



Adaptive AI-Driven Post-Quantum Cyber Defense Framework for Enterprise and Government Information Systems

Dr. Yogesh N. Chaudhari¹, Shubham M. Koshti², Dr. Dhanpal N. Waghulde³, Harshal B. Patil⁴, Sneha A. Patil⁵

^{1, 2, 4, 5} Assistant Professor, KCES's Institute of Management and Research, Jalgaon, Maharashtra, India.

³ Associate Professor, KCES's Institute of Management and Research, Jalgaon, Maharashtra, India.

How to cite this paper:

Dr. Yogesh N. Chaudhari¹, Shubham M. Koshti², Dr. Dhanpal N. Waghulde³, Harshal B. Patil⁴, Sneha A. Patil⁵, "Adaptive AI-Driven Post-Quantum Cyber Defense Framework for Enterprise and Government Information Systems", IJIRE-V7I3-400-404.



Copyright © 2026
by author(s) and
Fifth Dimension
Research

Publication. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>

Abstract: The convergence of fast-tracked quantum hardware manufacturing paradigms and artificial intelligence (AI) brings radical transformations to systemic cyber-defense architectures. The impending arrival of a Cryptanalytically Relevant Quantum Computer (CRQC) invalidates the baseline asymmetric mathematical problems protecting modern enterprise and sovereign state secrets. Algorithms like RSA, Diffie-Hellman, and Elliptic Curve variants face immediate deprecation under Peter Shor's algorithm, exposing historical databases globally to retroactive decryption vectors through "Harvest Now, Decrypt Later" (HNDL) operational doctrines. Simultaneously, highly distributed adversarial advanced persistent threats (APTs) deploy autonomous generative machine learning agents to identify zero-day exposures and circumvent perimeter security topologies. This paper introduces the Adaptive AI-Driven Post-Quantum Cyber Defense Framework (AAI-PQCDF). The design integrates the primary Federal Information Processing Standards (FIPS 203, 204, and 205) for post-quantum cryptography with custom, decoupled deep reinforcement learning (DRL) models and semantic transformer layers. AAI-PQCDF implements a programmatic zero-trust fabric across hybrid networks, hardening complex agent communication interfaces like the Model Context Protocol (MCP) using automated micro-segmentation routines. Our empirical validations chart performance penalties, network latency inflation factors, and packet structure dynamics across extensive high-throughput data streams, detailing an agile deployment matrix suited for large-scale enterprise infrastructures.

I. INTRODUCTION

1.1 The Quantum Decryption Paradigm

The current global foundational framework for cryptographic data security is constructed almost entirely upon a narrow set of mathematically intensive asymmetric primitives. These structures, including the RSA scheme, Diffie-Hellman key agreement protocols, and various configurations of Elliptic Curve Cryptography (ECC), guarantee transactional secrecy, authenticity, and message integrity. The resilience of these systems relies upon the presumption of computational asymmetry: the underlying mathematical problems—such as the discrete logarithm challenge and the prime factorization of extraordinarily large integers—are trivial to compute in one direction but take billions of years to invert using conventional Von Neumann computing architectures.

However, this foundational security architecture is inherently time-bound and structurally vulnerable. The development of quantum information processing systems directly undermines these mathematical assumptions. By applying the physical properties of quantum mechanics—specifically superposition and entanglement—quantum computing structures represent a paradigm shift in processing power. A Cryptanalytically Relevant Quantum Computer (CRQC) eliminates the protective computational complexity of modern public-key cryptography. This vulnerability presents an immediate, systemic threat to corporate proprietary environments, critical national infrastructure, and classified military systems.

1.2 The Imminent Threat of 'Harvest Now, Decrypt Later' (HNDL)

A common misconception in the cybersecurity sector is that the quantum threat is a future issue that will only matter when large-scale fault-tolerant hardware is fully realized. This misunderstanding ignores the operational timeline of modern adversarial espionage, known as Harvest Now, Decrypt Later (HNDL). Nation-state intelligence agencies, corporate espionage cells, and well-funded Advanced Persistent Threat (APT) groups are actively intercepting, copying, and archiving huge amounts of high-value encrypted telemetry from global internet transit nodes.

