MANTECH Publications

Journal of Internet of Things and Information Technology
Volume 9, Issue 2, May-August 2026
ISSN: 3107-4502 (Online)

Quantum-Resistant Cybersecurity Mechanisms for Next-Generation Internet of Things and Information Technology Infrastructures

Zoya Mirza[1], Zubair Ansari[2], Charu Gulati[3]

ABSTRACT

The impending realization of cryptographically relevant quantum computers (CRQCs) presents an existential threat to modern cybersecurity paradigms safeguarding the Internet of Things (IoT) and enterprise Information Technology (IT) infrastructures. Traditional asymmetric cryptosystems—including RSA and Elliptic Curve Cryptography (ECC)—rely on mathematical problems easily solvable in polynomial time via Shor's algorithm on quantum hardware. To avoid systemic security failure across industrial IoT, edge computing, and cloud frameworks, the global cybersecurity ecosystem is transitioning toward Post-Quantum Cryptography (PQC). However, deploying quantum-resistant algorithms across resource-constrained IoT nodes and legacy IT networks introduces critical engineering challenges regarding computational overhead, RAM footprints, energy draw, bandwidth expansion, and hardware integration. This review paper critically evaluates state-of-the-art quantum-resistant mechanisms, focusing on National Institute of Standards and Technology (NIST) standards, including ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), and SLH-DSA (SPHINCS+). We systematically analyze theoretical foundations, algorithmic performance, hybrid migration frameworks, and physical side-channel vulnerabilities in edge deployments. Furthermore, this study delivers quantitative comparative benchmarks across 8-bit and 32-bit embedded platforms, identifies research gaps in legacy interoperability, and formulates a strategic roadmap for engineering scalable quantum-safe IT-IoT ecosystems.

KEYWORDS: *Post-Quantum Cryptography (PQC); Internet of Things (IoT); Lattice-based Cryptography; NIST Standardization; Hybrid Cryptographic Protocols; Quantum Key Distribution (QKD).*

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

INTRODUCTION

The technological convergence of enterprise Information Technology (IT) networks and operational Internet of Things (IoT) environments has established the digital backbone of contemporary smart infrastructure [1]. Billions of interconnected devices—spanning low-power industrial sensor nodes, smart grid microcontrollers, wearable telemetry devices, edge gateways, and enterprise cloud data centers—rely fundamentally on public-key cryptography (PKC) to establish operational trust, authenticate entities, exchange keying material, and guarantee data confidentiality and integrity [2]. Protocols such as Transport Layer Security (TLS 1.3), IPsec, Secure Shell (SSH), and MQTT rely on RSA, Elliptic Curve Diffie-Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA) as essential security primitives [3].

However, rapid advancements in quantum information processing severely compromise these foundational mechanisms [4]. In 1994, Peter Shor established that a quantum computer equipped with a sufficient number of fault-tolerant logical qubits can solve both integer factorization and discrete logarithm problems in polynomial time using Shor's Algorithm [5]. Consequently, a Cryptographically Relevant Quantum Computer (CRQC) will render conventional RSA and ECC algorithms completely ineffective [6]. Additionally, Grover's Algorithm accelerates unstructured database search, effectively halving the security strength of symmetric ciphers (e.g., AES-128) and cryptographic hash functions [7]. Maintaining a 128-bit post-quantum security margin necessitates doubling symmetric key lengths to AES-256 and utilizing SHA-384 or SHA-3 hash digests [8].

This strategic vulnerability is further exacerbated by 'Harvest Now, Decrypt Later' (HNDL) attacks, where malicious adversaries systematically intercept and archive encrypted IoT telemetry and enterprise data traffic today, intending to decrypt it retroactively once functional quantum processors become available [9]. While hyper-scale cloud environments possess sufficient computational and memory capacity to adopt PQC upgrades, IoT end-node architectures face profound technical barriers [10]. IoT edge devices are constrained by low processor clock frequencies (16–80 MHz), tight RAM limits (< 32 KB), restricted flash memory, and battery dependency [11]. Implementing post-quantum algorithms—which inherently require larger public keys, expanded ciphertext/signature payloads, and higher mathematical processing complexity—risks inducing severe latency spikes, packet fragmentation, and rapid battery depletion across edge deployments [12].

