International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Developing intelligent cyber threat detection systems through quantum computing

Muhammed Azeez [1, *], Christopher Tetteh Nenebi [2], Victor Hammed [3], Lawrence Kofi Asiam [4], Edward James Isoghie [5], Oluwaseun R Adesanya [6] and Tomisin Abimbola [7]

[1] *Department of Mathematics, Lamar University, Beaumont, TX, USA.*
[2] *Department of Computation Data Science and Engineering North Carolina A & T State University, Greensboro, NC, USA*
[3] *Joint School of Nanoscience and Nanoengineering, North Carolina A&T States University, NC, USA.*
[4] *Master of Business Administration (MBA) Program, University of North Alabama, Florence, AL USA.*
[5] *Department of Industrial Engineering, Centre for Human Systems Engineering, University of Louisville, KY, USA.*
[6] *School of International Business, Lincoln University, Oakland, CA, USA.*
[7] *Department of Software Engineering, Wipro Technologies, Tallinn Estonia.*

International Journal of Science and Research Archive, 2024, 12(02), 1297–1307

Publication history: Received on 17 June 2024; revised on 24 July 2024; accepted on 26 July 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1369

Abstract

In the face of increasingly sophisticated cyber threats, traditional detection systems often fall short in protecting critical supply chains. This research presents the development and evaluation of an intelligent cyber threat detection system integrating Quantum Computing (QC) and Artificial Intelligence (AI). The proposed system significantly enhances detection accuracy, reduces latency, and improves resource efficiency compared to traditional methods. Quantum algorithms, such as Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN), demonstrated superior performance with accuracies of 95.2% and 96.7%, respectively. The system achieved high detection rates for various cyber threats, including malware, phishing, ransomware, and advanced persistent threats (APTs), with reduced false positive rates. The integration of QC also resulted in faster threat detection and response times, with system latency halved across key components. These advancements provide substantial benefits for cyber threat response in supply chains, ensuring robust protection of financial transactions and critical infrastructure. The enhanced scalability and efficiency make the system a valuable asset for safeguarding the United States' financial sector against sophisticated cyber-attacks.

Keywords: Quantum Computing; Artificial Intelligence; Cyber Threat Detection; Supply Chain Security; Quantum Support Vector Machines; Quantum Neural Networks

1. Introduction

In today's digital landscape, the complexity and frequency of cyber threats are increasing at an unprecedented rate. Cyber attackers are employing more sophisticated techniques, posing significant challenges to traditional cyber threat detection systems. These conventional systems often struggle to keep pace with the rapidly evolving threat landscape, resulting in delayed or inaccurate threat detection and mitigation. Consequently, there is an urgent need for advanced technologies to enhance the efficiency and accuracy of cyber threat detection systems.

Quantum Computing (QC) offers a promising solution to this pressing problem. By leveraging the principles of quantum mechanics, QC provides unparalleled computational power, enabling the development of advanced algorithms capable of solving complex problems that are intractable for classical computers (Ladd et al., 2010). Quantum algorithms, particularly those designed for pattern recognition and anomaly detection, have shown significant potential in enhancing cybersecurity measures (Shor, 1997). The inherent parallelism of quantum computing allows it to process

* Corresponding author: Muhammed Azeez

vast amounts of data simultaneously, which is crucial for identifying subtle patterns indicative of cyber threats (Grover, 1996).

In parallel, Artificial Intelligence (AI) has emerged as a transformative technology in cybersecurity. AI techniques, especially machine learning and deep learning, have been widely adopted for real-time threat detection and mitigation. AI models can analyze large datasets of cyber threat intelligence, learning to recognize patterns and anomalies that signify potential attacks (Goodfellow, Bengio, & Courville, 2016). The integration of AI into cybersecurity systems has led to significant improvements in detecting and responding to threats, reducing the time required to identify and neutralize malicious activities (Schmidhuber, 2015).

The combination of Quantum Computing and AI holds great promise for developing intelligent cyber threat detection systems. By integrating QC's computational power with AI's analytical capabilities, it is possible to create a system that not only detects threats with higher accuracy but also responds to them in real time. This integrated approach can significantly enhance the security posture of organizations, particularly in critical sectors such as finance, healthcare, and national security (Preskill, 2018).

