Chapter 3
Quantum-Enhanced Edge Computing for Robust Cyber Threat Detection

S. Anand
https://orcid.org/0009-0008-1845-3901
Infant Jesus College of Engineering, India

ABSTRACT

The growing complexity of cyber threats has surpassed traditional detection systems, especially where real-time response and distributed protection are vital. This chapter explores a hybrid Quantum-Edge framework for cyber threat detection. Quantum Computing's parallelism and advanced data processing capabilities complement Edge Computing's low-latency, decentralized analysis. Our framework integrates quantum feature transformation, quantum-enhanced anomaly detection, and federated learning on edge nodes. Using Qiskit, simulated attacks, and real-time edge processing, we demonstrate improved detection accuracy, lower false positives, and faster responses. We also propose future directions in quantum-resilient, privacy-preserving, and scalable cybersecurity solutions.

1.INTRODUCTION

In the digital era, cyberspace has become the backbone of global economies, critical infrastructures, government operations, healthcare, and everyday life. The exponential growth of connected devices, Internet-of-Things (IoT) deployments, 5G networks, and cloud-based services has led to an unprecedented surge in data generation and interconnectivity (Ning et.al,2018). While this hyper-connectivity brings tremendous benefits, it also exposes systems to an ever-evolving landscape

DOI: 10.4018/979-8-3373-3551-3.ch003

of sophisticated cyber threats. Modern adversaries leverage advanced persistent threats (APTs), zero-day vulnerabilities, polymorphic malware, ransomware, and highly coordinated distributed denial-of-service (DDoS) attacks that are increasingly difficult to detect, classify, and mitigate with conventional cybersecurity approaches.

Traditional cyber threat detection systems—typically centralized, rule-based, or signature-driven—struggle to keep pace with the scale, diversity, and dynamic nature of contemporary attacks. These systems often suffer from high false positive rates, delayed detection times, limited scalability, and inability to generalize to previously unseen attack vectors. Moreover, the centralized nature of most existing architectures creates single points of failure and performance bottlenecks, particularly in geographically distributed or mission-critical environments. As cyber adversaries become more intelligent and adaptable, the need for next-generation threat detection mechanisms that are scalable, adaptive, and resilient has become paramount.

Two rapidly advancing technologies hold transformative potential for the cybersecurity domain: Quantum Computing and Edge Computing. Individually, both offer unique strengths that directly address the limitations of classical cyber defense architectures. When integrated synergistically, they present a powerful paradigm shift capable of reshaping the future of cyber threat detection.

The Promise of Quantum Computing in Cybersecurity

Quantum Computing operates on principles fundamentally distinct from classical computation, harnessing quantum bits (qubits) that can exist in multiple states simultaneously due to superposition. Quantum entanglement and amplitude amplification further enable complex computations that would be infeasible for classical systems. In the context of cybersecurity, these properties allow quantum algorithms to efficiently explore vast solution spaces, uncover hidden correlations in high-dimensional threat data, and detect subtle anomalies that evade classical detectors (Faruk,2022).

Quantum machine learning (QML) algorithms, such as quantum support vector machines, quantum neural networks, and variational quantum circuits, demonstrate potential for enhanced pattern recognition, classification, and feature extraction from large cybersecurity datasets. Quantum algorithms like Grover's search and Shor's factorization have also spurred urgency in cryptographic research, highlighting both the offensive and defensive dimensions of quantum technologies in cybersecurity.

However, practical deployment of quantum systems remains limited due to hardware constraints, qubit decoherence, error rates, and the current infancy of fault-tolerant quantum computing. As quantum hardware evolves, hybrid quantum-classical approaches provide an immediate opportunity to embed quantum subroutines within classical cybersecurity pipelines, yielding incremental yet meaningful gains.

Career Path Recommender Using Quantum Machine Learning