN are realized through the application of parameterized unitary operations on neighboring pairs of qubits. These operations are akin to the filters applied in classical CNNs, designed to detect specific features within the data. However, unlike classical filters that operate on pixel values, quantum convolutions manipulate the quantum states of qubits, enabling the extraction of quantum features.

Following the convolutional layers, QCNNs implement quantum pooling layers. The objective of pooling in classical CNNs—to reduce the dimensionality of the data and retain only the most relevant features—is achieved in QCNNs through the measurement of a subset of qubits. This measure-

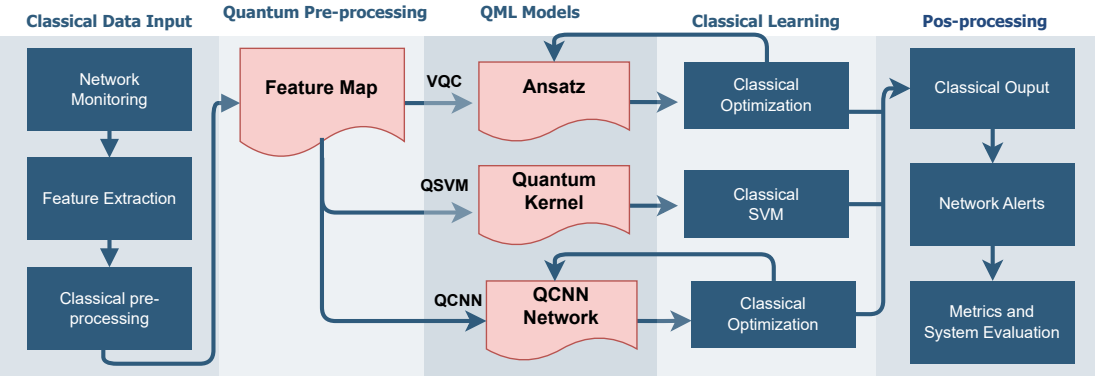


Fig. 2: Operational flowchart of QML-IDS.

ment effectively reduces the number of qubits in the system, analogous to the downsampling performed in classical pooling layers. The choice of which qubits to measure and discard is a critical aspect of the QCNN architecture, as it determines how information is condensed and propagated through the network. Training a QCNN involves adjusting the parameters of the convolutional and fully connected layers to minimize a loss function, similar to the process in classical neural networks. However, due to the quantum nature of the operations, gradient descent and other optimization techniques must be adapted for quantum circuits. This often involves the use of classical optimizers to adjust the quantum parameters based on the measurement outcomes, effectively creating a hybrid quantum-classical learning algorithm.

III. Related Work

Several studies have addressed the use of Quantum Machine Learning [5]. In this section, we highlight works that seek to utilize QML in the context of network security. Said et al. (2023) [9] explore the application of a QSVM model to detect Distributed Denial of Service (DDoS) attacks in smart micro-grids. The study evaluates the QML model using a reduced version (by sampling) of the CIC-DDoS2019 dataset [10], which includes data on both DDoS attacks and normal network behavior. The results demonstrate the superiority of the QML model compared to the classical approach, SVM. In the paper by Gong et al. [11], the application of a Neural Network (NN) in conjunction with the VQC for network attack detection is proposed. The authors apply the created model to a reduced subset of features from the KDD CUP99 dataset [12], incorporating a class balance approach to increase classification accuracy. Similarly, Kalinin and Krundyshev [13] propose a QSVM model with NN for network attack detection. The generated model is applied to a database created by the authors and compared with other techniques such as SVM and CNN. These works implemented their solutions using noiseless quantum computing simulators, which cannot accurately represent current NISQ systems. In our work, our proposal is implemented using noisy backends, which more closely represent current NISQ equipment.

Moreover, Suryotrisongko and Musahi [14] propose a VQC and a Hybrid Quantum Deep Learning (DL) to detect botnet domain generation algorithm (DGA) attacks. The Hybrid DL consists of adding one quantum layer to a NN model. While the DL model was tested using NISQ devices, the VQC was not. In [15], the Hybrid Quantum DL is also evaluated in regard to adversarial attack robustness.

The research contributions presented in this work differ by presenting a comprehensive analysis of the application of various QML techniques (VQC, QSVM, and QCNN), both for detection (binary scenario) and for the identification of attacks (multiclass scenario). Additionally, our work conducts tests on three reference datasets in network security, containing a wide variety of network attacks. Furthermore, unlike the related studies, we conducted tests in circuits with diverse optimization levels, incorporating resilience and dynamic decoupling, which contributed to the improvement of our results.

