IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, May 2025
Impact Factor: 7.67

Harnessing Quantum Computing to Revolutionize Cybersecurity in the Age of Advanced AI Threats

Mr. Atharva Jadhav and Prof. Omprakash Mandge
MET Institute of Computer Science, Mumbai, India
mca23_1420ics@met.edu, omprakashm_ics@met.edu

Abstract: *As artificial intelligence (AI) evolves, it is increasingly able to outsmart traditional cybersecurity measures, particularly encryption algorithms. Quantum computing, with its potential to break current encryption standards like RSA and ECC, presents both a major threat and an opportunity. This paper explores how quantum computing could revolutionize cybersecurity by enabling the development of quantum-resistant encryption methods while simultaneously posing risks to existing systems. The study combines a literature review, theoretical analysis, and simulations to investigate the impact of quantum computing on encryption. Shor's algorithm is used to demonstrate how quantum computing can break traditional encryption methods. Post-quantum cryptography and progress in developing quantum-resistant encryption protocols are also evaluated. Additionally, the research includes case studies of organizations integrating quantum technologies into their cybersecurity strategies and simulations comparing quantum-resistant algorithms with AI-driven cyberattacks. The findings reveal significant vulnerabilities in current encryption, highlight the promise and limitations of post-quantum cryptographic algorithms, and explore the potential of quantum enhanced AI systems in real-time threat detection. However, challenges in adoption and scalability persist.*

Keywords: quantum computing, AI threats, cybersecurity, post-quantum cryptography, quantum-resistant encryption

DOI: 10.48175/IJARSCT-27812