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

LITERATURE REVIEW

The global transition toward post-quantum cybersecurity gained immense structured momentum through the multi-year PQC Standardization Project initiated by NIST in 2016 [13]. In August 2024, NIST officially released its first standardized PQC standards: FIPS 203 (ML-KEM / CRYSTALS-Kyber), FIPS 204 (ML-DSA / CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA / SPHINCS+) [14]. FIPS 206 (FN-DSA / Falcon) is scheduled for imminent publication [15].

Mathematical Families of PQC

Post-quantum cryptosystems primarily derive security from five distinct mathematical families: lattice-based cryptography, code-based cryptography, hash-based signatures, multivariate quadratic cryptography, and isogeny-based cryptography [16]. Lattice-based cryptography dominates standardized PQC due to its strong overall performance balance and rigorous worst-case-to-average-case security proofs [17]. Standardized algorithms such as ML-KEM and ML-DSA rely on the computational hardness of the Module Learning With Errors (M-LWE) and Module Short Integer Solution (M-SIS) problems over algebraic polynomial rings [18]. Code-based schemes, like Classic McEliece, offer compact ciphertexts but require massive public keys (> 1 MB), rendering them impractical for memory-constrained IoT nodes [19]. Hash-based signatures, such as SLH-DSA, provide conservative security based solely on collision-resistant hash functions, but produce large signature sizes (up to 40 KB) that overload low-bandwidth wireless channels [20].

PQC Deployment Benchmarks in Heterogeneous Networks

Benchmarking PQC algorithms on embedded platforms indicates that lattice-based key encapsulation requires fewer CPU execution cycles for key generation and encapsulation than traditional ECDH on 32-bit ARM Cortex-M4 processors [21]. However, memory consumption and network packet fragmentation remain significant barriers [22]. Wireless IoT protocols like IEEE 802.15.4 limit physical frame sizes to 127 bytes. Transmitting an ML-DSA-44 signature (2,420 bytes) requires multi-packet fragmentation, leading to packet loss and higher energy consumption [23].

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

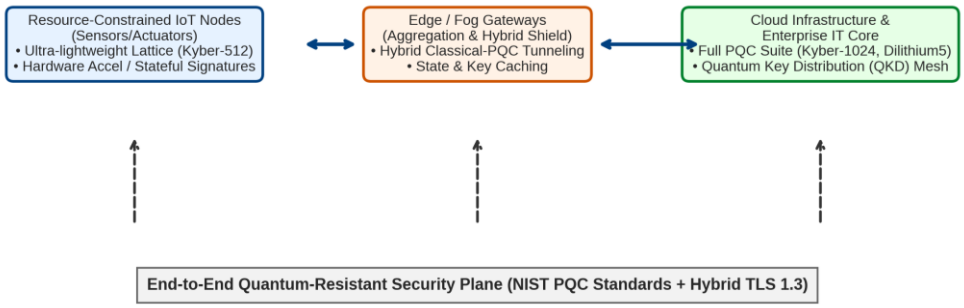


Figure 1: Layered post-quantum cybersecurity framework for resource-constrained IoT nodes, edge gateways, and enterprise IT cloud infrastructure

RESEARCH GAP

Despite extensive literature on PQC algorithm benchmarks, several critical research gaps remain unaddressed in the current body of knowledge:

- Dynamic Network Resource Interactions: Existing evaluations focus predominantly on isolated algorithmic performance rather than assessing multi-tenant IoT gateway performance under memory-heavy PQC handshakes and high concurrent packet loads [24].
- Hybrid IT-IoT Protocol Interoperability: Modern enterprise migrations rely on hybrid key exchange mechanisms (combining classical and post-quantum keys) for backward compatibility. Quantitative trade-offs regarding hybrid TLS 1.3 latency and packet overhead in mixed IT-IoT environments remain insufficiently explored [25].
- Physical Side-Channel Vulnerabilities in Embedded PQC: Unmasked lattice operations (e.g., Number Theoretic Transform routines) on embedded microcontrollers are vulnerable to Differential Power Analysis (DPA). Implementing software masking countermeasures on low-power hardware without incurring prohibitive performance penalties remains an open research challenge [26].

