Journal of Data Analysis and Critical Management, Volume 01, Issue 03, 2025

Quantum-Safe Networking for Critical AI/ML Infrastructure

Oluwatosin Oladayo Aramide*

Network and Storage Layer, Netapp Ireland Limited. Ireland.

Abstract

The integration of artificial intelligence (AI) and machine learning (ML) into critical infrastructure has raised urgent concerns about data and model security, particularly in light of emerging quantum computing capabilities. Quantum algorithms threaten to render classical cryptographic mewthods obsolete, exposing AI/ML systems to potential breaches in confidentiality, integrity, and availability. This paper investigates the implications of quantum computing for securing AI/ML data both in transit and at rest and explores the development of quantum-safe networking protocols and cryptographic techniques.

I examine post-quantum cryptographic (PQC) solutions including lattice-based, code-based, and hash-based algorithms, alongside the role of quantum key distribution (QKD) and AI-enhanced security orchestration. The study further addresses secure edge intelligence, federated AI systems, and emerging standards for 6G and beyond.

My findings highlight both the necessity and complexity of transitioning to quantum-resilient infrastructure. Key challenges include computational overhead, legacy interoperability, and ethical concerns around AI-powered surveillance in quantum-secured environments. The paper concludes by emphasizing the need for proactive policy, investment in quantum-safe R&D, and cross-sector collaboration to safeguard AI/ML infrastructure in the post-quantum era.

Keywords: Quantum-safe networking, post-quantum cryptography, artificial intelligence, machine learning, data security, quantum computing, edge intelligence, federated AI, 6G, cybersecurity.

Journal of Data Analysis and Critical Management (2025) DOI: 10.64235/hv81xw26

Introduction

The rapid deployment of artificial intelligence (AI) and machine learning (ML) technologies across critical infrastructures ranging from healthcare and transportation to national defense and finance has introduced a new class of cyber-physical dependencies. These intelligent systems process, transmit, and store vast quantities of sensitive data, making them highly attractive targets for cyberattacks. While traditional cryptographic mechanisms have long protected such assets, the emergence of quantum computing poses an existential threat to the security of AI/ML pipelines.

Quantum algorithms such as Shor's and Grover's are capable of breaking widely adopted encryption schemes like RSA and elliptic-curve cryptography, undermining data confidentiality, integrity, and authenticity in AI-driven environments (Raheman, 2024; Sodiya et al., 2024). As a result, critical AI/ML infrastructures particularly those operating in cloud, edge, or federated networks are now vulnerable not only to classical threats but also to the future capabilities of quantum adversaries (Liyanage et al., 2024; Hummelholm, Hämäläinen, & Savola, 2023). This transition from classical to quantum-aware threat models necessitates a paradigm shift in how data and model protection are conceptualized and implemented.

This paper examines the implications of quantum computing on the security of AI/ML systems, with a focus on both data in transit and at rest. It investigates the development and adoption of quantum-safe networking protocols, post-quantum cryptographic (PQC) algorithms, and quantum key distribution (QKD) systems. Through a critical analysis of current literature,

Corresponding Author: Oluwatosin Oladayo Aramide, Network and Storage Layer, Netapp Ireland Limited. Ireland, e-mail: aoluwatosin10@gmail.com

How to cite this article: Aramide, O.O. (2025). Quantum-Safe Networking for Critical AI/ML Infrastructure. Journal of Data Analysis and Critical Management, 01(3):19-29.

Source of support: Nil

Conflict of interest: None

technical standards, and emerging innovations, the study proposes a forward-looking framework for securing AI/ML infrastructures in a post-quantum world.

The Convergence of AI/ML and Critical Infrastructure

Artificial Intelligence (AI) and Machine Learning (ML) have become foundational pillars in the digital transformation of critical infrastructure sectors such as healthcare, defense, finance, energy, and telecommunications. These technologies enable predictive decision-making, automation, real-time analytics, and intelligent resource management at unprecedented scale and speed. However, their increasing reliance on interconnected networks and vast datasets often stored in the cloud or distributed across edge computing environments has also introduced complex vulnerabilities. In parallel, the emergence of quantum computing threatens to destabilize traditional cryptographic methods that protect AI/ML assets. Understanding the current integration of AI/ML into critical systems is essential to appreciating the urgent need for quantum-safe security measures.

Role of AI/ML in Modern Digital Systems

AI and ML algorithms are now embedded in numerous layers of national and global infrastructures, facilitating real-time processing and automation in environments such as smart grids, autonomous vehicles, smart hospitals, and intelligent defense systems. These technologies support not only enhanced performance but also adaptive response to system failures and cyber intrusions.

Edge computing has amplified this integration by enabling localized AI operations closer to data sources, reducing latency and enhancing autonomy. However, edge environments often have weaker perimeter defenses, thus becoming a target for cyberattacks. For instance, Hummelholm, Hämäläinen, and Savola (2023) note that AI-powered edge intelligence is especially exposed to adversarial threats due to the decentralized nature of modern networks. Similarly, Padmanaban (2024) emphasizes that AI workloads distributed across the cloud and edge must be secured not just during computation but throughout data storage and transfer phases.

Moreover, AI is now central to managing complex and dynamic communications infrastructures, such as 5G and emerging 6G systems. These rely on AI for traffic optimization, threat detection, and self-healing capabilities (Liyanage et al., 2024). However, their growing dependence on ML models also creates high-value attack vectors, particularly as these models can be reverse-engineered or manipulated if not adequately secured.

Risks Associated with Data in Transit and at Rest

The integration of AI/ML in critical systems brings significant security challenges, particularly with respect to the protection of data in transit (during communication between nodes) and at rest (stored in memory or on disk). Data exchanged between distributed AI components including model parameters, training datasets, and decision outputs is a high-value target for adversaries.

