Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Post-Quantum Secure Digital Transformation with AI-Driven Threat Detection

Anees Raza
Department of physics, Riphah international university, Islamabad
aneesrqza081@gmail.com

Jamil Ur Rehman *
MS (CE), SSUET
Designation : Senior General Manager (IT) / CTIO SSGCL
jamil94@yahoo.com
ORCID ID: 0009-0006-7218-3565

Shoaib Hayat
Computer Science and Technology Auckland University of Technology, New Zealand
shoaib.devpy@gmail.com

ABSTRACT

Two disruptive technologies — quantum computing and artificial intelligence (AI) — are coming together at a time when organisations around the world are rapidly rolling out digital transformation projects to surmount a host of cyber security challenges. In this paper, the authors combine the principles of NIST's post-quantum cryptography (PQC) standardization process (FIPS 203, 204, and 205), the concepts of artificial intelligence in threat detection architectures, and the zero-trust security model to present a unified approach to post-quantum-secure digital transformation. It integrates some lattice-based post-quantum cryptographic control plane functions (key encapsulation and digital signatures) with an AI-driven detection and response plane, managed by a zero-trust policy engine and a crypto-agility management service. The paper argues that it is not only about the strength of the cryptographic algorithms themselves, but also about crypto agility, regular AI-powered tracking and governance of the whole digital transformation stack. Policy implications, CISO suggestions and research directions are explored, as are limitations.

Keywords— Post-Quantum Cryptography, Artificial Intelligence, Threat Detection, Digital Transformation, Zero Trust, Nist, Lattice-Based Cryptography, Cybersecurity, Crypto-Agility, Machine Learning

1. Introduction

Digital transformation is no longer a competitive advantage, but a necessity for business. A large enough, fault-tolerant quantum computer with Shor's algorithm

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

running it could factor the large integers and solve the discrete-logarithm problems that underlie today's two major families of public-key algorithms: RSA and elliptic-curve cryptography (ECC) that secure the vast majority of internet traffic and virtual private networks, code-signing infrastructure and financial messaging systems.

This threat is exacerbated by what is broadly called "harvest-now, decrypt-later" (HNDL): adversaries (in particular nation-state intelligence agencies) can record the encrypted traffic today and retain it for future use, when a cryptographically relevant quantum computer (CRQC) is eventually available to decrypt it. NIST also expects to release a fourth algorithm as FIPS 206, and in March 2025, NIST also chose HQC, a code-based scheme, to diversify the mathematical basis of the PQC portfolio (NIST, 2025).

Simultaneously, AI has dramatically reshaped both cyber defense and cyber attack practices in history. Research from the industry indicates that the percentage of threats detected that are LLM generated or LLM-assisted has increased from an estimated 2% in 2021 to about 50% by 2025, making it necessary for defenders to implement AI-based detection in order to stay ahead of the curve (Ahi, 2026).

The challenges of the imminent end of classical public-key cryptography and the quick advancement of both attack and defense due to AI are not mutually exclusive.The two challenges, the imminent end of classical public-key cryptography and the rapid pace of both attack and defense due to the power of AI, do not exist in isolation. The paper says the three workstreams of post-quantum migration, threat detection via AI, and digital transformation are a strategic misstep. If plans are made independently, it is possible for organizations to be working on the same thing, the timelines to overlap, and — most importantly — the window of exposure in which legacy cryptography, immature detection tooling, and expanding digital footprints converge. This paper, however, presents and discusses an integrated control plane using a post-quantum cryptographic control plane, an AI-based detection and response layer, a zero-trust policy engine, and a crypto-agility management service, all designed and managed together.

1.1 Problem Statement

While there is no doubt that there is now a growing understanding of the quantum threat, empirical data suggests that the readiness of organizations to move to post-quantum is not uniform, and in some sectors, shockingly under-ripe (LaMacchia et al., 2025). At the same time, AI-based threat detection tools are shown to be more accurate than signature-based tools, but they come with their own challenges and vulnerabilities, such as the fact that they are prone to evasion attacks, model drift, and lack of sufficient quality labeled data (Apruzzese et al., 2022; He et al., 2023). This paper takes up this gap.

1.2 Significance and Scope

The value of this study is that it synthesizes two literatures that are not typically seen as connected or as a unified security paradigm for digital transformation – that of post-quantum cryptography and AI-driven security – and provides a view where they exist as interconnected parts of a single security risk surface for digital transformation. The paper builds on and critically reviews the current evidence base to create an actionable

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

framework, and explicitly identifies and quotes illustrative figures that are created for expository purposes and not from a single primary dataset.

2. Literature Review

The relevant literature falls broadly into four categories: (a) Post-quantum cryptographic theory and standardization, (b) AI and ML driven intrusion and threat detection, (c) Zero-trust and identity-centric security architectures and (d) sector specific digital transformation and migration studies. Each is discussed in turn, below, and noted points of convergence and unresolved tension between them.

2.1 Post-Quantum Cryptography Standardization Literature

In 2016, NIST opened the door to the public for proposals with the aim of developing a standard and, after three rounds of narrowing, four algorithms were selected for standardization in July 2022 (LaMacchia et al., 2025). Liu and Moody (2024), both senior NIST cryptographers, place these standards in the context of the physics of quantum computation, raising concerns that, although it is assumed that existing PQC candidates are safe from both classical and quantum cryptanalysis, cryptanalytic research is still continuing and algorithm agility is important. Moreover, the cost of the transition, estimated by LaMacchia et al. (2025) for the U.S. non-national security systems alone, is about $7.1 billion if the timeline for completion is set at an aggressive 2035 target—standardization is a necessary but not sufficient condition for organizational readiness.

There is a parallel stream of research looking at the performance of PQC in resource-limited settings. The fact that computational overhead remains an engineering challenge that is being solved, not insurmountable, is further demonstrated by hardware-acceleration research; including RISC-V instruction-set extensions specifically designed for lattice computations, which are able to reduce code size and execution cycles by more than 79%, compared to unoptimised implementations.

2.2 AI-Driven Threat Detection Literature

Literature around the use of machine learning for IDS is much more developed than the literature around PQC, with the first being at least as old as the work of Buczak and Guven (2016) that surveyed the data-mining approaches to IDS. Simultaneously, a body of literature on adversarial machine learning has emerged, describing how these models can be evaded and poisoned; He et al. (2023) give a thorough overview that adversarial perturbations of the traffic can significantly reduce detection accuracy even in state-of-the-art deep learning NIDS, while Arp et al. (2022) list a series of common methodological shortcomings that can lead to overly optimistic accuracy measurements reported in the published literature, such as unrealistic threat scenario and/or experimental leakage between the training and test sets.

Another thread looks into how generative AI and LLM are used in dual-use in cybersecurity. Operational considerations lead security analysts to be hesitant to rely on the outputs of models that they cannot explain; that is why explainable AI (XAI) is a common thread found in this literature, and Moustafa et al. (2023) review the approaches to XAI in the context of IoT intrusion detection, concluding that interpretability is now a requirement for deployment rather than an academic luxury.

