Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

CYBERSECURITY CHALLENGES AND STRATEGIC MIGRATION PATHWAYS IN THE ERA OF QUANTUM COMPUTING: RISKS, STANDARDS, AND POST-QUANTUM CRYPTOGRAPHIC READINESS

Syed Muhammad Mushtaher Uddin[*1], Nazia Azim[2]

[*1]*Lecturer, Indus University, Karachi, Pakistan*
[2]*Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan*

[*1]smmushtaher@indus.edu.pk, [2]n.azim@awkum.edu.pk

DOI:https://doi.org/10.5281/zenodo.17276520

Keywords
Post-quantum cryptography, quantum computing, cryptanalysis, TLS, PKI, QKD, MIGRATION, CNSA 2.0, NIST PQC.

Article History
Received: 15 July 2025
Accepted: 25 September 2025
Published: 06 October 2025

Copyright @Author

Corresponding Author: *
Syed Muhammad Mushtaher Uddin

Abstract
Quantum computers are likely to change the basis of current online security methods. Methods like Shor's and Grover's put at risk the math problems that keep safe many common ways to scramble and unscramble data, making for a future danger to keeping data private and proving identities. Even before very big quantum computers are real, enemies can use a "grab it now, decode later" plan by taking secret messages now and unscrambling them once quantum computers are good enough. This is a big problem for groups that deal with private or long-lasting data. Because of this, groups such as NIST, NSA, IETF, and ETSI have started projects to create and set rules for new kinds of codes that can resist quantum computers, releasing new methods such as ML-KEM, ML-DSA, and SLH-DSA. However, changing to these new methods brings its own problems, like bigger keys, slower speeds, things not working together, and possible weak spots when first used. This paper looks at the online security problems caused by quantum computers in coding methods, ways of talking online, computer hardware, and rule-making models. It also looks at current work to set standards and gives a step-by-step plan to help move to quantum-safe methods. The study stresses the need to be flexible with codes, use both old and new methods together, and keep a careful list of what you have to make sure to move to a quantum-safe world safely, bit by bit, and on time.

INTRODUCTION

The progress in quantum computing means a big shift for the world of computer security. Quantum computers, unlike regular computers, use superposition and entanglement to greatly speed up solving some math problems. Shor's algorithm can quickly break down very big numbers and figure out discrete logarithms, which puts the basic ideas behind RSA, Diffie-Hellman, and elliptic curve cryptography at risk. Grover's algorithm makes finding answers by trying all possibilities faster, lowering the security of symmetric algorithms such as AES and SHA-2.

Even though quantum computers that can break codes aren't around now, the chance they could be built is a present danger. Information coded now can be saved and decoded in the future when there are enough quantum computers; this idea is known as "harvest-now, decrypt-later". The effects are big for fields that deal with secret or long-lasting data, like the military, medicine, and finance.

To get ready, standards groups and government agencies have begun to create post-quantum cryptography (PQC). NIST has finished its initial set of algorithms, and the NSA's CNSA 2.0 and the IETF's mixed key exchange plans give advice on how to use them. Despite this progress, switching to systems that can stand up to quantum attacks has issues with size, getting along with other systems, and handling danger.

This paper looks at these problems, checks out worldwide projects to set standards, and suggests a step-by-step way to move toward security that can hold up against quantum attacks.

II. BACKGROUND: WHY QUANTUM MATTERS

A. Algorithmic Impact

Shor's algorithm runs integer factorization and discrete logarithms in polynomial time on a fault-tolerant quantum computer, breaking RSA and ECC [1]. Grover's algorithm provides a quadratic speed-up for unstructured search, implying that symmetric key sizes should be doubled to regain similar brute-force resistance [2] [3].

