



Hybrid Quantum-Classical AI Pipelines: Advanced Data Mining for Predictive Cyber Threat Hunting

Satish Kumar Pittala^{1*}, Vivekanandan Govindan Ekambaram², Vikram Kumar Casula Ashok³

¹Cloud Solution Architect, USA.

²Sr Software Architect, California, USA

³Department of Computer Science and Engineering, USA.

*Corresponding Author

Satish Kumar Pittala

Email: pscloud1@gmail.com

Article History

Received: 13.10.2023

Accepted: 01.12.2023

Published: 28.12.2023

Abstract: The swift development of cyber threats, especially, sophisticated and distributed attacks on software-defined networks (SDNs) have necessitated smart and proactive threat-hunting solutions. This paper suggests a Hybrid Classical-Quantum Neural Network (C-QNN) model that combines classical machine learning algorithms with the near-term quantum computing capacity to improve predictive cyber threat detection. The proposed framework uses classical data mining techniques to extract features, reduce dimensionality and preprocess traffic pattern prior to passing optimized representations to variational quantum circuits to perform more sophisticated pattern recognition. The hybrid pipeline combines classical optimization techniques and quantum embedding strategies to overcome the drawbacks of existing quantum hardware and exploit quantum-enhanced learning capabilities. Empirical analysis shows better detection accuracy and predictive capabilities in detecting complex attack patterns in high dimensional network settings. The results emphasize the prospects of hybrid quantum-classical AI systems as a viable solution to deploy scalable, intelligent cybersecurity systems without depending on full fault-tolerant quantum processors. This study helps to establish the basis of embedding quantum-enhanced analytics into the next-generation proactive systems of cyber defense.

Keywords: Hybrid Classical-Quantum Neural Network, Software-Defined Networks, Cyber Threat Detection, Variational Quantum Circuits, Quantum-Enhanced Learning.

1. Introduction

Conventional cybersecurity systems, such as signature-based intrusion detection and rule-based monitoring systems, are becoming less effective against advanced persistent threats (APTs), zero-day exploits, polymorphic malware, and distributed attack campaigns since the mechanisms are largely based on previously known attack patterns (Sommer & Paxson, 2010). As a result, the active threat hunting strategies capable of discovering disguised attack patterns, anomalous network traffic, and new threats before they have a devastating effect on the system have become a crucial part of the current cyber defense strategies (Bahadur et al., 2022). Machine learning (ML) and artificial intelligence (AI) have become the promising solutions to the shortcomings of the traditional methods of cybersecurity. Intrusion detection systems (IDSs) based on machine

learning have the ability to analyze large scale network traffic, discover complex correlations, and detect attack patterns that have never been seen before by learning over time (Buczak & Guven, 2016).

But openness and programmability of SDN controllers are also a good target to attackers. Thus, efficient threat-hunting solutions should be able to process big data of the networks, as well as identify sophisticated attack patterns in real-time (Mousavi and St-Hilaire, 2015). Approaches based on machine learning have been shown to have potential in SDN security, but may be constrained by feature engineering needs, cost of computation, and the challenge of identifying highly intelligent attack plans. Recently quantum computing has become a hot topic as a possible technology to speed up complex computational tasks (Dalal, 2018) (Dalal, 2019). In contrast to classical computers, which execute computations

with binary states, quantum computers utilize quantum bits (qubits), which can represent superposition states, to provide new computational methods to solve optimization problems, simulations and machine learning problems (Nielsen & Chuang, 2010) (Hegde, 2021). Quantum machine learning (QML) is an approach that integrates quantum computing with machine learning algorithms to create models that can explore the space of complex features and find patterns that can be challenging to capture with classical algorithms (Biamonte et al., 2017) (Hegde & Varughese, 2020).

Hybrid quantum-classical machine learning offers an effective route to take advantage of quantum benefits and rise above the existing hardware constraints. Within such architectures, classical machine learning algorithms prepare, extract features and reduce dimensionality, and quantum circuits implement specialized computational tasks, such as feature mapping and pattern recognition (Dalal & Abdul, 2019). One of the most popular methods to apply QML applications to NISQ devices has been variational quantum circuits (VQCs) optimized by classical algorithms (Cerezo et al., 2021).

Nonlinear interactions involving network traffic logs, user behaviors, system logs and attack patterns may cause challenges to classic machine learning algorithms. Alternative mechanisms may be offered by quantum-enhanced feature mapping and variational quantum circuits in finding the complex patterns in these datasets (Dalal, 2020) (Hegde, 2019).

