

Exploring Hybrid Quantum Classical and Traditional Machining Learning Algorithms for Detecting Cyber Attacks

Jessy Akaabo¹, Collins Ifeanyi Osuji² and Austin Johnson³

¹Department of Mathematics and Computer Science, Benue State University, Makurdi, Nigeria.

²Department of Computer Science, Federal University, Wukari, Nigeria.

³Department of Physics, Benue State University, Makurdi, Nigeria.

Received 3 January 2025; Acceptance 6 March 2025; Published 17 April 2025.

Abstract

Worldwide internet usage is expanding quickly, creating numerous opportunities in a variety of industries, such as sports, education, entertainment, and finance. Since network technology has grown and become more widely used, it is crucial to manage, maintain, and monitor networks in a bid to maximize economic efficiency and maintain smooth operations. Nonetheless, a major setback of the internet is cyber-attack. This leverages various tools, techniques, and vulnerabilities in systems, social engineering, insider threats, malware and ransomware to get user credentials and gain access to target network and active assets. This study explores hybrid quantum classical and traditional machining learning algorithms for detecting cyber attack by analyzing the attributes of transmitted packets in benign and scan samples of network traffic data collected by Lawrence Berkeley National Laboratory. Several models such as Hybrid quantum classical model, Convolutional Neural Network, logistic regression, Random Forest, Gradient boosting and support vector classifier were used for training, evaluation and classification of the network traffic data and the results reveal that the hybrid quantum classical modeling terms of time efficiency obtained a training time of 2.36 seconds and evaluation times of 0.02 seconds. In as much as research on quantum computing just began to gain momentum and without a fully functional quantum computer yet in existence, Quantum computing algorithms are already in very close competition with known state-of-the-art algorithms, showing an experimental realization of quantum supremacy over older and existing classical computing.

Keywords: Hybrid, Quantum, Classical, Machine Learning, Cyber attack.

Introduction

Nowadays, the world is thought of as a global village due to interconnected networks. Digitalization has emerged as a result, impacting industries like banking, real estate, healthcare, and education. Information technology, which is responsible for the digitization we now experience, has also caused cyberspace to grow extraordinarily. Over the past few years, there has been a massive global increase in the number of internet users [1]. People now have many more options to conduct a wide range of daily small- and large-scale activities online, including social networking, online shopping, banking, and advertising, thanks to technological advancements in IT and the Internet. However, as a result of this expansion, a brand-new

Correspondence to: Jessy Akaabo, e-mail: akaabojessy@yahoo.com; and

Austin Johnson: ajohnson17@bsum.edu.ng

criminal activity known as cybercrime has finally emerged [2]. Computers, smartphones, and other electronic devices are used in cyberspace crimes and poses a detrimental effect on enterprises by stealing vital data from compromised networks or shutting down victims' servers. The main source of these assault is that many endpoints' software lacks built-in security protections and requires frequent upgrades, which makes it easy for attackers to hack them, combine them into a botnet, and use that botnet to send malicious traffic [3]. For majority of applications, particularly those deemed crucial (like Internet Banking), having its assets compromised or being taken offline for an extended period of time is inadmissible due to the loss of revenue it will cause. However, to prevent cyberattacks from stopping corporate activities, it is increasingly essential to understand early threat detection and mitigation strategies [4].

The development of computer networks has changed society and increased the frequency and sophistication of cyberattacks. Cyberattacks are disruptive actions directed at computer systems, networks, or data. They are often planned, coordinated, and entail a series of steps to accomplish their objectives, which primarily include gaining unauthorized access, interrupting services, and stealing data. Maintaining privacy and trust requires safeguarding data against breaches, since more and more private and confidential information is kept online. According to Verizon Business's 2023 Data Breach Investigations Report, 83% of data breaches contained sensitive personal data. Furthermore, IBM 2024 reports that in 2023, the average cost of a data breach rose to USD 4.45 million, up by USD 100,000 from the previous year. This represents a 2.3% increase above the USD 4.35 million average cost from 2022 [5]. In terms of network administration and security, network traffic identification and categorization are crucial. In terms of security, it aids in keeping an eye on the network's services, such as intrusion detection, malware traffic identification and categorization, and application traffic generation. Several attempts have been made to classify internet traffic like Port Based, Pay Load Based and traditional Machine Learning Based technique. The most common technique being the traditional Machine Learning (ML) technique suffers different forms of setback one of which is its inability to process multiple calculation at a time, which makes it not well-suited for handling large amounts of data or performing complex calculations quickly making it difficult for classical computers to effectively analyse and respond to cyber threats in real-time.