IV. QML-IDS: Hybrid Quantum Machine Learning-Based Attack Detection System

In this work, we propose a network attack detection system based on Hybrid Quantum Machine Learning (QML-IDS). The proposal is to apply Hybrid QML techniques, which use both quantum and classical computing, to perform network attack detection. The operation of the proposal is presented in the flowchart in Figure 2.

QML-IDS begins with network monitoring and data collection, from which features are extracted. After this, data preprocessing is performed for normalization, handling missing values, and other techniques aimed at preparing the data for the system. Next, the mapping of classical data to quantum states occurs through the feature map. The Hybrid QML process is then initiated, with the quantum and classical parts according to the QML technique. In the case of VQC, a variational quantum circuit ansatz is generated, whose parameters are adjusted by a classical optimizer. For QSVM, a quantum kernel is generated, which is used to train the classical prediction model. In the QCNN, the quantum network is generated and optimized classically.

The final result of the process is a classical output, an interpretation of the quantum results that is used for the

TABLE I: Hyperparameters of Quantum Models.

Feature Maps	**Ansatz**	**Optimizer**
PauliFeatureMap	EfficientSU2	COBYLA
RawFeatureVector	ExcitationPreserving	ADAM
ZFeatureMap	RealAmplitudes	SPSA
ZZFeatureMap	TwoLocal	GradientDescent
Optimization Level	**Resilience**	**Decoupling**
Level 0,1,2,3	Level 0 or 1	0 or 1

generation of attack alerts. Based on the analyses performed, the system generates attack alerts whenever suspicious patterns are identified, contributing to network security. It is important to note that in this approach, other hybrid QML methods can also be used, respecting the particularities of each method. QML-IDS can then be implemented partly on a classical system and partly on a quantum system.

V. Experimental Setup

To evaluate the proposed system, we conducted a comprehensive case study, leveraging three prominent network security databases: UNSW-NB15 [16], CICIDS17 [17], and CICIoT2023 [18]. These datasets include both normal and various types of attack network traffic data and are frequently utilized for the detection and classification of attacks using ML techniques. Three classical ML methods were selected and will serve as a comparison to the quantum counterparts results: Support Vector Machine (SVM), Convolution Neural Network (CNN), and Random Forest (RF) as a representative classifier to compare with VQC, all implemented using the scikit-learn and TensorFlow frameworks.

To evaluate the performance of the QML-IDS system, three Quantum Machine Learning models were employed: VQC, QSVM, and QCNN, which were implemented using the Qiskit framework. For these models, the specific hyperparameters used are presented in Table I. We employ four feature maps from Qiskit (RawFeatureVector, PauliFeatureMap, ZFeatureMap, ZZFeatureMap) for encoding classical data into quantum states, alongside four Ansatz and classical optimizers within the Qiskit framework. The RawFeatureVector offers a direct mapping of classical data to quantum states, establishing a baseline. The PauliFeatureMap and ZFeatureMap utilize quantum gates to simulate Pauli operators and employ Hadamard and unitary gates for transforming classical inputs into quantum states, enabling the capture of nonlinear patterns and facilitating first-order data encoding. The ZZFeatureMap extends these capabilities by incorporating second-order qubit interactions for more complex correlation encoding [19].

Addressing the challenge of quantum circuit transpilation for real quantum hardware, our experiments leverage optimization levels from 0 to 3 for circuit adaptation, with each level introducing increasingly sophisticated optimization strategies, from basic gate collapsing to advanced techniques like peephole optimization and noise-adaptive qubit mapping. Additionally, we integrate resilience levels and dynamic decoupling to enhance error resilience, with resilience level 0 offering no mitigation and level 1 targeting readout errors through Matrix-free Measurement Mitigation, alongside dynamic decoupling to reduce environmental interactions, thereby optimizing the balance between accuracy and processing time in quantum computations.

VI. Results

A. NISQ Backend Results

In this section, we delve into the performance of QML-IDS across a variety of NISQ *Backend* configurations. For this, six different *backends* were used, including the noise-free quantum computing simulator *QASM* and five real quantum computing environments: *IBM_CAIRO*, *IBM_KYOTO*, *IBM_BRISBANE*, *IBM_OSAKA*, and *IBM_SHERBROOKE*. These environments incorporate the specific noise models, quantum logic gates, and topologies of actual quantum computers, providing a realistic assessment of quantum technologies in security applications.