While this captured data looks like random noise to classical systems, it is being cataloged in secure data repositories. The moment a CRQC becomes accessible, these archived logs will be run through Shor's algorithm. As a result, industrial

patents, national defense plans, diplomatic communications, and global financial records currently considered secure will be exposed in cleartext. Therefore, deploying post- quantum cryptographic perimeters is an urgent operational requirement to protect long-term data assets today.

1.3 The Convergence of Automated, Adversarial AI Vectors

The threat landscape is further complicated by the rapid rise of advanced Artificial Intelligence frameworks. Modern security operations centers no longer face only human attackers or predictable, signature-based malware scripts. Instead, defensive architectures must counter autonomous machine learning systems that can discover vulnerabilities, modify exploit payloads in real time, and orchestrate coordinated attacks across multi-cloud enterprise networks.

These adversarial AI systems can quickly analyze defensive code bases, spot minor logic gaps, and generate customized exploits. They can also automate multi-vector attack paths, tracking internal user behavior and altering communication signatures to mimic legitimate corporate data traffic. Static defense models and conventional security information and event management (SIEM) systems cannot keep pace with these automated, fast-evolving attacks. To protect modern enterprises, defensive frameworks must combine post-quantum cryptography with adaptive, machine-learning-driven telemetry engines.

II.THEORETICAL BACKGROUND AND LITERATURE REVIEW

2.1 Computational Hardness and Quantum Mechanics

To understand why quantum systems threaten traditional public-key infrastructure, it is necessary to examine the differences between classical bits and quantum qubits. A classical computer relies on silicon-based gates to process distinct binary states: 0 or 1. In contrast, a qubit can exist as a simultaneous combination of both states until it is measured. This superposition is mathematically defined as a vector within a complex Hilbert space:

$$\Psi = \alpha|0\rangle + \beta|1\rangle$$

In this equation, α and β represent complex amplitude values that determine the probability of each state occurring upon measurement, governed by the normalization rule $|\alpha|^2 + |\beta|^2 = 1$. When multiple qubits are entangled, their states become interconnected. This allows an array of n qubits to track and evaluate 2^n computational paths at the same time.

Shor's Algorithm takes advantage of this parallel processing capability by using the Quantum Fourier Transform (QFT) to find the period of a periodic function efficiently. This algorithm reduces the time required to solve prime factorization and discrete logarithms from sub-exponential down to polynomial time complexity. As a result, a quantum computer can break standard asymmetric algorithms, like RSA or ECC, in a matter of hours or days, rather than millennia.

Symmetric encryption algorithms face a different quantum challenge from Grover's Algorithm. Grover's algorithm provides a quadratic speedup for searching unstructured databases. Instead of breaking the underlying math, it effectively cuts the security bit-length of symmetric keys in half. For example, AES-128 is reduced to an effective security strength of only 64 bits, making it vulnerable to brute-force attacks. To maintain a secure 128-bit boundary against quantum-assisted attacks, organizations must upgrade symmetric encryption protocols to AES-256.

2.2 Deep Dive into NIST FIPS PQC Standards

To defend against these vulnerabilities, the National Institute of Standards and Technology (NIST) conducted a multi-year evaluation to standardize quantum-resistant primitives. This effort resulted in the finalization of three key Federal Information Processing Standards (FIPS), which form the foundation of modern post-quantum defensive architectures.

FIPS 203 standardizes the Module-Lattice-Based Key-Encapsulation Mechanism, derived from CRYSTALS-Kyber (ML-KEM). ML-KEM provides asymmetric key establishment and secure key exchange mechanisms, making it a drop-in replacement for Diffie-Hellman layers within transport protocols like TLS 1.3. The security of ML-KEM relies on the Module Learning with Errors (M-LWE) problem, which requires finding hidden vectors within multi-dimensional geometric lattices. Because these geometric problems do not rely on periodic structures, they are resistant to the Quantum Fourier Transform used in Shor's algorithm.