Different studies exist in the literature on computational modeling of cyber systems [5-7]. In their study, Lin et al in [8] proposed a time-related intrusion detection system that uses a stacked sparse autoencoder (SSAE) and variations of a recurrent neural network (RNN) on a dataset called UNSW-NB15. The dataset has 42 features, including flow, basic, content, time, and other generated features to detect network issues. During the research, to extract features using the greedy layer-wise strategy, a stacked sparse autoencoder (SSAE) is first constructed. This uses a non-linear transformation from high dimensional data space to low dimensional data space, which results in selective activation of neurons that help make encoded data easier to distinguish and well referred to after which single LSTM layer is connected. To fully utilize deep neural networks' learning capabilities, a batch normalization technique was used to compare the performance of four distinct RNN cell variations. Our time-related model has been shown to be successful in intrusion detection based on the analysis of the time-related parameter timestep. With a false alarm rate of 1.8% and an accuracy of over 98%, the experiment outperforms certain deep neural network and machine learning-based techniques. Similarly, Ahmad et al in [9] presented a quantum-enhanced approach to network intrusion detection that uses unsupervised Quantum Machine Learning (QML). In order to ascertain how successfully autoencoders can provide an encoding with PDFs related to the input variables and how the output can be used to interface with quantum computing systems, an NSL-KDD dataset was used. The study employed an autoencoder to preprocess the data and reduce dimensionality. The model was evaluated using the Quantum Support Vector Machines (QSVMs) technique, which was built using the Qiskit quantum computing platform. According to the study, the kernel matrices produced by the QSVM

algorithm were more unique, which improved the separability of the data classes. It also demonstrated the potential of autoencoders to produce an encoding with PDFs related to its input variables, allowing for unsupervised learning. More so, the results of the study show that the Quantum-Assisted NIDS based on the proposed approach achieved an accuracy of 0.92% in classifying network flows rivaling SVM with an accuracy of 0.93%. Future research, according to the study, should concentrate on examining the possibilities of quantum machine learning in the context of network intrusion detection using larger-scale quantum computers, which are capable of processing vast volumes of data quickly, carrying out a variety of complex calculations, and quickly identifying cyberthreats. Overall, there is a paradigm shift in computational modeling of cyber systems for which quantum computing seems to be taking the lead. It is on this premise that this study aims to exploring hybrid quantum classical and traditional machining learning algorithms for cyber attack detection prediction and prevention.

Research Method

The aim of the study was to evaluate the hybrid quantum-classical model [10], Convolutional Neural Network (CNN) and traditional machine learning models developed for the analyses of benign and scan samples from several thousand internal hosts collected by Lawrence Berkeley National Laboratory. The development of the hybrid quantum-classical model which combines a classical neural network layer with a single qubit simple variational quantum circuit layer was done using Google Colab, and a cloud-based Jupyter notebook environment that provides free GPU support making it suitable for machine learning experiments. Qiskit which is an open-source software development kit (SDK) designed for working with quantum computers at various levels, including circuits, pulses, and algorithms was used for the quantum circuit creation, simulation, and execution. At the Quantum Circuit Layer, the qubit is put into a superposition state using the Hadamard gate, and then a phase rotation is applied using the parameterized Rz gate. Finally, a measurement is performed to guarantees that all qubits are measured in the computational basis ($|0\rangle, |1\rangle$) and their states recorded in classical bits to obtain classical information from the quantum system. By specifying number of shots, the accuracy level of the model was adjusted based on their computational resources and requirements.

The performance of the hybrid quantum-classical model is assessed using various metrics to gauge its effectiveness in classifying benign and scan samples. The primary performance metric utilized is accuracy, which measures the proportion of correctly classified samples out of the total number of samples in the test set. In addition to the hybrid quantum-classical approach, the dataset was also evaluated against state-of-the-art deep neural network and traditional machine learning models such as Logistic Regression; Random Forest; Gradient Boosting; Support Vector Classifier for the purpose of comparison.

Results and Discussion

Evaluating the performance of the hybrid quantum-classical model is crucial in ascertaining the models effectiveness in classifying cyber security data within a network. The key metrics employed for the purpose of evaluating the models in this research include Accuracy, Precision, Recall, and F1 Score.