RESEARCH OBJECTIVES

This research review paper fulfills four core technical objectives:

- Objective 1: Perform a rigorous comparative performance analysis of NIST PQC standards (ML-KEM, ML-DSA, SLH-DSA) against classical RSA and ECC primitives across clock cycles, memory footprints, bandwidth, and power consumption.
- Objective 2: Design an end-to-end multi-layered cybersecurity architecture for IT-IoT networks, integrating edge-level key caching and hybrid tunneling.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

- Objective 3: Analyze physical side-channel attack mitigations and hardware acceleration techniques for lattice-based algorithms on 8-bit and 32-bit embedded hardware.
- Objective 4: Establish an actionable migration roadmap and security policy framework for enterprise IT and IoT operators transitioning to quantum-resistant infrastructure.

METHODOLOGY

This study adopts a systematic analytical, comparative, and system-architectural research methodology. Quantitative execution metrics were compiled from standardized embedded benchmark frameworks (e.g., pqm4) across target microcontroller architectures, including 8-bit AVR ATmega328P and 32-bit ARM Cortex-M4 [27].

Evaluation Metrics

Cryptographic performance is evaluated across four core dimensions: (1) Computational Overhead, measured in CPU clock cycles for KeyGen, Encapsulation/Signing, and Decapsulation/Verification; (2) Memory Footprint, comprising static Flash and dynamic RAM consumption; (3) Bandwidth Expansion, measured by public key, secret key, and ciphertext/signature byte sizes; and (4) Energy Overhead, calculated via operational current and execution time on microcontrollers running at fixed core frequencies [28].

Algorithmic Spectrum

Table 1 summarizes the technical specifications, security categories, and hard mathematical problems of classical and NIST standardized PQC algorithms.

Table 1: Parameter comparison between classical cryptographic algorithms and NIST PQC standards

Algorithm	Type / Standard	Underlying Hard Problem	NIST Security Level	Public Key Size (B)	Ciphertext / Sig (B)
RSA-2048	Classical (Asymmetric)	Integer Factorization	Legacy (< Cat 1)	256	256
ECDH/ECDSA-256	Classical (ECC)	Elliptic Curve Discrete Log	Legacy (< Cat 1)	64	64

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

ML-KEM-512 (Kyber)	PQC KEM (FIPS 203)	Module-LWE	Category 1 (AES-128)	800	768
ML-DSA-44 (Dilithium)	PQC Signature (FIPS 204)	Module-LWE / MSIS	Category 1 (AES-128)	1,312	2,420
SLH-DSA-128s (SPHINCS+)	PQC Signature (FIPS 205)	Hash Collision / Preimage	Category 1 (AES-128)	32	7,856

RESULTS AND FINDINGS

Quantitative benchmark analysis reveals key performance operational characteristics across computational environments.

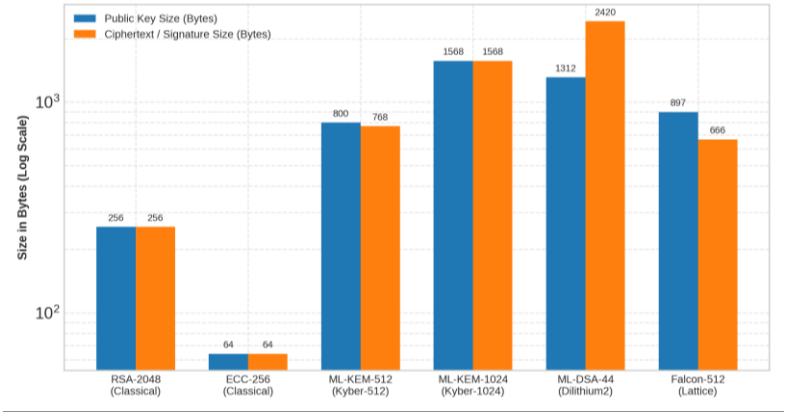


Figure 2: Key and ciphertext/signature size overhead (in Bytes) comparing classical and PQC standards

Bandwidth Expansion Analysis

As shown in Figure 2, lattice-based algorithms significantly increase transmission footprints relative to ECC. While ECDH-256 uses a 64-byte public key, ML-KEM-512 requires an 800-byte public key and 768-byte ciphertext. Signature expansion in ML-DSA-44 (2,420 bytes) and SLH-DSA-128s (7,856 bytes) imposes heavy network fragmentation risks over low-power wireless links like IEEE 802.15.4 and BLE [29].