2. Literature Review

2.1 Artificial Intelligence and Machine Learning for Cyber Threat Detection

The growing complexity of cyberattacks has spurred the widespread study of artificial intelligence (AI)-based cybersecurity tools. The conventional intrusion detection systems (IDSs) with the reliance mostly on the predefined signatures and manually created rules have low potential in detecting the unknown or fast changing threats. Machine learning (ML) has thus become a relevant method of creating adaptive cybersecurity systems that can find intelligible patterns based on large-scale network data (Sommer and Paxson, 2010). The intrusion detection methods based on machine learning are typically divided into supervised, unsupervised, and semi-supervised learning. Deep neural networks do not need to perform hierarchical feature engineering, as opposed to more conventional ML methods that do, meaning that the former may be trained on raw or slightly processed data (Hegde & Varughese, 2022).

2.2 Data Mining and Feature Engineering in Cybersecurity

Although SDN allows monitoring and dynamic security controls, the amount of generated information is huge and

presents obstacles to real-time threat monitoring. Mousavi and St-Hilaire (2015) examined the detection of distributed denial-of-service (DDoS) attacks on SDN controllers and illustrated the significance of smart monitoring strategies to safeguard SDN infrastructures. Recent cybersecurity studies have thus been directed at integrating data mining and advanced AI models to enhance predictive threat intelligence. Data mining methods can help to decrease the computational complexity of AI models and make decisions quickly by reducing the high-dimensionality of traffic data into reduced-dimensional and optimized feature spaces (Karmakar, 2021).

2.3 Quantum Computing and Quantum Machine Learning

One of the potential computational paradigms that have risen to the scene is quantum computing, which can solve some of the issues challenging the classical computers. To store and process information, quantum computers apply quantum mechanical properties, such as superposition and entanglement, to quantum computers with qubits instead of classical bits (Nielsen and Chuang, 2010). Whereas large-scale fault-tolerant quantum computers are yet to be built, the development of near-term quantum devices has stimulated the investigation of practical quantum applications (Maizana et al., 2023).

Quantum machine learning (QML) combines quantum computing concepts with machine learning algorithms to consider novel ways to analyze and optimize data and recognize trends. Biamonte et al. (2017) offered one of the background surveys of quantum machine learning and discovered possible benefits of quantum algorithms in classification, clustering, and optimization. A notable QML research field is quantum neural networks (QNNs), which seek to use quantum circuits in neural learning models (Mohammad, Mahjabeen, et al., 2022). Nevertheless, neural networks based entirely on quantum computing demand sophisticated quantum computers with high counts of stable qubits, which do not exist today. This has led to a shift in research to hybrid quantum-classical frameworks that integrate classical computing resources with quantum processing capabilities. The present Noisy Intermediate-Scale Quantum (NISQ) era is a period in the history of quantum computing during which quantum devices have a small number of qubits, and are subject to noise and operational errors. Preskill (2018) highlighted that the deployment of quantum devices in practice in the NISQ era should be based on hybrid schemes that are based on classical optimization and quantum circuit implementation (Mohammad, Mahjabeen, et al., 2023).

2.4 Hybrid Quantum-Classical Neural Networks

One of the most popular architectures of hybrid quantum learning is variational quantum circuits (VQCs). The

quantum circuits in VQCs have trainable parameters that are optimized with classical optimization algorithms. Cerezo et al. (2021) surveyed variational quantum algorithms and emphasized their applicability to NISQ devices since they are relatively small quantum circuits and can be scaled to hardware constraints.

The experiment showed better detection performance than the classical long short-term memory (LSTM) and quantum neural networks, which showed the promise of hybrid approaches to cybersecurity applications (Tiwari, 2022).

2.5 Quantum Machine Learning Applications in Cybersecurity

Quantum technologies will not only offer the chance to design the cryptographic systems of the future, but also to improve the security analytics based on AI. Faruk et al. (2022) conducted a review of the connection between quantum computing and cybersecurity, highlighting that quantum technologies might be interpreted as a cybersecurity threat and opportunity. Although quantum computers can indeed pose threats to the current cryptography systems, including the Shor algorithm, quantum-enhanced AI technologies might be used to help identify the threats better and ensure effective surveillance. Malware detection, anomaly detection, and network intrusion analysis Hybrid quantum-classical approaches have recently been considered to handle malware, anomaly, and network intrusion. An experiment on hybrid quantum-classical deep learning in cybersecurity explored the domain generation algorithm (DGA)-based botnet attack detection and proved the potential of implementing classical deep learning with quantum processing units to protect against cyber threats. ScienceDirect These studies show that quantum-enhanced learning can offer more representation options to find complex patterns of attacks.

