Towards Quantum Machine Learning for Malicious Code Analysis

Jesus Lopez[†], Saeefa Rubaiyet Nowmi[†], Viviana Cadena[†], and Mohammad Saidur Rahman[†]
[†]Department of Computer Science, University of Texas at El Paso, TX, USA
Email: {jlopez126, snowmi, vcadena1}@miners.utep.edu, msrahman3@utep.edu

Abstract:

Classical machine learning (CML) has been extensively studied for malware classification. With the emergence of quantum computing, quantum machine learning (QML) presents a paradigm-shifting opportunity to improve malware detection, though its application in this domain remains largely unexplored. In this study, we investigate two hybrid quantum-classical models - a Quantum Multilayer Perceptron (QMLP) and a Quantum Convolutional Neural Network (QCNN), for malware classification. Both models utilize angle embedding to encode malware features into quantum states. QMLP captures complex patterns through full qubit measurement and data re-uploading, while QCNN achieves faster training via quantum convolution and pooling layers that reduce active qubits. We evaluate both models on five widely used malware datasets - API-Graph, EMBER-Domain, EMBER-Class, AZ-Domain, and AZ-Class, across binary and multiclass classification tasks.

Our results show high accuracy for binary classification - 95–96% on API-Graph, 91–92% on AZ-Domain, and 77% on EMBER-Domain. In multiclass settings, accuracy ranges from 91.6–95.7% on API-Graph, 41.7–93.6% on AZ-Class, and 60.7–88.1% on EMBER-Class. Overall, QMLP outperforms QCNN in complex multiclass tasks, while QCNN offers improved training efficiency at the cost of reduced accuracy.