Figure 1: Quantum Impact on Cryptography

Classical Algorithms	Quantum Threat	Quantum-Safe Options
RSA, ECC	Shor's (breaks keys)	ML-KEM, ML-DSA
AES-128	Grover's (~AES-64 equiv.)	AES-256
SHA-256	Grover's (~128-bit equiv.)	SHA-384/512

B. The "Harvest-Now, Decrypt-Later" (HNDL) Threat

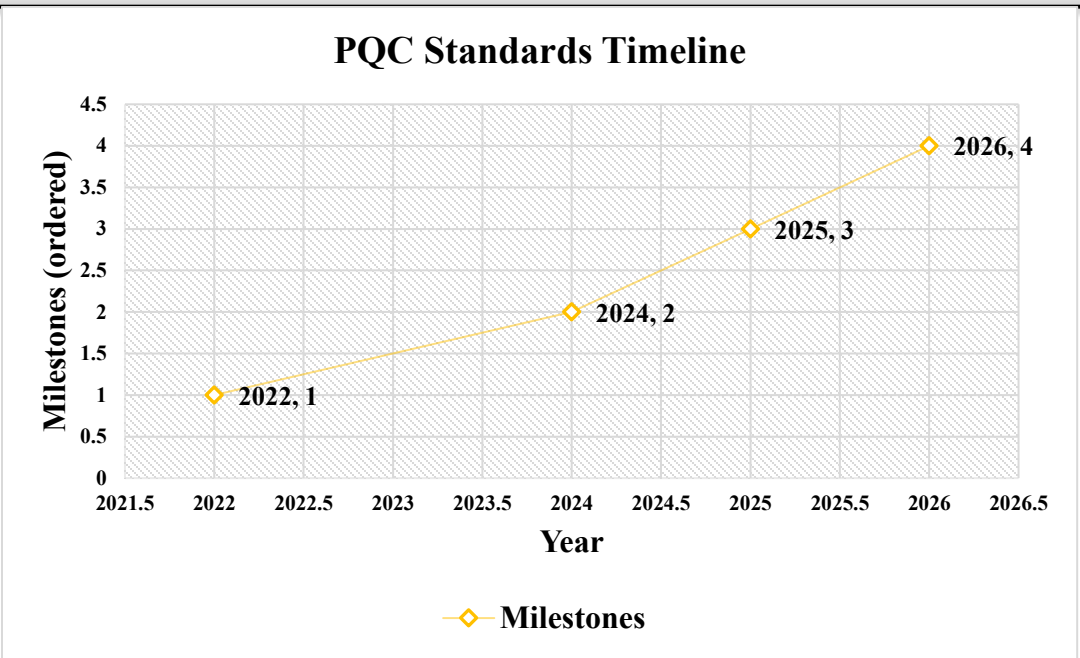
Adversaries can capture cipher text today and decrypt it in the future once quantum capabilities mature. This creates immediate risk for data with long confidentiality lifetimes (e.g., PII, health, industrial IP, state secrets) [11] [14].

III. STANDARDS, POLICY, AND ECOSYSTEM READINESS

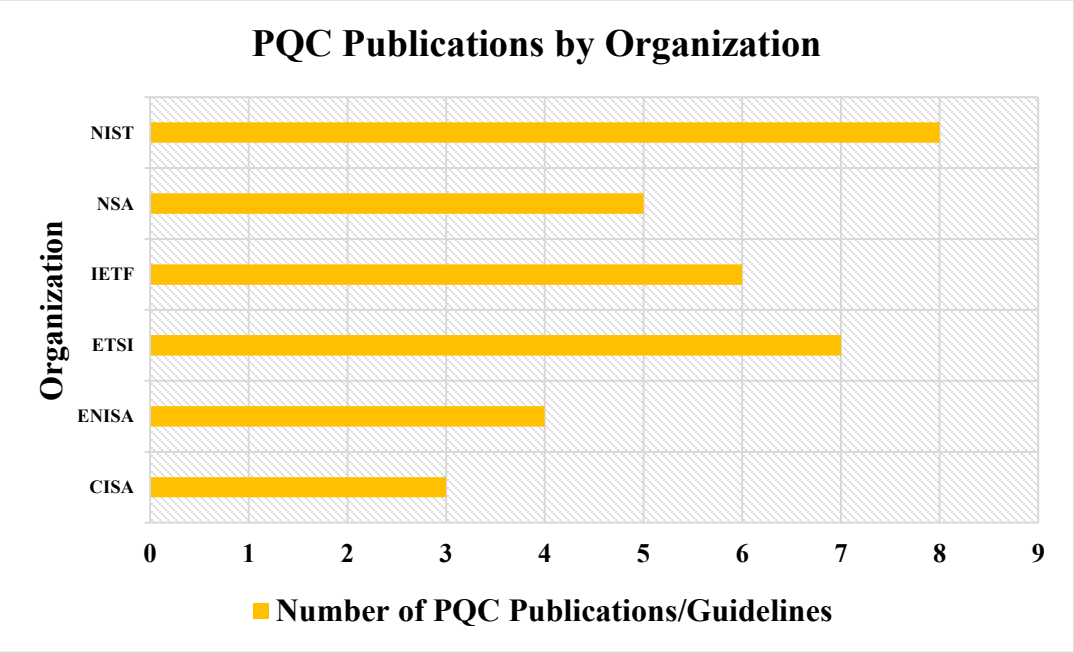
NIST published FIPS 203 (ML-DSA/Dilithium), FIPS 204 (ML-KEM/Kyber), and FIPS 205 (SLH-DSA/SPHINCS+) in August 2024 and continues Round-4 selections (e.g., HQC in 2025) [4], [8], [15]. NSA's CNSA 2.0 establishes a government migration baseline and ties into CSfC capability guidance [5], [6], [9], [16]. The IETF is progressing hybrid key exchange for TLS 1.3 to enable near-term deployments during transition [17], [18], while ETSI and ENISA publish migration and security analysis reports that inform enterprise planning [7] [10] [19] [20].

