Quantum Machine Learning: Performance and Security Implications in Real-World Applications

Zhengping Jay Luo
Department of Computer Science and Physics
Rider University
Lawrenceville, New Jersey, 08648
Email: zluo@rider.edu

Tyler Stewart

Department of Computer Science and Physics
Rider University

Lawrenceville, New Jersey, 08648

Email: stewartty@rider.edu

Mourya Narasareddygari
Department of Computer Science and Physics
Rider University
Lawrenceville, New Jersey, 08648
Email: mnarasaredd@rider.edu

Rui Duan School of Science and Engineering University of Missouri-Kansas City Kansas City, Missouri, 64110 Email: rdhk9@umkc.edu Shangqing Zhao
School of Computer Science
University of Oklahoma
Tulsa, Oklahoma, 74135
Email: shangqing@ou.edu

Abstract-Quantum computing has garnered significant attention in recent years from both academia and industry due to its potential to achieve a "quantum advantage" over classical computers. The advent of quantum computing introduces new challenges for security and privacy. This poster explores the performance and security implications of quantum computing through a case study of machine learning in a real-world application. We compare the performance of quantum machine learning (QML) algorithms to their classical counterparts using the Alzheimer's disease dataset. Our results indicate that QML algorithms show promising potential while they still have not surpassed classical algorithms in terms of learning capability and convergence difficulty, and running quantum algorithms through simulations on classical computers requires significantly large memory space and CPU time. Our study also indicates that QMLs have inherited vulnerabilities from classical machine learning algorithms while also introduce new attack vectors.

Index Terms—Quantum Security, Quantum Machine Learning, Quantum Advantage, Attack Vectors

I. Introduction

Since Richard Feynman first proposed the idea of harnessing quantum physics to build quantum computers more than 40 years ago [1], significant breakthroughs and progress have steadily been made toward realizing Feynman's vision and achieving "quantum advantage." With the development of quantum computing technologies, a natural question to ask is how to protect the security and privacy in a quantum age? We conduct a case study regarding performance and security implications of machine learning (ML) algorithms in quantum computing. In recent years, numerous quantum machine learning (QML) proposals have been published [2]–[4], paving the way for unleashing the full potential of ML algorithms on quantum computers.

In this poster, we want to know the performance of QML algorithms compared to their classical counterparts on a real-world dataset, and the corresponding security implications. We conduct a comparative study of the performance of

two major types of classical machine learning (CML) algorithms—support vector machines (SVMs) and multi-layer perceptron (MLP) classifiers—and their corresponding quantum versions, including quantum support vector machines (QSVMs), variational quantum algorithms (VQAs) and quantum convolutional neural networks (QCNNs). Our comparison and analysis are based on the real-world Alzheimer's disease dataset [5]. Then we'll discuss the potential security implications of the QML algorithms, including the inherited vulnerabilities from their classical counterparts and the new introduced attack vectors.

II. QUANTUM MACHINE LEARNING

QML is the quantum counterpart to CML. In CML, there are two main categories: supervised and unsupervised learning. This poster focuses on supervised learning. Kernel methods, such as SVMs, and neural network-based methods, including MLPs and Convolutional Neural Networks (CNNs), are among the most renowned families of supervised learning algorithms that have achieved significant success on classical computers.

The idea of kernel methods is to map the classification problem non-linearly to a high-dimensional feature space, making data easier to separate. QSVMs [4] use the quantum state space as feature space by mapping classically processed data nonlinearly to a quantum state Φ , i.e., $\overrightarrow{x} \in \Omega \to |\Phi(\overrightarrow{x})\rangle \langle \Phi(\overrightarrow{x})|$, in which $\Omega \subset \mathbb{R}^d$. This allows leveraging quantum feature maps to perform the kernel trick, with the feature vector kernel represented as $K(\overrightarrow{x}, \overrightarrow{z}) = |\langle \Phi(\overrightarrow{x})|\Phi(\overrightarrow{z})\rangle|^2$, where $\Phi(\overrightarrow{x})$ and $\Phi(\overrightarrow{z})$ are quantum feature maps. According to Havlíček et al. [4], a quantum advantage for QSVMs can only be achieved for feature maps with a kernel that is hard to estimate classically.

VQAs, the quantum analog of MLP neural networks, are designed to run on quantum computers using a classical optimizer to train parameterized quantum circuits. They are

currently considered the best hope and candidate for achieving quantum advantage on noisy intermediate-scale quantum (NISQ) devices [3]. The principle behind VQAs is to encode the problem into a cost function C with a set of parameters θ . The optimizer's task is to solve $\theta^* = \arg\min_{\theta} C(\theta)$, where $C(\theta) = f(\{\rho_k\}, \{O_k\}, U(\theta))$. Here $U(\theta)$ denotes a unitary operation, $\{\rho_k\}$ are the input states and $\{O_k\}$ denotes a set of observables. When the optimization task converges, the final ansatz and the corresponding learned model can be used for future applications.

