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 1, February 2026
Impact Factor: 8.2

Toward Quantum-Resilient Cloud and Edge Security: Post-Quantum Cryptographic Architectures

Dr. C. Nagesh[1], Chatta Balaji[2], K Sudhakar[3], Dr. V. Sujay[4]
Associate Professor, Department of CSE[1]
Assistant Professor, Department of CSE[2,3]
Associate Professor, Department of AI[4]
Tadipatri Engineering College, Tadipatri[2,]
GATES Institute of Technology, Gooty[1,3,4]

Abstract: *The rapid advancement of quantum computing threatens the security foundations of classical public-key cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC), which underpin cloud and edge infrastructures. With scalable quantum algorithms capable of breaking widely deployed cryptographic primitives, organizations must transition toward quantum-resilient security models. This paper proposes a comprehensive Quantum-Resilient Cryptographic Architecture (QRCA) designed specifically for cloud and edge computing environments. The framework integrates post-quantum cryptographic (PQC) algorithms, hybrid key exchange protocols, zero-trust principles, and hardware-assisted secure enclaves. We present a layered security model that balances computational overhead, latency constraints, and scalability requirements in distributed systems. Experimental simulations evaluate performance metrics including encryption latency, key exchange overhead, and throughput across cloud data centres and edge nodes. Results indicate that hybrid PQC deployments achieve strong quantum resilience with manageable performance trade-offs. The proposed architecture offers a practical migration pathway for organizations seeking future-proof cryptographic security in distributed computing ecosystems.*

Keywords*:* Post-Quantum Cryptography, Quantum-Resilient Security, Cloud Security, Edge Computing, Lattice-Based Cryptography, Hybrid Encryption, Zero Trust Architecture

DOI: 10.48175/IJARSCT-31117