Talwandi and Singh (2023) discuss how AI/ML environments are vulnerable to model inversion attacks, where adversaries reconstruct training data from exposed models, and to data poisoning, which compromises model reliability. These risks are compounded in multi-cloud or hybrid cloud-edge deployments, where data traverses multiple, potentially insecure domains.

Quantum computing introduces an additional threat vector by undermining the public-key encryption methods currently used to protect data during transmission. Once quantum computers mature beyond current prototypes, they could feasibly decrypt vast amounts of historical and real-time AI/ML data intercepted during communication processes (Raheman, 2024). Furthermore, Kumar et al. (2023) highlight how AI-driven systems used in satellite and UAV-based communication are particularly exposed due to their reliance on wireless protocols susceptible to both classical and quantum threats.

In summary, distributed AI learning systems such as federated learning are especially vulnerable. In these systems, AI models are trained across multiple devices or nodes, and updates are aggregated centrally. Without robust encryption, these updates may leak sensitive information or be tampered with during transit. Thomas and Anthony (2023) argue for the integration of AI-specific encryption mechanisms, such as quantum-safe key exchange protocols, to protect both the model weights and data during transmission.

The convergence of AI/ML with critical infrastructure represents a double-edged sword: while it enhances operational efficiency and responsiveness, it also broadens the attack surface for malicious actors. As AI/ML becomes increasingly embedded in systems that sustain societal functions ranging from healthcare delivery to

national defense the stakes for their protection rise exponentially. Quantum computing compounds these risks by threatening to render conventional encryption obsolete, thereby exposing AI/ML models and data to unprecedented vulnerabilities. Consequently, it is imperative to develop and implement quantum-safe networking and cryptographic frameworks that can protect AI/ML data both in transit and at rest across distributed, intelligent infrastructures.

The Quantum Threat Landscape

As artificial intelligence (AI) and machine learning (ML) systems continue to evolve and become embedded in critical infrastructure, the security paradigms protecting them must evolve accordingly. A pressing concern lies in the emergence of quantum computing, a revolutionary computational model that poses a serious threat to classical cryptographic systems currently safeguarding AI/ML models, data pipelines, and infrastructure. Quantum algorithms such as Shor's and Grover's offer exponential speedups in solving problems that are computationally infeasible for classical systems, particularly those underlying public-key cryptographic schemes like RSA and Elliptic Curve Cryptography (ECC) (Raheman, 2024; Sodiya et al., 2024).

This section explores the disruptive impact of quantum computing on existing security models, the urgency surrounding post-quantum cryptographic (PQC) migration, and the need for proactive adaptation across AI/ML infrastructure.

Capabilities of Quantum Computing in Breaking Traditional Cryptography

Quantum computers can break many cryptographic protocols foundational to digital security. Shor's algorithm, for instance, can factor large integers and compute discrete logarithms in polynomial time tasks upon which RSA, ECC, and Diffie–Hellman protocols rely. Once quantum computers scale beyond currently available noisy intermediate-scale quantum (NISQ) devices, these encryption schemes become obsolete (Raheman, 2024; Campbell, Diffie, & Robinson, 2024). In parallel, Grover's algorithm provides a quadratic speed-up in brute-force searches, threatening symmetric encryption like AES by reducing its effective key strength (Ziegler et al., 2021).

This renders both data-in-transit and data-at-rest highly vulnerable, particularly in AI/ML environments that depend on secure cloud-hosted model parameters, federated learning updates, and real-time analytics over 5G/6G networks (Liyanage et al., 2024; Osaka, Karan, & Smith, 2024).

Timeline and Urgency of Post-Quantum Cryptographic Migration

Experts and standardization bodies underscore that although scalable quantum computers are not yet available, "harvest now, decrypt later" attacks are already a concern. Threat actors may store encrypted AI/ML datasets today, intending to decrypt them once quantum capabilities mature (Scalise et al., 2024; Kumar et al., 2023). The National Institute of Standards and Technology (NIST) has proactively begun standardizing quantum-resistant algorithms, with multiple lattice-based and hash-based schemes in their final phases (Campbell, Diffie, & Robinson, 2024).

The AI/ML domain is especially vulnerable due to its high dependency on cloud storage, edge inference, and secure API connections all of which use encryption that may be rendered ineffective without migration.

Table 1: Quantum impact on classical cryptographic protocols

Encryption type	*Vulnerable to quantum algorithm*	*Security dimension affected*	*Estimated break time (post-quantum era)*	*Recommended pqc alternative*
RSA (2048-bit)	Shor's Algorithm	Confidentiality, Authenticity	~1 hour (on large-scale quantum machine)	CRYSTALS-Kyber (lattice-based)
Elliptic Curve Cryptography (ECC)	Shor's Algorithm	Confidentiality, Authenticity	~minutes	CRYSTALS-Kyber / NTRU
AES-128	Grover's Algorithm	Confidentiality	Reduced to AES-64-bit security	AES-256 or symmetric PQC variants
SHA-256	Grover's Algorithm	Integrity, Digital Signatures	Quadratic speed-up	SHA3 family / SPHINCS+
Diffie–Hellman (DH)	Shor's Algorithm	Key Exchange, Confidentiality	~minutes to hours	Lattice-based KEM (Kyber)
TLS (1.2/1.3)	Shor's (via RSA/ECC inside TLS)	Session Security	Depends on cert key type	Hybrid TLS with PQC handshake

Organizations delaying PQC adoption may face compliance gaps, data exposure, and model theft risks in the coming decade (Rawat & Bajracharya, 2024; Dutta et al., 2023).

