Chapter 6
Synergizing Edge AI and Quantum Machine Learning for Real-Time Cyber Threat Mitigation

Shashank Solanki
https://orcid.org/0009-0002-5923-0516
Christ University, India

Rituraj Sinha
https://orcid.org/0000-0001-5790-9571
Christ University, India

ABSTRACT

The escalation of the complexity of cyber threats must be countered by traditional signature- and rule-based security approaches. In this study, we propose a hybrid Edge AI–Quantum Machine Learning (QML) framework that employs variational quantum circuits and classical neural networks towards real-time per–device threat detection. Using three case studies, we validate the framework: (1) fraud detection in high frequency trading with 17% more true positives and 22% less false positives; (2) inference times under 100 ms for IoT anomaly detection; and (3) reduction of over 25% in deepfake misclassification. The built system is built end-to-end with an open-source stack. Finally, regulatory and ethical considerations (GDPR, data, privacy, international cybersecurity protocols, etc., Budapest Convention) are discussed. In presenting this work, we present a scalable and adaptive model for next-generation cybersecurity.

DOI: 10.4018/979-8-3373-3551-3.ch006

1. INTRODUCTION

There is urgent need to change cybersecurity due to ever changing cyber security threats we face keep repeating brick walls and evolving new forms of threats It is high time we changed our old methods of cyber security that are no longer sufficient to deal with repeating brick walls and the new forms of threats. With the emergence of more sophisticated attacks on the modern day digital network, it is now time to go beyond the existing cybersecurity measures which do not protect against zero-day exploits. As signatures detection and response activities are effective against known threats and do not check new threats, new solutions to cybersecurity are needed (Samia, Saha, & Haque, 2024). The Edge Artificial Intelligence and Quantum Machine Learning complement each other in enhancing the speed of situational processing and the adaptive presentation of security strategies to countermeasures the existing and emerging security threats. The addition of data processing and analysis nodes can reduce response time, as well as assist a system in adapting more quickly to novel threats manifesting at the edge of the network. Due to the fact that it relies on quantum mechanics, Quantum Machine Learning could be used to solve difficult tasks and allow us to observe the early indicators of cyber threat in a quick manner (Sutradhar, Venkatesh, & Venkatesh, 2024). When collaborating, Edge AI and Quantum Machine Learning will develop a means to secure digital assets that are currently interconnected everywhere.

As the number of devices that communicate and transmit data increases across the entire internet, these have increased the chances of bad guys doing bad things (Anisha, Reddy, & Nguyen, 2021). The list of organisations, which may be attacked, has been extended significantly. Cybersecurity issues have become even more challenging considering that the attacks initiated by nation-states and criminal organisations are well organised. Things are not funny in the cyberspace today, as the threats of attacks by agencies and organised crime syndicates seem to be evolving all the time. This is because such attacks are very perilous to essential facilities as well as confidential information, given their capability to remain undetected over a length of time. The majority of the affected businesses also experience financial difficulties and disruption in their operations following the ransomware attacks by attackers (Ragab et al., 2025). They are some of the most severe threats since they exploit vulnerabilities in software that most people do not know about and can evade detection by regular cyber security measures. Malware threat is increasing on a daily basis with more than 200,000 new viruses being identified on a daily basis and thus cybersecurity systems need to be both intelligent and adapt to respond to them as well (Ahmed et al., 2022). Outdated methods of cyber defense are dependent upon the matters that cannot be rolled back or modified in some way, thus the contemporary and rapidly evolving risks continue to slip through. Due to digital transformation,

Navigating the Cybersecurity Terrain: An Overview of Essential Tools and Techniques

Adithya P. Shetty, B. Prajwaland E. Saravana Kumar (2025). *Advancing Cyber Security Through Quantum Cryptography (pp. 259-306).*
www.irma-international.org/chapter/navigating-the-cybersecurity-terrain/360369