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 6, Issue 2, March 2026
Impact Factor: 8.2

Leveraging Quantum Computing to Strengthen Cybersecurity in Banking

Anish Shrimali
Chief Manager, Union Learning Academy- Digital Transformation
Union Bank of India, Mumbai, India

Abstract: *The banking sector remains a high-value target for cyberattacks due to its vital role in managing sensitive financial data and enabling large-scale digital transactions. As digital banking expands, cyber risks increasingly carry systemic implications. In this context, quantum computing represents a fundamental shift in the cybersecurity landscape. Widely used encryption mechanisms such as RSA and elliptic curve cryptography (ECC), which underpin digital banking, payments, and data protection, are vulnerable to future quantum attacks particularly under the "harvest now, decrypt later" (HNDL) threat model, where encrypted financial data collected today may be compromised once quantum computing capabilities mature. This research examines the role of quantum computing in reshaping banking cybersecurity, with emphasis on post-quantum cryptography (PQC), quantum key distribution (QKD), quantum random number generation (QRNG), and quantum machine learning (QML) for fraud detection. Drawing on global and Indian banking practices, regulatory guidance from RBI and SEBI, and policy initiatives such as India's National Quantum Mission, the study proposes a structured roadmap for quantum readiness. The NIST finalization of PQC standards (FIPS 203–205, August 2024) has removed a key barrier to action, enabling banks to begin quantum-safe migration immediately. The study concludes that quantum-safe migration is a strategic imperative requiring phased implementation, architectural modernization, and coordinated regulatory and institutional action.*

Keywords: Quantum Computing, Post-Quantum Cryptography, Quantum Key Distribution, Banking Cybersecurity, Harvest Now Decrypt Later, NIST Standards, Cryptographic Agility, Quantum Random Number Generation, Quantum Machine Learning, Indian Banking, RBI, SEBI

DOI: 10.48175/IJARSCT-31523