To illustrate the obtained results, the performance of three QML models (VQC, QSVM, QNCC) is presented in Table II, showcasing their F1 Scores across the mentioned *backends* for binary attack detection. The F1 Score is chosen for its balanced measure of precision and recall, crucial in security contexts for effectively detecting attacks while minimizing false positives. The *QASM* simulator, representing an ideal quantum computing scenario, consistently shows high F1 Scores across all databases, highlighting the potential of quantum computing in enhancing IDS capabilities. However, the focus of this research is on the performance within real quantum systems, where noise and operational limitations present substantial challenges.

Among the real quantum systems, there is a significant variation in performance, which reflects the impact of each system's unique noise model, quantum logic gates, and topology. This variation underscores the importance of selecting and tuning QML models according to the specific characteristics of the quantum hardware in use. For instance, VQC demonstrates robust performance on the *IBM_KYOTO* backend for the CICIDS17 dataset, while QSVM shows adaptability with strong results on *IBM_OSAKA* for the UNSW-NB15 database and on *IBM_BRISBANE* for the CICIoT2023 database. QNCC, in particular, stands out with the highest F1 Scores in several configurations, such as on the *IBM_KYOTO* and *IBM_BRISBANE* backends for the CICIDS17 and CICIoT2023 databases, respectively, showcasing its effectiveness in handling the complexities of real quantum systems.

The results indicate the potential of QML-IDS to leverage quantum computing for security applications, while also highlighting the critical role of hardware-specific considerations in optimizing performance. The varying results across different *backends* and models emphasize the necessity for ongoing research and development in quantum computing to address the challenges posed by noise and other physical limitations in NISQ systems. The best results obtained in each model and *backend* combination will be discussed in detail in the following subsections.

TABLE II: F1 Score of QML on each *Backend* across three databases (for binary case)

UNSW-NB15	QASM	IBM_CAIRO	IBM_KYOTO	IBM_BRISBANE	IBM_OSAKA	IBM_SHERBROOKE
VQC	88.56%	87.91%	**88.10** %	85.78%	87.75%	87.31%
QSVM	89.34%	**87.90**%	86.41%	86.39%	**87.90**%	86.55%
QNCC	87.45%	86.12%	87.12%	**87.32**%	87.19%	85.42%
CIC-IDS-17	QASM	IBM_CAIRO	IBM_KYOTO	IBM_BRISBANE	IBM_OSAKA	IBM_SHERBROOKE
VQC	95.12%	93.60%	**94.78**%	92.40%	94.12%	94.00%
QSVM	94.67%	92.92%	**94.40**%	92.80%	92.15%	94.38%
QNCC	95.88%	93.80%	**95.60**%	93.40%	94.15%	94.12%
CICIoT2023	QASM	IBM_CAIRO	IBM_KYOTO	IBM_BRISBANE	IBM_OSAKA	IBM_SHERBROOKE
VQC	82.55%	78.55%	76.15 %	77.12%	77.02%	**78.92**%
QSVM	84.22%	79.19%	80.00%	**82.40**%	80.55%	80.12%
QNCC	87.81%	82.55%	**82.56**%	82.00%	82.11%	81.93%

TABLE III: F1 score results for the binary classification.

QML	UNSW-NB15	CIC-IDS-17	CICIoT2023
VQC	88.10%	94.78%	78.92%
QSVM	87.90%	94.40%	82.40%
QCNN	87.32%	95.60%	82.56%
RF	82.67%	92.45%	71.95%
SVM	82.34%	93.78%	82.7%
CNN	86.72%	93.15%	78.52%

B. QML-IDS Results: Attack Detection

Table III provides a detailed comparison of Quantum Machine Learning models against traditional Machine Learning, in the context of binary classification for attack detection. The comparison spans three distinct datasets: UNSW-NB15, CIC-IDS-17, and CICIoT2023, showcasing the F1 score as a metric to evaluate the performance of each method. Notably, QML models, including Variational Quantum Classifier, Quantum Support Vector Machine, and Quantum Convolutional Neural Network, demonstrate competitive or superior performance compared to their ML counterparts across all datasets.