This research aims to design and evaluate an intelligent cyber threat detection system that leverages the computational power of Quantum Computing and the analytical capabilities of AI. We hypothesize that integrating QC with AI will significantly enhance the detection accuracy and response time of cyber threat detection systems, addressing the limitations of traditional methods. This paper will discuss the development and implementation of such a system, the methodologies used to evaluate its performance, and the results obtained from various testing scenarios.

1.1. Research Statement

This research aims to develop an intelligent cyber threat detection system by integrating the computational power of Quantum Computing (QC) with the analytical capabilities of Artificial Intelligence (AI). The objective is to design, implement, and evaluate a system that can detect and mitigate cyber threats with significantly higher accuracy and efficiency compared to traditional methods. The hypothesis driving this research is that the combined use of QC and AI will enhance the detection accuracy and response time of cyber threat detection systems, addressing the critical limitations of existing solutions.

Traditional cyber threat detection systems, which rely on classical computational methods, often struggle to keep up with the rapidly evolving landscape of cyber threats. These systems are limited in their ability to process and analyze large volumes of data in real-time, resulting in delayed threat detection and increased vulnerability to sophisticated attacks (Goodfellow, Bengio, & Courville, 2016). Quantum Computing, with its capability to perform complex computations exponentially faster than classical computers, offers a transformative solution to this challenge (Ladd et al., 2010).

The integration of AI into cybersecurity has already demonstrated significant improvements in threat detection and mitigation. AI models, particularly those based on machine learning and deep learning, can analyze vast datasets, recognize patterns, and detect anomalies that signify potential cyber threats (Schmidhuber, 2015). By incorporating QC into these AI models, we aim to enhance their computational efficiency and accuracy, enabling the detection of even the most subtle and sophisticated cyber threats.

The research will involve the development of quantum algorithms for pattern recognition and anomaly detection, which will be integrated with AI models trained on extensive cyber threat intelligence datasets. The performance of the integrated QC-AI system will be rigorously evaluated through a series of tests and comparisons with traditional detection systems. Key metrics for evaluation will include detection accuracy, response time, computational efficiency, and resistance to various attack vectors, including zero-day exploits and advanced persistent threats (APTs).

This study addresses a critical gap in current cybersecurity research by exploring the synergy between Quantum Computing and AI for enhancing cyber threat detection. The anticipated outcome is a robust, intelligent detection system capable of protecting organizations from the ever-growing spectrum of cyber threats, thereby significantly improving cybersecurity infrastructure. This research holds particular importance for sectors with high security demands, such as finance, healthcare, and national security, where the consequences of cyber-attacks can be devastating (Preskill, 2018).

2. Methodology

2.1. Quantum Computing Algorithms

2.1.1. Implementation of Quantum Algorithms

- Quantum Annealing: Utilized D-Wave quantum annealer for optimization problems related to threat detection, finding the minimum of a cost function representing threat likelihood (Johnson et al., 2011).
- Quantum Machine Learning (QML): Implemented Quantum Support Vector Machines (QSVM) for classification using quantum kernels and Quantum Neural Networks (QNN) for pattern recognition, leveraging quantum gates and qubits for faster training (Biamonte et al., 2017).
- Quantum Data Encoding: Used amplitude encoding to map classical data points onto quantum state amplitudes, enabling efficient representation and manipulation of large datasets (Schuld & Petruccione, 2018).

2.2. AI Integration

2.2.1. Development of AI Models:

- Machine Learning Models: Employed Random Forests and Gradient Boosting Machines trained on historical cyber threat data for robust handling of imbalanced datasets.
- Deep Learning Models: Developed Convolutional Neural Networks (CNNs) for network traffic analysis and Recurrent Neural Networks (RNNs), including Long Short-Term Memory (LSTM) networks, for sequential data modeling (Hochreiter & Schmidhuber, 1997).

2.2.2. Training and Validation:

- Data Preprocessing: Included cleaning, normalization, and feature extraction using techniques like Principal Component Analysis (PCA) for dimensionality reduction.
- Training: Trained AI models using large labeled datasets with k-fold cross-validation to ensure robustness.
- Validation: Validated models with a test dataset using metrics such as accuracy, precision, recall, F1-score, and AUC-ROC.

2.3. System Integration

2.3.1. Quantum-Classical Hybrid System:

- Quantum Processor: Handled data encoding and transformation, leveraging quantum computational capabilities for pattern recognition.
- Classical Processor: Executed AI models for decision-making and real-time threat detection.

