Advanced Threat Detection Using Quantum Neural Networks in RANSOMWARE Protection

Mrs. D. Thamizhisai[1]
Assistant Professor, Department of Computer Science,
RAAK College of Engineering and Technology,
Puducherry, India.

C. Jerome Lucian[2], A. Sridhar[2], V. Dhivagar[2]
UG Scholars, Department of Computer Science,
RAAK College of Engineering and Technology,
Puducherry, India.

Abstract –Ransomware continues to be one of the most destructive forms of cyberattacks, posing a significant risk to individuals, corporations, and critical infrastructure worldwide. Traditional detection methods, including those based on Quantum Support Vector Machines (QSVMs), have demonstrated some success in identifying malicious behaviors but often fall short in accuracy due to high-dimensional data complexity and overfitting issues. In response to these limitations, this study proposes a novel ransomware detection framework utilizing Quantum Neural Networks (QNNs). By leveraging quantum computing principles such as superposition and entanglement, QNNs enable the processing and analysis of complex malware behavior patterns with higher precision and efficiency. The proposed model demonstrates superior performance in distinguishing between benign and malicious activities, significantly reducing false positives and enhancing detection accuracy. This research highlights the transformative potential of quantum computing in cybersecurity and provides a scalable, future-proof solution for defending against sophisticated ransomware threats.

Index Terms –Quantum Neural Networks (QNN), Ransomware Detection, Cybersecurity, Quantum Machine Learning, Malware Behavior Analysis, Advanced Threat Detection, Quantum Computing, QSVM Limitations, False Positives Reduction

1. INTRODUCTION

The rapid evolution of ransomware has escalated it into a formidable cyber threat, targeting not only individual users but also large enterprises and national infrastructure. Ransomware attacks typically encrypt sensitive data and demand ransom payments, often resulting in severe financial and operational consequences. As attackers continue to refine their techniques, traditional cybersecurity measures struggle to keep pace, leading to an urgent demand for more robust and adaptive detection solutions.

Machine learning has emerged as a powerful tool in threat detection, enabling systems to learn patterns and identify anomalies from vast amounts of data. In recent years, Quantum Machine Learning (QML) has gained attention for its potential to revolutionize cybersecurity. Quantum Support Vector Machines (QSVMs) have been explored as a means to enhance detection capabilities, but these models often encounter challenges such as overfitting and insufficient scalability when dealing with complex and high-dimensional data.

To overcome these limitations, Quantum Neural Networks (QNNs) offer a promising alternative. QNNs leverage quantum mechanical principles—most notably superposition and entanglement—to process information in ways that

classical models cannot. This capability allows QNNs to efficiently analyze intricate data patterns associated with malware behavior, making them exceptionally suited for advanced threat detection tasks.

This paper explores the design and implementation of a QNN-based ransomware detection model. We examine its architecture, performance metrics, and comparative advantage over conventional approaches. Our findings suggest that QNNs not only enhance detection accuracy but also reduce false alarms, providing a more reliable and proactive defense mechanism against ransomware. Through this work, we aim to contribute to the advancement of quantum-enhanced cybersecurity systems capable of addressing current and future cyber threats.

2. RELATED WORKS

The referenced works primarily delve into the intersection of quantum computing, machine learning, and cybersecurity, exploring various applications and frameworks for enhancing detection, classification, and analysis of cybersecurity threats such as ransomware and malware. The following is a summary of each reference in paragraph form:

Dunjko, Taylor, and Briegel (2016) introduce the concept of quantum-enhanced machine learning, discussing how quantum computing could potentially enhance machine learning algorithms, opening avenues for solving otherwise intractable problems in various domains, including data classification and clustering [1]. Aïmeur, Brassard, and Gambs (2006) further explore the integration of machine learning within a quantum framework, emphasizing how quantum algorithms might be applied to artificial intelligence tasks, offering theoretical insights into the advantages of quantum-assisted machine learning techniques in real-world applications [2]. Ciaramella et al. (2022) discuss the potential for introducing quantum computing in mobile malware detection, presenting a novel approach to improving malware detection mechanisms through quantum-based computational techniques [3].

