RADemics

Post-Quantum Cryptography and Quantum Machine Learning for Resilient Encryption in AI-Driven Cybersecurity

Krishna Kumar, Sathea Sree.S, R. Baghia Laxmi

VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES, ST. JOSEPH'S COLLEGE OF ENGINEERING, (AN AUTONOMOUS INSTITUTION)

Post-Quantum Cryptography and Quantum Machine Learning for Resilient Encryption in AI-Driven Cybersecurity

[1]Krishna Kumar, AI Expert & Data Scientist, Artificial Intelligence, nitcseac@gmail.com

[2]Sathea Sree.S, Assistant Professor, Computer Science Engineering, Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, satheasree.se@vistas.ac.in

[3]R. Baghia Laxmi, Assistant Professor, Artificial Intelligence and Data Science, St. Joseph's College of Engineering (An autonomous institution), OMR, Chennai - 119, Tamilnadu. Mail id: laxmiram1995@gmail.com

Abstract

The rapid evolution of quantum computing poses a significant challenge to traditional encryption systems, with the potential to compromise the security of sensitive digital infrastructures. Post-Quantum Cryptography (PQC) has emerged as a vital field, aiming to develop encryption algorithms resilient to quantum attacks. Simultaneously, Quantum Machine Learning (QML) is revolutionizing the way machine learning models process data, offering new avenues for enhancing cybersecurity measures. This chapter explores the integration of PQC and QML to create robust, future-proof encryption systems capable of adapting to the evolving threat landscape. By examining hybrid models that combine the quantum resistance of PQC with the adaptability and efficiency of QML, this work highlights the potential for creating scalable and efficient cryptographic frameworks. The challenges and opportunities presented by the intersection of PQC and QML are discussed, with a focus on resource-constrained environments where computational power and memory are limited. Through this analysis, the chapter offers a comprehensive roadmap for advancing AI-driven, quantum-resistant cybersecurity solutions, addressing both theoretical advancements and practical implementation challenges.

Keywords: Post-Quantum Cryptography, Quantum Machine Learning, Cybersecurity, Quantum-Resistant Encryption, Hybrid Cryptographic Models, Scalable Security Solutions.

Introduction

The rapid advancements in quantum computing have raised significant concerns regarding the security of existing cryptographic systems that underpin modern digital infrastructures. Classical cryptographic algorithms, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), rely on mathematical problems that are computationally infeasible for classical computers to solve. However, quantum computers, leveraging the power of quantum mechanics, can potentially solve these problems exponentially faster, rendering widely used encryption methods vulnerable to decryption. This shift has necessitated a rethinking of cryptographic protocols, and Post-Quantum Cryptography (PQC) has emerged as the primary solution. PQC aims to develop encryption systems capable of resisting attacks from quantum computers, ensuring the continued security of sensitive data in a quantum-driven world.

The field of Quantum Machine Learning (QML) has gained significant traction, with researchers exploring the use of quantum computing techniques to enhance traditional machine learning models. QML offers the potential to process vast datasets exponentially faster than classical algorithms, making it an ideal candidate for applications in cybersecurity. By utilizing quantum computing's ability to handle complex and high-dimensional data, QML can improve threat detection, anomaly identification, and predictive analysis, providing a dynamic and adaptive approach to securing digital systems. As a result, the convergence of PQC and QML presents a promising avenue for enhancing the resilience of encryption systems in the face of evolving cyber threats.

The integration of PQC and QML to create hybrid cryptographic systems offers a powerful framework for building quantum-resistant, AI-driven cybersecurity solutions. This combination holds the potential to address the limitations of classical encryption methods by providing both quantum resistance and adaptability in a rapidly changing threat landscape. By incorporating machine learning into PQC, systems can evolve and strengthen in response to emerging attack strategies, effectively "learning" from past threats. This synergy between PQC's security guarantees and QML's dynamic data processing capabilities could enable the creation of encryption models that not only protect against quantum-based attacks but also adapt and improve based on ongoing threat intelligence.

The integration of PQC and QML into a single hybrid model is not without its challenges. The computational demands of both PQC and QML are significant, and their combined implementation in real-world systems raises concerns regarding efficiency and scalability. Cryptographic algorithms like lattice-based encryption require extensive computational resources, while QML models, particularly those based on quantum neural networks (QNNs), require substantial processing power. In resource-constrained environments, such as IoT devices, edge computing platforms, and mobile systems, these resource demands can become prohibitive. Therefore, optimizing these hybrid models for such environments is essential to ensuring their practical deployment in real-world applications.