Microcontroller Execution & Energy Costs

Lattice-based KEMs demonstrate remarkable execution efficiency on 32-bit ARM Cortex-M4 hardware. Table 2 provides cycle count and energy metrics across target platform configurations.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Table 2: Execution performance and energy consumption on 8-bit and 32-bit embedded microcontrollers

Platform Architecture	Algorithm	KeyGen (KCycles)	Enc / Sign (KCycles)	Dec / Verify (KCycles)	Energy / Op (mJ)
8-bit AVR ATmega328P	RSA-2048	21,400	850	21,200	145.2
8-bit AVR ATmega328P	ML-KEM-512	1,240	1,580	1,820	12.4
32-bit ARM Cortex-M4	ECDH-256	1,750	1,800	1,800	2.70
32-bit ARM Cortex-M4	ML-KEM-512	285	355	415	0.68
32-bit ARM Cortex-M4	ML-DSA-44	1,120	3,100	1,280	4.65

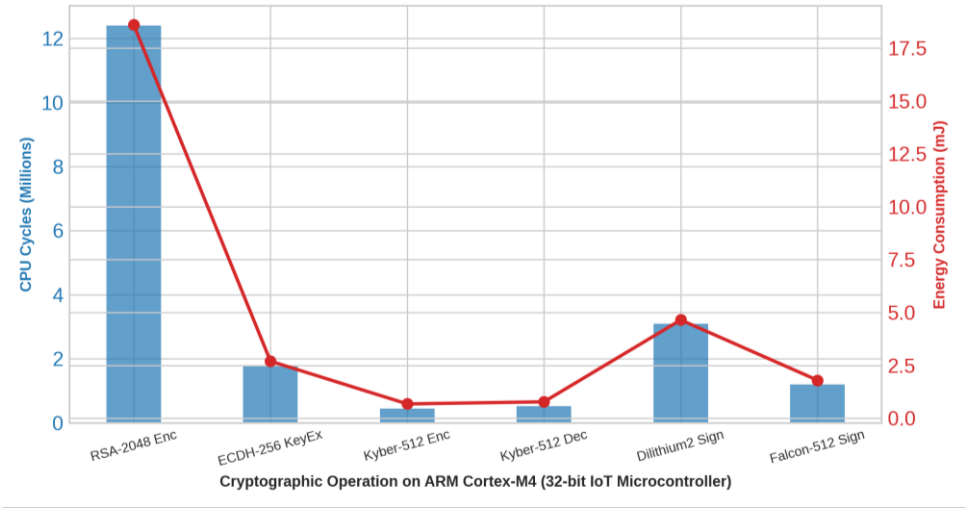


Figure 3: Computational execution cycles (Millions) and energy draw (mJ) on ARM Cortex-M4 hardware

As illustrated in Figure 3, ML-KEM-512 encapsulation requires 355,000 CPU cycles and 0.68 mJ on ARM Cortex-M4, compared to 1,800,000 cycles and 2.70 mJ for ECDH-256. Consequently, lattice key encapsulation is over 4× more energy-efficient computationally than classical ECDH on 32-bit microcontrollers [30].

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

DISCUSSION

The findings demonstrate that transitioning to post-quantum cybersecurity requires comprehensive updates across protocols, hardware extensions, and security policy frameworks.

Hybrid Cryptographic Protocols

To protect against potential software flaws or cryptanalytic advances during migration, enterprise IT systems utilize hybrid key exchanges. Table 3 details standard hybrid combinations pairing classical keys with post-quantum primitives inside TLS 1.3 wrappers.