Additionally, epoch vs. loss and epoch vs. accuracy plots offers important insights into the training dynamics of the models, showcasing how the loss and accuracy evolve over training epochs.

The results obtained from both the hybrid quantum-classical approach and traditional machine learning models undergo meticulous analysis and comparison to derive actionable insights.

Table1. Comparative analysis between the hybrid quantum classical model and other traditional machine learning models performances

	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Hybrid Quantum-Classical	99.74	99.74	99.87	99.80
CNN	99.99	99.99	100.00	99.99
Random Forest	99.98	100.00	100.00	100.00
Gradient Boosting	99.99	100.00	100.00	100.00
Support Vector Classifier	99.98	99.99	99.99	99.99

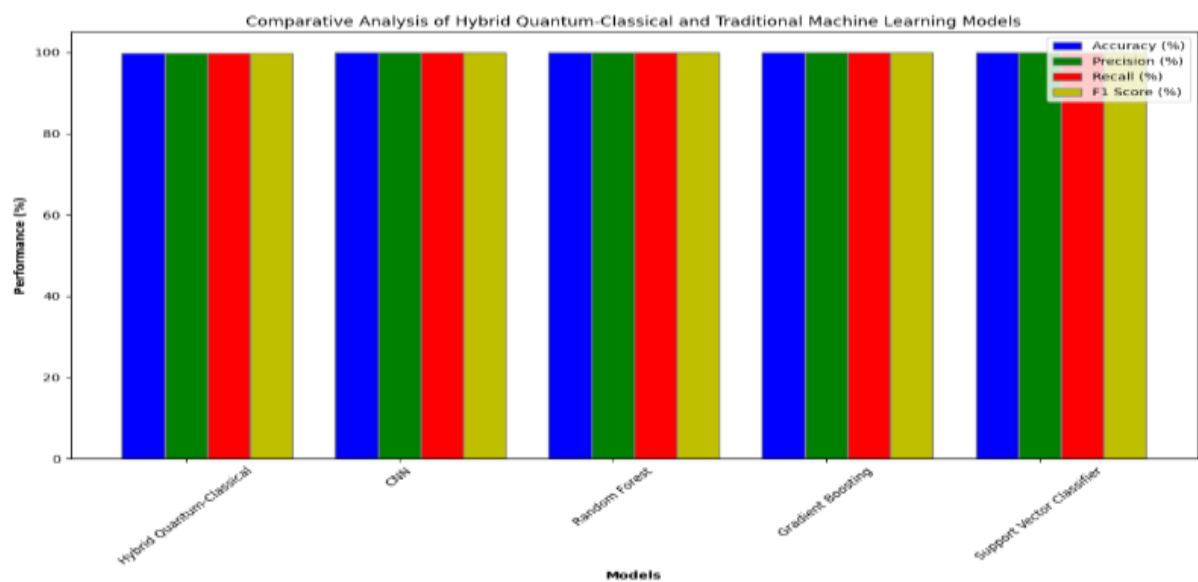


Figure1. A comparative plot of the performance metrics of each model

This is the comparative analysis of the results:

Performance Comparison:

Accuracy

All the other traditional machine learning models, including Random Forest, were able to achieve 99% accuracy. The hybrid quantum-classical approach also performed remarkably well with an accuracy of 99%.

Precision

Random Forest and Gradient Boosting achieved perfect precision scores of 100%, while the SVM and CNN got 99%, indicating their ability to minimize false positives. The hybrid approach also achieved a high precision score of 99%.

Recall

Random Forest, Gradient Boosting, and CNN demonstrated perfect recall scores of 100%, while the SVM got 99%, indicating their sensitivity in capturing true positives. The hybrid approach achieved a recall score of 99%.

F1 Score

Random Forest and Gradient Boosting achieved perfect F1 scores of 100%, while the CNN got 99%, reflecting a balanced performance between precision and recall. The hybrid approach achieved an F1 score of 99%.