Table 1: PQC Standards Timeline

Year	Milestone	Standard
2022	CNSA 2.0 announced	NSA
2024	NIST FIPS 203, 204, 205	ML-DSA, ML-KEM, SLH-DSA
2025	NIST 4th Round	HQC under review
2026+	Migration deadlines (USG, EU)	To be defined



Organization	Number of PQC Publications/Guidelines
CISA	3
ENISA	4
ETSI	7
IETF	6
NSA	5
NIST	8

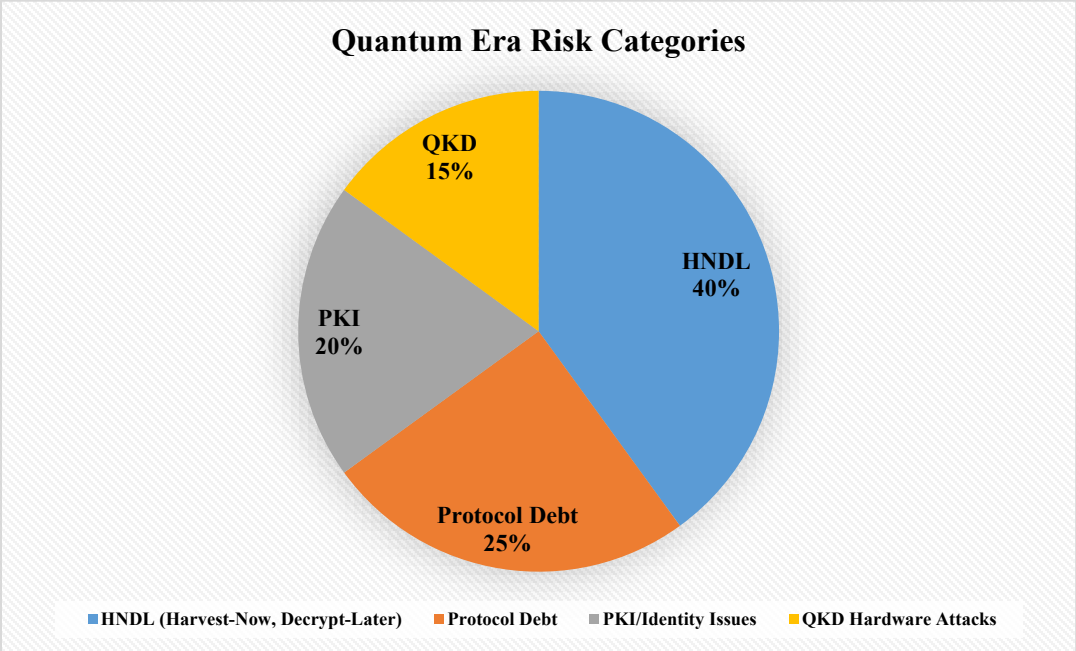


IV. TECHNICAL RISK AREAS

Table 2: Risk Categories in Quantum Era

Risk Area	Description	Examples
HNDL	Data stolen now, decrypted later	Medical, financial, defense data
Protocol Debt	Incompatibility during hybrid rollouts	TLS record size, handshake failures
PKI/Identity	Larger certs, reissuance at scale	IoT, embedded, smartcards
Hardware QKD	Device-level attacks	Detector blinding, Trojan horse

