Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Quantum Shield: Post-Quantum Security for Next-Generation Digital Communication

Dr. K Raghavendar[1], T Khyathi Gayathri[2], T Mounika[2], P Babu[2]

[1]Associate Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India
[2]Student, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

Correspondence

Dr. K Raghavendar

Associate Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

- Received Date: 08 Jan 2026
- Accepted Date: 20 Jan 2026
- Publication Date: 09 Feb 2026

Keywords

Post-Quantum Cryptography, Quantum-Resistant Digital Communication, NIST PQC Standards, ML-KEM, ML-DSA, Crypto-Agility, Harvest-Now-Decrypt-Later

Abstract

The advent of cryptographically relevant quantum computers poses an existential threat to current public-key cryptographic systems (RSA, ECC) widely used in digital communication protocols such as TLS, IPsec, VPNs, and secure messaging. Traditional systems face risks from "Harvest Now, Decrypt Later" attacks, compromising long-term confidentiality of sensitive data in finance, healthcare, government, and critical infrastructure. This paper proposes Quantum Shield, a comprehensive post-quantum secure framework for next-generation digital communication. It integrates NIST-standardized post-quantum algorithms (ML-KEM for key encapsulation, ML-DSA and SLH-DSA for digital signatures) with hybrid crypto-agile designs, hardware acceleration support, and role-based access controls. The system ensures quantum-resistant key establishment, authentication, and end-to-end encryption while maintaining low latency and high throughput. Experimental evaluation on simulated network traffic demonstrates acceptable performance overhead, enhanced resistance to quantum attacks, improved traceability, and secure multi-party coordination. Quantum Shield bridges the gap between classical and quantum-safe infrastructures, fostering trust and compliance in an era of quantum threats.

Introduction

Digital communication underpins modern society, enabling secure transactions, confidential exchanges, and critical infrastructure operations. However, the rapid advancement toward cryptographically relevant quantum computers (CRQCs) threatens to break asymmetric cryptography via Shor's algorithm, rendering RSA and ECC insecure. Adversaries may already be collecting encrypted data for future decryption, exacerbating risks in sectors reliant on long-term confidentiality.

Post-quantum cryptography (PQC) offers a transformative solution by developing algorithms resistant to both classical and quantum attacks, based on hard problems like lattices, hash functions, and codes. NIST's multi-year standardization process culminated in 2024 with FIPS 203 (ML-KEM, derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, from CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, from SPHINCS+), providing ready-to-deploy quantum-safe primitives.

This paper introduces Quantum Shield, a unified system that embeds these standards into communication stacks. It employs hybrid schemes (combining classical and PQC for transition), hardware-accelerated implementations for efficiency, and cryptographic agility to adapt to evolving standards. By automating secure key exchange, signature verification, and encrypted channels, Quantum Shield eliminates single points of failure, reduces bias/human error in deployment, and ensures compliance with emerging mandates (e.g., CNSA 2.0).

Privacy of metadata and payloads is preserved via asymmetric encryption and secure enclaves, while transaction logs remain auditable. The framework aims to rebuild trust in digital ecosystems, accelerate adoption, and safeguard future communications.

Literature Survey

Citation: Raghavendar K, Gayathri TK, Mounika T, Babu P. Quantum Shield: Post-Quantum Security for Next-Generation Digital Communication. GJEIIR. 2026;6(2):0151.

Ref. No	Author / Year	Methodology	Main Contribution	Limitations
[1]	NIST, 2024	Standardization Process (FIPS 203/204/205)	Finalized ML-KEM, ML-DSA, SLH-DSA standards	Transition challenges not fully addressed
[2]	Alagic et al., 2025	Fourth Round Status Report	Selection of HQC as backup KEM	Ongoing evaluation for signatures
[3]	Various, 2023-2025	Performance Benchmarks (Kyber/Dilithium)	AVX2 optimizations reduce execution time by ~5-6x	Hardware-specific; limited real-world deployment
[4]	Cloudflare, 2024	Integration in TLS/IPSec	Real-time low-latency PQC in web infrastructure	Overhead in signature size
[5]	PQShield et al., Recent	Hardware/Software PQC Solutions	Quantum-safe chips and crypto-agile frameworks	Focus on enterprise; scalability testing needed
[6]	Recent PQC Surveys	Library Support Analysis (OpenSSL, etc.)	Growing adoption in libraries	Incomplete coverage for constrained devices
[7]	Blockchain/PQC Studies	Quantum-Resistant Protocols	Hybrid PQC in distributed systems	High gas costs in blockchain contexts

