UR-363 Quantum Machine Learning in Cybersecurity

INTRO/ABSTRACT

Quantum machine learning is a very new field of machine learning that utilizes quantum computing techniques to achieve a higher level of performance. This project explores several quantum models trained to solve cybersecurity-related problems that suit those respective models. The project compares the performances of these quantum models to their classical counterparts to find ways to better understand and optimize quantum machine learning algorithms.

METHODS

The models tested include quantum naïve bayes, quantum neural network, and quantum SVM. The classical versions of these models were also implemented in order to compare their performance with that of the quantum versions. The models were evaluated on their performance time, accuracy, precision, and f1 scores. Based on how the quantum models compared to the classic models, the quantum models were then optimized to gain knowledge on how to better optimize quantum models.

RESULTS

The quantum models consistently had a poorer performance compared to their classical implementations. This was expected due to the quantum models being designed to take advantage of quantum computers. However, this experiment allowed for an opportunity to learn how to better optimize these algorithms on classical computers.

REFERENCES

Borujeni, S. E., Nannapaneni, S., Nguyen, N. H., Behrman, E. C., & Steck, J. E. (2021, April 12). *Quantum Circuit representation of Bayesian Networks*. arXiv.org.

Quantum Machine Learning Models For Testing, Viability, Performance, and Optimization Techniques

python™ colab TensorFlow PENNYLANE

Scan this QR code to view the project website and view step-by-step implementation explanations.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Authors: Anna Destito, Joseph Ragsdale, Adam Waugh
Advisors: Dr. Yong Shi, PHD, Professor Sharon Perry