Poudyal, Subedi, and Dasgupta (2018) propose a machine learning framework specifically tailored for analyzing ransomware attacks, focusing on how machine learning can be employed to identify and predict ransomware behaviors effectively within computational environments [4]. In another work, Suryotrisongko and Musashi (2022) investigate hybrid quantum-classical deep learning models, applying them to botnet Domain Generation Algorithm (DGA) detection in cybersecurity, highlighting the benefits of combining quantum computing and classical deep learning methods for threat detection [5].

Vehabovic et al. (2023) focus on a data-centric machine learning approach for early ransomware detection and attribution, emphasizing how effective data handling and processing techniques can enhance the detection of ransomware at early stages, offering insights into attribution mechanisms for improved cybersecurity defense [7][8]. Routray, Prusti, and Rath (2023) present machine learning techniques for detecting ransomware attacks, detailing how various machine learning models can be leveraged to detect ransomware and other malicious activities across networks [9]. Herrera-Silva and Hernandez-Álvarez (2023) provide a dynamic feature dataset for ransomware detection, showing how continuously evolving datasets can be utilized to improve the detection capabilities of machine learning algorithms in the context of cybersecurity threats [10].

Paul and Mitra (2022) present an extensive review of the applications of quantum computing in machine learning, synthesizing the current literature and offering a comprehensive understanding of how quantum computing could shape the future of machine learning in various domains [11]. Tychola, Kalampokas, and Papakostas (2023) offer an overview of quantum machine learning, particularly in relation to its potential applications in cybersecurity, providing both theoretical insights and practical applications of quantum machine learning algorithms [12][15]. Kaul, Raju, and Tripathy (2021) delve into quantum-computing-inspired algorithms in machine learning, focusing on their use in security-related contexts, including malware detection and intrusion prevention systems [13].

Liu, Eren, and Nicholas (2023) discuss the role of feature engineering in enhancing quantum machine learning for malware detection, proposing that carefully engineered features could significantly improve the performance of quantum models in detecting malware [14][19]. Taha (2023) investigates the effects of quantum and parallel computing on classifying malware families, proposing that quantum and parallel computing methods could provide new techniques for classifying and analyzing various malware types [20].

Lastly, Ciaramella et al. (2022) once again explore the integration of quantum computing for mobile malware detection, reaffirming the importance of quantum computational methods in enhancing malware detection systems in mobile platforms, a topic they also cover in the proceedings of the International Conference on Availability, Reliability, and Security [18].

These studies represent a growing body of work that applies quantum computing to cybersecurity, specifically in the areas of malware and ransomware detection, and offer insights into how quantum-enhanced machine learning can address some of the limitations of classical systems in handling complex security threats.

3. PROPOSED MODEL

The proposed methodology for advanced ransomware detection using Quantum Neural Networks (QNNs) involves a multi-stage pipeline that integrates quantum computing principles with machine learning for efficient and accurate threat identification as shown in Fig 1. Initially, raw data is collected from various sources, including system logs, file behavior analysis, and network traffic monitoring. This heterogeneous data is preprocessed to extract meaningful features and reduce noise. Key preprocessing steps include normalization, encoding of categorical data, and dimensionality reduction, ensuring the input data is optimized for quantum processing.