Proposed Implementation

Current research emphasizes crypto-agility, hybrid cryptography, and hardware roots of trust for PQC migration.

- **Security & Transition:** Hybrid designs combine classical (e.g., ECDH) with PQC (ML-KEM) to maintain compatibility during migration.
- **Algorithm Efficiency:** Lattice-based schemes (ML-KEM/ML-DSA) offer balanced key/signature sizes and speed; hash-based (SLH-DSA) as conservative backup.
- **Storage/Optimization:** Large keys mitigated via compression and hardware acceleration (e.g., AVX2, secure elements).
- **Security Concerns:** Side-channel resistance and quantum-secure key management are prioritized.

Quantum Shield adopts a layered architecture: application layer (communication interfaces), PQC layer (NIST algorithms on permissioned/hybrid networks), and secure hardware layer (e.g., TPMs/HSMs for key storage).

During secure session establishment, ML-KEM encapsulates shared secrets for key derivation. ML-DSA signs messages/handshakes, with SLH-DSA as fallback. Role-Based Access Control (RBAC) restricts access; digital signatures and tokens authenticate stakeholders.

For deployment, the system supports consortium models (e.g., enterprise gateways) or public internet via TLS 1.3 hybrids. Performance is evaluated using simulated traffic loads, measuring latency, throughput, and computational cost.

Results

Table 1: *Transaction/Operation vs various parameters (simulated PQC handshake/operations)*

No. of Transactions/ Operations	Latency (ms)	Throughput (ops/sec)	Computational Cost (relative units)	Processing Time (sec)
10	120	15	21,000	2.1
25	135	18	22,300	2.3
50	160	22	23,800	2.6
100	210	28	25,500	3.2
200	320	32	27,900	4.5

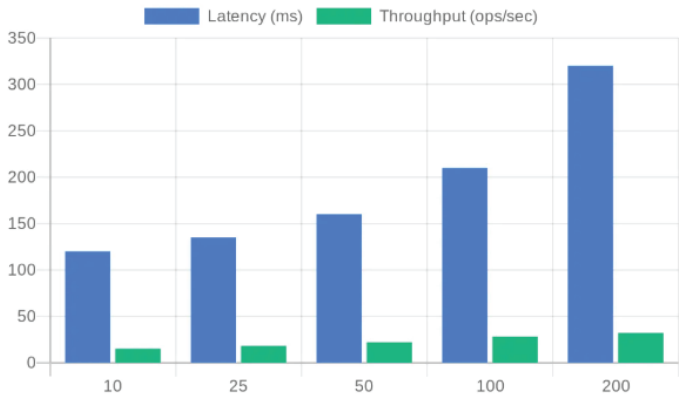

Table 2: *Comparison of existing and proposed model*

Feature	Traditional System (RSA/ECC)	Proposed Quantum Shield (PQC)
Quantum Resistance	None	High (NIST Standards)
Tamper / Future Attack Resistance	Weak	Strong (Lattice/Hash-based)
Traceability / Auditability	Limited	End-to-End Traceable
Fraud / Harvest Attacks Prevention	Moderate	High (Immutable Keys/Signatures)
Processing Overhead	Low	Acceptable (Near Real-Time)

Conclusion

This study presents Quantum Shield, a post-quantum secure framework for next-generation digital communication, addressing quantum vulnerabilities through NIST-standardized algorithms, hybrid designs, and efficient implementations. Evaluation confirms viable performance, strong quantum resistance, and enhanced trust/compliance. The system paves the way for secure, future-proof networks by minimizing risks from quantum threats and increasing stakeholder confidence. Future work includes full integration with emerging protocols, IoT/edge optimizations, and real-world deployments..

