ADScAI
Applied Data Science & Artificial Intelligence Symposium

Quantum Deep Learning for Encrypted Malicious Traffic Detection A Hybrid Approach for Secure Network Analysis

Nirusan Hariharan
Department of Computing
Informatics Institute of Technology
Colombo, Sri Lanka
hariharan.20200094@iit.ac.lk

Guhanathan Poravi
Department of Computing
Informatics Institute of Technology
Colombo, Sri Lanka
guhanathan.p@iit.ac.lk

Keywords—Quantum Deep Learning, Transport Layer Security, Quantum Neural Networks, Quantum Gated Recurrent Units, Encrypted Malicious Traffic Detection

I. INTRODUCTION

Cybersecurity threats have become more advanced, making encrypted network traffic essential for security while also challenging to monitor. Transport Layer Security (TLS) is widely used to protect online communications by ensuring data integrity and confidentiality. However, a small number of malicious users exploit encryption for malicious activities, making it difficult to detect attacks using traditional Machine Learning (ML) and Deep Learning (DL) models. Which makes it very difficult to detect attacks using traditional Machine Learning (ML) and Deep Learning models. Majority of the Network Intrusion Detection Systems (NIDS) struggle with encrypted malicious network traffic. As decrypting the data for analysis would compromise the security, privacy and break the confidentiality of the servers, decrypting is not considered as good suggestion at most.

Recent progress in Quantum Machine Learning (QML) provides a new path to detect anomalies in encrypted traffic without decrypting the traffic. Quantum Deep Learning can process complex network data more efficiently than classical methods. This research introduces a Hybrid Quantum Deep Learning framework, that combines Quantum Neural Networks (QNN), and Quantum Gated Recurrent Units (QGRU) to improve TLS malicious network traffic detection.

This research evaluates the performance of QDL-based threat detection compared to traditional ML models. To be more specific in this VPN/Tor based TLS malicious network traffic detection will be explained through. It demonstrates that QDL models improve detection accuracy while maintaining efficient processing using real-world traffic datasets such as CIC-Darknet 2020.

II. RELATED WORK

Detection of malicious encrypted malicious network traffic has been a critical research area in cybersecurity. The initial traditional ML approach of detecting encrypted malicious TLS traffic had been used CNN and LSTM algorithms to classify the anomaly traffic [1]. Another approach came across as using Multi-Level Feature Fusion Model (MFFusion) that combines byte, statistical feature and data timing from multiple perspectives and detect whether the network traffic is malicious or not [2].

Recent advances in QML provide an alternative method for traditional ML approach. QNN have shown promise in anomaly detection by understanding the complete patter of malicious network traffic efficiently [3]. Correspondingly, QGRU have been explored to their ability to handle sequential data which making them suitable for detecting up to date evolving attack patters in network traffic [4]. While maintaining the same computational manner, all the quantum driven models had improved classification performance in terms of comparing with traditional amplitude estimation as well [5].

Another study proposed a QCNN with transfer learning to detect malware targeting smart grid devices [6]. It converts binary files to grayscale images, applies quantum convolution via an IBM processor to extract hidden features, and leverages CNN-based classification. Results indicate accuracy and reduced overhead compared to classical CNN. Implemented on IBM Watson Studio, this pipeline underscores the promise of quantum-enhanced solutions for critical infrastructure.

Similarly, an isolated research analyzed the vulnerabilities of conventional neural networks (NN) and quantum neural networks (QNN) under adversarial attacks in software supply chain malware detection [7]. By injecting noise and measuring precision and recall, both proved susceptible. However, QNN retained higher recall under adversarial conditions. Implemented with Pennylane, these findings highlight QML's promise in securing ML pipelines.

integrating multiple cryptographic paradigms in existing TLS frameworks.

Despite extensive research, detecting encrypted malicious network traffic using a QDL approach remains underexplored. Although TLS has been studied, no work has specifically addressed malicious traffic detection within TLS, nor compared QNN and QGRU in this context. Most studies rely on simulated quantum environments with limited real-world applicability [8]. This work bridges that gap by implementing a Hybrid Quantum Deep Learning (QDL) framework that

https://doi.org/10.31705/ADScAI.2025.56

integrates QNN and GRU, evaluated on real-world encrypted datasets.

ML based detection of encrypted malicious traffic faces challenges such as data imbalance and the lack of publicly available dataset [9]. A proposed six step framework outlined data collection, feature selection and model evaluation, demonstrating that TLS/SSL-specific features enhance classification accuracy. Comparative studies of supervised and unsupervised models highlights the effectiveness of methods like Boost and SVM. Expanding on the on finding now this research leverages on QDL to improve malicious TLS network traffic detection.

III. Methodology

A. Experimental Setup and Dataset

The proposed Hybrid QDL framework was evaluated using the CIC Darknet 2020 dataset. Which contains real world encrypted malicious network traffic. The initial stage of dataset preprocessing was conducted as filtering TLS Specific Ports. After filtering the TLS network traffic the data was encoded, so entire data will be in numeric type so the rest of the task can be done easily. Finally the features for the model was selected based on correlation method and 11 features got selected for the model.

