IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 4, Issue 1, October 2024
Impact Factor: 7.57

Designing a Zero-Trust Post-Quantum Encryption Framework for Adaptive End-to-End Network Security in Dynamic Threat Environments

Samuel Amoateng[1*], Omolola A. Akinola[2], Victor Ogechukwu Anuebunwa[3], Jesudunsin Olaobaju[4]
Department of Informatics, Fort Hays State University, Hays, Kansas, USA[1]
Department of Information Technology, University of Cumberlands, Kentucky, USA[2]
Department of Computer Science, University of Nigeria, Nsukka, Nigeria[3]
NHS Derby and Derbyshire ICB, United Kingdom[4]

Abstract: *The advent of quantum computing poses a fundamental threat to classical encryption protocols, demanding urgent transformation in cybersecurity architectures. This study presents a U.S.-focused Zero-Trust Enabled Post-Quantum Encryption Framework (ZT-PQEF) designed to deliver adaptive end-to-end network security in dynamic threat environments. ZT-PQEF integrates NIST-standard post-quantum cryptographic algorithms (CRYSTALS-Kyber and Dilithium) with behavior-informed trust scoring, real-time key rotation, and telemetry-driven microsegmentation. A U.S. federal network simulation was used to benchmark the framework across nine performance metrics and seven critical system dimensions. Compared to conventional zero-trust and static PQC-enabled architectures, ZT-PQEF achieved a 22% improvement in cryptographic agility, reduced breach containment time by over 40%, and significantly lowered false-positive rates in behavioral anomaly detection. The framework preserved bandwidth viability and minimized resource overhead, confirming its suitability for high-throughput, resource-sensitive government deployments. These results demonstrate that ZT-PQEF delivers scalable, quantum-resilient, and policy-adaptive security, representing a critical advancement in post-quantum infrastructure protection and future-proof zero-trust implementation across the United States.*

Keywords: Post-Quantum Cryptography, Zero Trust Architecture, Adaptive Network Security, Quantum-Resilient Encryption, Trust Scoring, Key Rotation, Behavioral Anomaly Detection, U.S. Cybersecurity, Dynamic Threat Environments, CRYSTALS-Kyber, CRYSTALS-Dilithium