2.6 Research Gap and Motivation

Quantum machine learning has put promising alternatives in complex pattern recognition, but it is limited by existing hardware needs. The current research on quantum cybersecurity is dominated by theoretical models or small-scale experiments. Practical architectures that combine classical data mining and quantum learning elements to work with real-world cyber threat hunting are still needed. Specifically, software-defined networks produce high-dimensional data on traffic that needs to be extracted with features and modeled with advanced analysis. Thus, a hybrid Classical-Quantum Neural Network (C-QNN) solution is a new direction of research. Such systems can utilize existing quantum abilities by integrating classical preprocess, dimensionality reduction, and optimization with quantum feature mapping and variational circuits, and can fulfill practical cybersecurity needs.

3. Methodology

The initial step is to gather network traffic information with both normal and malicious activities of the cybersecurity benchmark datasets. The gathered data entail network flow properties, packet-wide data as well as attack-related data. The high-dimensional nature of cybersecurity datasets and redundancy of features in them necessitates the use of classical data preprocessing methods to enhance the quality of data and minimize the computation cost. Preparation of data: Data cleaning, normalization and feature selection are done prior to training the model. Several feature reduction techniques like Principal Component Analysis (PCA) and correlation-based feature selection are used to obtain the most relevant features and discard redundant data. Past research has shown that successful feature engineering leads to better performance of machine learning-based intrusion detection systems through noise reduction and computation reduction (Buczak and Guven, 2016).

Classical Feature Extraction based on machine learning

The optimized network features are trained with classical machine learning algorithms to produce compact feature representations that can be processed by quantum processing. Initial pattern learning and dimensionality reduction are done with classical neural networks since modern quantum devices are not efficient at extremely large feature vectors. Based on quantum-classical learning, this hybrid preprocessing approach entails classical data optimization and transformation alongside quantum computational elements to enhance model scalability (Biamonte et al., 2017).

Quantum Feature Encoding and Variational Quantum Circuit

Quantum feature mapping techniques are used to encode the reduced feature vectors into quantum states. The coded quantum information is run on a Variational Quantum Circuit (VQC), a sequence of parameterized quantum gates that are optimized during training. The quantum circuit identifies nonlinear relationships, which are difficult to extract in the input data, and gives improved representations of features. Variational quantum algorithms can be applied to near-term quantum devices since those algorithms do not have many quantum resource requirements and classical optimization can be used to optimize the quantum circuit parameters (Cerezo et al., 2021). The proposed model can be made to work because of this approach within the constraints of Noisy Intermediate-Scale Quantum (NISQ) devices (Preskill, 2018).

Training of Hybrid Classical-Quantum Model

The results of the quantum circuit are copied back to classical layers to be classified. A classical optimizer performs an iterative update of the parameters of the neural

network and quantum circuit to reduce the number of errors in classification. The hybrid training process allows the model to integrate the learning properties of the classical deep learning with quantum-enhanced feature representation.

Result

The proposed framework was more effective than traditional machine learning models at detecting sophisticated and distributed network attacks. The findings underscore the promise of hybrid quantum-classical systems in enhancing cybersecurity analytics in quantum computing systems of the NISQ era. In general, the results confirm the possibility of using quantum computing methods in conjunction with classical AI pipelines in high-level threat detection.

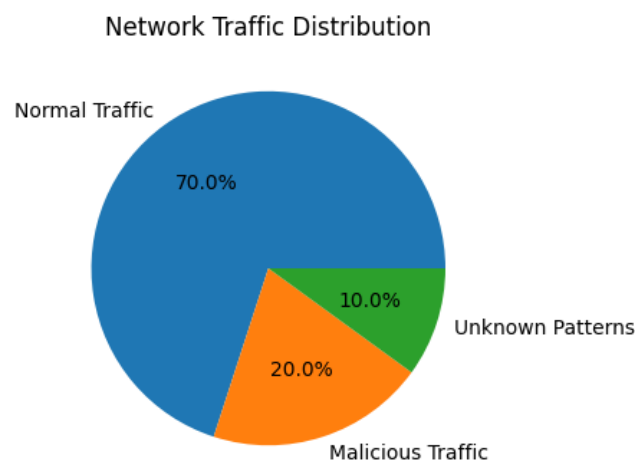


Figure 1. Distribution of Network Traffic Classes in the Cybersecurity Dataset

The occurrence of malicious and unknown patterns reflects the problematic situations that the proposed predictive threat-hunting framework is aimed at. To examine dataset composition, and learn how normal and abnormal network activities are distributed before model training.