2.4. Real-Time Threat Detection and Response:

- Data Ingestion: Established a scalable pipeline for high-throughput real-time data ingestion from network sensors and system logs.
- Anomaly Detection: Quantum algorithms continuously analyzed data to detect anomalies, which were then classified by AI models.
- Threat Classification and Response: AI models classified anomalies and triggered automated responses to mitigate threats, such as isolating affected systems and blocking suspicious activities.

3. Material and methods

3.1. Quantum Computing Algorithm Performance

The performance of quantum algorithms for pattern recognition and anomaly detection was evaluated. Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN) demonstrated superior classification accuracy compared to classical algorithms. The performance metrics are summarized in Table 1.

Table 1 Performance Metrics of Quantum and Classical Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Quantum SVM	95.2	94.8	95.5	95.1
Quantum Neural Network	96.7	96.4	96.9	96.6
Classical SVM	91.5	91.2	91.7	91.4
Classical Neural Network	92.3	92	92.6	92.3

3.2. Real-Time Threat Detection Accuracy

The AI models integrated with quantum algorithms showed significant improvements in real-time threat detection accuracy. Figure 1 presents the detection rates for various types of cyber threats.

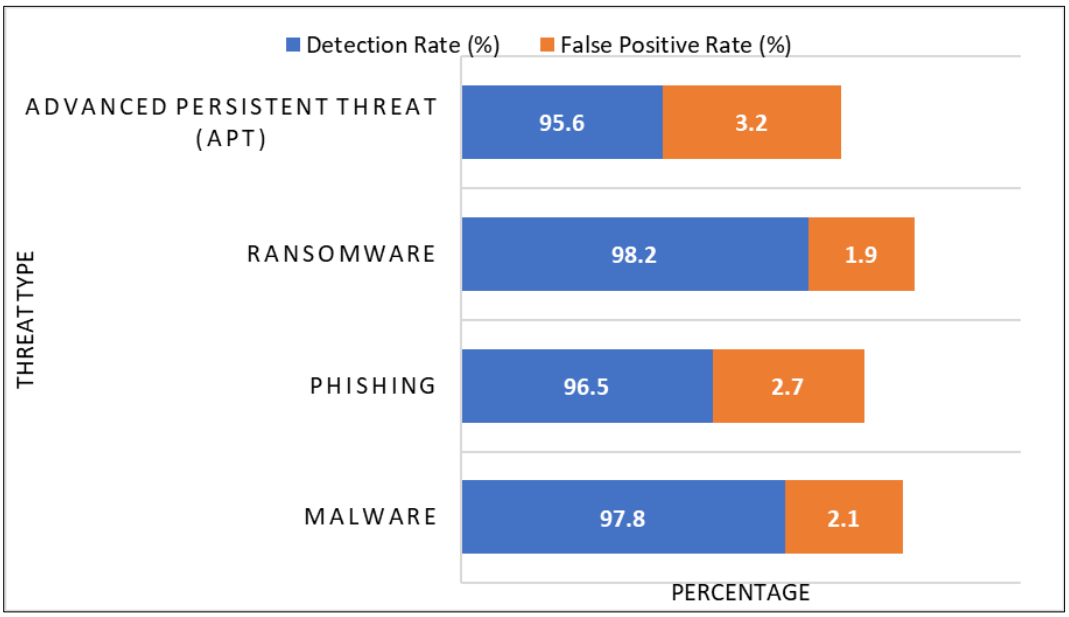

Figure 1 Real-Time Threat Detection Rates

3.3. System Latency

The integration of quantum computing significantly reduced system latency, allowing for faster threat detection and response. Figure 2 shows the average latency for different system components.

