Chapter 2
Quantum AI for Cybersecurity and Threat Intelligence

Nizirwan Anwar
https://orcid.org/0000-0003-1189-9093
Universitas Esa Unggul, Indonesia

Titik Khawa Abdul Rahman
Asia e University, Malaysia

Husna Sarirah Husin
https://orcid.org/0009-0004-9578-7877
Taylor's University, Malaysia

ABSTRACT

The rise in sophisticated cyber threats necessitates innovative defense strategies that transcend traditional approaches. This chapter explores the integration of Quantum Computing, Edge Computing, and Artificial Intelligence to enhance cyber threat detection and intelligence. Edge devices enable real-time anomaly detection with minimal latency, while quantum-enhanced AI models, such as quantum SVMs and variational circuits, offer scalable analysis for large-scale threat intelligence. By combining localized response with advanced quantum analytics, a multi-layered security framework is proposed to support adaptive, intelligent, and resilient cybersecurity infrastructures. This fusion not only strengthens detection capabilities but also enhances predictive insight and cryptographic resistance.

DOI: 10.4018/979-8-3373-3551-3.ch002

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

I. INTRODUCTION

The intersection of quantum computing, edge computing, and artificial intelligence (Figure 1) has the potential to transform cyber threat detection and enhance cybersecurity overall. Recent scholarly contributions highlight the importance of combining these advanced technologies to better address the growing cyber threats and improve the capabilities of security systems. Quantum computing has shown promise in developing intelligent cyber threat detection systems. Azeez et al. propose a framework that utilizes the computational power of quantum systems to analyse complex datasets for recognizing patterns indicative of cyber threats, thereby enhancing the efficiency and accuracy of threat detection mechanisms (Azeez et al., 2024). The ability of quantum computing to process large volumes of data rapidly enables the real-time analysis necessary to counteract sophisticated attacks, improving response times and mitigating potential damage. Edge computing is also essential for advancing cybersecurity. As digital infrastructures move closer to data sources, the attack surface expands, necessitating multi-layered security protocols to protect sensitive information. Emphasizes the need for an array of security measures in edge-based applications, including encryption, intrusion detection, and advanced threat intelligence systems to safeguard critical data (Dornala, 2023). This integration of security practices at the edge minimizes latency and boosts the capability to manage threats in real-time, which is crucial for contemporary security operations.

Machine learning techniques have increasingly been employed alongside edge computing to enhance threat detection capabilities. Discuss using hyperdimensional computing models to improve unsupervised learning for threat detection at the edge of the Internet of Things (IoT) (Christopher et al., 2021). Their work demonstrates how adaptive machine learning algorithms can enhance detection rates while effectively managing dynamic edge environments. This adaptability allows for the timely identification and neutralization of threats, reducing the risk associated with vulnerabilities in edge devices.

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/quantum-ai-for-cybersecurity-and-threat-intelligence/388295

Related Content

Electronic and Optical Properties of Quantum Nano-Structures: Quantum Well Systems

Shivakumar Hunagund (2023). *Principles and Applications of Quantum Computing Using Essential Math (pp. 54-76).*
www.irma-international.org/chapter/electronic-and-optical-properties-of-quantum-nano-structures/330439

Quantum Machine Learning (QML) Techniques for Enhancing Online Marketing and Business

S. Varalakshmi, Anupam Sharma, Latifa Saud Al Habsiand Yasmeen Sultana (2025). *Exploring the Fusion of Quantum Computing and Machine Learning (pp. 199-226).*
www.irma-international.org/chapter/quantum-machine-learning-qml-techniques-for-enhancing-online-marketing-and-business/375928

Introduction and Beginners Guide to Quantum Computing

Poornima Nedunchezhianand Rajkumar Rajasekaran (2022). *Technology Road Mapping for Quantum Computing and Engineering (pp. 1-10).*
www.irma-international.org/chapter/introduction-and-beginners-guide-to-quantum-computing/300513

Fundamentals of Quantum Computation and Basic Quantum Gates

Swathi Mummadiand Bhawana Rudra (2024). *Quantum Computing and Cryptography in Future Computers (pp. 33-50).*
www.irma-international.org/chapter/fundamentals-of-quantum-computation-and-basic-quantum-gates/352406

Smart Healthcare Innovations Using Intelligent Systems in Industry 4.0

Swathi Sree, Kishor Kumar Reddyand Srinath Doss (2025). *Integration of AI, Quantum Computing, and Semiconductor Technology (pp. 391-414).*
www.irma-international.org/chapter/smart-healthcare-innovations-using-intelligent-systems-in-industry-40/360870