2.3 Zero-Trust and Identity-Centric Architecture Literature

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Although the literature on zero-trust architecture (ZTA) varies, it follows a few core principles: never trust, always verify; continuous authentication; and least-privilege access (Hasan, 2024). The case study by Ahmed et al. (2025) demonstrates a 87% increase in cyber-threat mitigation efficiency by combining QNN with anomaly scoring and a zero-trust framework, although the authors note that while this improvement is promising, the results were only tested on a small-scale in a homogeneous production environment and have not yet been validated in a large-scale deployment across a wider range of diverse production environments.

2.4 Sector-Specific Migration and Digital Transformation Literature

There is a significant amount of literature available for the financial services sector, which has high value data and a more developed security governance. The recent systematic review of financial-sector PQC readiness, which compiled seventeen peer-reviewed studies, identified lattice-based schemes, such as ML-KEM and ML-DSA, as the top contenders for adoption and hybrid cryptographic deployments (running classical and post-quantum algorithms concurrently) as the dominant near-term migration pattern (Wibowo & Santoso, 2026). From a government sector point of view, the U.S. Department of Defense literature provides a description of the operational challenges of synchronizing PQC migration, zero-trust deployment, and AI-security assurance as three concurrently implemented, separate modernization programs, and documents that the lack of coordination in their execution results in measurable integration failures at technical dependency points (U.S. Department of Defense, 2026). While there has been comparatively little published on health care and industrial-IoT, there is mostly conceptual work in these areas, which this paper revisits in Section 7.

2.5 Synthesis and Research Gap

In total, the literature reviewed shows significant and autonomous research efforts in the fields of post-quantum cryptography, artificial intelligence-based recognition and zero-trust architecture, as well as a growing albeit still disjointed realisation of the need for coordination. This paper's contribution will be to be able to synthesize these strands into one reference framework (Section 6), and to examine this reference framework against the readiness evidence of the sectors (Section 7).

3. The Quantum Threat Landscape

The need for post-quantum migration has been thrusted at the top of the digital-transformation agenda, but this is not because quantum computers threaten to pose a danger to computers, the Internet, or cybersecurity. Superposition and entanglement are used in quantum computers to evaluate some mathematical structures much more efficiently than classical computers. There are two quantum algorithms which are relevant to cybersecurity. The same algorithm — first described in 1994 by Shor — was used to show integer factorization and discrete logarithm computation can be done exponentially faster than previously thought, which is exactly the type of problems that make RSA and elliptic-curve cryptography secure to classical computers. If a CRQC with a qubit size large enough and a sufficiently high error-correction fidelity could run Shor's algorithm, it would not only break through RSA or ECC, but it would do so without being concerned by qubit size. (Ye & O'Neill, 2026). Commercial National Security Algorithm Suite 2.0 (Mastercard, 2025).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The primary point of debate is not when a CRQC will exist, but when and how it will be compared to the residual confidentiality value of data encrypted today. There are a number of diverse estimates for the onset of a CRQC that could break RSA 2048, some as early as the early 2030s, but others many decades into the future, which is indicative of real scientific uncertainty about any error-correcting breakthrough (LaMacchia et al., 2025). This transforms an ambiguous future risk into a pressing current mandate to move (The White House Office of Science and Technology Policy, 2024), for data that has a long lifespan, such as state secrets, genomic records, long-term financial and legal agreements.

3.1 Timeline of the Standardization Response

NIST's response to this threat has taken nearly 10 years, starting with an open solicitation for candidate algorithms in 2016, followed by rounds of elimination, to finally publishing its completed federal standards in 2024, and an additional increase in the number of algorithms in the portfolio slated for 2025. This path forward is summarized in Figure 1, and predicted to reach the 2030 and 2035 milestones as called out in the current U.S. federal migration guidance (NIST, 2024d; The White House Office of Science and Technology Policy, 2024).

Figure 1. Timeline of the NIST Post-Quantum Cryptography Standardization Process (2016–2035)

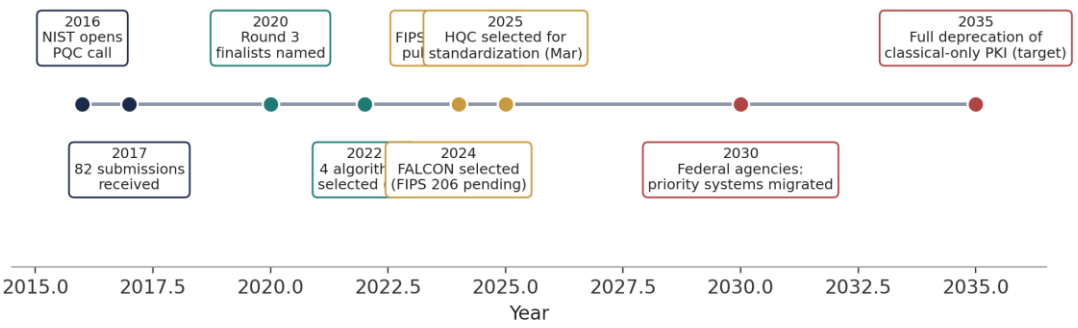

Figure 1. Timeline of the NIST post-quantum cryptography standardization process (2016–2035). Data synthesized from NIST (2024a, 2024b, 2024c, 2024d, 2025) and The White House Office of Science and Technology Policy (2024).

3.2 The Harvest-Now-Decrypt-Later Risk Model

HNDL risk is not equal across data types or industries, but actually depends on three factors: the number of confidentiality lifetimes required for a particular data asset, the probability distribution for the arrival dates of CRQC to a data asset, and the cost of retroactive damage if the asset is ever decrypted. Table 1 shows that there are indicators defined in the financial-sector migration literature and the migration literature by the government, which are representative of the various asset classes, based on the composite risk reasoning in both migrations literature. Table 1 shows that there are indicators that are defined in financial-sector literature and government migration literature, which are representative of the various asset classes, based on the composite risk reasoning of both migrations literature.

Table 1. Illustrative Harvest-Now-Decrypt-Later Risk Profile by Data Asset Class

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Data Asset Class	Required Confidentiality Lifetime	HNDL Exposure Level	Illustrative Sectors
State and defense intelligence	25+ years	Critical	Government, defense
Genomic and biometric records	Lifetime of subject (50–80 yrs)	Critical	Healthcare, research
Long-term financial contracts	10–30 years	High	Banking, insurance
Corporate M&A and trade secrets	5–15 years	High	Enterprise, manufacturing
Payment card transaction data	3–7 years	Moderate	Retail, e-commerce
Session-level web traffic	Minutes to hours	Low	General consumer web

3.3 Attack Surface Expansion Through Digital Transformation

Digital transformation efforts exacerbate quantum risk by quickly increasing the number of endpoints that organizations will have to eventually migrate, which must be cryptographically protected. All of these transformation patterns add to a "cryptographic inventory problem" faced by migration practitioners: locating classical cryptographic use cases is often more operationally challenging than migration to the post-quantum algorithms themselves (Ye & O'Neill, 2026).

4. Foundations of Post-Quantum Cryptography

Post- quantum cryptography is not one algorithm, but a collection of mathematical methods that are thought to be secure against classical and quantum cryptanalysis. In this section, the four main mathematical families will be looked at, along with the particular algorithms that are standardized by NIST based on these families.