FIPS 204 defines the Module-Lattice-Based Digital Signature Standard, known as ML-DSA (derived from CRYSTALS-Dilithium). ML-DSA provides identity validation, transaction non-repudiation, and source verification. Like ML-KEM, it is built on M-LWE lattice problems, balancing performance efficiency with small signature sizes.

FIPS 205 establishes the Stateless Hash-Based Digital Signature Standard, or SLH-DSA (derived from SPHINCS+). Unlike lattice-based options, SLH-DSA relies on the security of underlying cryptographic hash functions, such as SHA-256 or SHAKE-256. This design makes it a robust backup choice: even if unexpected mathematical breakthroughs compromise lattice-based cryptography, hash-based signatures will remain secure as long as the underlying hash functions are unbroken. However, this security model comes with a performance trade-off, as SLH-DSA requires significantly larger signature sizes and more processing overhead.

III.THE AAI-PQCDF ARCHITECTURE

The Adaptive AI-Driven Post-Quantum Cyber Defense Framework (AAI-PQCDF) provides a multi-tiered, zero-trust security architecture. Instead of relying on rigid, perimeter-based defenses, the framework uses a decoupled design across three core planes to protect distributed enterprise and government information systems.

3.1 The Cryptographic Transformation Layer (CTL)

The CTL isolates cryptographic implementations from the underlying application logic. Instead of hardcoding specific algorithms directly into local microservices, all encryption, decryption, signing, and verification tasks are handled through an abstract middleware layer accessed via secure, policy-driven application programming interfaces (APIs).

This abstraction enables a capability called Cryptographic Agility. If a specific algorithm develops a vulnerability or a new standard is released, administrators can update the centralized cryptographic policies to swap out the underlying primitive across the entire enterprise instantly, without changing any application code.

To ensure safety during early deployments, the CTL uses a hybrid negotiation strategy for network data streams. When establishing communication tunnels (such as TLS 1.3 or IPsec connections), the framework negotiates a dual key exchange combining classical Elliptic Curve Diffie-Hellman (X25519) with Module Lattice-Based Key Encapsulation (ML-KEM-768). The final session keys are generated by running both secrets through a Hash-based Key Derivation Function (HKDF):

$$\text{Shared Secret} = \text{HKDF-Extract}(\text{Salt}, K_{\text{X25519}} \parallel K_{\text{ML-KEM}})$$

This hybrid design provides dual protection. If a future vulnerability is discovered in the new lattice math of ML-KEM, the classical X25519 layer still prevents access by classical network attackers. At the same time, the ML-KEM layer protects the data stream from retroactive quantum decryption via HNDL schemes. This approach allows organizations to adopt quantum-resistant defenses immediately while managing operational risk.

3.2 The Adaptive AI Telemetry and Analytics Engine (AITAE)

The AITAE provides continuous, real-time threat monitoring and mitigation across distributed corporate infrastructures. It moves away from traditional, rule-based detection models, using instead a combination of sequential transformer models and deep reinforcement learning to identify and respond to complex, multi-vector attacks.

The engine streams system logs, API calls, identity verification requests, and network data into a specialized Transformer decoder architecture. This model converts system events into tokenized sequences, allowing it to evaluate system behavior contextually over time rather than looking at individual events in isolation. By tracking long-term event dependencies, the model computes an anomaly score based on how much current activity deviates from established enterprise baselines. This approach allows the framework to detect subtle, slow-moving attack vectors that typical security tools often miss.

When the anomaly score crosses an authorized risk threshold, the framework activates a Deep Reinforcement Learning (DRL) agent to handle containment. The DRL agent operates within a defined corporate environment state space, monitoring active user sessions, asset criticality rankings, and current cryptographic configurations. The agent can select from several automated actions, such as revoking specific access permissions, forcing an immediate post-quantum re-authentication, or dynamically shifting network segments to higher-strength lattice parameters (e.g., moving from ML-KEM-512 to ML-KEM-1024).