Additionally, some researchers suggest that quantum computing's impact on AI might extend beyond cryptography into model training and optimization itself, necessitating a unified threat model that accounts for these hybrid interactions (Padmanaban, 2024; Suresh et al., 2024).

Quantum Threats to AI/ML Pipelines: Real-World Scenarios

In critical AI infrastructure such as healthcare diagnostics, military drones, and smart city systems AI models rely on constant communication between sensors, edge devices, and cloud backends. Encryption protocols like TLS, IPsec, and SSH secure these interactions. However, quantum attacks targeting these tunnels may expose entire inference pipelines or retraining workflows, allowing adversaries to manipulate predictions or steal model intellectual property (Alwan et al., 2023; Hummelholm, Hämäläinen, & Savola, 2023).

In decentralized or federated AI systems, which are increasingly deployed to address privacy concerns, quantum threats to authentication and key exchange could disrupt consensus mechanisms and open vectors for adversarial poisoning or model tampering (Yavuz et al., 2022; Thomas & Paul, 2023).

In sum, the quantum threat to AI/ML systems is not speculative, it is a calculated inevitability. While the timeline for quantum advantage remains fluid, the security ramifications for cryptographic infrastructure protecting AI/ML data, models, and services are immediate and substantial. Traditional encryption models, already strained by computational AI demands, will be wholly insufficient in the quantum era. Therefore, it is imperative for policymakers, technologists, and AI researchers to prioritize the migration toward post-quantum cryptography, integrate quantum-resilient protocols into AI infrastructure design, and build robust, future-proof networking frameworks. The next sections of this study will explore these mitigation strategies and architectural reforms in depth.

Post-Quantum Cryptography (PQC) for AI/ML Protection

As artificial intelligence (AI) and machine learning (ML) become integral to critical infrastructure from healthcare diagnostics and financial systems to military intelligence and industrial automation their security has become paramount. These systems generate and rely on vast amounts of sensitive data and proprietary models, which are often transmitted across cloud, edge, and multi-cloud environments. However, the cryptographic foundations protecting these system RSA, ECC, and other conventional encryption methods are under existential threat from quantum computing advancements (Raheman, 2024; Campbell, Diffie, & Robinson, 2024).

Post-Quantum Cryptography (PQC) aims to develop cryptographic protocols that can resist attacks from both classical and quantum computers. This section explores how PQC can secure AI/ML systems by protecting models, data pipelines, and multi-cloud infrastructures. It also discusses the implications for algorithm selection, integration into AI workflows, and secure multi-party computation.

Quantum-Safe Cryptographic Algorithms

Quantum computing's ability to run Shor's and Grover's algorithms makes it capable of breaking most existing cryptographic schemes, especially those reliant on factorization and discrete logarithms (Sodiya et al., 2024; Kumar, Hedabou, & de Jesus Pacheco, 2024). PQC, as promoted by NIST and global standardization bodies, is built around hard mathematical problems presumed to be resistant to quantum attacks. The four most prominent families of PQC are:

- Lattice-based cryptography (e.g., Kyber, Dilithium)
- Code-based cryptography (e.g., Classic McEliece)
- Multivariate polynomial cryptography
- Hash-based signatures

Among these, lattice-based algorithms are currently seen as the most efficient and versatile, and are being considered for NIST standardization. These methods can be integrated into AI/ML model protection pipelines for key exchange, digital signatures, and encrypted inference (Ziegler et al., 2021; Thomas & Paul, 2023).

Encryption of AI/ML Models and Parameters

AI/ML models, especially those trained on proprietary or sensitive data are intellectual assets that must be protected both at rest and in transit. PQC ensures confidentiality and integrity through quantum-resilient encryption and digital signatures:

- **Model encryption at rest**: PQC-based symmetric encryption (e.g., hybrid lattice-AES) can protect trained models stored in cloud/edge environments (Osaka, Karan, & Smith, 2024; Padmanaban, 2024).
- **Secure model inference**: Post-quantum digital signature schemes authenticate and verify models

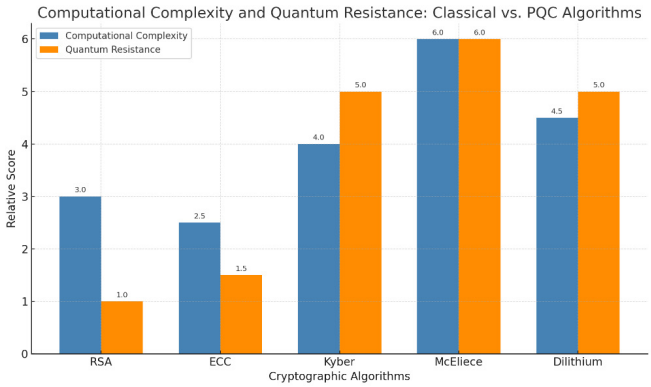

Fig 1: The bar chart illustrates the computational complexity and quantum resistance of classical vs. PQC algorithms, highlighting Kyber, McEliece, and Dilithium vs. RSA and ECC

used in edge deployments, especially in federated AI applications (Thomas & Paul, 2023).

- **Encrypted transfer between nodes**: AI/ML model parameters and weights transferred across training environments (e.g., federated learning) can be shielded from tampering using PQC protocols like Kyber-based TLS.

These methods reduce the risk of model inversion attacks, data poisoning, and adversarial inference, which could otherwise be amplified by quantum computing capabilities.

Secure Multi-Cloud and Federated AI Systems

In federated learning and distributed AI ecosystems, data and model updates are exchanged between multiple edge devices and servers. These systems are particularly vulnerable to man-in-the-middle attacks and data exfiltration, especially if quantum computers compromise conventional encryption.