4.1 Lattice-Based Cryptography

Lattice-based cryptography is based on the difficulty of certain lattice problems, like Learning With Errors (LWE) and its structured form Module-LWE, in high-dimensional lattices. The digital signature scheme ML-DSA (FIPS 204) is based on CRYSTALS-Dilithium and is designed to be used in code signing, certificate issuance and certificate authentication applications instead of RSA and ECDSA signatures (NIST, 2024a, 2024b). When used for general purpose deployments, lattice-based schemes, except for their larger public keys and ciphertexts compared to their classical counterparts, tend to have a good mix of key size, speed and signature size and are widely preferred across all other post quantum families.

4.2 Hash-Based Cryptography

The security of hash-based signatures depends entirely on the collision resistance of the underlying cryptographic hash functions, which is thought to be very conservative and makes no assumptions about any new, or less known, mathematical object. The downside is significant, SLH-DSA signatures are much larger and slower than ML-DSA signatures, and are therefore well suited for the low throughput, high assurance applications like firmware and software signing but not transactional signing.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

4.3 Code-Based and Isogeny-Based Cryptography

The McEliece cryptosystem and its NIST selected successor HQC are examples of cryptography based on codes, where the security is based on the difficulty of decoding random linear error-correcting codes. While isogeny-based cryptography has the smallest key sizes of any post-quantum family of cryptographic primitives, it suffered a large blow when the prominent isogeny-based candidate, SIKE, was broken via classical cryptanalysis in 2022, a warning that PQC candidates must be carefully examined even in the advanced standardization rounds (Ye & O'Neill, 2026).

4.4 Comparative Performance: Key and Signature Sizes

One of the recurring practical challenges in all post quantum families is the size of the data that needs to be handled as opposed to classical algorithms. The size increase will directly impact network protocols like TLS, where larger handshake payloads may lead to longer round-trip times, as well as memory limits in constrained environments like embedded IoT devices (as discussed in the PQC performance literature focused on IoT applications; National Institute of Standards and Technology, 2024a; a Programmable Crypto-Processor for NIST PQC Standardization).

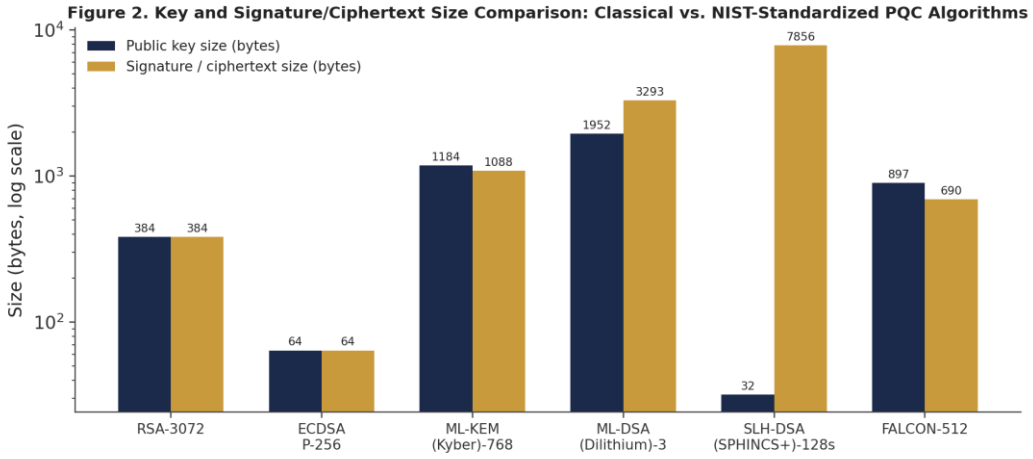

Figure 2. Key and signature/ciphertext size comparison: classical vs. NIST-standardized post-quantum cryptography algorithms. Values are representative parameter-set figures compiled from NIST (2024a, 2024b, 2024c) specification documents.

4.5 Hybrid Cryptography and Crypto-Agility

The most prevalent deployment scenario reported in the literature in the near term is hybrid cryptography, that is, use of a classical algorithm (like ECDHE) and post-quantum algorithm (like ML-KEM) in the same protocol handshake, where security is guaranteed if the classical algorithm is unbroken or the post-quantum algorithm is unbroken, but not if both are broken (Weerasinghe et al., 2025). The ability to replace cryptographic primitives without re-engineering the entire system is repeatedly cited as the most important enabling function for a successful transition, more crucial in practice than the selection of any particular algorithm (Wibowo & Santoso, 2026; Ye & O'Neill, 2026).

4.5.1 Core Components of a Crypto-Agility Program

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

- Cryptographic inventory and discovery: automated scanning of certificates, libraries, firmware, and configuration files to build a live map of every cryptographic dependency across the enterprise.
- Abstraction of cryptographic primitives behind standardized APIs, so that algorithm substitution does not require application-level code changes.
- Centralized key management and hardware security module (HSM) support for post-quantum key types, including larger key and signature storage requirements.
- Policy-driven certificate lifecycle management capable of issuing, rotating, and revoking hybrid or pure post-quantum certificates at scale.
- Continuous compliance monitoring against evolving NIST and sector-specific regulatory guidance.

4.6 Table: Comparative Summary of NIST-Standardized PQC Algorithms

Table 2. Comparative Summary of NIST-Standardized and Finalist Post-Quantum Cryptographic Algorithms

Algorithm	FIPS Standard	Mathematical Basis	Primary Use Case	Relative Performance
ML-KEM (Kyber)	FIPS 203	Module-LWE (lattice)	Key encapsulation / exchange	Fast; compact
ML-DSA (Dilithium)	FIPS 204	Module-LWE (lattice)	General-purpose digital signatures	Fast; moderate size
SLH-DSA (SPHINCS+)	FIPS 205	Hash-based	Conservative / firmware signing	Slow; large signatures
FALCON	FIPS 206 (pending)	NTRU lattice	Compact signatures, constrained devices	Fast; complex implementation
HQC	Selected Mar. 2025	Code-based	KEM diversification / backup	Moderate; larger ciphertext

5. AI-Driven Threat Detection

Whereas, creating systems that ensure the confidentiality and integrity of data is a question of post-quantum cryptography, ensuring the availability and observability of the systems that create and consume the data is a question of AI-driven threat detection. With the increasing number of endpoints, transactions, and identities to monitor, a purely rule or signature based detection method has proven to be inadequate, and the literature is now bursting with machine learning and deep learning techniques that learn normal behaviour baselines and can detect statistical deviation in real time (Buczak & Guven, 2016; Sarker, 2023).