The agent's decision-making is guided by a custom reward function designed to maximize threat containment while minimizing operational disruption to the business:

$$\text{Reward} = -c1(\text{Exploit Depth}) - c2(\text{Service Latency Penalty}) + c3(\text{Containment Success})$$

3.3 Securing the Model Context Protocol (MCP)

As enterprise networks increasingly integrate autonomous AI agents and large language model workflows into daily business operations, securing internal data transfers becomes a critical priority. The Model Context Protocol (MCP) has emerged as a standard interface allowing cooperative AI systems to access corporate databases, file repositories, and internal developer tools. However, this protocol creates an attractive target for attackers, who can use malicious prompt injections or compromised agent identities to move laterally through sensitive internal systems.

To mitigate this risk, the AAI-PQCDF implements an inline MCP Security Gateway. This gateway acts as a security proxy for all context data exchanges. First, it requires all participating AI agents to verify their identities using post-quantum digital signatures (ML-DSA). Second, it inspects incoming context payloads using natural language processing models to spot prompt-injection patterns or unauthorized data requests before they reach internal resources. This mechanism allows organizations to adopt productive AI agent workflows safely within a zero-trust architecture.

IV. OPERATIONAL PERFORMANCE AND EMPIRICAL EVALUATION

Transitioning to post-quantum cryptographic standards requires analyzing how these new algorithms affect system performance. Lattice-based and hash-based primitives require larger key sizes, bigger signatures, and more computational cycles than classical alternatives like RSA or ECC. To understand these impacts, we conducted benchmark testing of the framework across a distributed enterprise network simulation.

Algorithm Family	Standard Primitive	Public Key Size (Bytes)	Signature / Ciphertext (Bytes)	Key Generation Complexity	Sign / Encrypt Efficiency
Classical RSA	RSA-4096	512	512	$O(n^3)$	Moderate / Low
Classical ECC	ECDSA P-256	32	64	$O(1)$	High / Optimal
NIST Lattice KEM	ML-KEM-768	1,184	1,088	$O(k \cdot d^2)$	High / Balanced
NIST Lattice Sign	ML-DSA-65	1,952	3,309	$O(k \cdot d)$	Moderate / Balanced
NIST Hash Sign	SLH-DSA-256s	64	29,792	$O(2^h)$	Low / Heavy Overhead

Table 1: Computational Resource Allocation and Operational Profiles for Selected Algorithms.

4.2 Network Traffic and Latency Analysis

Our benchmark testing shows that lattice-based choices like ML-KEM-768 introduce manageable processing and network overhead. The increase in execution time for standard network connections is minimal, making it an effective choice for daily production traffic. However, signature algorithms like SLH-DSA-256s present a more significant challenge. Because hash-based signatures can exceed 29 kilobytes, they can cause packet fragmentation over standard networks with a typical 1,500-byte Maximum Transmission Unit (MTU). This fragmentation can lead to packet drops or increased latency on congested network paths, meaning organizations must carefully configure their network routing to handle larger post-quantum packet sizes.

V.ENTERPRISE MIGRATION STRATEGY AND COMPLIANCE ROADMAP

Transitioning a large enterprise or government organization to a post-quantum security model requires a structured, phase-based deployment plan. Organizations cannot simply flip a switch to update all systems overnight. Instead, migration should follow a clear path to manage operational risk and maintain continuous compliance with evolving regulations.

5.1 Phase 1: Inventory and Cryptographic Discovery

The first step is to perform a comprehensive automated inventory of all cryptographic assets across the organization. Security teams must scan internal software applications, cloud databases, firmware configurations, and communication tools to catalog every active key, digital certificate, and encryption algorithm. This discovery phase identifies legacy asymmetric algorithms (such as RSA or ECC) that are vulnerable to quantum attacks, helping the organization build a prioritized risk registry of high-value data assets.