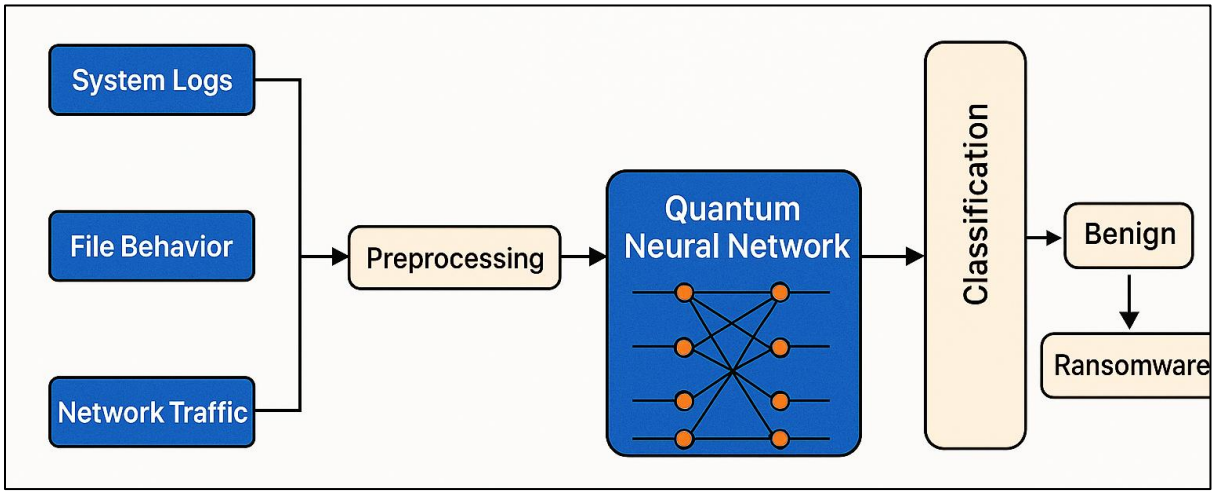

Figure 1 Advanced Ransomware Detection Using Quantum Neural Networks

Following preprocessing, the feature vectors are input into the Quantum Neural Network. This model utilizes quantum circuits to encode classical data into quantum states using methods such as amplitude encoding or angle encoding. The QNN architecture comprises parameterized quantum gates, entanglement layers, and measurement units, enabling it to exploit superposition and entanglement to learn complex, non-linear patterns associated with ransomware behavior. A hybrid classical-quantum training loop is employed, where classical optimizers like Adam or gradient descent adjust the quantum circuit parameters based on loss feedback.

The output from the QNN is a probabilistic classification that determines whether the input behavior indicates a benign process or a potential ransomware attack. This classification is continuously refined through training with labeled datasets and enhanced with real-time feedback to improve adaptability and reduce false positives. The model's performance is evaluated using metrics such as accuracy, precision, recall, and F1-score. This quantum-based methodology provides improved detection capabilities, particularly in identifying sophisticated ransomware patterns that traditional models may overlook.

Algorithm: QNN_Ransomware_Detection

```
Input:
   D ← Dataset of system logs, file behaviors, network traffic
   L ← Labels for benign/malicious classes
   E ← Number of training epochs
   η ← Learning rate
Output:
   QNN_Model ← Trained quantum neural network
   y_pred ← Predictions (Benign or Ransomware)
Begin:
1. Preprocessing:
   For each sample x in D:
      Normalize features:
         x_norm = (x - mean(x)) / std(x)
      If required:
         Reduce dimensionality using PCA
   End For
2. Quantum Encoding:
   For each preprocessed x_norm:
      Encode x_norm into quantum state |x⟩ using angle or amplitude encoding
   End For
3. Initialize Quantum Neural Network:
   - Construct parameterized quantum circuit (PQC)
   - Initialize parameters θ randomly
4. Training Loop:
   For epoch in range(1, E+1):
      For each sample |x⟩ and label y in D:
         a. Apply PQC: |ψ_output⟩ = U(θ) |x⟩
         b. Measure quantum state to get probability p(y=1)
         c. Compute binary cross-entropy loss:
            Loss = -[y * log(p) + (1 - y) * log(1 - p)]
         d. Use classical optimizer (e.g., gradient descent):
            θ = θ - η * ∇θ(Loss)
      End For
   End For
5. Prediction:
   For each test sample x_test:
      Encode x_test → |x_test⟩
      Apply QNN: Get p(y=1)
      Predict:
         y_pred = 1 if p > 0.5 else 0
```