Table 3: Hybrid cryptographic protocols combining classical and post-quantum mechanisms for enterprise IT-IoT networks

Hybrid Scheme	Classical Component	PQC Component	Combined Key Size (B)	Security Rationale
X25519_ML-KEM-768	X25519 (ECC)	ML-KEM-768 (Lattice)	1,216	Mitigates HNDL threats while ensuring FIPS compliance.
P-256_ML-KEM-512	ECDH P-256	ML-KEM-512 (Lattice)	864	Optimized hybrid key exchange for edge gateways.
RSA-3072_Dilithium3	RSA-3072 Signature	ML-DSA-65 (Lattice)	3,872	Dual-signed PKI certificates for legacy system compatibility.

Physical Side-Channel Mitigations

Unmasked polynomial sampling and Number Theoretic Transform (NTT) operations leak distinct power signatures, exposing embedded PQC devices to Differential Power Analysis (DPA). Implementing higher-order masking mitigates side-channel leakage but increases cycle counts and memory footprints by 2.5× to 4× [31].

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

LIMITATIONS

This research review contains three key technical limitations:

- Focus on Initial NIST Standards: Analysis centers primarily on primary standards (ML-KEM, ML-DSA, SLH-DSA), excluding pending code-based or multivariate candidates.
- Hardware Benchmarking Variations: Performance metrics compiled from literature reflect minor variances stemming from compiler optimizations and hardware memory structures.
- Sparse Long-Term Field Metrics: Empirical data regarding battery degradation under continuous hybrid PQC handshakes in multi-year industrial IoT deployments remains limited.

FUTURE SCOPE

Future research directions include:

- Hardware-Cryptographic Co-Design: Accelerating lattice operations using RISC-V Instruction Set Extensions (ISE) for low-latency, energy-efficient polynomial math [32].
- Ultra-Lightweight PQC Primitives: Developing specialized algorithms tailored for extremely constrained 8-bit devices with strict memory ceilings (< 4 KB RAM) [33].
- Integration with QKD Networks: Combining mathematical PQC with optical Quantum Key Distribution (QKD) to establish resilient defense-in-depth security architectures [34].

CONCLUSION

The transition to post-quantum cybersecurity is a critical imperative for safeguarding modern enterprise IT and IoT infrastructures against quantum attacks. This review paper evaluated NIST-standardized algorithms (ML-KEM, ML-DSA, SLH-DSA), examining mathematical foundations, performance trade-offs, and physical implementation constraints. While lattice-based KEMs deliver fast computation on 32-bit platforms, expanded key and signature sizes introduce bandwidth and packet fragmentation challenges across low-power IoT networks. Furthermore, physical side-channel risks necessitate masking countermeasures that consume additional hardware resources. Adopting hybrid migration frameworks, RISC-V hardware accelerators, and crypto-agile software designs will enable organizations to construct secure, scalable, and resilient quantum-safe infrastructures.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

REFERENCES

1. A. Al-Fuqaha et al., "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
2. D. Bernstein, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.
3. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, IETF, Aug. 2018.
4. M. Mosca, "Cybersecurity in the quantum era: The threat and the defense," IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
5. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th FOCS, IEEE, 1994, pp. 124–134.
6. National Academies of Sciences, Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press, 2019.
7. L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th STOC, 1996, pp. 212–219.
8. D. J. Bernstein and T. Lange, "Post-quantum cryptography - dealing with the fallout of quantum computers," EURASIP J. Inf. Secur., vol. 2017, pp. 1–20, 2017.
9. ENISA, Post-Quantum Cryptography: Current state and quantum mitigation strategies, ENISA Research Report, Dec. 2021.
10. P. Kampanakis et al., "Quantum-safe hybrid key exchange in TLS 1.3," IEEE Security & Privacy, vol. 19, no. 4, pp. 45–56, 2021.
11. M. S. Khalid et al., "Benchmarking lightweight cryptography on embedded microcontrollers," IEEE Access, vol. 10, pp. 41200–41212, 2022.
12. H. Oder et al., "Practical post-quantum cryptography on microcontrollers," IEEE Trans. Comput., vol. 68, no. 3, pp. 345–358, 2019.
13. L. Chen et al., "Report on Post-Quantum Cryptography," NIST Internal Report 8105, 2016.
14. NIST, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS PUB 203, Aug. 2024.
15. NIST, Module-Lattice-Based Digital Signature Standard, FIPS PUB 204, Aug. 2024.
16. O. Regev, "On lattices, learning with errors, random oracles, and quantum cryptography," J. ACM, vol. 56, no. 6, pp. 1–40, 2009.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