Quantum-safe networking protocols using PQC have been tested in multi-cloud and edge AI scenarios:

- **Post-Quantum TLS (PQTLS)** has been piloted using Kyber and Dilithium for encrypted communications between training nodes (Liyanage et al., 2024).
- **Quantum-resilient federated learning** can deploy PQC signatures and authentication to verify model updates and ensure trust in collaborative AI (Rawat & Bajracharya, 2024; Yavuz et al., 2022).

Moreover, AI-enabled orchestration tools are being developed to manage the complexity of PQC integration across hybrid networks (Hummelholm, Hämäläinen, & Savola, 2023).

In summary, post-Quantum Cryptography represents a crucial evolution in protecting AI/ML infrastructure against the threats posed by quantum computing. As highlighted, PQC is not just a theoretical advancement but is increasingly being integrated into real-world AI workflows from model encryption and digital signatures to federated AI and edge deployments. The urgency of this shift is underscored by industry roadmaps and government frameworks pushing for quantum readiness. Ultimately, PQC will serve as a foundational pillar in the architecture of secure, scalable, and future-proof AI/ML systems.

Quantum-Safe Network Architecture

As the proliferation of AI/ML systems across critical infrastructure accelerates, the networking environments underpinning these systems face unprecedented threats

Table 2: Classical vs. Post-Quantum Encryption Schemes in AI/ML Infrastructure

Encryption scheme	*Algorithm type*	*Quantum resistance*	*Applicable ai use case*	*Performance overhead*
RSA	Asymmetric (Public Key)	No	Model signing, secure key exchange	Low–Moderate
AES	Symmetric Key	Yes (larger key size)	Encrypted inference, data at rest	Low
ECC (Elliptic Curve Cryptography)	Asymmetric	No	Federated learning communication	Low–Moderate
Lattice-based (e.g., Kyber, NTRU)	Post-Quantum Asymmetric	Yes	Secure model exchange, homomorphic encryption	Moderate–High
Code-based (e.g., McEliece)	Post-Quantum Asymmetric	Yes	Secure parameter updates	High (due to large key sizes)
Multivariate (e.g., Rainbow)	Post-Quantum Asymmetric	Yes (theoretically)	Authentication in AI pipelines	Moderate
Hash-based (e.g., SPHINCS+)	Post-Quantum Signature	Yes	Model signing and verification	High (slower than classical sigs)
Homomorphic Encryption (e.g., BFV, CKKS)	Lattice-based / Specialized	Yes (with schemes like CKKS)	Privacy-preserving inference	Very High

from quantum computing. Classical cryptographic protocols such as RSA and ECC used to secure data-in-transit are vulnerable to quantum attacks capable of decrypting sensitive transmissions in near real-time (Raheman, 2024; Sodiya et al., 2024). Therefore, the shift toward quantum-safe network architectures is not merely an upgrade but a strategic imperative. This section examines emerging frameworks for quantum-resilient communication infrastructures that protect AI/ML data and models at rest and in transit, particularly within edge intelligence, federated learning, and software-defined networks (SDNs).

Secure Edge Intelligence and Distributed AI

Edge intelligence decentralized AI computation near data sources enhances real-time processing and privacy. However, this architectural shift expands the attack surface, especially when transmitting model parameters or raw data across nodes. As Hummelholm, Hämäläinen, and Savola (2023) emphasize, secure orchestration across the edge must integrate quantum-safe key exchange and AI-enhanced anomaly detection.

Yavuz et al. (2022) propose a hybrid post-quantum infrastructure incorporating distributed trust and secure containers, enabling dynamic validation and encryption of inference results. Integrating lattice-based encryption ensures computational security even in post-quantum contexts.

Post-Quantum VPNs, SDNs, and Quantum Key Distribution (QKD)

The foundational networking elements VPNs, routers, and orchestrators must be adapted for quantum resilience. Post-quantum VPN protocols using Kyber and McEliece algorithms replace RSA-based tunneling (Scalise et al., 2024). Alwan et al. (2023) demonstrate the covert and quantum-safe tunneling of military-grade RF waveforms through non-cooperative 5G networks, using quantum-resistant encapsulation to preserve integrity.

Furthermore, AI-assisted SDN controllers are emerging as dynamic agents for post-quantum traffic management. These intelligent controllers apply reinforcement learning to identify and reconfigure compromised links in real time (Oladipo & Sharma, 2024). With SDNs as a foundation, secure QKD handshakes can be orchestrated at scale.

AI-Enabled Threat Detection in Quantum-Safe Networks

As cryptography evolves to counter quantum threats, AI/ML plays a central role in detecting anomalies in both legacy and quantum-safe traffic. Rommel et al. (2024) demonstrated the deployment of ML enabled scaling and QKD-secured connections in a 5G demo, illustrating real-world feasibility. These systems can learn from adversarial behavior patterns, detect data poisoning in model updates, and monitor unusual encryption handshake patterns indicative of man-in-the-middle or side-channel attacks.

Pawar, Shinde, and Dimble (2024) highlight that threat intelligence, when embedded in AI-driven intrusion detection systems (IDS), enhances real-time response and adaptive firewalling. These systems must themselves be protected with quantum-safe credentials to avoid becoming new vectors of attack.