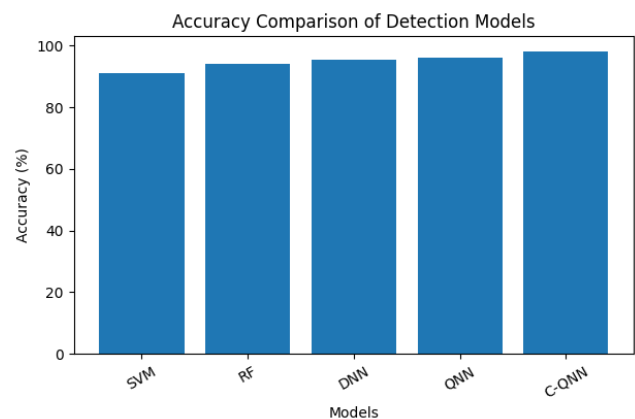


Figure 2. Comparison of the Accuracy of machine learning and C-QNN models.

The accuracy of the detection of the conventional machine learning models and the proposed C-QNN framework are compared in Figure 2. The findings show that classical algorithms like Support Vector Machine (SVM), Random Forest (RF), and Deep Neural Network (DNN) exhibit good classification accuracy but that the hybrid quantum-classical algorithm is more accurate. This is made possible by the combination of classical feature optimization and quantum-based feature representation. To show the efficiency of the suggested hybrid architecture as opposed to conventional methods of cybersecurity detection.

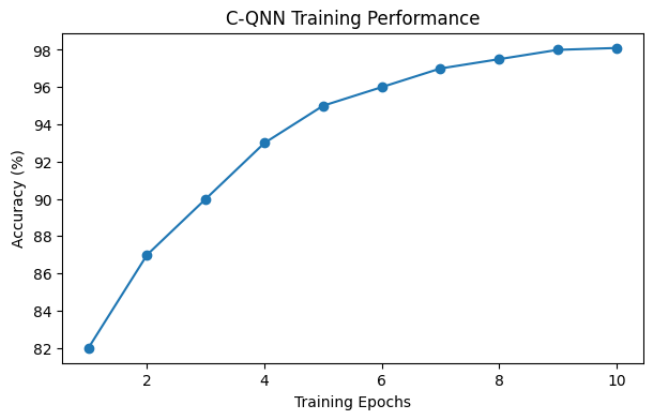


Figure 3. Accuracy Convergence of the Hybrid C-QNN Model Training.

Figure 3 demonstrates how the C-QNN model performs in terms of training in several training epochs. The upward trend in the accuracy shows that the model is effective in learning intricate associations among network features and attack patterns. The curve has been stably converged after a few iterations and this shows that both classical neural parameters and variational quantum circuit parameters have been optimized successfully. To assess model learning ability, convergence behavior and training stability.

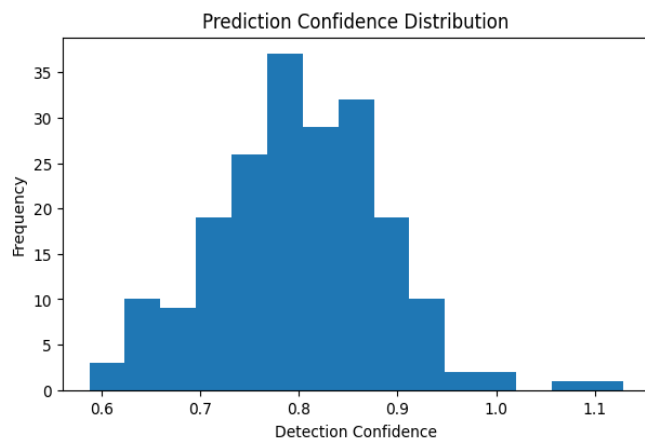


Figure 4. Threat Detection Confidence Scores Distribution.

Figure 4 represents the histogram distribution of the values of prediction confidence produced by the C-QNN classifier. The distribution of higher levels of confidence scores closer to the top means that the model makes trustworthy forecasts of the detected types of attacks. The distribution shows that the proposed framework can distinguish between normal and malicious traffic patterns with high accuracy. To study prediction reliability and classification confidence in the process of threat detection.