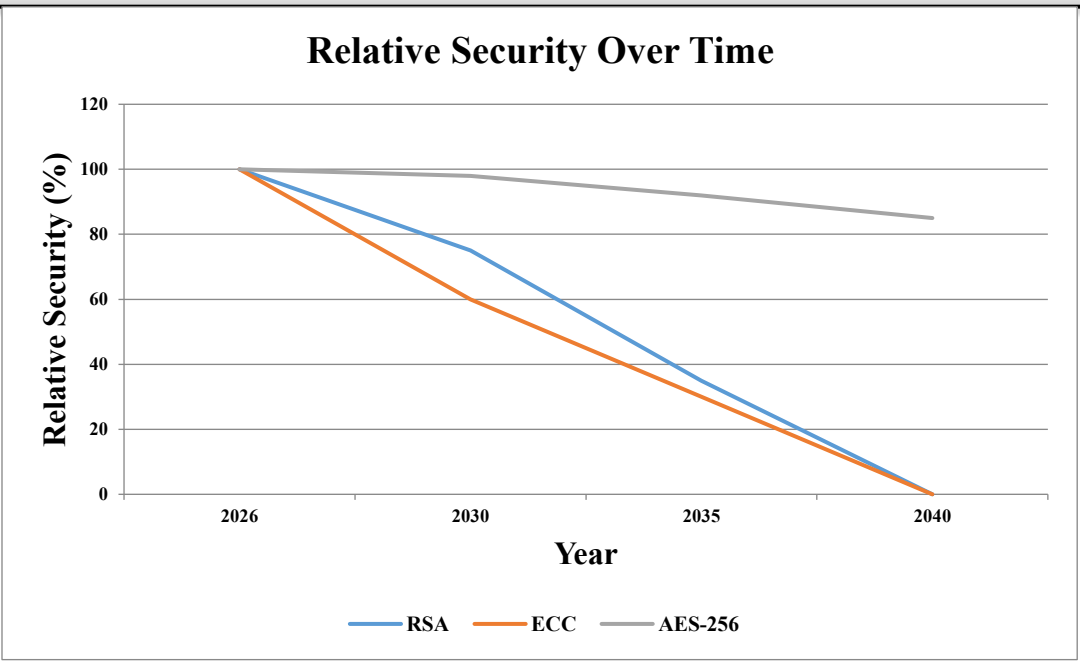
Risk Area	Percentage
HNDL (Harvest-Now, Decrypt-Later)	40
Protocol Debt	25
PKI/Identity Issues	20
QKD Hardware Attacks	15



A. Cryptography & Protocols

1. **Public-Key Schemes:** RSA, Diffie-Hellman, and ECC become vulnerable to Shor's algorithm. Organizations must replace them with NIST-approved PQC algorithms for key establishment and signatures [1] [4] [12].
2. **Symmetric/Hashing:** Grover's algorithm suggests doubling security parameters (e.g., AES-128→˜AES-256; SHA-256 remains robust with margin) [2] [3].
3. **Protocol Integration:** TLS, IPsec, and QUIC need hybrid KEMs and careful record sizing, Hello message bloat control, and performance engineering to avoid handshake regressions or amplification issues [17] [18].

Year	RSA	ECC	AES-256
2026	100	100	100
2030	75	60	98
2035	35	30	92
2040	0	0	85



B. PKI, Identity, and Supply Chain

Certificate sizes and verification costs rise with PQ signatures. Chains may exceed legacy size limits; embedded devices and TPMs may need firmware updates. Multi-year reissuance waves will stress CAs, MDMs, and inventory systems [10] [12] [19].