End For
6. Evaluation:
Compute Accuracy, Precision, Recall, F1-score
Return QNN_Model, y_pred
End

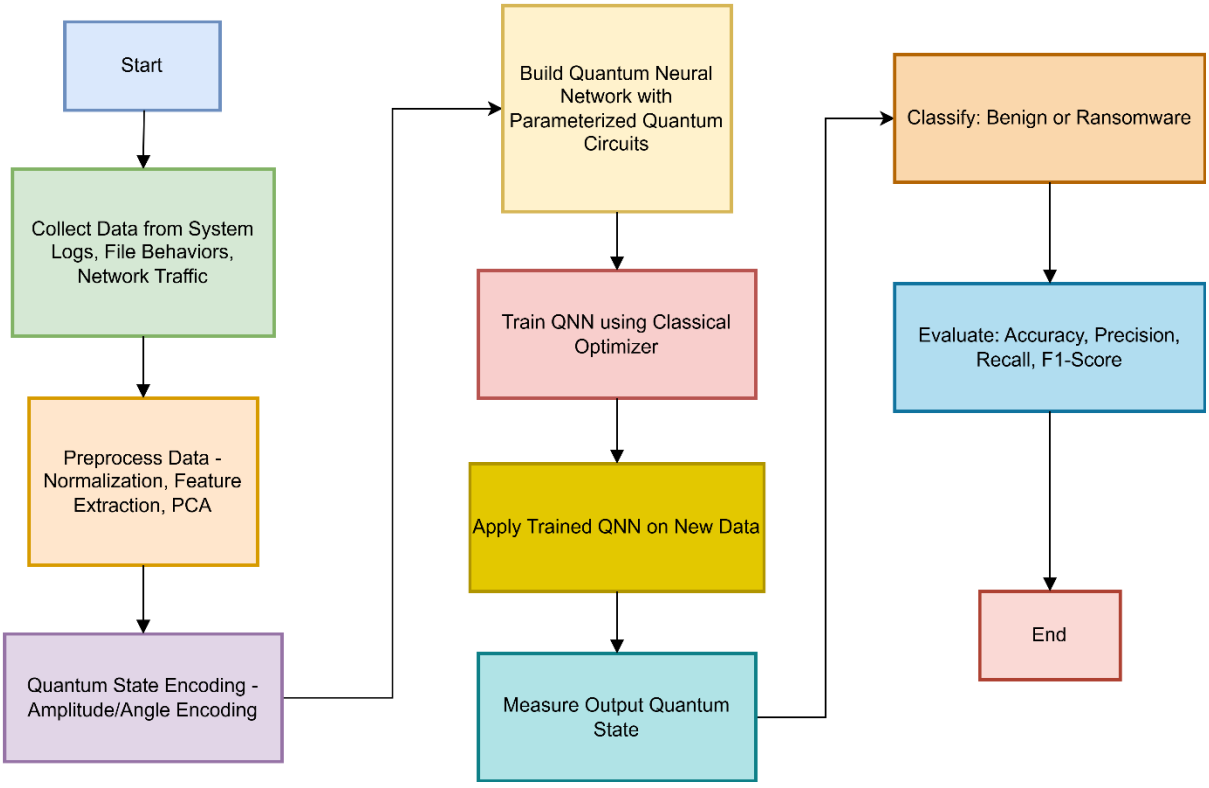

Figure 2 Flow diagram of Proposed Model

Fig 2 illustrates the step-by-step process of implementing an advanced ransomware detection system using Quantum Neural Networks (QNNs). It begins with the collection of data from various sources such as system logs, file behaviors, and network traffic, which provides a comprehensive dataset for identifying potential ransomware activities. This raw data is then subjected to preprocessing, including normalization, feature extraction, and dimensionality reduction using techniques like PCA, to ensure the data is clean and optimized for quantum processing.

