Chapter 7
Quantum-Enhanced Machine Learning for Next-Gen Cyber Defense

Ushaa Eswaran
https://orcid.org/0000-0002-5116-3403
Mahalakshmi Tech Campus, India

Vishal Eswaran
https://orcid.org/0009-0000-2187-3108
CVS Health Centre, India

ABSTRACT

As cyber threats become more complex, traditional machine learning increasingly struggles with real-time detection and response. Rising data volumes, adversarial tactics, and classical computing limits call for new cybersecurity approaches. This chapter explores quantum-enhanced machine learning (QeML), leveraging quantum parallelism, entanglement, and amplitude amplification to improve data processing, pattern recognition, and classification in complex threat landscapes. We present a QeML framework combining quantum kernel estimation and variational circuits within a supervised learning pipeline for intrusion detection. Experiments on benchmark datasets using quantum simulators and hardware show improved accuracy, resilience, and efficiency over classical models. Case studies highlight practical challenges and future directions for scalable deployment. This chapter provides a foundation for applying QeML in cyber defense, offering guidance for leveraging quantum advantage to protect digital infrastructure.

DOI: 10.4018/979-8-3373-3551-3.ch007

1. INTRODUCTION

In the rapidly evolving landscape of digital communication and interconnected systems, cybersecurity has emerged as a cornerstone of technological resilience. The proliferation of connected devices, coupled with the digitization of critical infrastructure, has led to an exponential increase in the volume, velocity, and variety of data that needs to be secured (Argyroudis et.al,2022). Malicious actors now operate with unprecedented sophistication, leveraging automation, artificial intelligence, and complex exploit strategies to breach defenses, compromise privacy, and disrupt essential services. Traditional rule-based defense mechanisms, while foundational, have proven inadequate in dealing with the dynamic and polymorphic nature of modern cyber threats. In response, the cybersecurity community has turned to machine learning (ML) to build adaptive, data-driven systems capable of learning from patterns and anomalies, thereby offering scalable and proactive threat detection capabilities.

Machine learning has been pivotal in enhancing cyber defense, particularly in intrusion detection systems (IDS), anomaly detection, malware classification, and behavioral analytics. Supervised and unsupervised learning methods, including support vector machines (SVM), decision trees, k-nearest neighbors (KNN), random forests, and deep learning architectures such as convolutional and recurrent neural networks, have achieved significant success in detecting known attack signatures and modeling normal system behavior. However, these models are increasingly being challenged by adversarial attacks, the curse of dimensionality, computational bottlenecks, and the need for massive labeled datasets. Moreover, the scalability and latency constraints in real-time applications underscore a critical limitation: conventional ML models, running on classical computing hardware, are approaching their practical computational limits when tasked with high-dimensional, time-sensitive cybersecurity problems.

In parallel, quantum computing has emerged as a transformative paradigm with the potential to redefine computational boundaries. Based on the principles of quantum mechanics—such as superposition, entanglement, and quantum interference—quantum computing offers exponential speed-up for specific classes of problems that are otherwise intractable for classical machines. Quantum-enhanced machine learning (QML) is a nascent but rapidly developing field that seeks to leverage quantum processors to accelerate and improve the performance of ML algorithms. By encoding classical data into quantum states and exploiting the parallelism inherent in quantum operations, QML algorithms have demonstrated theoretical advantages in optimization, clustering, and pattern recognition tasks (Sachin Khurana,et.al,2024). This intersection of quantum computing and machine learning presents a compelling opportunity to develop next-generation cybersecu-