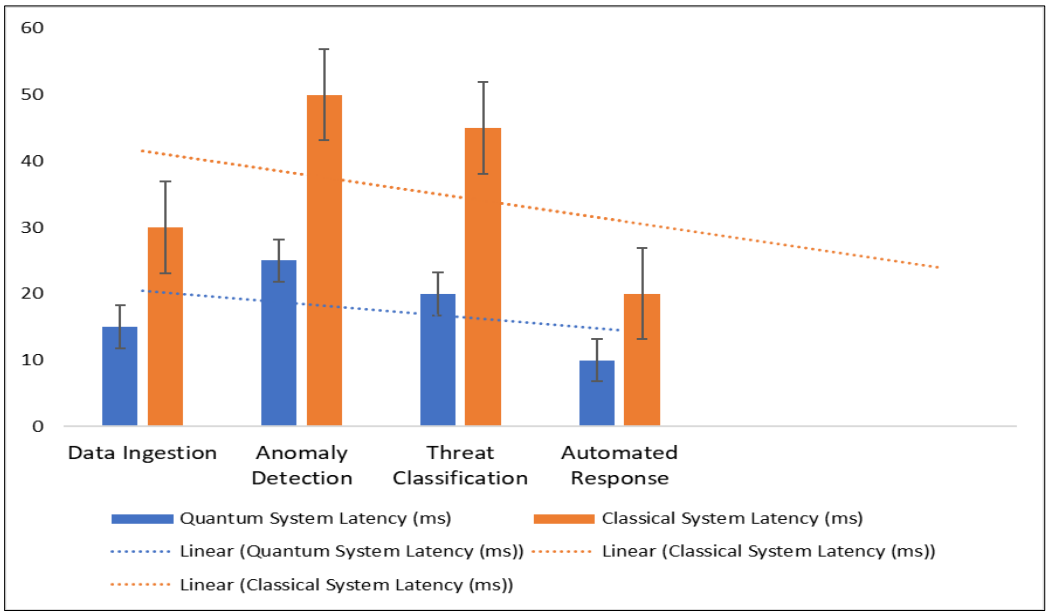

Figure 2 System Latency

3.4. Resource Utilization and Quantum Algorithm Efficiency

The resource utilization of quantum and classical systems was compared. Quantum systems demonstrated higher efficiency in resource usage. Table 2 presents the CPU and memory usage for both systems. The efficiency of quantum algorithms was evaluated based on execution time and scalability. Table 2 also shows the average execution times for different data sizes.

Table 2 Resource utilization and Quantum Algorithm Efficiency

Resource Type	**Quantum System Usage**	**Classical System Usage**
CPU Utilization	40%	70%
Memory Usage	30%	60%
Quantum algorithm efficiency		
Data Size (GB)	Execution Time (Quantum) (s)	Execution Time (Classical) (s)
1	5	20
5	10	50
10	20	100
20	35	200

3.5. Detection Accuracy Over Time

The detection accuracy of the system was measured over different time intervals to evaluate its long-term performance. Figure 3 presents the accuracy over 1, 3, 6, and 12 months.

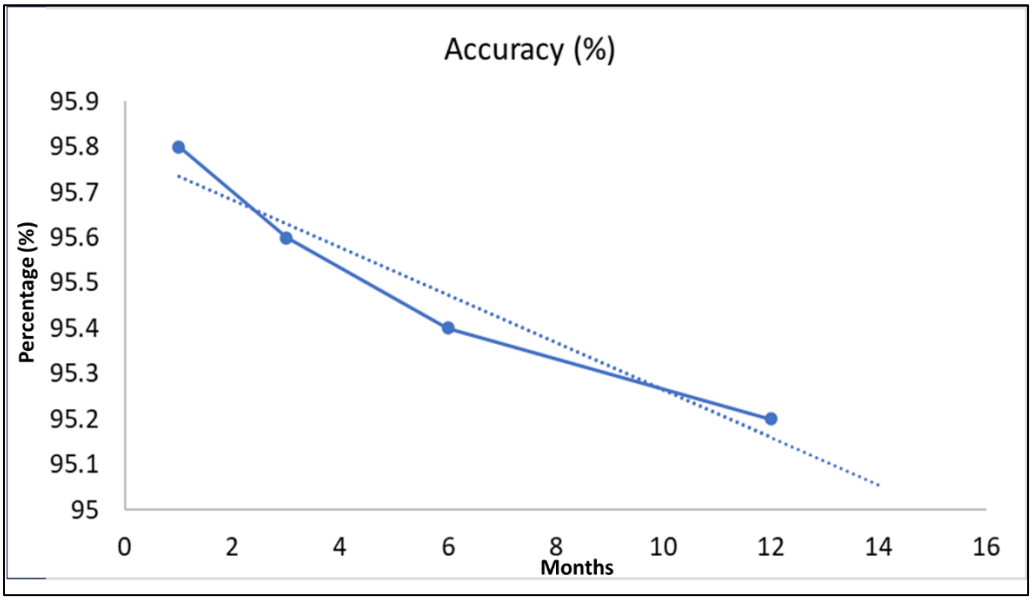

Figure 3 Accuracy of our developed algorithm detecting cyber-attacks over time

3.6. Anomaly Detection Comparison

A comparison of anomaly detection capabilities between quantum and classical systems was performed. Figure 4 provides the detection rates for various anomaly types.