The performance of VQC is particularly impressive, marking the highest F1 scores among QML models across the datasets, which underscores its effectiveness in detecting attacks. This is evident in the comparison where VQC achieves an F1 score of 88.10% on the UNSW-NB15 dataset, surpassing the best performing traditional ML method, SVM, which scores 82.34%. Similar trends are observed in the CIC-IDS-17 and CICIoT2023 datasets, where QML models generally outperform traditional ML methods, albeit with varying margins. QSVM and QCNN also show strong performance, with QCNN achieving the highest F1 score of 95.60% on the CIC-IDS-17 dataset, indicating the potential of QML models in enhancing cybersecurity measures.

C. qIDS Results: Identification of Attacks

The multiclass classification results for attack identification across the UNSW-NB15, CIC-IDS-17, and CICIoT2023 datasets, as shown in Tables IV, V, and VI, reveal insightful trends about the capabilities of Quantum Machine Learning (QML) models versus traditional Machine Learning (ML) methods. In the UNSW-NB15 dataset, QML models such as VQC, QSVM, and QCNN display varied performance across different attack types. They show exceptional proficiency in identifying attacks like Analysis and Reconnaissance, where QCNN notably excels with scores reaching up to 98.88% for Analysis attacks. However, for categories like Worms and Shellcode, these quantum models lag behind, suggesting that while QMLs are promising for certain attack vectors,

TABLE IV: Multiclass F1 score Results: UNSW-NB15 dataset.

Attack	**VQC**	**QSVM**	**QCNN**	**RF**	**SVM**	**CNN**
Analysis	95.55	87.85	98.88	90.23	96.45	95.15
Backdoor	84.16	82.08	91.05	92.11	90.78	90.13
DoS	89.29	88.68	93.23	82.56	92.45	80.26
Exploits	95.23	93.78	94.44	85.89	79.01	78.16
Fuzzers	76.12	96.55	93.14	79.78	77.56	76.89
Generic	97.01	94.45	95.00	99.01	99.34	94.83
Recon	98.88	99.72	97.48	82.89	86.12	90.46
Shellcode	68.23	76.67	79.94	80.12	76.23	72.00
Worms	22.86	55.89	65.11	35.78	20.56	48.15

TABLE V: Multiclass F1 score Results: CIC-IDS-17 dataset.

Attack	**VQC**	**QSVM**	**QCNN**	**RF**	**SVM**	**CNN**
BoT	88.23	97.11	98.45	92.12	94.67	91.45
BruteForce	95.87	99.99	99.99	96.24	93.45	94.42
DoS	90.32	90.79	92.45	98.02	99.67	96.15
DDoS	90.54	99.99	96.55	99.34	94.32	96.32
Infiltration	90.99	99.66	97.42	97.53	99.87	97.15
PortScan	95.45	96.32	97.48	97.45	97.89	96.88
WebAttack	92.78	96.67	97.83	96.89	98.21	96.55

TABLE VI: Multiclass F1 score Results: CICIoT2023 dataset.

Attack	**VQC**	**QSVM**	**QCCN**	**RF**	**SVM**	**CNN**
BruteForce	64.19	70.25	74.76	62.55	60.41	66.31
DoS	92.03	95.59	96.43	95.13	92.86	94.41
DDoS	92.81	95.48	96.37	95.78	92.52	95.27
Mirai	90.32	96.92	97.48	96.44	93.00	97.92
Recon	83.40	80.60	92.53	85.88	81.95	88.44
Spoofing	74.95	70.20	76.08	65.73	60.69	68.27
Web	60.00	72.85	74.56	60.48	58.10	68.63

traditional ML methods like SVM and RF still hold the upper hand in others.

Moving to the CIC-IDS-17 dataset, the pattern of QML models, particularly QSVM and QCNN, achieving high F1 Scores in detecting specific types of attacks such as Brute-Force and DDoS is evident. This indicates their potential in accurately identifying these attacks, with QSVM and QCNN reaching near-perfect scores in BruteForce detection. Yet, in scenarios involving DoS and WebAttack, traditional methods like SVM and RF present competitive or superior performance, highlighting the nuanced effectiveness of QML models depending on the nature of the attack.

The analysis of the CICIoT2023 dataset further underscores the strengths and limitations of QML in the realm of cybersecurity. Here, QML models demonstrate robust performance in identifying DoS attacks, with QCNN showing a remarkable F1 Score of 96.43%. However, for other attack types such as Spoofing and Web attacks, the performance of QML models is less dominant, with traditional ML methods occasionally outperforming or matching the quantum approaches. This comparative analysis across three datasets illustrates the evolving landscape of intrusion detection, where QML models offer significant advantages for certain attack types but still require advancements to consistently outperform traditional ML methods across the board.