5.1 Taxonomy of AI-Driven Detection Approaches

AI threat detection ranges from traditional supervised machine learning to deep neural networks to more recent AI techniques involving generative and large-language-models. The main categories of this study are summarized in Table 3.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Table 3. Taxonomy of AI-Driven Threat Detection Approaches

Category	Representative Techniques	Primary Strength	Primary Limitation
Classical supervised ML	Decision trees, random forests, SVM	Interpretable; low compute cost	Limited on high-dimensional, unstructured data
Deep learning (supervised)	FFNN, CNN, LSTM, CNN-LSTM hybrids	High accuracy on sequential/spatial patterns	Requires large labeled datasets; opaque
Unsupervised / semi-supervised	Autoencoders, clustering, isolation forests	Detects novel / zero-day anomalies	Higher false-positive rates
Graph-based learning	Graph neural networks (GNN)	Models relational, lateral-movement patterns	Computationally intensive at scale
Generative AI / LLM-based	LLM-based SOC copilots, RAG-augmented triage	Natural-language reasoning over alerts	Dual-use risk; hallucination; prompt injection

5.2 Empirical Performance Across the Literature

The above results are typical of the range found in the literature. The results above are representative of the range across the literature. The accuracy of intrusion detection reported in literature surveyed is consistently high; however, the accuracy values cannot be compared between the different studies due to varying datasets, different evaluation process, and different methods of handling the class imbalance. These figures are representative and illustrate the performance ordering of the various model families, as summarized in Figure 3; due to the differences in underlying datasets from the various studies, these figures should be interpreted as an illustrative synthesis of the reported trends rather than as a controlled head-to-head comparison.

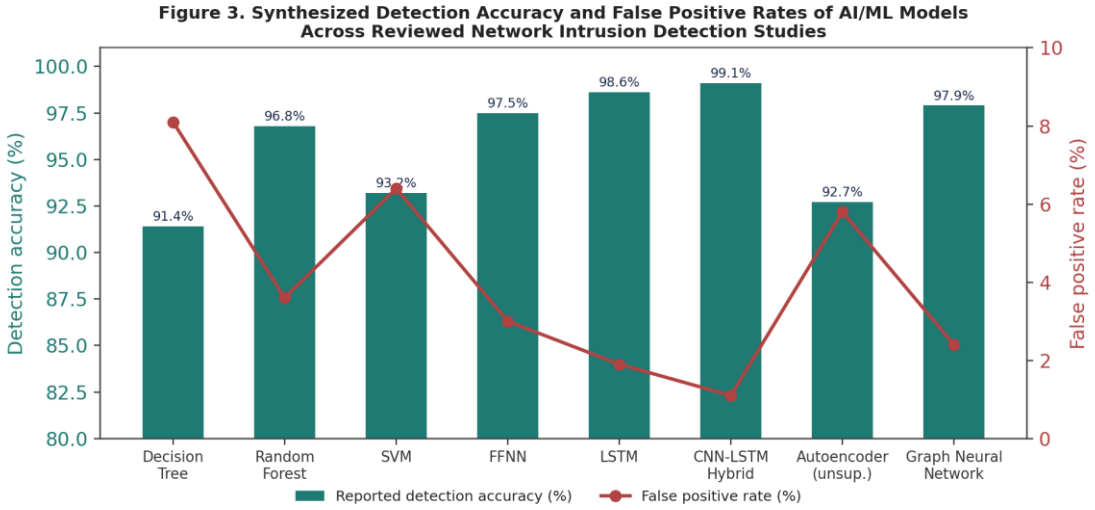

Figure 3. Synthesized detection accuracy and false-positive rates of AI/ML models

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

across reviewed network intrusion detection studies. Compiled from Bakhsh et al. (2023), Talukder et al. (2024), and Wang et al. (2025).

There are two patterns in the literature. Second, methods like autoencoders have relatively high false positive rates, but are the only ones that can reliably alert to novel, zero-day attack patterns that have never before been seen by supervised models trained solely on previously observed classes of attacks (Pinto et al., 2023).

5.3 Explainability and Analyst Trust

One thing that runs throughout the literature that was reviewed is a mismatch between the accuracy of the models and the analysts' trust. Therefore, several of the reviewed frameworks (Moustafa et al., 2023) have adopted the process of Explanable AI (XAI), such as the attribution of values using the SHAP value and attention visualization. Alert-fatigue research also paints a more complex picture: SOCs are constantly inundated with much more alerts than analysts can manually process and a major barrier to operational effectiveness is not only the detection accuracy but also the ability of AI tools to correlate and prioritize those alerts (as identified in the alert-fatigue literature synthesized for this study by Chhetri et al.).

5.4 Adversarial Machine Learning: The Detection Arms Race

AI-based detection systems are not neutral tools — they are an object of attack. By contrast, adversarial attacks under realistic operational constraints, in which the attacker is not allowed to arbitrarily change network packets without violating the rules of the protocol, have been shown to be effective by Apruzzese et al. (2022) on production-grade NIDS, casting doubt on previous adversarial ML literature that has assumed attacks are performed under an unconstrained model of perturbation. Arp et al. (2022) also list a number of methodological flaws across the published ML-security literature which allow information to leak between training and test data, inflating reported robustness. Combined, these findings suggest that relying on AI-based detection is not a solved problem, and an arms race is unfolding between the attackers and the defenders of which they should be wary, not to mention constantly retraining, adversarial-robustness testing, and defense-in-depth.

5.5 Generative AI and the Dual-Use Dilemma

The use of Generative AI and large language models has brought a new dimension to threat detection, as their use on defense is advancing at the same time, if not at a faster pace, than on the front line. On the defense side, LLM-based SOC copilots now can summarize complex, multi-stage attack chains in natural language to aid with root cause analysis, and can augment otherwise time-gated model knowledge with retrieval-augmented generation (RAG) that provides up-to-date vulnerability intelligence. This is a dual use scenario, which further strengthens the argument for defense-in-depth architectures, like those proposed in Section 6, in which the deployment of AI in detection is not the only point of trust.

5.6 Integrating AI Detection with Cryptographic Telemetry

One area that has not been widely investigated, but is of practical significance, is what to do with cryptographic-layer telemetry when migrating to post-quantum cryptography. This idea of integrating AI-informed behavioral analytics and cryptographic protocol telemetry, as opposed to implementing them as distinct

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

monitoring domains is a design principle that is clearly embedded in the design of the proposed framework presented in the next section.

6. Proposed Integrated Framework

Based on the literature gathered in the sections 2–5, the present work introduces a reference framework for post-quantum secure digital transformation, formed by an integration of six layers, where the artificial intelligence-based threat detection is integrated as a layer. The framework is intended to be descriptive of good practice already being developed in the literature, and not a totally new invention, but in linking together layers which tend to be separated, the framework provides a useful contribution.

Figure 5. Proposed Integrated Framework for Post-Quantum-Secure Digital Transformation with AI-Driven Threat Detection

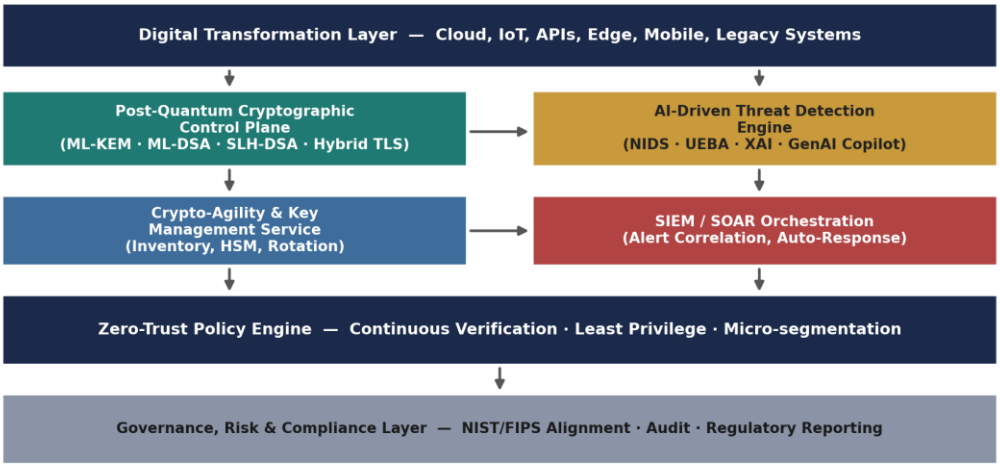

Figure 5. Proposed integrated framework for post-quantum-secure digital transformation with AI-driven threat detection.