C. Quantum Key Distribution (QKD) Caveats

QKD can provide information-theoretic key exchange but real systems have been compromised via implementation flaws: detector blinding, calibration and timing attacks, and Trojan-horse techniques [21] [25]. QKD deployments require rigorous, hardware-level countermeasures and do not replace authentication or broader crypto agility.

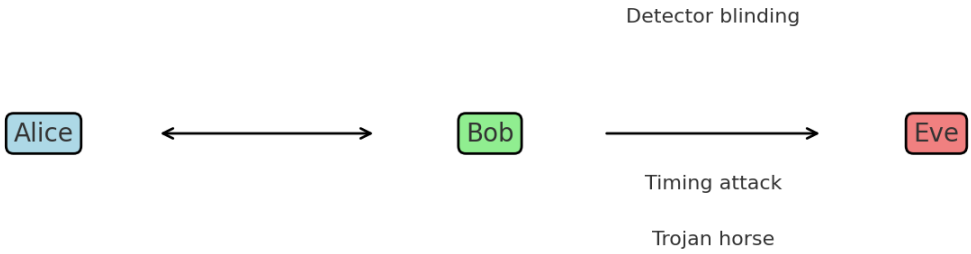
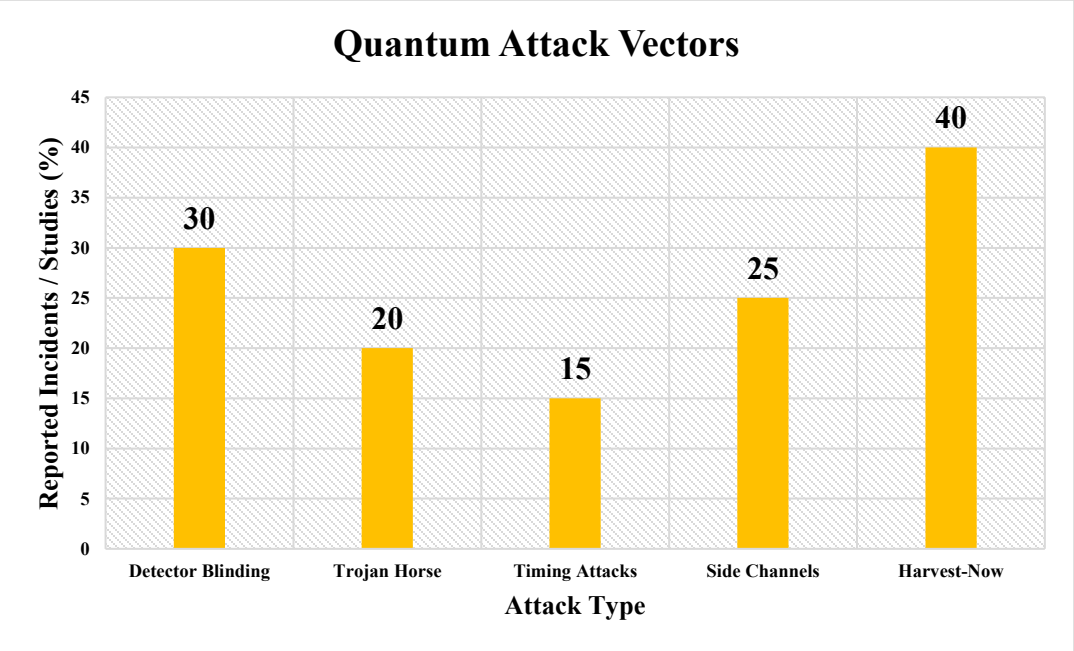


Figure 2: Quantum Key Distribution Attack Surface

Attack Type	Reported Incidents / Studies (%)
Detector Blinding	30
Trojan Horse	20
Timing Attacks	15
Side Channels	25
Harvest-Now	40



D. Operational & Governance Risks

- HNDL exposure for long-lived secrets;
- Shadow crypto and unknown dependencies;
- Interoperability debt during hybrid phases;
- Regulatory drift as policies evolve (e.g., CNSA 2.0 adoption timelines, sector guidance from CISA/ENISA) [5] [7] [10] [13].