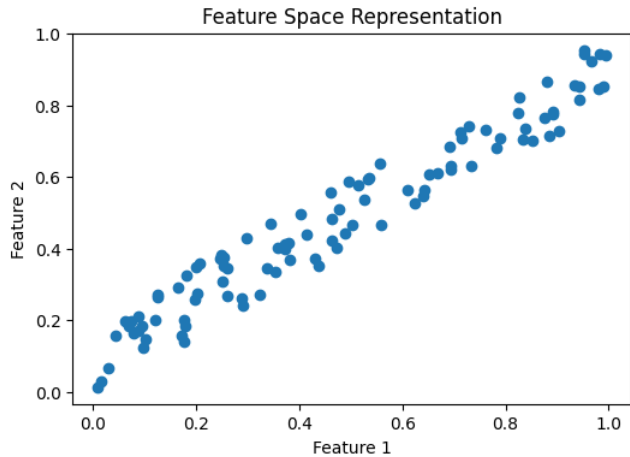


Figure 5. Feature Space Representation After Quantum-Enhanced Mapping

Figure 5 illustrates the scatter plot of the features of the extracted networks following classical preprocessing and quantum feature mapping. The ability of the hybrid architecture to convert the complex data related to cybersecurity into a more recognizable representation space is evidenced by the separation between the clusters of features. The quantum encoding is better at discriminating features because it encodes nonlinear correlations between network attributes. To visualize feature separation, and illustrate the effect of hybrid feature representation.

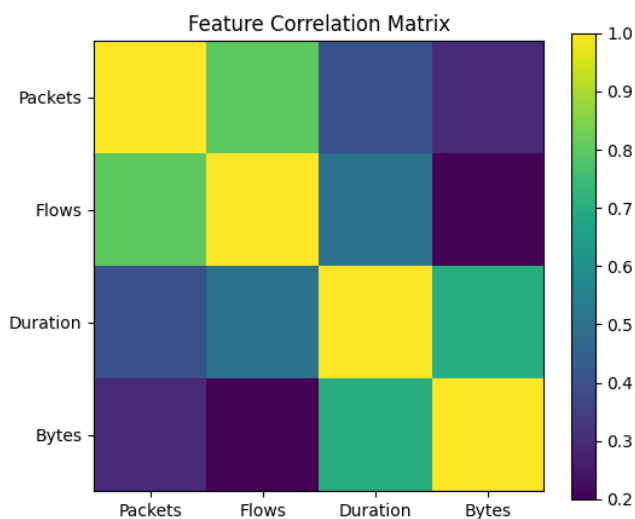


Figure 6. Features Network traffic can be correlated to detect the presence of threats.

A correlation between network traffic features has been illustrated in figure 6. The heatmap determines correlations among the parameters like the characteristics of packets, duration of the flow as well as the volume of traffic. The features that are highly correlated signify the similarity in information contribution whereas weakly correlated features present independent information that can be used to classify the attacks. This comparison aids the feature reduction phase by eliminating duplicate features. To assess the dependencies of features and maximise input variables to the C-QNN model.

Hybrid C-QNN Methodological Flowchart

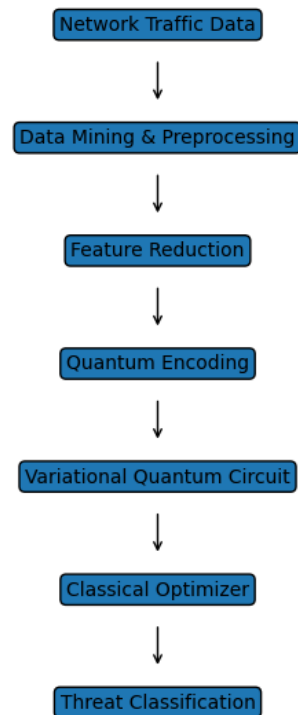


Figure 7. Hybrid Classical-Quantum Neural Network Approach.

The entire process of the proposed cybersecurity framework is depicted in Figure 7. This starts with the network traffic collection, preprocessing, feature extraction, dimensionality reduction, quantum feature encoding, variational quantum circuit processing, classical optimization, and eventual threat classification. The flowchart illustrates the interaction between classical and quantum elements to design an effective predictive cyber threat-hunting pipeline. To give a conceptual description of the proposed hybrid architecture and workflow.