5.2 Phase 2: Hybrid Testing and Validation

In the second phase, organizations should introduce hybrid cryptographic connections into non-critical testing environments. By deploying dual-key arrangements (such as X25519 paired with ML-KEM), engineering teams can verify that new post-quantum protocols interact correctly with existing business software. This phase focused on monitoring network latency, validating application stability, and ensuring that security monitoring tools can properly inspect hybrid data traffic without causing operational issues.

5.3 Phase 3: Infrastructure and HSM Upgrades

The third phase involves upgrading the core identity and key management systems of the enterprise. Organizations must update physical and cloud-based Hardware Security Modules (HSMs) with vendor firmware that natively supports FIPS 203, 204, and 205 parameters. Once the hardware layer is updated, administrators can rotate root authority certificates, update code-signing pipelines, and establish a secure, quantum-resistant foundation for corporate identity verification.

5.4 Phase 4: Production Deployment and Full Agility

The final phase transitions production network channels to post-quantum standards and deprecates legacy asymmetric cryptography. By enforcing centralized, policy-driven cryptographic agility through the framework's middleware layer, administrators can manage encryption settings dynamically across all corporate environments. This phase also establishes continuous monitoring routines to track compliance metrics against sovereign data protection rules and global cybersecurity directives, ensuring long-term institutional resilience.

VI.CONCLUSION AND FUTURE DIRECTIONS

The combination of quantum computing capabilities and advanced adversarial AI creates new challenges for traditional enterprise and government security systems. Legacy architectures built on fixed perimeters and classical asymmetric encryption cannot fully protect sensitive data from long-term risks like retroactive decryption or fast-evolving, automated network attacks.

The Adaptive AI-Driven Post-Quantum Cyber Defense Framework (AAI-PQCDF) addresses these vulnerabilities by integrating standardized post-quantum cryptography (FIPS 203, 204, and 205) with dynamic, machine-learning-driven telemetry models. This integration creates a crypto-agile, zero-trust security structure that can adapt to changing mathematical standards and automated threat behaviors. Future research will focus on optimizing lattice-based algorithms for low-power Internet of Things (IoT) hardware, developing defenses against quantum-assisted machine learning attacks, and refining multi-party threshold signature protocols to secure distributed digital ledgers and cloud ecosystems.

References

1. National Institute of Standards and Technology. (2024). FIPS PUB 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce.
2. National Institute of Standards and Technology. (2024). FIPS PUB 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce.
3. National Institute of Standards and Technology. (2024). FIPS PUB 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce.
4. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134.
5. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212-219.
6. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.
7. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y. K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413.
8. U.S. Department of War. (2026). Department of War Post-Quantum Cryptography (PQC) Operational Migration Strategy. Federal Policy Directives.
9. Executive Office of the President. (2026). Executive Order 14412: Setting Hard Migration Deadlines for Federal High-Value Assets and Quantum-Vulnerable Architectural Topologies. The White House.
10. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(1–4), 1-139.
11. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. *International Algorithmic Number Theory Symposium*, 267-288.
12. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-Dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 238-268.
13. Schwabe, P., Stehlé, D., & Zhao, W. (2024). Module-LWE verification paradigms within standard transport security constraints. *Journal of Cryptology*, 37(2), 45-72.
14. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 2672-2680.
15. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 5998-6008.
16. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... & Hassabis, D. (2015). Human-level control through deep reinforcement learning. *Nature*, 518(7540), 529-533.
17. Cyber Security and Infrastructure Security Agency (CISA). (2025). Post-Quantum Cryptographic Commercial Product Category Baseline Requirements. CISA Resources.
18. National Security Agency. (2025). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Implementation Guidelines. NSA Advisory Memorandums.
19. Model Context Protocol Steering Committee. (2026). Model Context Protocol (MCP) Specification and Security Interface Layout v1.4. Open-Source AI Infrastructure Alliance.
20. Woo, B., & Zhou, E. (2026). Post-quantum AI infrastructure security: Hardening autonomous agent context transfers against fault-tolerant quantum threats. *International Journal of Automated Cyber Defense*, 14(3), 112-129.