International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.564
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3799-3802

Quantum Machine Learning Techniques for Network Defense: Comparative Study of Quantum vs. Classical Approaches

Rosemary J[1], Adrishya Maria Abraham[2]
[1,2]Assistant Professor, Kristu Jyoti College of Management and Technology, Changanacherry, Kerala, India.
Emails: *rosemary@kjcmt.ac.in[1], adrishya@kjcmt.ac.in[2]*

Abstract
With the potential for quantum computing to completely transform cybersecurity, quantum machine learning is becoming a ground-breaking technology. Cyber-attacks have been successfully countered by traditional network defense systems, which mostly use conventional machine learning (ML) techniques. However, the growing complexity of assaults and the exponential expansion of network data reveal the shortcomings of traditional methods, especially with regard to speed and scalability. By utilizing quantum algorithms like Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), and Variational Quantum Circuits (VQC), Quantum Machine Learning (QML) presents a viable substitute. These methods are especially well-suited for real-time network defense scenarios since they show the capacity to handle high-dimensional data, identify complex patterns, and increase computational efficiency. In this research, the effectiveness of QML techniques in network defense is thoroughly examined and contrasted with that of traditional machine learning techniques. The study emphasizes how QML may surpass conventional models in terms of accuracy, scalability, and resilience against sophisticated threats by concentrating on use cases like intrusion detection, malware analysis, and anomaly detection. The necessity for hybrid quantum-classical models and the present constraints of quantum hardware are among the difficulties that are discussed in the study. This study highlights the revolutionary potential of QML in strengthening network defense mechanisms and identifies crucial areas for further research, paving the road for a secure digital future by combining theoretical ideas with experimental discoveries.

Keywords: *Classical Machine Learning, Network Defense, Quantum Machine Learning*

1. Introduction
The emergence of quantum computing has brought about revolutionary changes in a number of scientific fields, with cybersecurity being one of the key beneficiaries. The computational and scalability constraints of traditional machine learning (ML) techniques, which have been crucial in tackling network defence issues, are currently being reached. Exploring sophisticated computational techniques has become necessary due to the growing complexity of cyberthreats and the need for real-time data processing. By improving accuracy and efficiency, quantum machine learning (QML), which makes use of the concepts of entanglement and superposition, has the potential to completely transform network defence systems. This study explores the intersection of machine learning and quantum computing, providing a thorough analysis of the literature that charts the evolution of QML, its underlying algorithms, and its uses in cybersecurity. The foundation for contemporary developments was established by the historical development of computation. From the earliest counting devices to the introduction of transistors in the 1950s, computing advanced quickly, with Turing machines and the von Neumann architecture serving as the foundation for classical computing. However, constraints on integrated circuit transistor density and processing speed opened the door for the investigation of alternative paradigms, which ultimately led to the development of quantum computing (Moore, 1964; Turing, 1969). By enhancing conventional ML techniques with quantum algorithms, QML connects the dots between ML and quantum computing. The Harrow-Hassidim-Lloyd (HHL) method and other seminal work showed how quantum principles may speed up linear algebra computations, which are essential to many machine learning applications. Principal component analysis

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.564
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3799-3802

and support vector machines have seen exponential speedups as a result of these developments (Harrow et al., 2009; Rebentrostet al., 2014). There is growing scholarly and practical interest in the application of artificial intelligence (AI) to cybersecurity and education. While bringing up ethical issues such as algorithmic bias and data privacy, emphasises that AI has the ability to revolutionise education by personalising it. Similar to this, investigate how AI and quantum computing intersect in cybersecurity, highlighting AI's function in protecting systems from advanced cyberthreats. (Antony.,2024; Singh and Goyal.,2024). In their 2024 study, Singh and Goyal explore the ways in which AI and quantum computing can work together to transform cybersecurity. They go over how threat detection can be sped up with quantum machine learning (QML), which offers unmatched computing benefits over traditional techniques. Cybersecurity systems can better analyse high-dimensional data by utilising quantum techniques, opening the door for improved network defences [1-4].