6.1 Layer 1: Digital Transformation Layer

This layer is the organization's growing digital presence: cloud workloads, IoT and edge devices, APIs, mobile apps, and legacy systems which can't be phased out right away. The framework does not consider this layer as a permanent perimeter, instead it defines it as a continuously evolving inventory that directly flows into the cryptographic control plane and the AI detection engine (Tariq et al., 2023).

6.2 Layer 2: Post-Quantum Cryptographic Control Plane

It is a layer whose algorithms are standardized by the NIST: ML-KEM for key establishment, ML-DSA for general purpose signature generation and SLH-DSA for high-assurance firmware and code signing, which have been deployed in hybrid mode with classical ECDHE and ECDSA (NIST, 2024a, 2024b, 2024c; Weerasinghe et al., 2025). The control plane also provides an abstracted API level on top of cryptographic operations, meaning that an application does not need to be rewritten if there is a change

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

in the algorithms used – directly operationalising the 'crypto-agility' principle introduced in Section 4.5.

6.3 Layer 3: AI-Driven Threat Detection Engine

This layer encompasses a hybrid CNN-LSTM architecture and graph-neural-network architecture, as detailed in Section 5 (Wang et al., 2025), alongside a user and entity behavior analytics layer, and an explainable-AI presentation layer. Most importantly, this layer is engineered to act as a first-class feature when it comes to detecting cryptographic-layer telemetry from Layer 2, like handshake downgrade events or anomalous certificate issuance, without being a separate monitoring stream, thereby directly addressing the integration gap identified in Section 5.6.

6.4 Layer 4: Crypto-Agility and Key Management Service

It provides an inventory of cryptographic resources that is always refreshed, provides management of key storage on hardware security modules for classical and post quantum key types and automates certificate lifecycle management. It is an operational basis that enables the organisation to adapt to a possible cryptanalytic attack on any one algorithm without undergoing a multi-year re-engineering process (Wibowo & Santoso, 2026).

6.5 Layer 5: SIEM/SOAR Orchestration

This layer correlates alerts triggered by the AI detection engine, uses AI-assisted prioritization to overcome alert fatigue and automates containment playbooks for known attack patterns, while escalating ambiguous or high-impact alerts to human detection teams. A layer on top of this is also where generative-AI copilots play, which are meant to help in natural-language incident summarization but come with a risk of being used for dual purposes and potential hallucinations (Ahi, 2026).

6.6 Layer 6: Zero-Trust Policy Engine and Governance Layer

The zero-trust policy engine is enforced on all layers above, making continuous verification, least-privilege, and micro-segmentation possible and using the status of the cryptographic control plane and the AI detection engine, to make risk-based, dynamic access decisions (Hasan, 2024; Zhang et al., 2026). Department of Defense, 2026).

7. Sector-Wise Migration Readiness and Case Discussion

The level of organizational preparedness to the framework outlined above is significantly different across sectors, depending on the level of regulatory pressure, the sensitivity of the data, legacy technical debt, and security investment. This section summarizes readiness indicators from the literature reviewed and provides a composite discussion, which is illustrated with a readiness index in Figure 6.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

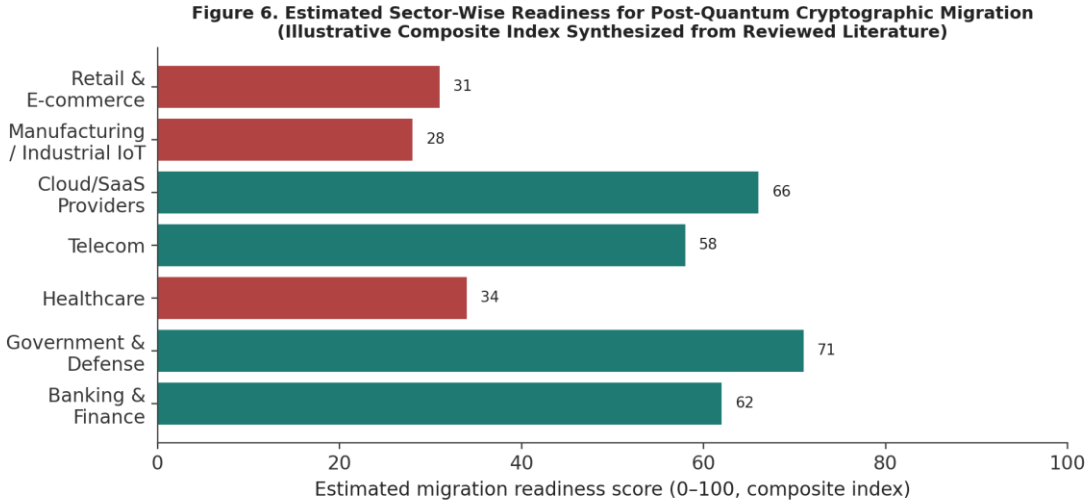

Figure 6. Estimated sector-wise readiness for post-quantum cryptographic migration. This composite index is an illustrative synthesis constructed by the authors from qualitative readiness indicators reported across the reviewed literature (ID Quantique, 2026; Mastercard, 2025; U.S. Department of Defense, 2026; Wibowo & Santoso, 2026) and should be interpreted as directional rather than as a validated quantitative measurement.

7.1 Banking and Financial Services

The literature on financial services is the most advanced of any of the sectors included in this study, and has received explicit attention from the Bank for International Settlements, the G7 and the national financial regulators for an ID Quantique harvest-now-decrypt-later risk. The biggest hurdle remains legacy mainframe infrastructure, while having to coordinate migration timing with other counterparties, which are not under the institution's direct control, but are part of SWIFT and card-payment networks.

7.2 Government and Defense

By binding regulatory requirements, such as the U.S. government's readiness regulations, government and defense readiness is influenced. The U.S. Department of Defense's own literature on systems-integration projects, however, shows that even high-resourcing government initiatives can still have trouble coordinating PQC migration with parallel zero-trust and AI-security modernization projects when those each have separate program offices with different timelines (U.S. Department of Defense, 2026).

7.3 Healthcare

Despite potentially similar or higher levels of HNDL, there is a significant disparity in healthcare readiness compared to banking and government.It's not that there's not a comparable or even greater HNDL exposure in healthcare, but that readiness is lagging significantly behind in the healthcare sector compared to banking and government. Like the previous, systematic reviews of AI-based security architectures in healthcare report that the current adoption of zero-trust is largely theoretical, rather than being embedded in practice, unless there is additional regulatory push in that sector. This paper hopes to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

continue that trend into the post-quantum migration landscape.