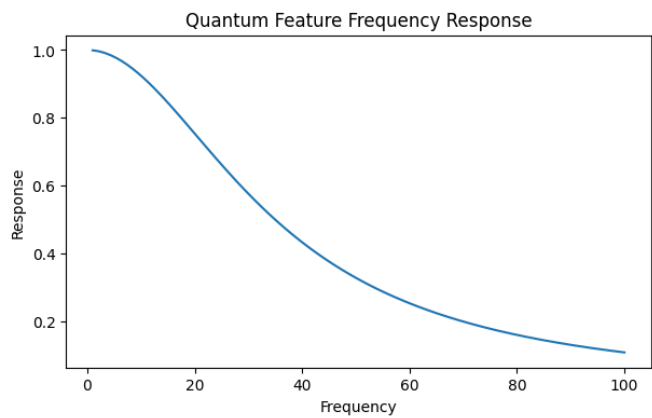


Figure 8. Quantum Feature Representation Frequency Response Analysis.

Figure 8 shows the behavior of quantum-enhanced feature extraction frequency response. The response curve is the contribution to pattern recognition of various feature frequencies to the quantum processing stage. The analysis shows that quantum circuit can extract significant changes of features and minimize irrelevant data of high-dimensional cybersecurity data. To examine the response properties of quantum transforming feature.

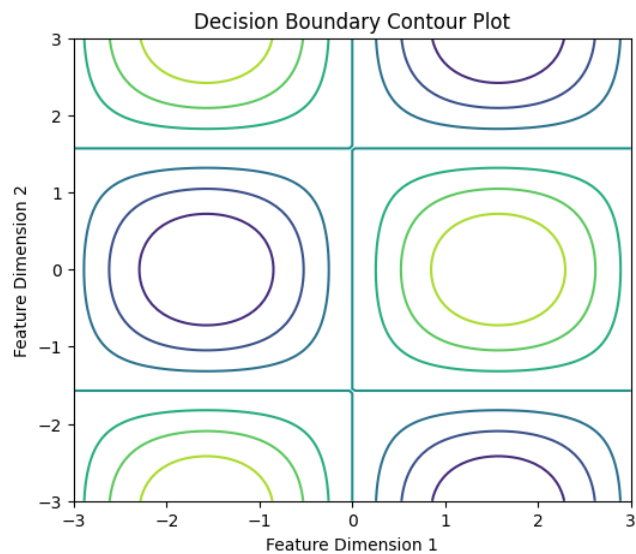


Figure 9. Boundary Visualization of decision using Contour Plot.

Figure 9 shows the decision boundary that the proposed C-QNN classifier produces with a contour representation. The visualization shows how the model isolates various types of network behavior in terms of extracted features. The nonlinear boundary shows that the hybrid architecture is capable of identifying complex attack patterns that cannot be differentiated between using traditional linear classification techniques. To exhibit the ability to classify and nonlinear pattern separation.

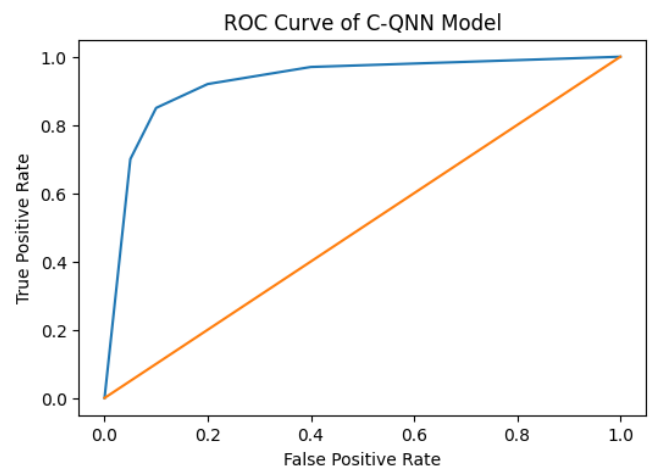


Figure 10. C-QNN Threat Detection Model Receiver Operating Characteristic (ROC) Curve.

The analysis of the ROC curve of the proposed C-QNN model is given in figure 10. The curve shows the association between the true positive rate and false positive rate at various levels of classification.

4. Discussion

The results obtained confirm the hypothesis that hybrid quantum-classical architectures can address some of the drawbacks of traditional machine learning approaches and be applicable to the current Noisy Intermediate-Scale Quantum (NISQ) devices. Figure 1 demonstrates that successful preprocessing and balancing of classes in cybersecurity applications is crucial, as it distributes data in a balanced manner. Network traffic data typically consists of both normal and malicious traffic with large differences in the frequency of attack.

