

Chapter 3

LLMs for Enhancing Privacy and Data Protection in Quantum Computing Environments

Angel Justo Jones

 <https://orcid.org/0009-0007-9740-6611>

University of Virginia, USA

ABSTRACT

The rapid advancement of quantum computing presents both tremendous opportunities and significant challenges for cybersecurity, particularly in the realms of privacy and data protection. Traditional encryption methods face obsolescence in the quantum era, as quantum algorithms like Shor's algorithm can efficiently break widely used cryptographic schemes. Large Language Models (LLMs), with their capacity for processing and analyzing vast amounts of data, have emerged as valuable tools in addressing privacy concerns in quantum computing environments. This chapter explores how LLMs can be leveraged to enhance privacy and data protection by facilitating the development of quantum-resistant cryptographic protocols, automating threat detection, and assisting in the creation of novel security architectures tailored to quantum technologies. By examining the intersection of LLMs and quantum computing, this work highlights their potential to reshape cybersecurity strategies to ensure that data remains secure in a post-quantum world.

DOI: 10.4018/979-8-3373-1102-9.ch003

1. INTRODUCTION

Quantum computing, with its potential to revolutionize computational paradigms, introduces both profound opportunities and complex challenges for cybersecurity, particularly regarding privacy and data protection. As quantum systems evolve, the cryptographic methods that have long safeguarded sensitive data, including symmetric and asymmetric encryption schemes, face obsolescence. The advent of quantum computing threatens to break widely used cryptographic protocols—such as RSA and ECC—due to its ability to solve certain mathematical problems much faster than classical computers, especially using algorithms like Shor’s algorithm (Rahul et al., 2024). These shifts in computational power necessitate the development of new approaches for safeguarding data and ensuring privacy in a quantum computing era.

Large Language Models (LLMs), a subset of artificial intelligence (AI), have shown significant promise in addressing cybersecurity challenges. Originally designed for natural language processing tasks, LLMs such as OpenAI’s GPT series and Google’s BERT have demonstrated remarkable abilities in understanding, generating, and interacting with human language. Recent studies show that these models can be harnessed to detect and mitigate cybersecurity threats, such as zero-day vulnerabilities and malware attacks (Jones et al., 2024; Huff et al., 2023). In particular, LLMs offer unique advantages in quantum computing environments, where traditional security tools may not be applicable (Jones, 2024).

LLMs are also poised to play a crucial role in the development of quantum-resistant cryptographic systems. As quantum algorithms evolve, post-quantum cryptography (PQC) has become important in the research community (Bishwas & Sen, 2024). LLMs, with their capacity to process large volumes of data and model complex patterns, can be leveraged to design and evaluate new cryptographic protocols that withstand the capabilities of quantum computers. Furthermore, they can be used to generate synthetic data for training other AI models, which is particularly beneficial for industries requiring quantum-resilient security systems (Gholami & Omar, 2023).

In addition to cryptography, LLMs can significantly improve privacy protection by enhancing threat detection and incident response capabilities in quantum computing environments. Quantum computing introduces novel attack vectors, such as quantum-enhanced eavesdropping, which could bypass current encryption methods. LLMs, when combined with quantum-specific security protocols, can proactively detect anomalies, identify potential threats, and automate response mechanisms in real-time. Their ability to process and analyze vast datasets enables them to recognize patterns that might be imperceptible to traditional security systems.

The intersection of quantum computing and LLMs in cybersecurity is still an emerging area of research, but it promises to offer innovative solutions to the challenges posed by quantum technologies. As this field develops, it is essential to

36 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/llms-for-enhancing-privacy-and-data-protection-in-quantum-computing-environments/366976

Related Content

Leveraging Chat GPT for Sustainable Marketing Practices and Pricing Insinuations

Rohit Soodand Ashwani Panesar (2025). *Intersecting Natural Language Processing and FinTech Innovations in Service Marketing* (pp. 323-336).

www.irma-international.org/chapter/leveraging-chat-gpt-for-sustainable-marketing-practices-and-pricing-insinuations/377513

Language Processing and Python

Belsini Glad Shiya V.and Sharmila K. (2021). *Deep Natural Language Processing and AI Applications for Industry 5.0* (pp. 93-119).

www.irma-international.org/chapter/language-processing-and-python/284205

Pronominal Anaphora Resolution on Spanish Text

Alonso García, Martha Victoria González, Francisco López-Orozcoand Lucero Zamora (2021). *Handbook of Research on Natural Language Processing and Smart Service Systems* (pp. 309-326).

www.irma-international.org/chapter/pronominal-anaphora-resolution-on-spanish-text/263108

Natural Language Processing in Online Reviews

Gunjan Ansari, Shilpi Guptaand Niraj Singhal (2021). *Natural Language Processing for Global and Local Business* (pp. 40-64).

www.irma-international.org/chapter/natural-language-processing-in-online-reviews/259783

Exploring the Relationship Between Customer Services and Fintech Adoption Among Generation X: An Empirical Study in Odisha, India.

Dusmant Kumar Sahoo, B.C.M. Patnaik, Ipseeta Satpathy, Vishal Jainand Shiva Ram Patnaik (2025). *Intersecting Natural Language Processing and FinTech Innovations in Service Marketing* (pp. 203-216).

www.irma-international.org/chapter/exploring-the-relationship-between-customer-services-and-fintech-adoption-among-generation-x/377508