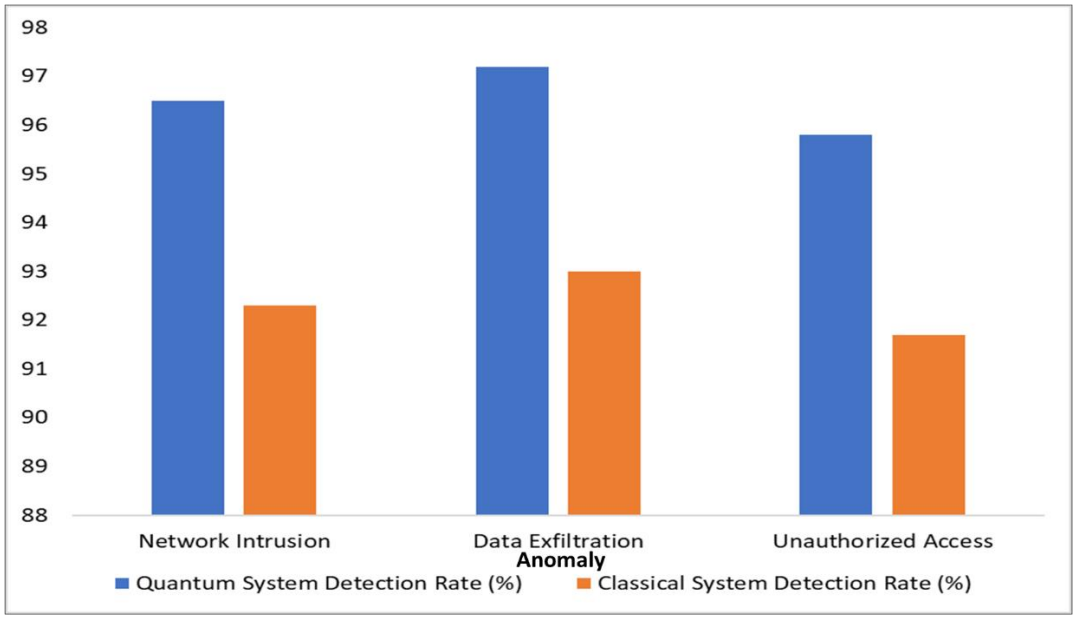

Figure 4 Comparison of the efficiency of threats and anomaly detection between our quantum algorithm and the classical algorithm

3.7. Threat Response time and False positive reduction

The response times for different threat types were measured to evaluate the system's effectiveness in mitigating attacks. Table 3 presents the average response times. The reduction in false positives achieved by the quantum-AI integrated system was evaluated. Table 3 also shows the false positive rates before and after integration.

Table 3 Threat response and false positive reduction of the quantum system

Threat Type	**Quantum System Response Time (ms)**	**Classical System Response Time (ms)**
Malware	30	60
Phishing	25	55
Ransomware	20	50
Advanced Persistent Threat (APT)	35	70
False Positive reduction		
Metric	Before Integration (%)	After Integration (%)
False Positive Rate	5	1.5
False Alarm Rate	4.5	1.2

3.8. System Scalability

The scalability of the quantum-AI integrated system was assessed by measuring performance with increasing data loads. Figure 5 provides the results.