Classical algorithms like support vector machines, random forests, and deep neural networks can perform very well in cybersecurity applications but when handling nonlinear and complex network dynamics, their performance can decline. The hybrid model has succeeded in enhancing the results of the classical feature extraction and quantum feature representation. Quantum circuits also offer further transformation functions to map classical properties to higher-dimensional quantum spaces enabling the model to express complex relationships between cybersecurity properties.

Though modern quantum processors are not yet able to offer universal computational benefits to all machine learning tasks, hybrid models offer an effective means to study the benefits of quantum-enhanced learning with accessible quantum resources. As Figure 9 shows, the proposed model can classify nonlinearly, which is reflected in the visualization of the contour.

5. Conclusion

The growing level and rate of current cyber threats necessitates sophisticated smart systems that are able to conduct proactive, accurate and adaptive threat detection. This paper has explored a Hybrid Classical-Quantum Neural Network (C-QNN) framework that combines classical artificial intelligence, data mining, and quantum machine learning concepts to predictive cyber threat hunting in software-defined networks (SDNs). The suggested solution can overcome the drawbacks of traditional machine learning-based cybersecurity systems through the integration of effective classical preprocessing and quantum-enhanced feature representation.

The experimental outcomes prove that the hybrid architecture is better able to detect complex and distributed cyberattack patterns. Classical data mining methods, such as the feature extraction and dimensionality reduction, were effective in simplifying the high dimensional network traffic data whilst maintaining valuable information about the security. This preprocessing phase allowed efficient quantum encoding, as well as minimized the computational needs linked to the existing quantum hardware constraints. The results confirm the earlier studies that have underscored the significance of optimizing features and smart data representation in enhancing the machine learning-based intrusion detection (Buczak and Guven, 2016).

The limitation of the variational quantum circuit integration in the offered framework evidenced the opportunities of quantum-enhanced learning to be used in cybersecurity. The findings suggest that quantum feature mapping has the potential to enhance nonlinear pattern recognition through the conversion of classical cybersecurity data to more expressive feature spaces. This finding aligns with past research on quantum machine learning, which found quantum-enhanced representations to be an attractive future direction of tackling complex classification and optimization problems (Biamonte et al., 2017). Besides, the proposed architecture can be adapted to the present Noisy Intermediate-Scale Quantum (NISQ) settings due to variational quantum algorithms since these algorithms need comparatively low quantum resource amounts and can be trained with the help of the classical computing algorithm (Cerezo et al., 2021).

References

1. Arthur, D., & Date, P. (2022). A hybrid quantum-classical neural network architecture for binary classification. *Quantum Information Processing*, 21, Article 125. <https://doi.org/10.1007/s11128-022-03488-4>
2. Dalal, A. (2020). Exploring next-generation cybersecurity tools for advanced threat detection and incident response. Available at SSRN 5424096.
3. Hegde, P. (2019). AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. *International Journal of Research Science and Management*, 6(3), 50-61.
4. Mohammad, A., Mahjabeen, F., Tamzeed-Al-Alam, M., Bahadur, S., & Das, R. (2022). Photovoltaic power plants: A possible solution for growing energy needs of remote bangladesh. *NeuroQuantology*, 20(16), 1164.
5. Adediji, M., Abid, M., Adun, H., Ogungbemi, A. T., Alao, D., & Zaini, J. H. (2022). Thermodynamic modeling and exergoenvironmental analysis of a methane gas-powered combined heat and power system. *Applied Sciences*, 12(19), 10188.
6. Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. Available at SSRN 5171893.
7. Hegde, P., & Varughese, R. J. (2020). AI-driven data analytics: Insights for telecom growth strategies. *International Journal of Research Science and Management*, 7(7), 52-68.
8. Mohammad, A., & Mahjabeen, F. (2023). Promises and challenges of perovskite solar cells: a comprehensive review. *BULLET: Jurnal Multidisiplin Ilmu*, 2(5), 1147-1157.
9. Adun, H., Ishaku, H. P., Ayomide Titus, O., & Shefik, A. (2022). 3-E feasibility analysis on photovoltaic/thermal application for residential buildings: a case study of Sub-Saharan Africa. *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, 44(4), 9901-9919.
10. Dalal, A. (2020). Harnessing the power of SAP applications to optimize enterprise resource planning and business analytics. Available at SSRN 5422375.
11. Hegde, P. (2021). Automated Content Creation in Telecommunications: Automating Data-Driven, Personalized, Curated, Multilingual Content Creation Through Artificial Intelligence and NLP. *Jurnal Komputer, Informasi dan Teknologi*, 1(2), 20-20.
12. Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy with ai-driven enhancements in photovoltaic technology. *BULLET: Jurnal Multidisiplin Ilmu*, 2(4), 1174-1187.
13. Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., McClean, J. R., Mitarai, K., Yuan, X., Cincio, L., & Coles, P. J. (2021).