To address class imbalance, SMOTE Technique was applied. It was executed to ensure a balance distribution across attack classes. One hot encoding was performed on categorical network attributes to enable compatibility with deep learning models. Principle Component Analysis was applied to reduce dimensionality, improving model efficiency while retaining essential variance in the dataset.

B. Model Implementation

The proposed Hybrid Quantum Deep Learning (QDL) framework integrates quantum circuits with classical neural architectures to detect encrypted malicious TLS traffic. Implemented using Pennylane, Qiskit, and TensorFlow, the model features a QNN and a QGRU. The QNN uses a 3-qubit quantum circuit with AngleEmbedding to encode classical inputs into quantum states, followed by StronglyEntanglingLayers that apply trainable gate operations. The outputs are the expectation values of Pauli-Z measurements, capturing high-dimensional feature interactions beyond classical capacity. Additionally, quantum circuits were tested with sample inputs and visualized using Pauli-Z expectation plots, aiding interpretability and showcasing observable responses from entangled qubit states. Quantum layers were implemented as custom TensorFlow layers with trainable weights, simulating quantum behavior and supporting hybrid end-to-end training through classical backpropagation and optimizers.

These quantum-derived features are passed through dense layers and combined with classical components in a fusion layer, enabling efficient classification. In the QGRU model, a similar quantum feature extraction process is applied, followed by stacked GRU layers that capture temporal attack patterns. This structure enhances the model's ability to detect evolving threats within TLS traffic by learning sequential dependencies.

Both models were trained on a simulated quantum backend and saved for evaluation. While the QNN performed well, the QGRU faced generalization challenges. Future work aims to optimize temporal-quantum integration and deploy the system on a real quantum runtime.

IV. Results and Discussion

A. Performance Evaluation

The model were evaluated using accuracy, precision, recall and F1-score to measure classification performance. Table 1 presents the results.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
QNN	99.95	99.95	99.95	99.95
QGRU	59.21	53.24	49.09	45.84

Table 1 - QNN and QGR model evaluation results

The QNN model demonstrated superior classification performance, with near-perfect scores across all metrics, highlighting its effectiveness in detecting encrypted TLS traffic. In contrast, the QGRU model exhibited significant performance degradation during testing, indicating overfitting and limited generalizations. This may be attributed to the difficulty of modelling temporal patterns with high-dimensional quantum embeddings. Future improvements may involve hyperparameter tuning, dimensionality reduction refinements, or replacing stacked GRU layers with Transformer-based quantum-classical hybrids to better capture sequential dependencies in encrypted traffic.

Acknowledgment

The author sincerely Mr. Isala Piyasiri and Mr. Nuvin Godakanda Arachchi for their mentorship and expertise in TLS security and quantum computing. Appreciation is also extended to the Department of Computer Science and Engineering, University of Moratuwa.

References

[1] S. Lucia and D. Cotton, "Convolutional Neural Networks for Encrypted Malicious Traffic Detection," Proc. IEEE Int. Conf. Security and Privacy, 2019, pp. 1–6.

[2] K. Lin, X. Xu, and F. Xiao, "MFFusion: A Multi-Level Features Fusion Model for Malicious Traffic Detection Based on Deep Learning," Computer Networks, vol. 202, p. 108658, 2022.

[3] R. Kukliansky, J. Alon, and A. Barak, "Optimized Quantum Neural Networks for Network Activity Classification on Noisy Quantum Computers," Quantum Machine Intelligence, vol. 6, p. 26, 2024.

[4] M. Hdaib, S. Rajasegarar, and L. Pan, "Quantum Deep Learning-Based Anomaly Detection for Enhanced Network Security," Quantum Machine Intelligence, vol. 6, p. 34, 2024.

[5] M. Guo, H. Liu, Y. Li, W. Li, F. Gao, S. Qin, and Q. Wen, "Quantum Algorithms for Anomaly Detection Using Amplitude Estimation," Physica A: Statistical Mechanics and Its Applications, vol. 604, p. 127936, 2022.

[6] A. Nasif, M. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," IEEE Access, vol. 9, pp. 78658–78700, 2021.

[7] G. Ciaramella, G. Iadarola, F. Mercaldo, M. Storto, A. Santone, and F. Martinelli, "Introducing quantum computing in mobile malware detection," Proc. ACM, pp. 1–8, 2022.

[8] M. S. Akter, H. Shahriar, S. I. Ahamed, K. D. Gupta, M. Rahman, A. Mohamed, M. Rahman, A. Rahman, and F. Wu, "Case study-based approach of QML in cybersecurity: Quantum support vector machine for malware classification and protection," Proc. IEEE COMPSAC, Torino, Italy, 2023.

[9] Z. Wang, K. W. Fok, and V. L. L. Thing, "Machine Learning for Encrypted Malicious Traffic Detection: Approaches, Datasets, and Comparative Study," *Computers & Security*, vol. 113, p. 108658, 2022