

Hybrid Quantum-Classical Cyber Threat Intelligence Detection and Response Framework Using Quantum Kernels

Deepthi K C Kakumani

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India

Mohammad Assad Shaik

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India

Shanvitha Guntupalli

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India

Dimple Lakshmi Sindhuja Tallam

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India

Naga Sai Kusuma Priya Konduri

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India

Abstract:

The rising frequency and sophistication of cyber-attacks require intelligent and reliable intrusion detection systems that have the ability to detect different threat patterns with a high level of confidence. This paper proposed a hybrid quantumclassical cyber threat detection system that combines quantum-inspired support vector machine and classical ensemble learning techniques. The proposed framework integrates a quantum-inspired kernel-based SVM, Random Forest and XGBoost models that classifies network traffic into several attack categories, such as Denial of Service, Probe, Remote-to-Local and normal traffic. Feature preprocessing consists in categorical encoding, normalization and dimension reduction using principal component analysis for the efficiency of detection. A method of using a weighted ensemble approach is used to enhance the reliability of the predictions and then severity is evaluated and automated recommendations for response are made. The system is implemented as a web-based system with real-time prediction, batch analysis, database logging, and automated email alerts if critical threats are detected. Experimental evaluation based on network traffic data has proven the proposed approach to be effective for improving the accuracy of intrusion detection, while offering actionable security insights which can be applied in practical cybersecurity environments for monitoring and analysis.

Keywords:

Cyber Threat Detection, Intrusion Detection System, Quantum-Inspired Machine Learning, Ensemble Learning, Support Vector Machine, Random Forest, XGBoost, Network Traffic Analysis, Cybersecurity.