Computational Training and Evaluation Time Comparison**Hybrid Quantum-Classical VS CNN**

The QNN completes training in approximately 2.36 seconds by iterating over 10 epochs, whereas the CNN requires 300.09 seconds for training alone. This significant difference in training time highlights the QNN's efficiency in achieving convergence with much lower computational overhead compared to the CNN, demonstrating its potential for efficient training. Similarly, QNN demonstrates substantially lower evaluation time compared to CNN. With an evaluation time of approximately 0.02 seconds, QNN exhibits rapid inference capabilities, suiting it for real-time applications where the ability to make decisions quickly is crucial. In contrast, the CNN's evaluation time of 5.40 seconds underscores the substantial computational resources required for validating a deep learning model with multiple layers and parameters.

Hybrid Quantum-Classical VS Classical Scikit Learn ML models

The time efficiency of the Hybrid Quantum-Classical model is striking when compared to traditional machine learning models. The Hybrid Quantum-Classical model demonstrated a significant advantage in both training and evaluation times compared to all classical models. Despite Random Forest showing relatively short training and evaluation times (13.79 seconds and 0.77 seconds, respectively), the Hybrid Quantum-Classical model was substantially faster with training completed in 2.36 seconds and evaluation in just 0.02 seconds.

Table 2. Comparative analysis between the hybrid quantum classical model and other traditional machine learning models training and evaluation time.

Model	Training Time (seconds)	Evaluation Time (seconds)
Hybrid Quantum-Classical	2.3579	0.0164
CNN	300.0925	5.4010
Random Forest	13.7930	0.7718
Gradient Boosting	221.8108	0.6687
Support Vector Classifier	10.6517	8.2519

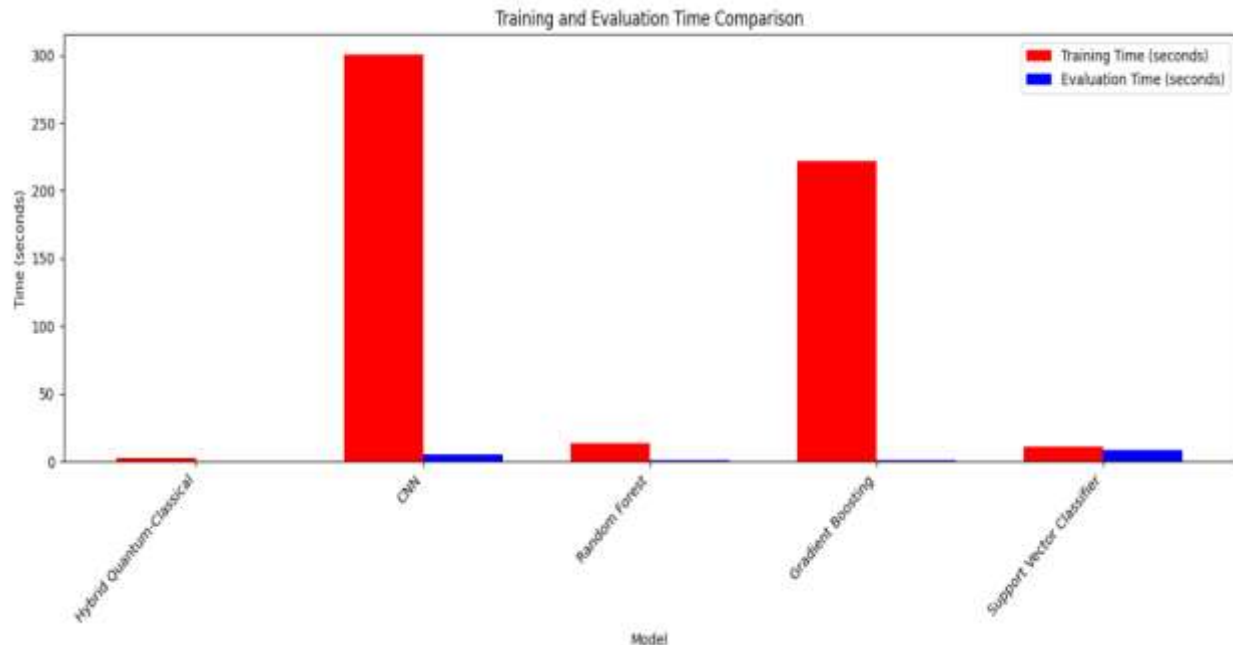


Figure 2. A comparative plot of the various training and evaluation time of each model

This efficiency highlights the potential of quantum-enhanced models to not only match but exceed traditional methods in computational speed. The Hybrid Quantum-Classical model's rapid training and evaluation times, combined with its robust performance in accuracy and precision, make it a highly promising tool for applications requiring swift and reliable classification, such as in cyber security [11-12]. Through meticulous evaluation and comparison, this study sheds light on how effective hybrid quantum classical and traditional machine learning models are and applicability in real-world scenarios. From the results, the hybrid quantum-classical approach seamlessly integrated classical neural network layers with a quantum-classical layer, leveraging both classical and quantum computing paradigms, demonstrated excellent results that outperformed the ones of the traditional models. Additionally, it received F1 rating of 99% with outstanding accuracy, precision, and recall, albeit slightly trailing behind some traditional machine learning models in terms of precision and recall scores.