2. Method

This study evaluates Quantum Machine Learning (QML) and Classical Machine Learning (CML) techniques for network defense. Publicly available datasets like NSL-KDD and CICIDS2017 are used to test and compare both methods.

2.1.Steps

2.1.1.Select Algorithms

- QML: Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN).
- CML: Decision Trees, Support Vector Machines (SVM).

2.1.2.Pre-process Data

- Clean and normalize datasets.
- Extract features to enhance model accuracy.

2.1.3.Train and test models

- Evaluate metrics like accuracy, speed, and scalability.

2.2.Tools

- **QML:** IBM Quantum Experience, Google Cirq.
- **CML:** Scikit-learn.
- **Data Analysis:** Excel or Python-based libraries for results

2.3.Validation

Results are validated using cross-validation and comparisons with existing benchmarks.

2.4.Tables

Table 1 Algorithm Comparison Table

Algorithm Type	Algorithm Name	Key Features
QML	Quantum Support Vector (QSVM)	Exploits quantum superposition for classification
QML	Quantum Neural Networks (QNN)	Efficient pattern recognition in high dimensions
CML	Decision Trees	Simple and interpretable model
CML	Support Vector Machines (SVM)	Effective for linear and non-linear data

QSVM and QNN algorithms leverage quantum superposition and entanglement to process high-dimensional data more efficiently than classical methods. Table 1, Decision Trees are interpretable models ideal for smaller datasets, while SVMs are robust for both linear and non-linear classification tasks [5-7].

Table 2 Dataset Summary Table

Dataset Name	Total Records	Features	Use Case Example
NSL-KDD	125,973	41	Intrusion detection
CICIDS2017	2,830,743	80	Network traffic analysis

NSL-KDD is an improved version of the KDD CUP 99 dataset, Table 2 specifically designed to address redundancy and irrelevant records for intrusion detection research. CICIDS2017 is a comprehensive

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.564
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3799-3802

dataset created to simulate realistic network traffic, including benign and malicious activities [8-10].

3. Results and Discussion

3.1. Results

- **Accuracy**
  1. QML models (e.g., QSVM, QNN) typically demonstrate better accuracy in detecting network anomalies and malware, especially in high-dimensional datasets.
  2. CML models like SVM or Decision Trees may perform well on smaller, simpler datasets but can struggle with scalability.
- **Efficiency:**
  1. QML offers speedup in processing complex computations due to quantum parallelism.
  2. For smaller datasets or low-complexity tasks, classical methods are faster due to simpler implementation and lower hardware requirements.
- **Scalability:**
  1. QML: Better scalability for handling high-dimensional data due to quantum state representations.
  2. CML: Performance deteriorates as the dataset size and complexity increase.

3.2. Discussion

This paper provides important insights into the possible advantages and difficulties of using quantum computing in cybersecurity by comparing quantum machine learning (QML) with classical machine learning (ML) approaches for network defense. Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN) are two examples of QML algorithms that consistently outperform their conventional counterparts in terms of performance. This is especially noticeable when dealing with high-dimensional, complicated datasets, when QML models show noticeably better accuracy and efficiency. Despite the encouraging outcomes, the actual implementation of large-scale QML applications is severely restricted by the constraints of current quantum hardware, such as noise and qubit coherence. The study's performance improvements are mostly theoretical, and unless quantum hardware develops further, they could not be fully achievable in practical settings.

- **Hybrid Methods:** Based on the study, hybrid methods that combine the advantages of quantum and classical computing could provide a more workable and effective network defense solution. Hybrid models may be able to get around the drawbacks of both classical and quantum computing by using classical hardware for data pretreatment and post-processing chores and quantum hardware for computationally demanding processes.
- **Effects on Network Defense:** The study's conclusions have important significance for network defense. QML has the potential to completely transform network security by utilizing the capability of quantum computing to enable anomaly detection, intrusion prevention, and more precise and effective cyberattack detection. However, more developments in quantum hardware and the creation of reliable QML algorithms that can lessen the impacts of noise and decoherence are necessary to realize this potential [11-12].