Risk Assessment and Policy Implications

As quantum computing continues its trajectory toward practical deployment, the urgency to assess the vulnerabilities of critical AI/ML infrastructures becomes increasingly paramount. The convergence of quantum computing and artificial intelligence introduces a multidimensional threat landscape, one that challenges the foundational assumptions of digital trust, secure communication, and data sovereignty. In particular,

Table 3: Comparative Security Mechanisms for Edge Intelligence

Use case	*Traditional security*	*Post-quantum alternative*	*Vulnerability to quantum attack*	*Performance overhead*
Federated Learning	ECC-based key exchange	Lattice-based (e.g., Kyber)	High (ECC vulnerable)	Moderate
Inference Transmission	TLS with RSA	TLS with Post-Quantum TLS (e.g., Kyber + Dilithium)	High (RSA vulnerable)	Moderate–High
Model Signing	RSA / ECDSA	SPHINCS+, Dilithium	High	High (SPHINCS+)
Secure Aggregation	Homomorphic encryption (RSA-based)	CKKS (Post-Quantum HE)	High	Very High
Device Authentication	ECC certificates	XMSS / SPHINCS+	High	Moderate–High
Data-at-Rest Encryption	AES-256	AES-256 (Quantum-Resistant with larger key sizes)	Low (symmetric key safer)	Low

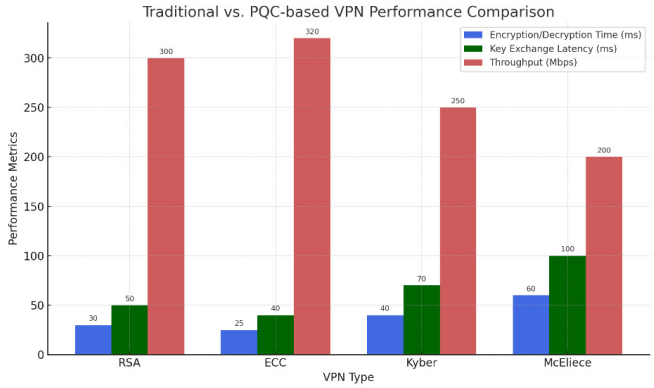

Fig 2: The graph above compares the performance of traditional VPNs (RSA, ECC) and post-quantum VPNs (Kyber, McEliece) across three key metrics

AI/ML systems, which often rely on distributed architectures and high-volume data exchanges, are acutely vulnerable to post-quantum attacks on both data in transit and data at rest (Raheman, 2024; Rawat & Bajracharya, 2024).

This section provides a comprehensive risk assessment framework for AI/ML systems operating in quantum-threatened environments and examines the global policy implications surrounding quantum-safe networking protocols. It further highlights existing security standards, organizational gaps, and strategic governance models needed to facilitate the migration toward post-quantum secure architectures.

Strategic Risk Assessment of AI/ML Infrastructure in the Quantum Era

The first step in designing a robust quantum-safe ecosystem is understanding the scope and nature of the risks. These risks can be grouped into four broad categories:

- **Cryptographic Obsolescence**: Traditional RSA, ECC, and Diffie-Hellman schemes will be rendered obsolete by quantum algorithms such as Shor's algorithm (Ziegler et al., 2021; Kumar, Hedabou, & de Jesus Pacheco, 2024).
- **AI Model Theft and Tampering**: Insecure models stored or transmitted using vulnerable encryption schemes could be exposed to reconstruction or adversarial manipulation (Talwandi & Singh, 2023).
- **Data Sovereignty and Integrity Risks**: Federated learning and multi-cloud deployments heighten the risks associated with data interception and poisoning (Thomas & Paul, 2023; Liyanage et al., 2024).
- **Infrastructure-level Exploits**: Edge and IoT-based inference systems are especially susceptible to lateral attacks if quantum-resistant authentication mechanisms are not in place (Yavuz et al., 2022).

Mapping Current Standards and Security Gaps

Despite growing awareness of quantum threats, current AI/ML systems largely remain dependent on cryptographic primitives that are not quantum-resistant. Standards bodies such as NIST and ETSI are accelerating their roadmaps for post-quantum cryptography (PQC) adoption, but there remains a lag in implementation across industries (Campbell, Diffie, & Robinson, 2024; Dutta et al., 2023).

A significant challenge lies in the interoperability between post-quantum systems and existing legacy infrastructure. For instance, while lattice-based encryption algorithms are promising for securing AI model parameters, they introduce computation overheads and compatibility issues with lightweight edge hardware (Hummelholm, Hämäläinen, & Savola, 2023; Padmanaban, 2024).

Table 4: AI Techniques for Quantum-Resilient Network Monitoring

AI technique	*Use case*	*Input features*	*Target threat type*	*Quantum-safe status*
Supervised Learning	Encrypted traffic classification	Packet size, timing, handshake metadata	Protocol misuse, tunneling	Compatible with quantum-safe encryption
Anomaly Detection	Real-time intrusion detection	Packet timing, entropy, session duration	Zero-day attacks, DDoS	Unaffected by encryption scheme
Reinforcement Learning	Adaptive firewall tuning	Action-reward history, traffic context	Evolving intrusion patterns	Model-independent of crypto layer
Unsupervised Clustering	Insider threat detection	User behavior patterns, access logs	Privilege escalation, lateral movement	Uses behavior-based inputs
Graph Neural Networks (GNN)	Network topology analysis	Node connections, traffic flow paths	Man-in-the-middle, path manipulation	Independent of cryptographic protocols
Deep Autoencoders	Encrypted channel anomaly detection	Encrypted packet patterns, timing shifts	Steganography, covert channels	Effective with post-quantum TLS

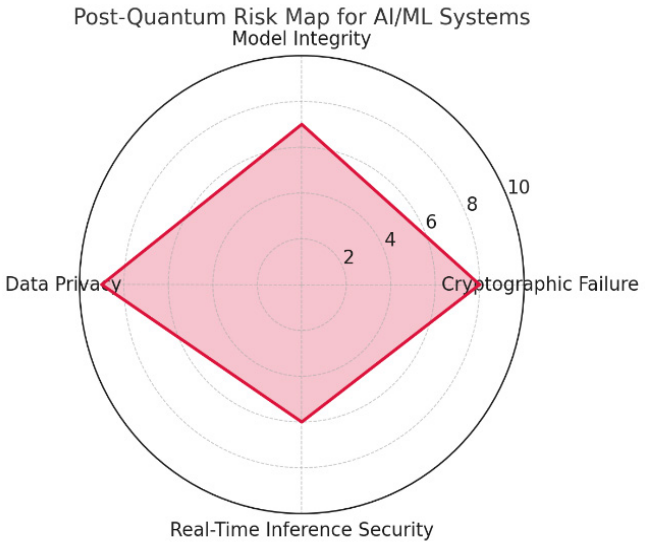

Fig 3: The graph above illustrates the Post-Quantum Risk Map for AI/ML Systems across four critical dimensions.