Conclusion

The study concludes that the Hybrid Quantum-Classical model demonstrates competitive performance, achieving accuracy comparable to traditional machine learning models, all of which reached approximately 99%. While some traditional models outperformed the Hybrid Quantum-Classical model in terms of precision and recall, achieving 100% in both metrics, the hybrid approach exhibited superior training and evaluation times, significantly outperforming the classical models. Moreover, the Hybrid Quantum-Classical model's efficiency in computational time for both training and evaluation highlights its potential for real-world applications, especially in scenarios where time is critical. Despite this, traditional machine learning models, particularly Random Forest and Gradient Boosting, continue to excel in classification accuracy, precision, and reliability. Invariably, these models remain robust and effective options for deployment in operational settings, particularly in cyber security applications where high accuracy and reliability are essential. Based on these results, the study recommends that further advancements in quantum computing technology could

amplify the benefits observed in the hybrid model. As quantum processors become more powerful and accessible, their integration with classical machine learning techniques will likely result in even greater improvements in anomaly detection accuracy and efficiency. Therefore, it is crucial for the cyber security industry to continue monitoring developments in quantum computing and be prepared to incorporate these advancements into their security strategies.

References

1. Hussain, A. H., Hasan, M.N., Prince, N. U., Islam, M. M., Islam, S. and Hasan, S.K. (2021). Enhancing cyber security using quantum computing and Artificial Intelligence: A review. *World Journal of Advanced Research and Reviews*, 10 (3): 448-456.
2. Ibor, A. E., Oladeji, F. A., & Okunoye, O. B. (2018). A survey of cyber security approaches for attack detection prediction and prevention. *International Journal of Security and its Applications*, 12(4): 15-28.
3. Draper-Gil, G., Lashkari, A. H., Mamun, M. S. I., & Ghorbani, A. A. (2016). Characterization of encrypted and vpn traffic using time-related. In *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, pp. 407-414.
4. Pimenta Rodrigues, G. A., de Oliveira Albuquerque, R., Gomes de Deus, F. E., de Sousa Jr, R. T., de Oliveira Júnior, G. A., Garcia Villalba, L. J., & Kim, T. H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. *Applied Sciences*, 7(10): 10-82.
5. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*. 17(2): 2071-8330.
6. Naresh, S. (2011). Are Quantum Computers the Future of Fast Computation, *International Journal of Science and Research*, 10, 219-220.
7. Gharibvand, V., Karimzadeh, K., Mohammad, Z., Qasim, C., Zeki, Sahmani, S., Asmael, M. & Safaei, B. (2024). Cloud based manufacturing: A review of recent developments in architectures, technologies, infrastructures, platforms and associated challenges. *The International Journal of Advanced Manufacturing Technology*. 131. 1-31. 10.1007/s00170-024-12989-y.
8. Lin, Y., Wang, J., Tu, Y., Chen, L., & Dou, Z. (2019). Time-Related Network Intrusion Detection Model: a deep learning method. *2015 IEEE Global Communications Conference (GLOBECOM)*, 1–6. <https://doi.org/10.1109/globecom38437.2019.9013302>
9. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1). <https://doi.org/10.1002/ett.4150>
10. Akaabo et al. (2025). Investigation of Benign and Scan Samples of Cyber Security Network Traffic Data: A Hybrid Quantum- Classical Study. *Scholar J Computational Science*, 2(2). DOI: 10.5281/zenodo.14947966

11. Mehmet, T. (2021). Future Networks, Services and Management Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing. Springer. <https://doi.org/10.1007/978-3-030-81961-3>
12. Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017, January). Malware traffic classification using convolutional neural network for representation learning. In 2017 International conference on information networking (ICOIN) (pp. 712-717). IEEE.

Publisher's Note: *Scholar J* remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.