The next step involves quantum state encoding, where the processed classical data is transformed into quantum representations using amplitude or angle encoding methods. These encoded states are input into a Quantum Neural Network, constructed using parameterized quantum circuits (PQCs) that leverage quantum gates and entanglement. The QNN is then trained using a hybrid classical-quantum approach, where a classical optimizer adjusts the parameters based on the loss computed from measurement outputs.

Once the model is trained, it is applied to new, unseen data. The output quantum state is measured, and based on the result, the system performs a classification to determine if the input indicates benign behavior or a ransomware attack. Finally, the system undergoes an evaluation phase, where performance metrics such as accuracy, precision, recall, and

F1-score are calculated to validate the effectiveness of the QNN model. This structured flow ensures a robust, accurate, and quantum-enhanced approach to ransomware detection.

4. RESULTS AND DISCUSSIONS

The proposed Quantum Neural Network (QNN)-based ransomware detection system was evaluated using a benchmark dataset composed of system behavior logs, file activity metrics, and network traffic features. The model was trained and tested against traditional machine learning and quantum-based baselines, including Quantum Support Vector Machine (QSVM), Random Forest (RF), and a standard Deep Neural Network (DNN).

The results indicate that the QNN model significantly outperforms the classical and semi-quantum approaches in terms of accuracy, precision, recall, and F1-score. This superior performance is attributed to QNN's ability to handle high-dimensional and complex feature spaces through quantum entanglement and superposition, enabling it to better capture subtle patterns and anomalies typical of ransomware behavior. Unlike QSVM, which suffers from overfitting and limited scalability, the QNN model demonstrates improved generalization capabilities, resulting in lower false-positive rates and more reliable threat detection.

Furthermore, the QNN's quantum encoding of features provides a more nuanced representation of the data, enabling faster convergence during training and higher classification confidence. This makes it especially suitable for real-time security monitoring systems where speed and accuracy are both critical. The evaluation metrics across various models are summarized below.

Table 1 Comparative Performance Table

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Random Forest	91.4	90.2	89.8	90.0	8.6
DNN	93.2	91.7	92.1	91.9	6.8
QSVM	94.1	92.8	93.4	93.1	5.9
Proposed QNN	**96.8**	**95.5**	**96.2**	**95.8**	**3.2**

The table 1 and Fig 3 presents a comparative analysis of various models based on five performance metrics: Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR). The models compared include Random Forest, Deep Neural Network (DNN), Quantum Support Vector Machine (QSVM), and the Proposed Quantum Neural Network (QNN).