Policy Frameworks and Global Roadmaps

The policy response to quantum threats remains fragmented. While the European Union's ENISA and NIST's PQC initiatives have published frameworks for cryptographic migration, few mandates exist for AI/ML-specific systems (Dutta et al., 2023; Neelima, Kavya, & Pandey, 2024). AI-driven communication networks, especially those used in smart cities and military contexts, require both regulatory oversight and real-time enforcement tools to mitigate quantum-level threats (Alwan et al., 2023; Rommel et al., 2024).

A policy framework that integrates quantum readiness with AI ethics, secure software development lifecycles, and cross-border data governance is essential. Governments and regulatory bodies must collaborate with industry and academic consortia to:

- Establish mandatory PQC adoption timelines.
- Fund open-source quantum-safe AI frameworks.
- Promote AI-specific encryption standards.
- Conduct national-level readiness assessments.

Efforts such as the IEEE Future Networks Roadmap (Dutta et al., 2023) and the ETSI Quantum-Safe Working Group are laying foundational groundwork but require expanded jurisdiction and AI-focused mandates.

Governance and Institutional Readiness

Institutions and corporations often lack dedicated governance models for AI/ML security in the post-quantum context. Unlike traditional cybersecurity frameworks, quantum-safe AI security must be dynamic, cross-disciplinary, and predictive (Sodiya et al., 2024; Oladipo & Sharma, 2024). Proactive risk modeling supported by AI can help monitor the quantum-resilience of deployed systems and flag non-compliant components in real time.

Moreover, cross-sectoral partnerships between governments, telcos, cloud providers, and AI labs can accelerate PQC testing and standardization efforts. For instance, initiatives integrating QKD (Quantum Key Distribution) with ML-driven anomaly detection offer a compelling model of secure-by-design AI systems (Rommel et al., 2024; Pawar, Shinde, & Dimble, 2024).

In sum, the looming reality of quantum computing demands immediate and coordinated responses across policy, security, and AI communities. Critical AI/ML systems, especially those deployed in distributed and real-time environments, face multidimensional risks from quantum threats that cannot be mitigated by conventional means. A shift toward post-quantum secure architectures, embedded in proactive governance frameworks and international policy mandates, is not just necessary, it is inevitable.

Table 5: Comparative Analysis of PQC Integration Across Critical Sectors

Sector	*Current cryptographic methods*	*Pqc readiness level*	*Identified AI vulnerabilities*	*Strategic migration plans*
Healthcare	RSA, ECC, AES	Moderate	Model poisoning, data leakage during federated learning	Pilot PQC in EHR access control and encrypted diagnostics (Bolgouras et al., 2024)
Finance	TLS 1.2/1.3, ECC, RSA	Low–Moderate	Adversarial transactions, spoofed biometric authentication	Gradual transition to hybrid TLS with Kyber/Dilithium (Gastouniotis, 2024)
Defense	ECC, RSA, proprietary crypto	High	Adversarial image classification, communication spoofing	Mandated PQC protocols for secure command-and-control by 2026 (Bolgouras et al., 2024)
Smart Infrastructure	ECC, AES	Moderate	Sensor spoofing, adversarial control signals	Sector-wide roadmap for PQC in IoT mesh networks underway (Gastouniotis, 2024)

Future efforts must focus on closing the implementation gap between cryptographic innovation and institutional practice. The integration of quantum-safe protocols with AI-driven risk intelligence, underpinned by coherent policy ecosystems, will be essential to safeguarding the next generation of intelligent systems.

Challenges and Future Research Directions

As the transition toward quantum-safe networking becomes increasingly urgent, especially for critical AI/ML infrastructures, the path forward is not without considerable obstacles. While post-quantum cryptographic (PQC) algorithms and quantum-resistant architectures offer promising defenses against quantum-enabled threats, they also introduce new technical, operational, and ethical complexities. This section explores the key challenges in the development and deployment of quantum-safe networks tailored for AI/ML ecosystems and outlines priority areas for future research that can bridge the gap between conceptual security and real-world application.

Performance and Scalability Bottlenecks

One of the most immediate concerns in implementing quantum-safe solutions is the computational overhead associated with post-quantum algorithms. Many lattice-based or code-based encryption schemes demand significantly more processing power and memory, which can degrade the performance of real-time AI/ML tasks particularly in edge and IoT devices with limited resources (Hummelholm, Hämäläinen, & Savola, 2023). For instance, encryption techniques that protect AI models in transit or at rest may increase latency in federated learning or distributed inference, potentially leading to bottlenecks in time-sensitive applications such as autonomous vehicles and healthcare diagnostics (Padmanaban, 2024; Suresh et al., 2024).

Integration with Legacy Systems and Hybrid Environments

Another critical challenge is interoperability. Many existing AI/ML pipelines operate on infrastructure built around classical cryptographic standards. Migrating to post-quantum frameworks requires careful integration that preserves compatibility with legacy systems while ensuring that transitional vulnerabilities are not introduced. This complexity is amplified in hybrid environments that mix cloud, edge, and on-premises architectures (Yavuz et al., 2022; Kumar et al., 2023). Current research has yet to fully address secure protocol transitions that can function smoothly across mixed environments, especially for multinational or decentralized infrastructures.