Conclusion

This study offers a thorough analysis of QML strategies for network defense. It illustrates how QML may greatly improve network security systems' scalability, accuracy, and speed. Although the full potential of QML is currently limited by the constraints of quantum hardware, these issues should be resolved with continued study and technical breakthroughs. By combining classical and quantum technology, network defense will advance and provide a more robust and safer online environment.

References

[1]. Alchieri, Leonardo, et al. “An Introduction to Quantum Machine Learning: From Quantum Logic to Quantum Deep Learning.” Quantum Machine Intelligence, vol. 3, no. 2, 15 Nov. 2021, https://doi.org/10.1007/s42484-021-00056-8.

[2]. Alluhaibi, Reyadh. “Quantum Machine Learning for Advanced Threat Detection in

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.564
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3799-3802

Cybersecurity." International Journal of Safety and Security Engineering, vol. 14, no. 3, 24 June 2024, pp. 875–883, https://doi.org/10.18280/ijsse.140319. Accessed 28 Oct. 2024.

[3]. Cerezo, M., et al. "Challenges and Opportunities in Quantum Machine Learning." Nature Computational Science, vol. 2, no. 9, 1 Sept. 2022, pp. 567–576, www.nature.com/articles/s43588-022-00311-3, https:// doi.org/10.1038/s43588-022-00311-3.

[4]. Mahesh, Batta. "Machine Learning Algorithms - a Review." International Journal of Science and Research (IJSR) ResearchGate Impact Factor, vol. 9, no. 1, 2018, www.ijsr.net/archive/v9i1/ART20203995.pdf, https://doi.org/10.21275/ART20203995.

[5]. M. S. Akter et al., "Exploring the Vulnerabilities of Machine Learning and Quantum Machine Learning to Adversarial Attacks Using a Malware Dataset: A Comparative Analysis," 2023 IEEE International Conference on Software Services Engineering (SSE), Chicago, IL, USA,2023, pp. 222-231, doi:10.1109/SSE60056.2023.00037

[6]. Pujari, M., Pacheco, Y., Cherukuri, B., & Sun, W. (2022). A Comparative Study on the Impact of Adversarial Machine Learning Attacks on Contemporary Intrusion Detection Datasets. SN Computer Science, 3(5). https://doi.org/10.1007/s42979-022-01321-8

[7]. Schuld, Maria, and Nathan Killoran. "Is Quantum Advantage the Right Goal for Quantum Machine Learning?" PRX Quantum, vol. 3, no. 3, 14 July 2022, https://doi.org/10.1103/prxquantum.3.030101.

[8]. Tychola, Kyriaki A., et al. "Quantum Machine Learning—an Overview." Electronics, vol. 12, no. 11, 1 Jan. 2023, p. 2379,www.mdpi.com/20799292/12/11/2379, https://doi.org/10.3390/electronics12112379.

[9]. Zeguendry, Amine, et al. "Quantum Machine Learning: A Review and Case Studies." Entropy, vol. 25, no. 2, 1 Feb. 2023, p. 287, www.mdpi.com/1099-4300/25/2/287, https://doi.org/10.3390/e25020287.

[10]. K Naja, SF Yelin, et al. "The development of quantum machine learning" https:// assets.pubpub.org/05lwd2lr/5a9fd72c-212a-4a7d-91ba-07219d24359d.pdf

[11]. T Bikku, SB Chandolu, et al "Enhancing Real-Time Malware Analysis with Quantum Neural Networks" https:/ /www.researchgate.net/profile/SPraveen/publication/378658707_Enhancing_RealTime_Malware_Analysis_with_Quantum_Neural_Networks/links/65e2d7beadc608480af5372c/Enhancing-Real-Time-Malware-Analysis-with-Quantum-Neural-Networks.pdf

[12]. MM Singh, A Goyal "A Study of Quantum Computing and AI: The Future of Cyber-Security and Cryptography" https:// ajantaprakashan.in/pdf/National%20Conference_ISBN/PDF.pdf#page=44