7.4 Telecommunications and Cloud/SaaS Providers

Comparatively, the readiness posture of telecommunications and key cloud providers are favorable, as they manage large pieces of the TLS termination infrastructure that can facilitate the rollout of hybrid PQC deployment at scale with minimal end-user disruption. The ongoing research on emerging 7G and next-generation networks also points to a potential early adoption of framework Layer 6 zero-trust integration in telecommunications, with deeper integration planned to be implemented directly into the network infrastructure (Ahmed et al., 2025).

7.5 Manufacturing and Industrial IoT

The manufacturing and industrial IoT sector is the least mature one of the literature that was surveyed. The results of the PQC performance research presented below confirm that several lattice-based schemes can be efficiently computed in an OT environment using constrained devices; however, the real-world deployment pipelines and processes for the deployment of firmware in OT environments are still immature and fragmented across vendors, which is reflected by the low score in the readiness evaluation (Figure 6).

7.6 Retail and E-Commerce

Payment-card-industry compliance cycles will drive retail/e-commerce readiness, and the literature reviewed indicated that this sector is likely to adopt this infrastructure in a reactive manner, following the card networks and payment processors mandating post-quantum-compliant infrastructure (ID Quantique, 2026).

8. Performance, Cost, and Operational Trade-offs

Operating alongside AI-based detection, hybrid post quantum cryptography is not without cost. This section summarizes the key performance/cost compromises reported in the literature.

8.1 Network Latency and Handshake Overhead

The sizes of post-quantum public keys, ciphertexts, and signatures are typically much larger than the sizes of their classical counterparts (Section 4.4), resulting in a higher latency for hybrid TLS handshakes, especially in bandwidth-limited or high-latency environments. To provide a general sense of handshake latency in representative network environments, illustrative data are summarized in Figure 4, which has been compiled from this literature to illustrate the general trend.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

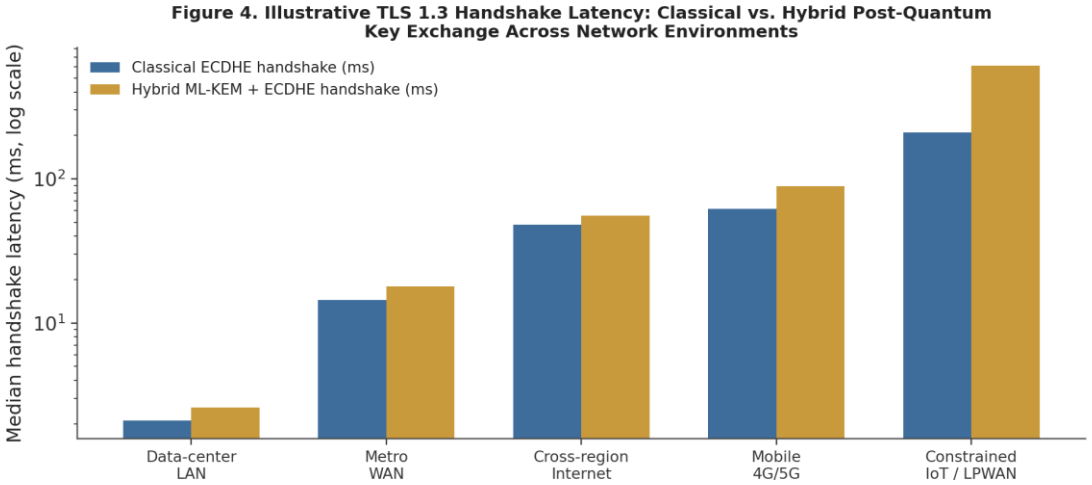

Figure 4. Illustrative TLS 1.3 handshake latency: classical vs. hybrid post-quantum key exchange across network environments. Synthesized from reported overhead patterns in Ye and O'Neill (2026) and related PQC-for-IoT performance literature.

The take-away message is that a single, standard migration plan is probably not best practice. For data-center and cloud-to-cloud traffic, the overhead of hybrid PQC can be absorbed without any noticeable impact from the user, and for constrained deployments of IoT and low-power wide-area network (LPWAN) traffic, algorithm choices favoring smaller signature schemes (e.g., FALCON) and/or protocol-level session resumption optimizations or staged rollout (with the higher-value traffic going first) may be more suitable.

8.2 Financial Cost of Migration

Migration also has an up-front cost, in addition to network performance. Similarly, industry white papers warn that the cost of migrating grows non-linearly with the size and diversity of the organisation's cryptographic footprint, which is why the initial investment is often found to be in discovering the cryptographic inventory (rather than in the algorithm) as it has been many times before (Cryptomathic, 2024).

8.3 AI Model Operating Cost and Total Cost of Ownership

AI-driven detection adds a new cost model to consider: model training and retraining compute, labeled-data acquisition, and continuously analyzing the model output and deciding if it's relevant or not (as done by human analysts). While enterprise integration of AI security tools comes with licensing costs and potential vendor lock-in, industry cost analysis suggests that organizations with AI-powered detection and response systems suffer from significantly reduced average breach costs, and a more rapid time to containment, compared to organizations that do not adopt AI (International Business Machines Corporation, 2025).

8.4 Table: Trade-off Summary

Table 4. Summary of Principal Trade-offs in the Integrated Framework

Dimension	Benefit	Cost / Risk	Mitigation Strategy
Hybrid PQC deployment	Quantum + classical safety net	Larger handshake payloads, latency	Staged rollout; algorithm selection by

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

			environment
AI-driven detection	Higher accuracy, faster containment	Adversarial evasion, false positives	XAI, adversarial testing, human-in-the-loop
Crypto-agility tooling	Future-proof against algorithm breaks	Upfront engineering investment	Phase into existing DevSecOps pipelines
Zero-trust integration	Reduced lateral movement risk	Implementation complexity	Incremental, identity-first rollout
Generative AI copilots	Faster analyst triage	Dual-use, hallucination risk	Human review; retrieval-augmented grounding

9. Challenges and Open Research Problems

9.1 Cryptographic Inventory Discovery at Scale

As discussed in Sections 3.3 and 8.2, the majority of organisations do not have a full and accurate picture of where classical cryptography is used throughout their technology estate, including all third-party libraries, embedded firmware and legacy systems that have stopped being developed. Compared to the size of the problem, the automation of discovery tooling is still very young and the literature reviewed to date confirms that it is the most critical practical constraint on migration, more important than the performance of the algorithms themselves (Ye & O'Neill, 2026).

9.2 Adversarial Robustness of AI Detection Systems

The adversarial machine learning research presented in this section (Section 5.4) shows that production-realistic attacks can work very well even in very limited perturbation models, and that many of the published robustness results have methodological flaws that put a false spin on the robustness of the deep learning NIDS in the real world (Apruzzese et al., 2022; Arp et al., 2022). To close this gap, a series of benchmark datasets and evaluation protocols should be standardized and adversarial, with no consensus solution in the current literature.

9.3 Post-Quantum Readiness of Third Parties and Supply Chains

The security of an organisation is always as strong as the weakest link in the supply chain and API partner. Coordination with payment networks and counterparties is highlighted as one of the bottlenecks for migration outside of any individual financial institution's control (Wibowo & Santoso, 2026), a challenge that is applicable not only in the financial sector but also in any sector that has a large number of third-party APIs as part of its digital transformation.