V. MIGRATION STRATEGY

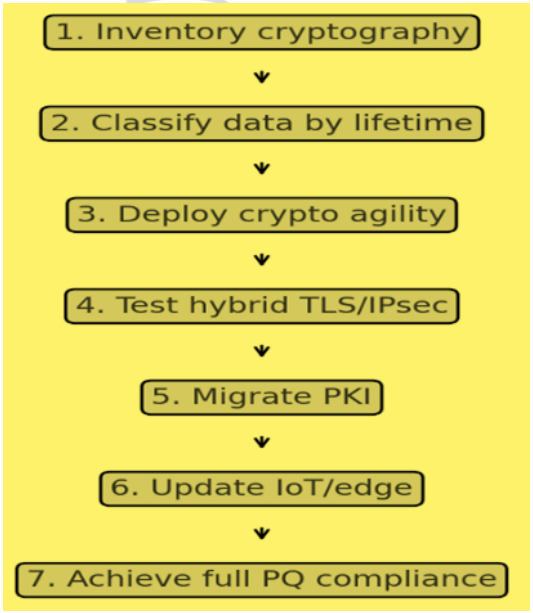
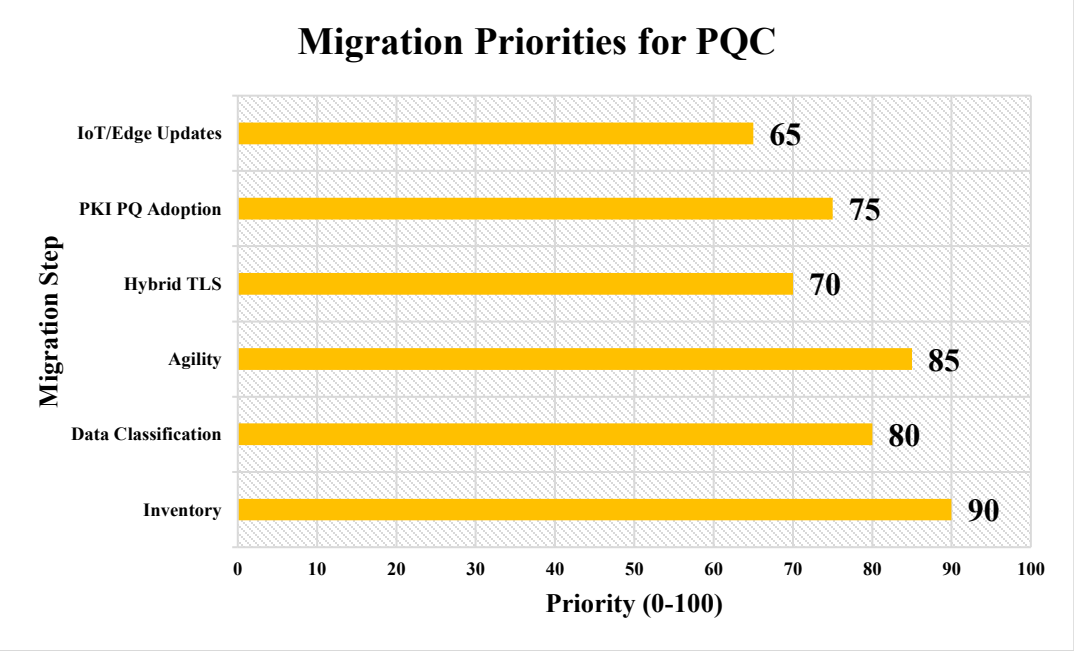


Figure 3: Migration Roadmap to PQC

Step	Action	Stakeholders
1	Crypto inventory	Security architects
2	Data classification	Compliance, risk teams
3	Agility frameworks	Dev, Ops
4	Pilot hybrid TLS	Network/security teams
5	PKI PQ adoption	PKI admins, vendors
6	IoT/edge updates	Engineering, product teams

