Chapter 1
Introduction to Quantum-Aware Cybersecurity: The Need for LLMs

Hewa Majeed Zangana
https://orcid.org/0000-0001-7909-254X
Duhok Polytechnic University, Iraq

Marwan Omar
Illinois Institute of Technology, USA

ABSTRACT

The advent of quantum computing poses unprecedented challenges to the security of classical cryptographic systems, driving the need for innovative approaches in cybersecurity. This chapter introduces the concept of quantum-aware cybersecurity, highlighting the pivotal role of large language models (LLMs) in addressing emerging threats. By leveraging LLMs' advanced capabilities in data analysis, threat detection, and adaptive learning, organizations can enhance resilience against quantum-era vulnerabilities. The chapter emphasizes the integration of LLMs with quantum-resistant cryptographic techniques, fostering a secure foundation for the next-generation digital ecosystem. This exploration underscores the urgency of adopting quantum-aware strategies to safeguard critical infrastructures and data integrity.

DOI: 10.4018/979-8-3373-1102-9.ch001

1. INTRODUCTION

The rapid advancements in quantum computing present both opportunities and challenges for the cybersecurity landscape. While quantum technologies promise to revolutionize various domains through unparalleled computational power, they also pose significant risks to classical encryption systems, which are foundational to current cybersecurity frameworks. With this backdrop, the integration of Large Language Models (LLMs) into quantum-aware cybersecurity is emerging as a novel paradigm, combining the predictive and analytical prowess of AI with strategies to mitigate quantum threats.

1.1 Quantum Computing: A Double-Edged Sword

Quantum computing introduces an era where classical cryptographic techniques, such as RSA and ECC, are rendered vulnerable due to algorithms like Shor's and Grover's. The quantum threat compels researchers and industry stakeholders to explore quantum-resistant algorithms and frameworks. Sodiya et al. (2024) provide an exhaustive review of the potential impacts of quantum computing on U.S. cybersecurity, emphasizing the urgency of adapting to this paradigm shift.

In parallel, quantum advancements have catalyzed developments in industrial quantum networks (Bush et al., 2021), showcasing opportunities for enhanced communication and computation. However, these advancements also underscore the importance of robust quantum-aware security measures to prevent vulnerabilities in interconnected systems.

To understand the implications of quantum computing on classical cryptography, it is essential to compare the computational approaches of classical and quantum systems. The diagram below illustrates the key differences in their functioning and highlights how quantum algorithms disrupt the foundations of cryptographic systems like RSA and ECC.