UNIVERSITY OF CENTRAL ARKANSAS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Proposed Course Information

Course Name : CSCI 6397 – Special Topics in Quantum Machine Learning for Cybersecurity
Course Level : Senior Undergraduate / Graduate Special Topics
Department : Computer Science and Engineering, University of Central Arkansas
Credits : 3
Prerequisites : Introduction to Artificial Intelligence or Machine Learning

Course Description:

This course introduces the principles and practical applications of Quantum Machine Learning (QML) for cybersecurity. The course bridges foundational quantum computing concepts with advanced machine learning techniques to address emerging cyber defense challenges. Students will implement hybrid quantum–classical learning models for cybersecurity applications including AI model poisoning detection, adversarial attack detection, deepfake identity spoofing detection, post-quantum cryptography migration risk analysis, software supply chain vulnerability analysis, and malware classification. The course emphasizes hands-on experimentation using open-source quantum computing frameworks and real cybersecurity datasets.

Course Learning Outcomes:

Upon successful completion of the course, students will be able to:

1. Explain the principles of quantum computing relevant to machine learning and cybersecurity.
2. Implement parameterized quantum circuits and quantum machine learning models.
3. Design QML models for detecting adversarial attacks, deepfake identity spoofing, software supply chain vulnerabilities, and malware families.
4. Benchmark quantum machine learning approaches against classical machine learning models using empirical evaluation metrics.

Key Course Topics:

1. Foundations of Quantum Computing: Quantum bits, superposition, entanglement, quantum gates, and quantum circuit models.
2. Fundamentals of Quantum Machine Learning: Parameterized quantum circuits, quantum embeddings, hybrid quantum–classical models.

3. Quantum Frameworks and Development Tools: Hands-on development using IBM Qiskit, PennyLane, and TensorFlow Quantum.
4. Trustworthy AI and Adversarial Defense: Quantum Neural Networks for detecting data poisoning and adversarial manipulation of AI systems.
5. Deepfake and Identity Spoofing Detection: Quantum Boltzmann Machines and hybrid QML approaches for multimedia spoofing detection.
6. Software Supply Chain Vulnerability Analysis: Quantum Decision Trees and QML-based techniques for identifying vulnerabilities in open-source software repositories.
7. Malware and Ransomware Classification: Quantum Support Vector Machines for detecting and classifying malware families using executable features.
8. Post-Quantum Cryptography Migration Risk Analysis: Quantum Kernel Classifiers to evaluate migration risks and potential vulnerabilities of post-quantum cryptography.
9. Evaluation and Benchmarking of QML approaches: Performance analysis, model robustness, computational cost, and practical deployment considerations.

Laboratory and Experiential Learning:

Students will complete multiple hands-on laboratory modules derived from the "Quantum Machine Learning for Next-Generation Cyber Defense" labware repository. Lab exercises include constructing parameterized quantum circuits, preparing cybersecurity datasets, implementing QML classifiers, and benchmarking their performance against classical machine learning models. Example laboratory modules include:

- Lab 1 – Malware Classification with Quantum Support Vector Machines (QSVM).
- Lab 2 – AI Model Poisoning Detection using Quantum Neural Networks (QNN).
- Lab 3 – Deepfake Identity Spoofing Detection with Quantum Boltzmann Machines (QBM).
- Lab 4 – Post-Quantum Cryptography Migration Risk Analysis with Quantum Kernel Classifier.

Each lab requires students to preprocess datasets, design parameterized quantum circuits, run experiments on quantum simulators, and document results comparing QML models with classical machine learning baselines.

Workforce and Research Integration:

This course supports the ARISE CyberAI Scholarship for Service program by preparing students to apply quantum-enabled analytical methods to cybersecurity problems relevant to federal agencies, including malware analysis, AI system protection, identity verification, and software supply chain security. Students completing the course will gain practical experience with emerging technologies expected to influence next-generation cyber defense systems.