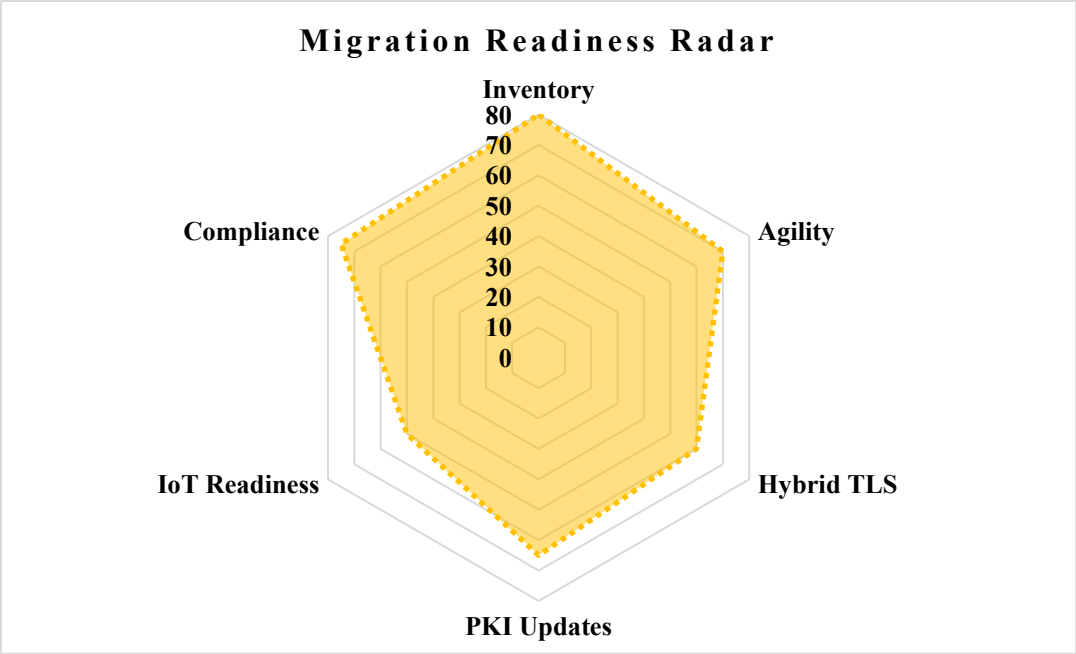
Migration Step	Priority (0-100)
Inventory	90
Data Classification	80
Agility	85
Hybrid TLS	70
PKI PQ Adoption	75
IoT/Edge Updates	65



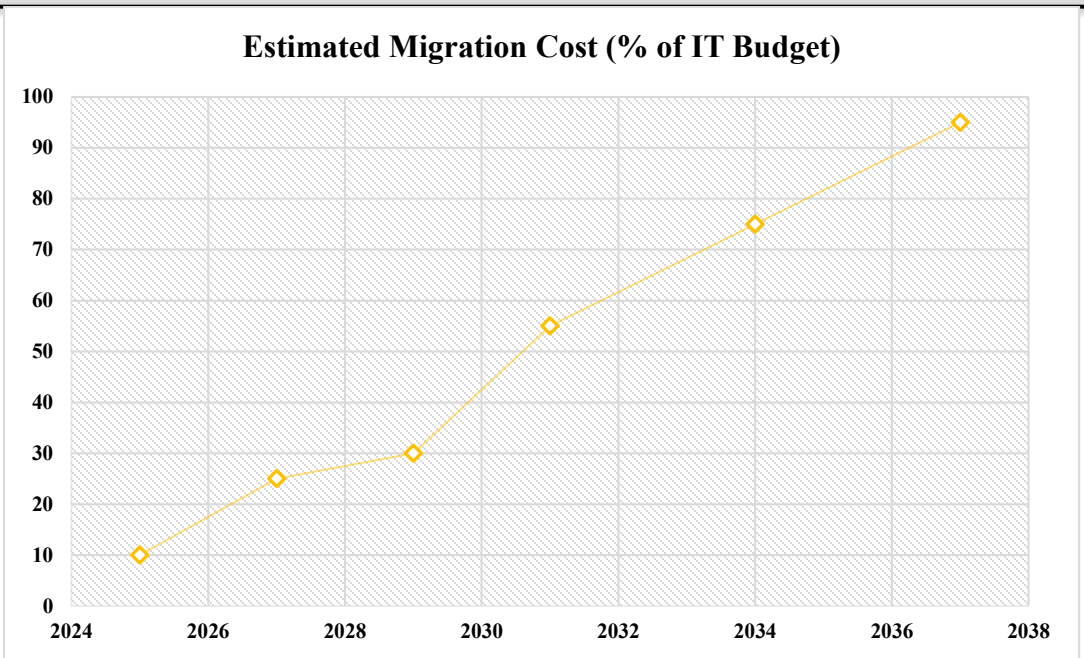
1. **Create a crypto inventory and SBOM-grade bill of cryptography.** Identify where RSA/ECC live in code, firmware, protocols, certificates, and third-party services [12] [19].
2. **Classify data by confidentiality lifetime.** Prioritize workloads at risk from HNDL (e.g., health records, industrial telemetry) [11] [14].
3. **Adopt crypto agility.** Externalize crypto from business logic; use policy-driven libraries and upgradable key stores; design for algorithm agility and version negotiation [12] [17].
4. **Pilot hybrids in transport.** Use IETF hybrid KEMs for TLS 1.3 in controlled pilots; measure handshake size/latency and failure modes; ensure graceful fallback [17] [18].
5. **Plan for PQC in PKI.** Test ML-DSA/SLH-DSA certificates in private PKI; validate chain sizes, OCSP/CRLs, HSM support, and client parsing limits [4] [12].