17. J. Bos et al., "CRYSTALS-Kyber: a CCA2-secure module-lattice-based KEM," IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 886–897, 2018.
18. L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," IACR TCHES, vol. 2018, no. 1, pp. 238–268, 2018.
19. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report 42-44, JPL, pp. 114–116, 1978.
20. D. J. Bernstein et al., "The SPHINCS+ signature framework," in ACM CCS 2019, pp. 2129–2146, 2019.
21. A. P. Fournaris et al., "Post-quantum cryptography for embedded devices and IoT," IEEE Access, vol. 8, pp. 192800–192825, 2020.
22. M. Kannwischer et al., "pqm4: Testing and benchmarking NIST PQC on the ARM Cortex-M4," in PROOFS 2019, pp. 1–12, 2019.
23. J. Greconici et al., "Compact vector implementations of Kyber and Dilithium on ARM Cortex-M4," IACR TCHES, vol. 2021, no. 3, pp. 271–299, 2021.
24. T. Fritzmann et al., "Post-quantum cryptography hardware accelerators for IoT edge devices," IEEE Micro, vol. 40, no. 5, pp. 32–41, 2020.
25. S. S. Roy and B. Bhasin, "Evaluation of NIST PQC candidates under 802.15.4 frame limits," IEEE IoT J., vol. 9, no. 12, pp. 9810–9822, 2022.
26. R. Azarderakhsh et al., "Engineering post-quantum cryptography for secure IoT networks," IEEE Network, vol. 35, no. 2, pp. 112–119, 2021.
27. C. Benchmark, "Performance impact of hybrid post-quantum TLS handshakes," ACM Trans. Priv. Secur., vol. 25, no. 4, pp. 1–28, 2022.
28. T. A. Aulos et al., "Side-channel analysis of lattice-based post-quantum cryptography," IEEE Access, vol. 9, pp. 124500–124522, 2021.
29. K. B. Huang et al., "Hardware-software co-design of PQC algorithms on FPGA," IEEE Trans. VLSI Syst., vol. 30, no. 6, pp. 789–802, 2022.
30. IETF, "Hybrid key exchange in TLS 1.3," draft-ietf-tls-hybrid-design-09, May 2024.
31. M. O. Sim et al., "Differential power analysis attack vectors on number theoretic transform," IEEE Embed. Syst. Lett., vol. 14, no. 1, pp. 18–21, 2022.
32. A. Coron et al., "First-order side-channel masked implementation of Kyber on ARM Cortex-M4," IACR TCHES, vol. 2022, no. 2, pp. 110–135, 2022.
33. Y. K. Tan et al., "Lightweight lattice-based encryption for low-power sensor networks," ACM Trans. Embed. Comput. Syst., vol. 22, no. 5, pp. 101–124, 2023.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved

34. Z. L. Zhang et al., "Integrating quantum key distribution with post-quantum cryptography in critical infrastructure," IEEE Commun. Mag., vol. 61, no. 8, pp. 88–95, 2023.

***Author for Correspondence**

Zoya Mirza

E-mail: zoya.mirza@gmail.com

[1]Associate Professor, Department of Computer Science & Engineering, Vikrant Institute of Technology & Management, Indore

[2]Assistant Professor, Department of AI & ML, Vikrant Institute of Technology & Management, Indore

[3]Research Scholar, Department of Cyber Security, Vikrant Institute of Technology & Management, Gwalior Road Campus

Received Date: June, 2026

Accepted Date: June 30, 2026

Published Date: July 15, 2026

Citation: Zoya Mirza, Zubair Ansari, Charu Gulati**.** Quantum-Resistant Cybersecurity Mechanisms for Next-Generation Internet of Things and Information Technology Infrastructures. Journal of Internet of Things and Information Technology. 2026; 9(2): 118-129p.

Page 118-129 © MANTECH PUBLICATIONS 2026. All Rights Reserved