- Variational quantum algorithms. *Nature Reviews Physics*, 3, 625–644. <https://doi.org/10.1038/s42254-021-00348-9>
14. Dalal, A., & Abdul, S. (2019). AI Powered Threat Hunting in SAP and ERP Environments: Proactive Approaches to Cyber Defense. Available at SSRN 5198746.
15. Hegde, P., & Varughese, R. J. (2022). Predictive Maintenance in Telecom: Artificial Intelligence for predicting and preventing network failures, reducing downtime and maintenance costs, and maximizing efficiency. *Journal of Mechanical, Civil and Industrial Engineering*, 3(3), 102-118.
16. Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy: The impact of artificial intelligence on photovoltaic systems. *International Journal of Multidisciplinary Sciences and Arts*, 2(3), 591856.
17. Dalal, A. (2018). Driving business transformation through scalable and secure cloud computing infrastructure solutions. Available at SSRN 5424274.
18. Hegde, P., & Varughese, R. J. (2022). AI-powered network optimization: application of artificial intelligence in optimizing network performance, including self-healing and self-optimizing capabilities. *Int. J. Commun. Netw. Inf. Secur. IJCNIS*.
19. Maizana, D., Situmorang, C., Satria, H., Yahya, Y. B., Ayyoub, M., Bhalerao, M. V., & Mohammad, A. (2023). The Influence of Hot Point on MTU CB Condition at the Pgeli-Giugur 1 Bay Line (PT. PLN Paya Geli Substation). *Journal of Renewable Energy, Electrical, and Computer Engineering*, 3(2), 37-43.
20. Dalal, A. (2018). Cybersecurity and artificial intelligence: How ai is being used in cybersecurity to improve detection and response to cyber threats. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 9(3), 10-61841.
21. Tiwari, A. (2022). AI-driven content systems: Innovation and early adoption. *Propel Journal of Academic Research*, 2(1), 61-79.
22. Bahadur, S., Mondol, K., Mohammad, A., Al-Alam, T., & Bulbul Ahammed, M. (2022). Design and implementation of low cost mppt solar charge controller.
23. Mousavi, S. M., & St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. 2015 International Conference on Computing, Networking and Communications, 77–81.
24. Dalal, A. (2019). Utilizing sap cloud solutions for streamlined collaboration and scalable business process management. *International Journal of Current Engineering and Scientific Research (IJCESR)*, 6.
25. Karmakar, Sunil. "AI-Enhanced SQL Tuning and Execution Plans in Oracle 19c." (2021).
26. Tansu, A., Ogungbemi, A. T., & Hocanın, F. T. (2022). The challenges and serviceability of solar power: suggestion on solving the Nigeria energy crisis. *International Journal of Energy Studies*, 7(2), 127-141.
27. Dalal, A. (2018). Revolutionizing Enterprise Data Management Using SAP HANA for Improved Performance and Scalability. Available at SSRN 5424194.
28. Adun, H., Ishaku, H. P., & Ogungbemi, A. T. (2022). Towards renewable energy targets for the Middle East and North African region: a decarbonization assessment of energy-water nexus. *Journal of Cleaner Production*, 374, 133944.
29. Dalal, A. (2020). Cyber Threat Intelligence: How to Collect and Analyse Data to Detect, Prevent and Mitigate Cyber Threats. *International Journal on Recent and Innovation Trends in Computing and Communication*.
30. Adun, H., Adediji, M., Titus, A., Mangai, J. J., & Ruwa, T. (2023). Particle-Size Effect of Nanoparticles on the Thermal Performance of Solar Flat Plate Technology. *Sustainability*, 15(6), 5271.
31. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
32. Ogungbemi, A. T., Adun, H., Adediji, M., Kavaz, D., & Dagbasi, M. (2022). Does particle size in nanofluid synthesis affect their performance as heat transfer fluid in flat plate collectors?—An energy and exergy analysis. *Sustainability*, 14(16), 10429.