Advancements in Quantum Computing for Next-Generation Cybersecurity

Hamed Taherdoost
University Canada West, Vancouver, Canada
GUS Institute, Global University Systems, London, UK

Abstract

Quantum computing represents a paradigm shift in computational power, offering unprecedented capabilities to solve complex problems that classical computers cannot efficiently handle. This paper explores the intersection of quantum computing and cybersecurity, highlighting how quantum algorithms, such as Shor's and Grover's algorithms, impact data encryption, cryptanalysis, and secure communication protocols. The study examines the development of quantum-resistant cryptography, including lattice-based and post-quantum encryption schemes, to safeguard sensitive information against potential quantum attacks. Additionally, it discusses practical challenges in implementing quantum security solutions, such as hardware limitations, error correction, and scalability. By analyzing recent research and emerging trends, this paper provides a roadmap for integrating quantum technologies into secure computing systems, emphasizing their transformative potential for the future of secure digital infrastructure.

Keywords

Quantum Computing, Cybersecurity, Post-Quantum Cryptography, Quantum Algorithms, Data Encryption, Secure Communication, Cryptanalysis, Emerging Technologies.