Chapter 1
A Comprehensive Introduction to Cyber Threat Detection Through Quantum Computing and Comparative Study of Classical and Quantum-Enhanced Convolutional Neural Networks

Humera Shaziya
https://orcid.org/0000-0002-7584-0990
Nizam College, India

Saif Ali Alsaidi
https://orcid.org/0000-0002-9907-7221
Wasit University, Iraq

ABSTRACT

This chapter explores the potential of integrating quantum computing and edge computing technologies to enhance cyber threat detection and response capabilities. It also discusses theoretical foundations, current research, practical implementations, and future prospects of combining quantum and edge computing for cybersecurity. Further, this work investigates quantum computing concepts infused in traditional convolutional neural networks (CNNs) for image classification. We present the

DOI: 10.4018/979-8-3373-3551-3.ch001

discussion of traditional versus quantum convolution practices when applied to the MNIST database. Our findings show that the quantum-enhanced model has a highest validation accuracy of 82.67%, which is higher than the 74.33% of the classical model. In addition, the quantum model displays greater confidence in accurate predictions (90.09%) than the 76.87% confidence of the classical model. These results indicate the promise of quantum-enhanced convolutional networks for enhancing image classification.

1.1 INTRODUCTION

In the digital age, the proliferation of interconnected systems and devices has given rise to an ever-growing number of cyber threats. As organizations increasingly rely on cloud infrastructure, Internet of Things (IoT), artificial intelligence (AI), and big data analytics, the attack surface has widened, making cyber defense a paramount concern. Traditional cybersecurity systems are often reactive and centralized, which limits their ability to detect and respond to threats in real-time. Meanwhile, adversaries are using sophisticated tools such as AI-driven malware, advanced persistent threats (APTs), and coordinated attacks to exploit system vulnerabilities. Need for Advanced Cyber Threat Detection Existing cybersecurity strategies struggle to keep pace with the rapidly evolving threat landscape. Signature-based systems fail to identify zero-day exploits, and heuristic models often generate false positives. In such a context, there is a compelling need for cybersecurity solutions that are not only proactive and intelligent but also capable of operating in a distributed and high-speed environment. The fusion of quantum computing and edge computing technologies represents a promising approach to addressing these challenges by enabling real-time, scalable, and intelligent threat detection capabilities.

Emerging technologies such as quantum computing and edge computing have the potential to disrupt and transform the field of cybersecurity. Quantum computing introduces a paradigm shift by leveraging quantum phenomena to solve complex mathematical problems exponentially faster than classical computers. This can be used to break classical encryption but also to create virtually unbreakable quantum-resistant encryption protocols. Edge computing, on the other hand, brings processing closer to the data source, minimizing latency and enhancing the capability to detect threats at the network's edge before they propagate. Objectives of the Study This study aims to explore the intersection of quantum computing and edge computing as a novel paradigm for enhancing cyber threat detection. The primary objectives are:

- To examine the principles and capabilities of quantum and edge computing in the context of cybersecurity.