Chapter 4
LLMs for Quantum-Aware Threat Detection and Incident Response

Luay Albtosh
https://orcid.org/0009-0009-0338-9123
Capitol Technology University, USA & Houston Community College, USA

ABSTRACT

The integration of Large Language Models (LLMs) into cybersecurity offers significant potential for enhancing threat detection and incident response, particularly in the context of emerging quantum computing capabilities. As quantum computing threatens to undermine traditional cryptographic systems, there is a pressing need for quantum-aware cybersecurity measures. This chapter explores the application of LLMs in identifying and mitigating threats in a quantum-aware environment. It examines how LLMs can aid in detecting quantum-related vulnerabilities, analyzing quantum-aware attack vectors, and automating incident response protocols. Additionally, the chapter discusses the challenges of adapting LLMs to the quantum landscape, including the need for specialized training datasets and the consideration of quantum-resistant algorithms. Through case studies and theoretical models, this chapter provides a comprehensive view of how LLMs can be leveraged to strengthen cybersecurity in the era of quantum computing.

1. INTRODUCTION

As quantum computing continues to evolve, its potential to revolutionize the fields of cryptography and cybersecurity is becoming increasingly apparent. Quantum computing's ability to process vast amounts of data and perform complex calculations

DOI: 10.4018/979-8-3373-1102-9.ch004

at unprecedented speeds introduces both opportunities and challenges in securing digital assets. Traditional security measures, particularly cryptographic protocols that form the backbone of modern cybersecurity systems, are vulnerable to quantum computing's capabilities (Sodiya et al., 2024). This vulnerability underscores the need for quantum-aware cybersecurity systems, which can detect, mitigate, and respond to threats in environments where quantum computing may be actively utilized by malicious actors.

In this context, Large Language Models (LLMs), which have shown exceptional capabilities in natural language processing (NLP), are emerging as powerful tools for enhancing cybersecurity frameworks. LLMs, such as OpenAI's GPT models, are capable of processing and analyzing massive datasets to detect anomalous patterns, predict attack vectors, and generate responses in real-time. Their application in cybersecurity, particularly in threat detection and incident response, is of significant interest due to their ability to learn from vast datasets and adapt to emerging cyber threats. Furthermore, as quantum computing becomes more accessible, LLMs must be adapted to understand quantum-aware attack vectors and integrate quantum-resistant mechanisms into their models.

The potential for LLMs in quantum-aware cybersecurity is multifaceted. For instance, LLMs can aid in the identification of quantum-related vulnerabilities, such as those posed by quantum key distribution (QKD) and the vulnerability of current encryption algorithms to quantum attacks (Rahul et al., 2024). By training LLMs on quantum-specific datasets, researchers can develop systems that are capable of predicting and mitigating these novel types of attacks before they impact critical systems.

Moreover, the integration of LLMs into quantum-aware cybersecurity systems can facilitate more efficient incident response. LLMs can analyze attack logs, identify patterns indicative of a quantum-enhanced cyberattack, and autonomously trigger countermeasures. This ability is particularly important for detecting zero-day threats, which are notoriously difficult to identify using traditional security measures (Jones & Omar, 2024). LLMs' capacity to understand the context of a cyberattack, whether quantum-related or not, makes them an invaluable tool in minimizing damage and restoring system integrity swiftly.

However, the adoption of LLMs in quantum-aware threat detection and incident response is not without challenges. One of the main hurdles is the need for specialized training datasets that can represent both classical and quantum-aware cybersecurity threats (Gholami & Omar, 2024). While LLMs excel at identifying patterns in large datasets, they are only as good as the data on which they are trained. Quantum-specific datasets are still in their infancy, and significant efforts are required to develop data that accurately represents the evolving landscape of quantum cyber threats. Addi-