9.4 Talent and Organizational Capacity

Post quantum cryptography and adversarially robust AI security require unique skill sets which are not as abundant as they are needed (Department of Defense, 2026).

9.5 Generative AI as an Escalating Offensive Force Multiplier

The dual use issue outlined in Section 5.5 is an open and ever-changing problem and not a solved one. The technical barrier to creating sophisticated malware and social-engineering attacks is also being lowered, as LLM-assisted attack tooling continues to move at a similar pace to the defensive AI systems' capabilities, a pattern which doesn't

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

have historical precedent in previous cycles of attack and defense in cybersecurity technology (Ahi, 2026).

9.6 Standardization Gaps and Algorithm Maturity Risk

Compared to the initial three standards (NIST, 2025), organisations using the most recent additions to the PQC portfolio (ML-KEM, ML-DSA and SLH-DSA) have to deal with a slightly less mature implementation and level of tools across the portfolio. Confidence in these algorithms must be sustained through sustained cryptanalytic research over the next few decades—and the SIKE algorithm is a late-stage candidate that has been broken in 2022 by unexpected classical cryptanalytic breakthrough (Ye & O'Neill, 2026).

10. Policy, Governance, and Regulatory Implications

The transition examined in this paper is not exclusively a "technical" one, but rather is heavily influenced by regulatory requirements and international coordination. However, the European Union has taken a more flexible approach, with no binding regulations, and instead leaving it to national and EU-level bodies to provide recommendations in most instances; Europol has promoted coordination since 2024, for instance, with the creation of the Quantum Safe Financial Forum (Mastercard, 2025).

Regulatory focus is less sophisticated and still emerging for AI security tools, though it is advancing quickly on the governance of AI systems that support security decision-making. According to the literature reviewed, addressing the model explainability needs for automated response actions, establishing liability for when an AI detection system generates a false positive or a false negative with material business impact and the constraints of cross-border data-sharing for threat intelligence sharing between AI-powered security platforms will be critical to effective governance frameworks (Moustafa et al., 2023; Sharma et al., 2025).

As noted in the reviewed literature, another common governance recommendation is to establish a formal governance program for PQC migration, zero-trust deployment and AI-security assurance as a single program instead of a separate program for each, as these are all inherently dependent on each other (U.S. Department of Defense, 2026). This recommendation directly pushes the unified governance layer (Layer 6) of the governance framework recommended in Section 6.

11. Future Directions

11.1 Empirical validation of Integrated frameworks

The framework presented in Section 6 is a combination of patterns that have been described individually in different studies in the literature, but to the best of the authors' knowledge, this framework has not, as a whole, been tested in an actual production system. Future studies should seek to perform longitudinal case studies of the combined impact of the framework on migration velocity and efficacy of detection using AI compared to organizations that follow the workstreams alone.

11.2 Quantum-Enhanced Detection Systems

In addition to being an offensive application for cryptography, quantum computing is a new tool being considered for defensive pattern matching and anomaly detection (Ahmed et al., 2025). Moving forward, as quantum hardware continues to evolve, it

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

will be important to investigate whether the quantum enhancement of anomaly scores can be seamlessly incorporated into the AI detection layer of frameworks like the one proposed in this work, while maintaining the same types of dependency risks to the same emerging quantum hardware that motivated the quantum migration in the first place.

11.3 Standardized Adversarial Benchmarks

The field would greatly benefit from the creation of community standardized, adversarially realistic benchmark datasets for which the robustness of the detection of AI algorithms can be fairly compared between studies, reminiscent of the approach used by NIST for post-quantum cryptography.

11.4 Sector-Specific Migration Playbooks for Underserved Sectors

The readiness gap noted in Section 7 also illustrates the need for applied research focused on the creation of sector-specific migration playbooks, adapted to the operational challenges specific to healthcare and industrial IoT, such as the mechanisms for updating embedded-device firmware and the validation requirements for clinical systems, which are quite different from those in banking or government IT.

11.5 Governance of Generative AI in Security-Critical Automation

Future research should consider establishing suitable thresholds where humans can be excused for the automated process's mistake, as well as liability structures and technical controls against prompt injection and hallucination in incident response automation, particularly in sensitive contexts (as discussed in Section 5.5).

12. Conclusion

We have looked at how two paradigms of disruptive technology transformation — moving to post-quantum crypto and the adoption of AI-based threat detection — are converging to change the future of the security underpinnings of digital transformation. At the same time, AI based detection has evolved from an experimental research path to an essential operational requirement with hybrid deep learning architectures consistently beating legacy signature based technologies, while adversarial machine learning research is showing that these operational AI systems create new classes of vulnerabilities that will need constant monitoring (He et al., 2023; Wang et al., 2025).

It is the central argument of this paper that these two transitions cannot be planned and resourced and governed independently without risks to the structure. The study, in Section 7, reveals how unevenly prepared the various sectors are for such integration; financial and government sectors are relatively advanced because of the explicit regulatory pressure and harvest-now-decrypt-later risk awareness; and healthcare and industrial IoT sectors are significantly behind the curve, despite facing the same or greater potential for data-confidentiality exposure in the long term.

Finally, the results of this study indicate that the transition to post-quantum era will not be a success only because the cryptographic strength is sufficient. The journey as described in this paper is likely to take 10 years or more, but the time period for harvest-now-decrypt-later risks is open now, and the approach outlined in this paper is not just a theory of best practice, but an operational best practice for any organisation seeking to make meaningful digital transformation in the coming years.

Online ISSN 3007-3197
Print ISSN 3007-3189

References

Ahi, K. (2026). Large language models (LLMs) and generative AI in cybersecurity and privacy: A survey of dual-use risks, AI-generated malware, explainability, and defensive strategies. arXiv. https://doi.org/10.48550/arXiv.2607.06963

Ahmed, S., Shihab, I. F., & Khokhar, A. (2025). Quantum-driven zero trust framework with dynamic anomaly detection in 7G technology: A neural network approach. arXiv. https://doi.org/10.48550/arXiv.2502.07779

Alhajjar, E., Maxwell, P., & Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. Expert Systems with Applications, 186, Article 115782. https://doi.org/10.1016/j.eswa.2021.115782

Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling realistic adversarial attacks against network intrusion detection systems. Digital Threats: Research and Practice, 3(3), 1–19. https://doi.org/10.1145/3469659

Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2022). Dos and don'ts of machine learning in computer security. In Proceedings of the 31st USENIX Security Symposium (pp. 3971–3988). USENIX Association.

Bakhsh, S. A., Khan, S., Ahmed, F., & Alshehri, M. D. (2023). Enhancing IoT network security through deep learning-powered intrusion detection systems. Sensors, 23(11), Article 4996. https://doi.org/10.3390/s23114996

Bhat, J. (2023). Strengthening ERP security with AI-driven threat detection and zero-trust principles. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 45–58.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Cryptomathic. (2024). A banker's guide to quantum-safe cryptography, Part 3: Roadmap to PQC migration for financial institutions. Cryptomathic Publications.

Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. Internet of Things, 28, Article 101351. https://doi.org/10.1016/j.iot.2024.101351

European Union Agency for Cybersecurity. (2024). Post-quantum cryptography: Integration study. ENISA Publications.

Fayyazi, R., Zuzak, M., & Yang, S. J. (2026). LLM embedding-based attribution (LEA): Quantifying source contributions to generative model's response for vulnerability analysis. arXiv. https://doi.org/10.48550/arXiv.2506.12100

Fu, C., Li, Q., Shen, M., & Xu, K. (2023). Point cloud analysis for reducing false positives in network intrusion detection systems. IEEE Transactions on Network and Service Management, 20(4), 4590–4604. https://doi.org/10.1109/TNSM.2023.3271301

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Hasan, M. (2024). Enhancing enterprise security with zero trust architecture: Mitigating vulnerabilities and insider threats through continuous verification and least privilege access. arXiv. https://doi.org/10.48550/arXiv.2410.18291

He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(1), 538–566. https://doi.org/10.1109/COMST.2022.3233793

ID Quantique. (2026). Quantum-safe security for banking and financial services. ID Quantique White Paper Series.

International Business Machines Corporation. (2025). Cost of a data breach report 2025. IBM Security.

Iyengar, S. S., Nabavirazavi, S., Hariprasad, Y., HB, P., & Mohan, C. K. (2025). Cyber threat intelligence and security for federated learning in digital forensics. In Artificial intelligence in practice: Theory and application for cyber security and forensics (pp. 177–199). Springer Nature.

LaMacchia, B., Campagna, M., & Gropp, W. (2025). The post-quantum cryptography transition: Making progress, but still a long road ahead. Computing Research Association Quadrennial Paper. https://arxiv.org/abs/2503.04806

Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. Physical Review Applied, 21(4), Article 040501. https://doi.org/10.1103/PhysRevApplied.21.040501

Mastercard. (2025). Migration to post-quantum cryptography: R&D white paper. Mastercard Publications.

Moin, M. N. (2022). Artificial intelligence driven threat detection for strengthening cyber defense. Journal of Primeasia, 3(1), 1–8.

Montasari, R. (2022). Cyber threats and national security: The use and abuse of artificial intelligence. In Handbook of security science (pp. 679–700). Springer International Publishing. https://doi.org/10.1007/978-3-319-51761-2_39-1

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions. IEEE Communications Surveys & Tutorials, 25(3), 1775–1807. https://doi.org/10.1109/COMST.2023.3280465

National Institute of Standards and Technology. (2024a). Module-lattice-based key-encapsulation mechanism standard (FIPS Publication No. 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024b). Module-lattice-based digital signature standard (FIPS Publication No. 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024c). Stateless hash-based digital signature standard (FIPS Publication No. 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2024d). Transition to post-quantum cryptography standards (NIST Internal Report No. 8547, Initial Public Draft). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8547.ipd

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

National Institute of Standards and Technology. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST Internal Report No. 8545). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8545

Nurul, S., & Kumar, A. (2023). AI-enabled cyber-physical power systems: Review of smart grid security, optimization, and decision support. Applied IT & Engineering, 1(1), 1–9.

Oreyomi, M., & Jahankhani, H. (2022). Challenges and opportunities of autonomous cyber defence (ACyD) against cyber attacks. In Blockchain and other emerging technologies for digital business strategies (pp. 239–269). Springer.

Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors, 23(5), Article 2415. https://doi.org/10.3390/s23052415

Raghavendran, C. (2022). Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. International Journal of Electrical Engineering Research, 10(2), 33–41.

Raji, A., Olawore, A., Mustapha, A., & Joseph, J. (2023). Integrating artificial intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. World Journal of Advanced Research and Reviews, 20(3), 2005–2024. https://doi.org/10.30574/wjarr.2023.20.3.2510

Raza, H. (2021). Proactive cyber defense with AI: Enhancing risk assessment and threat detection in cybersecurity ecosystems. Journal of Cybersecurity Research, 4(2), 12–24.

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space. IEEE Access, 12, 53497–53516. https://doi.org/10.1109/ACCESS.2024.3385107

Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy, 6(5), Article e295. https://doi.org/10.1002/spy2.295

Sharma, C., Sharma, S., Bhardwaj, V., & Dhaliwal, B. K. (2025). Generative artificial intelligence for sustainable development: Predictive trend analysis in key sectors using natural language processing. Discover Applied Sciences, 7(6), Article 596. https://doi.org/10.1007/s42452-025-06975-w

Shaukat, K., Luo, S., & Varadharajan, V. (2023). A novel deep learning-based approach for malware detection. Engineering Applications of Artificial Intelligence, 122, Article 106030. https://doi.org/10.1016/j.engappai.2023.106030

Talukder, M. A., Islam, M., Uddin, M. A., Akhter, A., Hasan, K. F., & Moni, M. A. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. Journal of Big Data, 11, Article 33. https://doi.org/10.1186/s40537-024-00886-w

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), Article 4117. https://doi.org/10.3390/s23084117

Technology Review Insights. (2025, November 10). Reimagining cybersecurity in the era of AI and quantum. MIT Technology Review. https://www.technologyreview.com/2025/11/10/1127774/reimagining-cybersecurity-in-the-era-of-ai-and-quantum/

The White House Office of Science and Technology Policy. (2024). Report on post-quantum cryptography. Executive Office of the President.

U.S. Department of Defense. (2026). Synchronizing concurrent security modernization programs: A systems integration framework for post-quantum cryptography, zero trust architecture, and AI security. Information (Basel), 14(3), Article 233. https://doi.org/10.3390/info14030233

Vectra AI. (2023). 2023 state of threat detection. Vectra AI Resources.

Wang, Y., Zhu, Y., Chen, Z., Shen, X., & Li, Z. (2025). AI-driven network intrusion detection systems: A survey of techniques, datasets and deployment challenges. In Proceedings of the IEEE International Conference on Emerging Technologies (pp. 1–8). IEEE. https://doi.org/10.1109/EmTech.2025.11265502

Weerasinghe, S., Naik, R., & Alazab, M. (2025). Quantum leap in finance: Economic advantages, security, and post-quantum readiness. arXiv. https://doi.org/10.48550/arXiv.2508.21548

Wibowo, A., & Santoso, B. (2026). Post-quantum migration in the financial sector: A systematic review of readiness, risks, and transition frameworks. Journal of Information Systems and Informatics, 8(1), 210–229. https://doi.org/10.51519/journalisi.v8i1.1477

Ye, J., & O'Neill, M. (2026). Operationalising post-quantum TLS: Automated configuration profiling and hybrid PQC deployment in financial infrastructure. arXiv. https://doi.org/10.48550/arXiv.2605.17955

Zhang, T., Osei, K., & Farooq, U. (2026). Autonomous identity-based threat segmentation in zero trust architectures. arXiv. https://doi.org/10.48550/arXiv.2501.06281

Zhu, L., Niyato, D., Lu, R., Du, X., Hussain, F., Sun, Y., & Yan, S. (2025). Special issue editorial: Generative AI for secure communications and networking. IEEE Network, 39(5), 8–11. https://doi.org/10.1109/MNET.2025.10012345