2nd International Conference on Intelligent Digitization of Systems and Services, Valencia, Spain, 18-21 August 2025

Post-quantum cryptography standards for future proof IoT security: A literature review

Nelufule, Nthatheni

Abstract

The advent of quantum computing technology has transformed computing technologies into a machine with higher computing power. However, this has also introduced vulnerability challenges, as traditional cryptographic systems are prone to vulnerability to cyber threats, particularly in the context of the IoT. This paper presents a systematic literature survey of the landscape of postquantum cryptographic systems and their impact on the security of connected systems. The paper has explored various key encapsulation mechanisms that are resistant to quantum attacks, existing post-quantum standards, and assessed their applicability in the IoT environments and implementation challenges. The paper highlighted some of the limitations for adopting post-quantum cryptography due to limited existing standards which can be used to enforce the confidentiality, integrity, security, and privacy of data transmitted particularly by IoT connected devices.