Another notable proposal for QML models is the QCNN developed by Cong et al. [2]. QCNNs extend the key properties of classical CNNs to the quantum field by incorporating all major components of CNNs, including convolutional layers and pooling layers, with the input transformed into quantum states. Convolution, pooling operations, and fully connected layers are implemented using unitary rotations. The nonlinearity in QCNNs arises from reducing the degrees of freedom. The variational parameters required in QCNNs are only $O(\log(\mathcal{N}))$, given an input size of $\mathcal N$ bits, which allows for efficient training and implementation.

From the models introduced above, we know that there are many structural similarities between QML models and their corresponding CML models. Thus from a security perspective, QML models will inevitably inherit many of the vulnerabilities in CML, such as the crafted adversarial examples attack. However, as stated in [6], it will be more difficult to perform robust adversarial training due to the increased dimensions of the space used in QML, making it more sensitive to minor perturbations near the decision boundary.

III. EXPERIMENTAL RESULTS AND ANALYSIS

We compared the performance of the aforementioned representative QML algorithms to their classical counterparts on the real-world Alzheimer's disease dataset [5], which is a public dataset containing health information for 2,149 patients, including demographic details, lifestyle factors, medical history, and more. We used this dataset to train learning models to predict whether a patient will be diagnosed with Alzheimer's disease, framing it as a binary classification problem. We implemented our learning models using the scikit-learn library [7] and the IBM Qiskit software stack. [8]. we employed two CML models—SVM and MLP—to train models. Additionally, we trained three types of QML models for performance comparison: QSVM, VQA, and QCNN, respectively.

We first studied the amount of training data required to achieve a "reasonably" good learning model using SVM and MLP models. Our findings indicate that as the size of the training data increases, the performance, measured by prediction accuracy on the test dataset, improves moderately from 80% (when using 10% of the dataset for training) to 87% (when using 90% for training). Notably, among the 32 features in the dataset, the most influential factor contributing to the diagnosis of Alzheimer's disease is "Memory Complaints," providing an intuitive way to assess whether a patient has Alzheimer's with high probability. The best accuracy we achieved using either

SVM or MLP was 87% on the testing data, with 90% of the data allocated for training.

When trained using QML algorithms, our models generally did not surpass their classical counterparts in both time and accuracy, except for the QCNN model, which has the same prediction accuracy as the SVM model. This is understandable, as CML algorithms have been refined and optimized over many years by numerous researchers. Accessing real-world quantum computers remains challenging; therefore, we ran our algorithms on local computers with simulations, which typically result in significantly longer training times compared to classical methods. For example, training a classical SVM model takes only 0.03 seconds of CPU time, while training the same-sized OSVM model on a local computer via simulation takes 132.07 seconds—over 4,000 times longer in terms of time cost. We anticipate that as real-world quantum computers become more accessible, this gap will be narrowed and potentially reversed.

Given above experimental results, we can arguably infer that it will be easier for adversarial example attacks to succeed when the prediction from QML models are less accurate than CML models, often resulted by defective decision boundaries. Further more, in quantum scenarios, new attack vectors could also be introduced, including exploiting quantum noise to degrade the performance of quantum models [6].

IV. CONCLUSION

Security concerns of quantum computing has been an emerging problem. We employed ML as a case study to explore the performance and security implications of quantum computing. Our results indicate that QML algorithms such as QSVM, VQA, QCNN models still have not surpassed CML models in terms of learning performance on our real-world dataset in a simulated environment. The security implications of quantum computing are multi-faceted. In our future work, we'll continue to explore more security implications of quantum computing in ML domain.

REFERENCES

- J. Preskill, "Quantum computing 40 years later," in Feynman Lectures on Computation. CRC Press, 2023, pp. 193–244.
- [2] I. Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," *Nature Physics*, vol. 15, no. 12, pp. 1273–1278, 2019.
- [3] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio et al., "Variational quantum algorithms," *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.
- [4] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.
- [5] R. E. Kharoua, "Alzheimer's disease dataset," 2024. [Online]. Available: https://www.kaggle.com/dsv/8668279
- [6] N. Franco, A. Sakhnenko, L. Stolpmann, D. Thuerck, F. Petsch, A. Rüll, and J. M. Lorenz, "Predominant aspects on security for quantum machine learning: Literature review," arXiv preprint arXiv:2401.07774, 2024.
- [7] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
- [8] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, "Quantum computing with Qiskit," 2024.