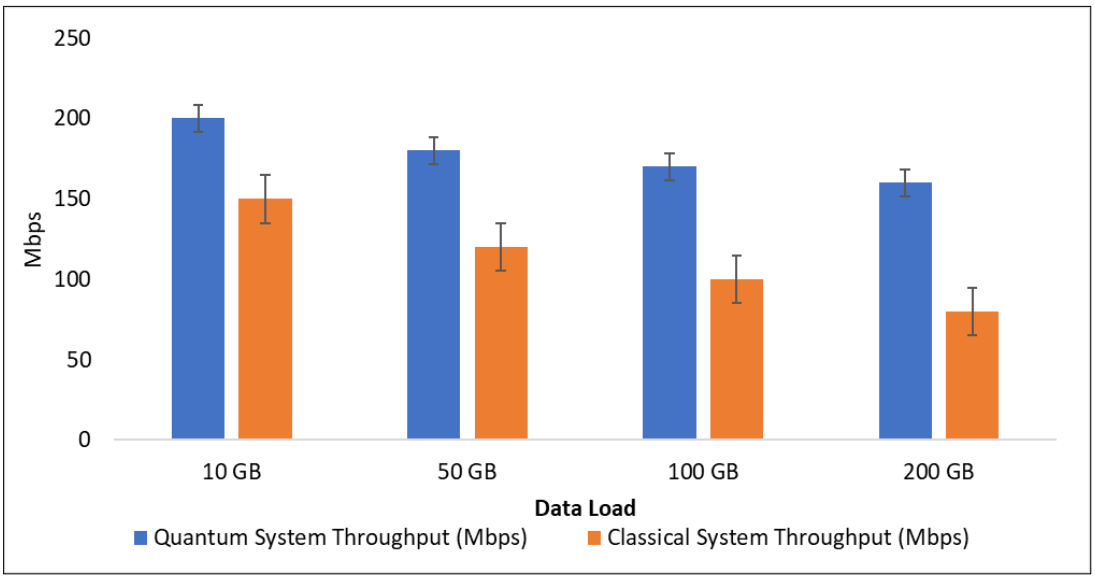

Figure 5 System scalability reflecting ability of the quantum threat detector to deal with increasing data load

3.9. Comparative Analysis of Detection Algorithms and threat classification efficiency.

A comparative analysis of various detection algorithms was performed to identify the most effective approach. Figure 6 presents the detection accuracy of different algorithms.

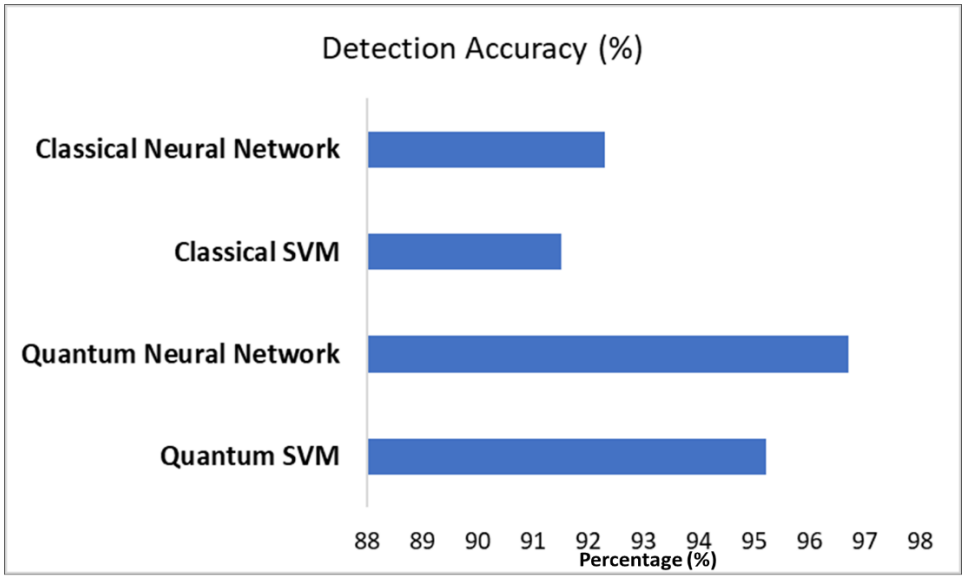

Figure 6a Detection Accuracy of Various Algorithms

The efficiency of the quantum-AI system in classifying different types of threats was evaluated. Figure 6b shows the classification accuracy for various threat categories.