Therefore, despite the promising results, the performance gap between QML and traditional ML methods is not overwhelmingly large, suggesting that while QML offers potential advantages in certain scenarios, it does not yet decisively outperform traditional approaches in all aspects. This highlights the importance of further research and development in QML to fully exploit its capabilities and potentially achieve substantial improvements over traditional ML methods in the field of cybersecurity.

VII. Conclusion and Future Work

This work introduced QML-IDS, a Hybrid Quantum Machine Learning-based attack detection system, designed to tackle emerging challenges in cybersecurity scenarios. Through experimental evaluations conducted on different public datasets, QML-IDS proved to be effective in detecting attacks, both in binary and multiclass classifications, showing competitive results compared to traditional Machine Learning methods.

In the current NISQ and quantum utility scenarios, the application of qIDS already demonstrates competitive results compared to other ML techniques in the detection and identification of attacks. However, there are still challenges and limitations to be overcome for the practical implementation of the proposal in real network environments, which continues to be an active area of research and opens up space for future works. Among the points to be explored are integration with existing classical IDS frameworks and with traditional ML-based IDS systems to create a more robust defense mechanism. Moreover, addressing the constraints of quantum hardware availability and navigating the privacy concerns associated with processing data on platforms like IBM's will be crucial in pushing the boundaries of quantum-enhanced cybersecurity solutions.

Acknowledgements

This work was partially supported by the São Paulo Research Foundation (FAPESP), Grant 2021/00199-8, CPE SMARTNESS. It was also financed in part by CAPES Finance Code 001.

References

[1] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. Van Den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme *et al.*, "Evidence for the utility of quantum computing before fault tolerance," *Nature*, vol. 618, no. 7965, pp. 500–505, 2023.

[2] G. De Luca, "A survey of nisq era hybrid quantum-classical machine learning research," *Journal of Artificial Intelligence and Technology*, vol. 2, no. 1, pp. 9–15, 2022.

[3] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[4] G. Torlai and R. G. Melko, "Machine-learning quantum states in the nisq era," *Annual Review of Condensed Matter Physics*, 2020.

[5] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, "Challenges and opportunities in quantum machine learning," *Nature Computational Science*, vol. 2, no. 9, pp. 567–576, 2022.

[6] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.

[7] J. Jäger and R. V. Krems, "Universal expressiveness of variational quantum classifiers and quantum kernels for support vector machines," *Nature Communications*, 2023.

[8] I. Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," *Nature Physics*, vol. 15, no. 12, pp. 1273–1278, 2019.

[9] D. Said, "Quantum computing and machine learning for cybersecurity: Distributed denial of service (ddos) attack detection on smart microgrid," *Energies*, vol. 16, no. 8, p. 3572, 2023.

[10] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–8.

[11] C. Gong, W. Guan, A. Gani, and H. Qi, "Network attack detection scheme based on variational quantum neural network," *The Journal of Supercomputing*, vol. 78, no. 15, pp. 16 876–16 897, 2022.

[12] C. Elkan, "Results of the kdd'99 classifier learning," *Acm Sigkdd Explorations Newsletter*, vol. 1, no. 2, pp. 63–64, 2000.

[13] M. Kalinin and V. Krundyshev, "Security intrusion detection using quantum machine learning techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 1, pp. 125–136, 2023.

[14] H. Suryotrisongko and Y. Musashi, "Hybrid quantum deep learning and variational quantum classifier-based model for botnet dga attack detection," *International Journal of Intelligent Engineering and Systems*, 2022.

[15] H. Suryotrisongko, Y. Musashi, A. Tsuneda, and K. Sugitani, "Adversarial robustness in hybrid quantum-classical deep learning for botnet dga detection," *Journal of Information Processing*, 2022.

[16] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 military communications and information systems conference (MilCIS)*. IEEE, 2015, pp. 1–6.

[17] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." *ICISSp*, vol. 1, pp. 108–116, 2018.

[18] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," 2023.

[19] G. Buonaiuto, F. Gargiulo, G. De Pietro, M. Esposito, and M. Pota, "Best practices for portfolio optimization by quantum computing, experimented on real quantum devices," *Nature Scientifc Reports*, 2023.