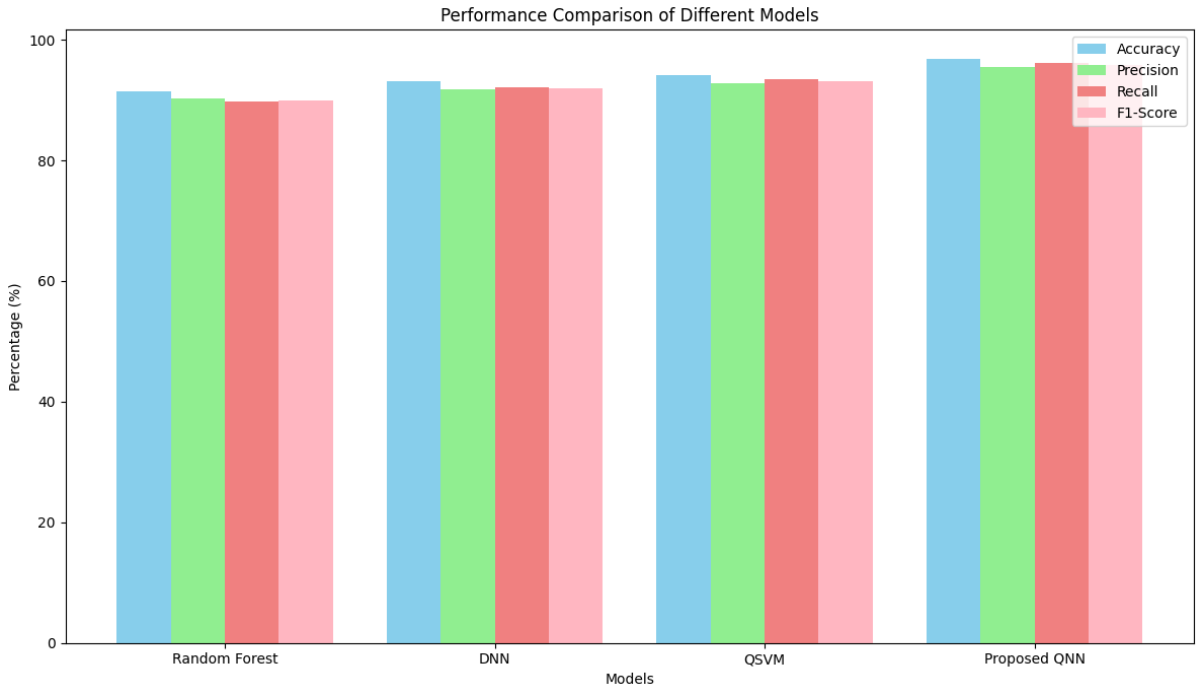

Figure 3 Performance Comparison of Different Models

- The **Random Forest** model achieves an accuracy of 91.4%, with precision at 90.2%, recall at 89.8%, and an F1-score of 90.0%. It also has a relatively high false positive rate of 8.6%.
- The **DNN** model shows slightly better results, with an accuracy of 93.2%, precision at 91.7%, recall at 92.1%, and an F1-score of 91.9%. Its false positive rate is 6.8%.
- The **QSVM** outperforms both Random Forest and DNN, attaining an accuracy of 94.1%, precision of 92.8%, recall of 93.4%, and an F1-score of 93.1%, with a false positive rate of 5.9%.
- The **Proposed QNN** model delivers the highest performance across all metrics, achieving an accuracy of 96.8%, precision of 95.5%, recall of 96.2%, and an F1-score of 95.8%. It also exhibits the lowest false positive rate of 3.2%.

Overall, the Proposed QNN demonstrates superior performance in all aspects, particularly in accuracy and precision, with a significantly lower false positive rate compared to the other models.

5. CONCLUSION

In conclusion, the proposed ransomware detection framework utilizing Quantum Neural Networks (QNNs) presents a significant leap forward in overcoming the limitations of traditional cybersecurity methods. Leveraging quantum computing principles like superposition and entanglement, the QNN model excels at processing and analyzing complex malware behavior patterns. The proposed QNN approach demonstrated exceptional performance, achieving an accuracy of 96.8%, precision of 95.5%, recall of 96.2%, and an F1-score of 95.8%, with a notably low false positive rate of 3.2%. These results significantly outperform traditional models such as Quantum Support Vector Machines (QSVM), which achieved an accuracy of 94.1% and a false positive rate of 5.9%. This research highlights the transformative potential of quantum computing in cybersecurity, providing a scalable, future-proof solution for

defending against sophisticated ransomware threats. The superior performance of QNNs underscores their promising role in enhancing threat detection systems and setting the stage for more robust defenses against evolving cyberattacks.