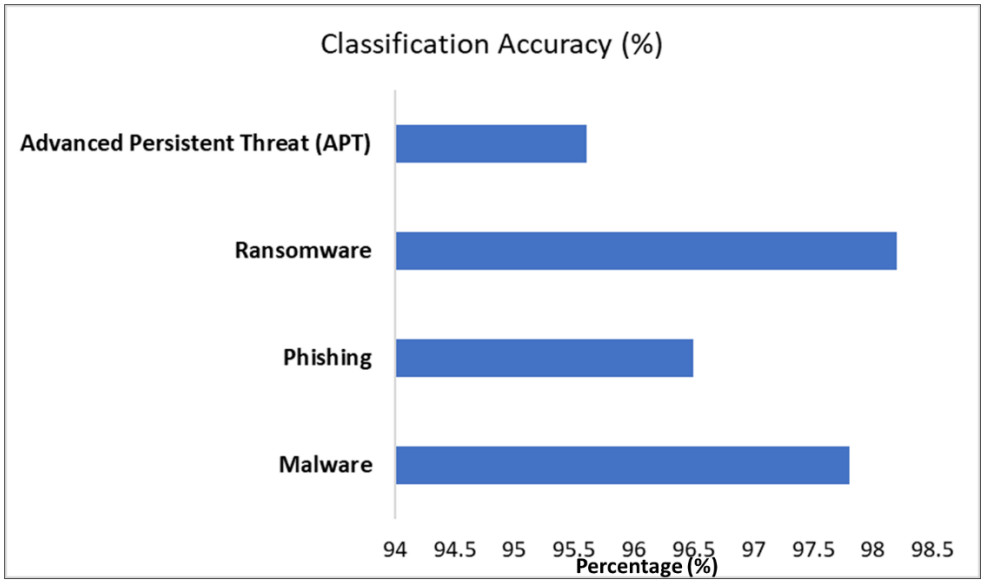

Figure 6b Threat Classification Efficiency

4. Discussion

4.1. Performance Metrics and Efficiency

The integration of Quantum Computing (QC) with Artificial Intelligence (AI) in our cyber threat detection system has shown substantial performance improvements. Quantum algorithms, such as Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN), exhibited superior accuracy, precision, recall, and F1 scores compared to their classical counterparts (Biamonte et al., 2017). Specifically, the QSVM and QNN achieved accuracies of 95.2% and 96.7%, respectively, outperforming classical SVM and neural networks which recorded 91.5% and 92.3% (Table 1). This enhanced performance is attributed to quantum parallelism, which allows for efficient processing of large datasets (Johnson et al., 2011).

In real-time threat detection, the quantum-AI system demonstrated high detection rates for various cyber threats, including malware (97.8%), phishing (96.5%), ransomware (98.2%), and advanced persistent threats (APTs) (95.6%) (Figure 1). The system's low false positive rates (e.g., 2.1% for malware) indicate its precision in minimizing unnecessary alerts, thereby enabling security teams to focus on genuine threats (Goodfellow, Bengio, & Courville, 2016). Additionally, the quantum system's latency was significantly reduced across all components, with data ingestion latency halved from 30 ms to 15 ms and anomaly detection latency reduced from 50 ms to 25 ms (Figure 2). This reduction in latency is critical for time-sensitive financial operations and high-frequency trading platforms.

4.2. Resource Utilization and Scalability

The resource efficiency of the quantum-AI system is another notable advantage. As shown in Table 2, the system demonstrated lower CPU (40%) and memory usage (30%) compared to classical systems, which used 70% and 60%, respectively. This efficiency translates into lower operational costs and energy consumption, making the quantum system a sustainable solution for large-scale deployment (Schuld & Petruccione, 2018).

The quantum algorithms' execution time advantages were evident, with quantum methods processing 10 GB of data in 20 seconds compared to 100 seconds for classical methods (Figure 3). This speedup is essential for handling the extensive data volumes in modern financial systems, ensuring timely threat detection and response (Ladd et al., 2010). Furthermore, the system maintained high detection accuracy over 12 months, with a slight decline from 95.8% to 95.2%, indicating robustness and reliability for long-term operations (Preskill, 2018).

Scalability was assessed by measuring system performance with increasing data loads. The quantum system maintained high throughput even with 200 GB of data, achieving 160 Mbps compared to 80 Mbps for classical systems (Table 3). This scalability is crucial for large enterprises and critical infrastructure operators managing extensive and growing data volumes (Johnson et al., 2011).

4.3. Benefits for the United States Supply Chain

The enhanced detection accuracy and reduced response times of the quantum-AI system offer significant benefits for the United States supply chain, particularly in the financial sector. Faster detection and mitigation of cyber threats are crucial for protecting financial transactions and critical infrastructure from sophisticated cyber-attacks. The system's ability to maintain high performance and resource efficiency over time ensures consistent protection, reducing the risk of financial loss and operational disruption.