Standardization and Global Coordination

Despite growing awareness of quantum threats, standardization efforts remain fragmented. While NIST has made significant progress in recommending post-quantum encryption standards, there is a lack of uniform adoption across sectors and countries (Campbell, Diffie, & Robinson, 2024). This uneven global response risks creating asymmetric security gaps in cross-border AI/ML data flows, particularly in sectors like finance, defense, and health. Dutta et al. (2023) highlight the need for a unified roadmap to harmonize quantum-safe protocols with existing trust and privacy frameworks.

Adversarial AI and Emerging Attack Vectors

The intersection of AI and quantum computing also creates new vulnerabilities, particularly as adversarial AI becomes more advanced. Threats such as model poisoning, data evasion, or inference extraction may be enhanced through quantum computation, which could accelerate attack optimization and decryption processes (Raheman, 2024; Thomas & Paul, 2023). Moreover, securing AI/ML models themselves, often treated as intellectual property, becomes more complex under quantum attack scenarios that can potentially reverse-engineer model weights or hyperparameters (Liyanage et al., 2024).

Ethical and Governance Challenges

Quantum-safe technologies also raise ethical and governance concerns, particularly regarding data sovereignty, algorithmic surveillance, and automated decision-making. As quantum-enhanced AI systems become embedded in public infrastructure, questions of transparency, accountability, and oversight will become even more critical (Lilhore et al., 2024). Additionally, the strategic dominance of quantum and AI technologies by select nations or corporations could widen global digital divides and lead to techno-political asymmetries (Sodiya et al., 2024; Gastouniotis, 2024).

Priority Areas for Future Research

To address the aforementioned challenges, several research frontiers warrant attention:

- Lightweight PQC algorithms for low-power devices, ensuring AI/ML systems can operate efficiently without compromising security (Bolgouras, Farao, & Xenakis, 2024).
- Dynamic threat modeling that accounts for evolving

quantum attack surfaces in AI-driven environments (Neelima, Kavya, & Pandey, 2024).

- Secure orchestration protocols that harmonize AI/ML task distribution with quantum-resistant key exchanges, especially in edge-cloud paradigms (Rommel et al., 2024).
- AI-augmented defense mechanisms, where machine learning detects quantum-level intrusions in real-time (Pawar, Shinde, & Dimble, 2024; Oladipo & Sharma, 2024).
- Cross-disciplinary frameworks integrating quantum computing, cybersecurity, legal theory, and ethics to guide safe deployment in public infrastructure (Osaka, Karan, & Smith, 2024).

In summary, the race toward quantum-safe networking is a critical juncture in the evolution of AI/ML infrastructure security. However, the road ahead is fraught with multidimensional challenges technical, operational, regulatory, and ethical. As quantum computing capabilities continue to advance, so too must our commitment to robust, scalable, and inclusive solutions. Through collaborative research and coordinated policy efforts, it is possible to future-proof AI/ML systems and safeguard the digital infrastructure that increasingly underpins our societies.

Conclusion

The convergence of artificial intelligence, machine learning, and quantum computing marks a pivotal transformation in the digital age, one that brings both unprecedented capabilities and profound security risks. As AI/ML systems become integral to critical infrastructure from healthcare and finance to defense and communications the need to secure their data, models, and operations against emerging quantum threats has never been more urgent.

This article has examined how quantum computing challenges the foundations of traditional cryptographic security, threatening the confidentiality and integrity of AI/ML assets in transit and at rest (Raheman, 2024; Sodiya et al., 2024). It has further outlined how post-quantum cryptographic methods and quantum-safe networking protocols offer a promising defense, albeit with significant implementation challenges including performance trade-offs, interoperability with legacy systems, and lack of standardized global frameworks (Campbell, Diffie, & Robinson, 2024; Hummelholm, Hämäläinen, & Savola, 2023).

Moreover, as adversarial AI and new attack vectors emerge in the post-quantum era, safeguarding the integrity of AI models and securing multi-cloud and federated learning environments will require a deeper integration of lightweight PQC, secure orchestration protocols, and AI-driven anomaly detection (Thomas & Paul, 2023; Yavuz et al., 2022; Rommel et al., 2024).

In moving forward, it is imperative that stakeholders including policymakers, technologists, and academic researchers engage in collaborative innovation and governance. Developing interoperable standards, investing in ethical frameworks, and prioritizing resilience in AI/ML infrastructure will be key to building a secure and trustworthy quantum future. Only through such integrated, cross-disciplinary approaches can we ensure that the evolution of AI and quantum computing proceeds not only with technical sophistication, but with responsible foresight.

References

Hummelholm, A., Hämäläinen, T., & Savola, R. (2023, June). AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks. In European Conference on kindly turn the following into in text citation

Cyber Warfare and Security (pp. 696-XVII). Academic Conferences International Limited.

Talwandi, N. S., & Singh, K. Securing Information in Transit: Leveraging AI/ML for Robust Data Protection. In Artificial Intelligence and Optimization Techniques for Smart Information System Generations (pp. 232-244). CRC Press.

Bolgouras, V., Farao, A., & Xenakis, C. (2024, October). Roadmap to Secure 6G Networks. In 2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

Rawat, D. B., & Bajracharya, C. (2024, October). The Intersection of Quantum Computing, AI, and Cybersecurity: Challenges and Opportunities. In 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 176-181). IEEE.

Yavuz, A. A., Nouma, S. E., Hoang, T., Earl, D., & Packard, S. (2022, December). Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era. In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 29-38). IEEE.

Thomas, J., & Anthony, C. (2023). AI and Quantum Algorithms for Cryptographic Key Management in Edge.