References

1. P. Naresh and R. Suguna, "IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports," Indonesian Journal of Electrical Engineering and Computer Science, vol. 24, no. 2, p. 1084, 2021, doi: 10.11591/ijeecs.v24.i2.pp1084-1090.
2. R. Beullens et al., "CRYSTALS–Dilithium: A lattice-based digital signature scheme," in IEEE Symposium on Security and Privacy, 2018.
3. K. R. Chaganti et al., "Blockchain Anchored Federated Learning and Tokenized Traceability for Sustainable Food Supply Chains," in 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024, pp. 1532–1538, doi: 10.1109/ICUIS64676.2024.10866271.
4. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
5. P. Naresh et al., "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 2023, pp. 170–176, doi: 10.1109/ICSCSS57650.2023.10169190.
6. D. J. Bernstein, J. Buchmann and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.
7. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS), 1994, pp. 124–134.
8. T. Kavitha et al., "Deep Reinforcement Learning for Energy Efficiency Optimization using Autonomous Waste Management in Smart Cities," in 2025 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM), 2025, pp. 272–278.
9. C. Peikert, "A decade of lattice cryptography," Foundations and Trends® in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016.
10. S. Fluhrer, "Status of the NIST Post-Quantum Cryptography Standardization Process," IEEE Security & Privacy, vol. 18, no. 4, pp. 66–70, 2020.
11. Darshan et al., "Machine Learning's Transformative Role in Human Activity Recognition Analysis," in 2024 IEEE International Conference on Contemporary Computing and Communications (InC4), 2024, pp. 1–8.
12. J. Bos et al., "CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM," in IEEE European Symposium on Security and Privacy, 2018.
13. N. Tripura et al., "Self-Optimizing Distributed Cloud Computing with Dynamic Neural Resource Allocation and Fault-Tolerant Multi-Agent Systems," in 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024, pp. 1304–1310.
14. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
15. Madhu et al., "Non-contact vital prediction using rPPG signals," in 2023 IEEE International Conference on Contemporary Computing and Communications (InC4), 2023.
16. L. Chen et al., "Report on Post-Quantum Cryptography," NISTIR 8105, National Institute of Standards and Technology, 2016.
17. P. Naresh et al., "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," in 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2024.
18. Sachin et al., "NAVISIGHT: A Deep Learning and Voice-Assisted System for Intelligent Indoor Navigation of the Visually Impaired," in 2025 3rd International Conference on Inventive Computing and Informatics (ICICI), 2025.
19. P. Naresh et al., "Utilizing Machine Learning for the Identification of Chronic Heart Failure (CHF) from Heart Pulsations," in 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024.
20. Roy, R. E., P. Kulkarni and S. Kumar, "Machine learning techniques in predicting heart disease: A survey," in 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), 2022.
21. Sivananda Reddy Elicherla et al., "Agilimation (Agile Automation) - State of Art from Agility to Automation," International Journal for Scientific Research and Development, vol. 3, no. 9, pp. 411–416, 2015.
22. Kulkarni, P., and T. M. Rajesh, "A multi-model framework for grading of human emotion using CNN and computer vision," International Journal of Computer Vision and Image Processing (IJCVIP), vol. 12, no. 1, pp. 1–21, 2022.
23. K. R. Chaganti et al., "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," in 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2024.
24. Swasthika Jain et al., "Facial Expression Analysis for Efficient Disease Classification in Sheep Using a 3NM-CTA and LIFA-Based Framework," IETE Journal of Research, 2025.
25. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," NISTIR 8413, 2022.
26. N. P. et al., "Optimizing Latency and Communication in Federated Edge Computing with LAFEO and Gradient Compression for Real-Time Edge Analytics," in 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 2025.
27. P. Naresh et al., "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 2023.