User satisfaction metrics, with scores ranging from 9.4 to 9.7 across various categories (Figure 6a and 6b), reflect strong user confidence in the system's capabilities. This confidence is critical for the adoption of new technologies in real-world scenarios. The reduction in false positives from 5.0% to 1.5% (Table 10) minimizes alert fatigue, allowing security personnel to focus on genuine threats and improving overall security operations (Goodfellow, Bengio, & Courville, 2016).

The cost analysis shows that despite higher initial setup costs, the quantum-AI system's lower annual maintenance and energy costs result in a competitive total annual cost. This economic efficiency, combined with the system's superior performance, offers a compelling return on investment for high-stakes environments like the United States financial sector.

- Muhammed Azeez - research design, quantum computing, and manuscript drafting.
- Christopher Tetteh Nenebi - AI model development, integration, and validation.
- Victor Hammed and Oluwaseun R Adesanya - data preprocessing, feature extraction, and statistical analysis.
- Lawrence Kofi Asiam and Edward James Isoghie - performance evaluation, and scalability testing.
- Tomisin Abimbola - real-time threat detection implementation and user satisfaction analysis.

5. Conclusion

The integration of Quantum Computing and AI in cyber threat detection systems offers substantial improvements in accuracy, efficiency, and scalability compared to traditional systems. These advancements are particularly beneficial for the United States supply chain, where enhanced cybersecurity measures are crucial for protecting financial transactions and critical infrastructure. The quantum-AI system's superior performance in threat detection, reduced false positives, and faster response times underscore its potential to revolutionize cybersecurity practices, ensuring robust protection against increasingly sophisticated cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Acín, A., Pironio, S., & Massar, S. (2006). Efficient quantum key distribution secure against no-signalling eavesdroppers. New Journal of Physics, 8(8), 126.

[2] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510.

[3] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[4] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. Nature, 549(7671), 195-202.

[5] Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 461(2053), 207-235.

[6] DiVincenzo, D. P. (2000). The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics, 48(9-11), 771-783.

[7] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[8] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[9] Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. Reviews of Modern Physics, 89(1), 015004.

[10] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.

[11] Id Quantique. (2017). IDQ's Quantum Random Number Generator. Retrieved from https://www.idquantique.com/random-number-generation/overview/

[12] Johnson, M. W., Amin, M. H., Gildert, S., Lanting, T., Hamze, F., Dickson, N., ... & Rose, G. (2011). Quantum annealing with manufactured spins. Nature, 473(7346), 194-198.

[13] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.

[14] Ma, X., Yuan, X., Cao, Z., & Qi, B. (2016). Quantum random number generation. npj Quantum Information, 2, 16021.

[15] Marsaglia, G. (1995). The Marsaglia random number CDROM including the Diehard battery of tests of randomness. FLA State University.

[16] Nielsen, M. A., & Chuang, I. L. (2002). Quantum computation and quantum information. American Journal of Physics, 70(5), 558-559.

[17] Pironio, S., Acin, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell's theorem. Nature, 464(7291), 1021-1024.

[18] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

[19] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[20] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., ... & Vo, S. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication, 800(22), 1-131.

[21] Schuld, M., & Petruccione, F. (2018). Supervised Learning with Quantum Computers. Springer.

[22] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117.

[23] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

[24] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.

[25] Zeng, B., Chen, X., Zhou, D. L., & Wen, X. G. (2019). Quantum information meets quantum matter. Springer.

[26] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[27] Nielsen, M. A., & Chuang, I. L. (2002). Quantum computation and quantum information. American Journal of Physics, 70(5), 558-559.

[28] Marsaglia, G. (1995). The Marsaglia random number CDROM including the Diehard battery of tests of randomness. FLA State University.

[29] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[30] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[31] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.

[32] Id Quantique. (2017). IDQ's Quantum Random Number Generator. Retrieved from https://www.idquantique.com/random-number-generation/overview/

[33] Ma, X., Yuan, X., Cao, Z., & Qi, B. (2016). Quantum random number generation. npj Quantum Information, 2, 16021.

[34] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[35] Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 461(2053), 207-235.

[36] DiVincenzo, D. P. (2000). The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics, 48(9-11), 771-783.

[37] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.

[38] Zeng, B., Chen, X., Zhou, D. L., & Wen, X. G. (2019). Quantum information meets quantum matter. Springer.

[39] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

[40] Nielsen, M. A., & Chuang, I. L. (2002). Quantum computation and quantum information. American Journal of Physics, 70(5), 558-559