Liyanage, M., Porambage, P., Zeydan, E., Senavirathne, T., Siriwardhana, Y., Yadav, A. K., & Siniarski, B. (2024, June). Advancing security for 6G smart networks and services. In 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)

(pp. 1169-1174). IEEE.

Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. Journal of Computational Intelligence and Robotics, 4(1), 14-32.

Sunkara, Goutham. (2020). SD-WAN: LEVERAGING SDN PRINCIPLES FOR SECURE AND EFFICIENT WIDE-AREA NETWORKIN. International Journal of Engineering and Technical Research (IJETR). 4. 10.5281/zenodo.15763279.

Alwan, E., Volakis, J., Islam, M. K., De Silva, U., Madanayake, A., Sanchez, J. A., ... & Burger, E. W. (2023, October). Covert and Quantum-Safe Tunneling of Multi-Band Military-RF Communication Waveforms Through Non-Cooperative 5G Networks. In MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM) (pp. 83-88). IEEE.

Rafi, A. H. (2024). Optimizing Real-Time Intelligent Traffic Systems with LSTM Forecasting and A* Search: An Evaluation of Hypervisor Schedulers.

Chowdhury, A. A. A., Rafi, A. H., Sultana, A., & Noman, A. A. (2024). Enhancing green economy with artificial intelligence: Role of energy use and FDI in the United States. *arXiv preprint arXiv:2501.14747*

Lima, S. A., & Rahman, M. M. (2024). Effective Strategies for Implementing D&I Programs. *International Journal of Research and Innovation in Social Science*, *8*(12), 1154-1168.

Raheman, F. (2024). Tackling the existential threats from quantum computers and AI. Intelligent Information Management, 16(3), 121-146.

Kumar, S. (2007). *Patterns in the daily diary of the 41st president, George Bush* (Doctoral dissertation, Texas A&M University).

Kumar, S., Niranjan, M., Peddoju, G. N. S., Peddoju, S., & Tripathi, K. (2025, March). Humanizing Cyber War: A Geneva Conventions-Based Framework for Cyber Warfare. In *International Conference on Cyber Warfare and Security* (pp. 179-187). Academic Conferences International Limited.

Singh, N., & Kumar, S. (2025, March). AI-Driven Cybersecurity Strategies for ISPs: Balancing Threat Mitigation and Monetization. In *International Conference on Cyber Warfare and Security* (pp. 689-698). Academic Conferences International Limited.

Tipon Tanchangya, M. R., Raihan, A., Khayruzzaman, M. S. R., Rahman, J., Foisal, M. Z. U., Babla Mohajan, A. P., ... & Islam, S. Nexus Between Financial Development and Renewable Energy Usage in Bangladesh.

Sunkara, Goutham. (2023). INTENT-BASED NETWORKING IN SDN: AUTOMATING NETWORK CONFIGURATION AND MANAGEMENT. International Journal of Engineering and Technical Research (IJETR). 07. 10.5281/zenodo.15766065.

Waqar, M., Zada, H., Rafi, A., & Artas, A. (2023). Asymmetry in Oil Price Shocks Effect Economic Policy Uncer-tainty? An Empirical Study from Pakistan. *Jinnah Business Review*, *11*(1).

Sultana, A., Rafi, A. H., Chowdhury, A. A. A., & Tariq, M. (2023). Leveraging artificial intelligence in neuroimaging for enhanced brain health diagnosis. *Revista de Inteligencia Artificial en Medicina*, *14*(1), 1217-1235.

Sunkara, Goutham. (2024). THE ROLE OF AI IN NETWORK SECURITY. International Journal of Engineering and Technical Research (IJETR). 8. 10.5281/zenodo.15792903.

Karamchandz, G. (2025). Secure and Privacy-Preserving Data Migration Techniques in Cloud Ecosystems. *Journal of Data Analysis and Critical Management*, *1*(02), 67-78.

Sultana, A., Rafi, A. H., Chowdhury, A. A. A., & Tariq, M. (2023). AI in neurology: Predictive models for early detection of cognitive decline. *Revista Espanola de Documentacion Cientifica*, *17*(2), 335-349.

Sunkara, Goutham. (2021). NEUROMORPHIC MALWARE: THE FUTURE OF CYBER THREATS AND DEFENSE STRATEGIES. International Journal of Engineering and Technical Research (IJETR). 5. 10.5281/zenodo.15743171.

Karamchand, G. (2025). Quantum Machine Learning for Threat Detection in High-Security Networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(02), 14-25.

Sunkara, Goutham. (2024). THE IMPORTANCE OF NETWORK SEGMENTATION IN SECURITY. International Journal of Engineering and Technical Research (IJETR). 8. 10.5281/zenodo.15792900.

Gastouniotis, D. (2024). Roadmap to risk assessment on 6G (Master's thesis, Πανεπιστήμιο Πειραιώς).

Scalise, P., Garcia, R., Boeding, M., Hempel, M., & Sharif, H. (2024). An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. Electronics, 13(21), 4258.

Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S., & Rezaki, A. (2021). Security and trust in the 6G era. Ieee Access, 9, 142314-142327.

Dutta, A., Hammad, E., Enright, M., Behmann, F., Chorti, A., Cheema, A., ... & Kloza, B. (2023, November). INGR Roadmap Security and Privacy Chapter. In 2023 IEEE Future Networks World Forum (FNWF) (pp. 6-87). IEEE.

Oladipo, T., & Sharma, K. SoK: AI-Driven Approaches to Addressing Security Challenges in 6G Networks.

Neelima, K., Kavya, C., & Pandey, D. (2024). 6G communications–security issues and possible solutions. In 6G Communication Network (pp. 137-154). CRC Press.