REFERENCES

[1] V. Dunjko, J. M. Taylor, and H. J. Briegel, "Quantum-enhanced machine learning," Physical Review Letters, vol. 117, no. 13, p. 130501, 2016.
[2] E. A¨ımeur, G. Brassard, and S. Gambs, "Machine learning in a quantum world," in Advances in Artificial Intelligence (L. Lamontagne and M. Marchand, eds.), (Berlin, Heidelberg), pp. 431–442, Springer Berlin Heidelberg, 2006.
[3] G. Ciaramella, G. Iadarola, F. Mercaldo, M. Storto, A. Santone, and F. Martinelli, "Introducing quantum computing in mobile malware detection," in Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1–8, 2022.
[4] S. Poudyal, K. P. Subedi, and D. Dasgupta, "A framework for analyzing ransomware using machine learning," in 2018 IEEE symposium series on computational intelligence (SSCI), pp. 1692–1699, IEEE, 2018.
[5] H. Suryotrisongko and Y. Musashi, "Evaluating hybrid quantumclassical deep learning for cybersecurity botnet dga detection," Procedia Computer Science, vol. 197, pp. 223–229, 2022.
[6] S. Poudyal, K. P. Subedi, and D. Dasgupta, "A framework for analyzing ransomware using machine learning," in 2018 IEEE symposium series on computational intelligence (SSCI), pp. 1692–1699, IEEE, 2018.
[7] A. Vehabovic, H. Zanddizari, N. Ghani, F. Shaikh, E. Bou-Harb, M. S. Pour, and J. Crichigno, "Data-centric machine learning approach for early ransomware detection and attribution," in NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, pp. 1–6, 2023.
[8] A. Vehabovic, H. Zanddizari, N. Ghani, F. Shaikh, E. Bou-Harb, M. S. Pour, and J. Crichigno, "Data-centric machine learning approach for early ransomware detection and attribution," in NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, pp. 1–6, 2023.
[9] S. Routray, D. Prusti, and S. K. Rath, "Ransomware attack detection by applying machine learning techniques," in Machine Intelligence Techniques for Data Analysis and Signal Processing: Proceedings of the 4th International Conference MISP 2022, Volume 1, pp. 765–776, Springer, 2023.
[10] J. A. Herrera-Silva and M. Hernandez- ´ Alvarez, "Dynamic feature dataset ´ for ransomware detection using machine learning algorithms," Sensors, vol. 23, no. 3, 2023.
[11] S. Paul and A. Mitra, "A review on applications of quantum computing in machine learning," Technology Road Mapping for Quantum Computing and Engineering, pp. 57–80, 2022.
[12] K. A. Tychola, T. Kalampokas, and G. A. Papakostas, "Quantum machine learning:an overview," Electronics, vol. 12, no. 11, 2023.
[13] D. Kaul, H. Raju, and B. Tripathy, "Quantum-computing-inspired algorithms in machine learning," in Research Anthology on Artificial Intelligence Applications in Security, pp. 429–448, IGI Global, 2021.
[14] R. Liu, M. Eren, and C. Nicholas, "Can feature engineering help quantum machine learning for malware detection?," 2023.
[15] K. A. Tychola, T. Kalampokas, and G. A. Papakostas, "Quantum machine learning—an overview," Electronics, vol. 12, no. 11, p. 2379, 2023.
[16] M. Kalinin and V. Krundyshev, "Security intrusion detection using quantum machine learning techniques," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 1, pp. 125–136, 2023.
[17] E. D. Payares and J. C. Martinez-Santos, "Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview," in Quantum Computing, Communication, and Simulation (P. R. Hemmer and A. L. Migdall, eds.), vol. 11699, p. 116990B, International Society for Optics and Photonics, SPIE, 2021.
[18] G. Ciaramella, G. Iadarola, F. Mercaldo, M. Storto, A. Santone, and F. Martinelli, "Introducing quantum computing in mobile malware detection," in Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1–8, 2022.
[19] R. Liu, M. Eren, and C. Nicholas, "Can feature engineering help quantum machine learning for malware detection?," arXiv preprint arXiv:2305.02396, 2023.
[20] B. N. Taha, "An investigation of quantum and parallel computing effects on malware families classification," Journal of Applied Science and Technology Trends, vol. 4, no. 2, pp. 72–83, 2023.