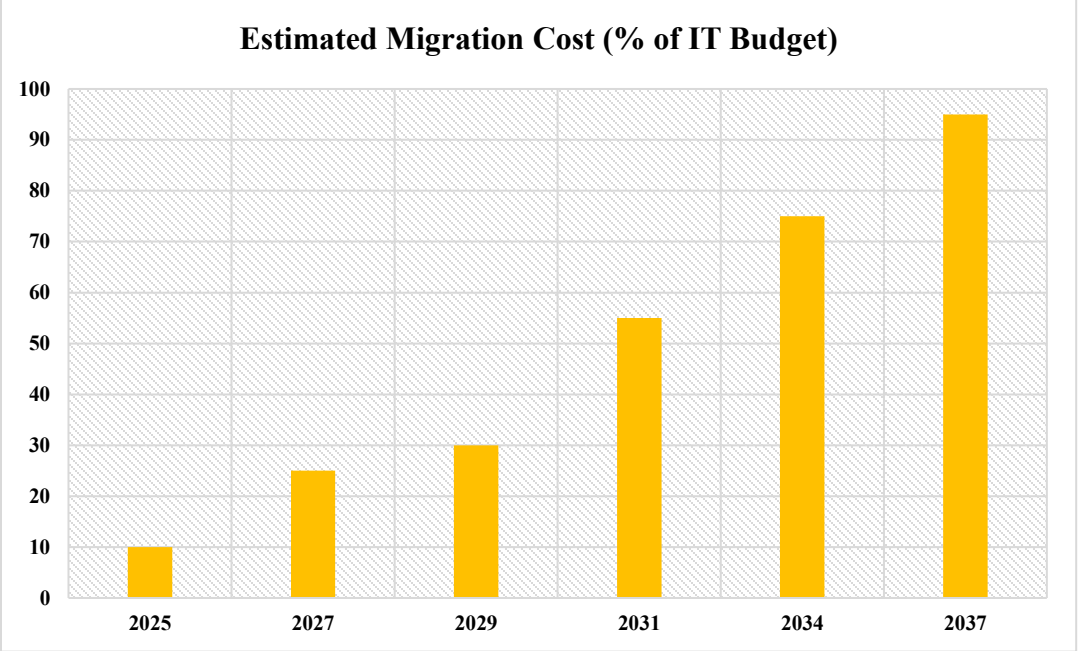
6. **Edge/IoT considerations.** Budget for firmware updates, increased key sizes, and constrained-device performance; stage replacements for non-upgradable hardware [10] [12].
7. **Compliance alignment.** Track NIST FIPS 203/204/205, NIST IR 8547 transition guidance, NSA CNSA 2.0 milestones, and sector regulators (CISA, ENISA) [4] [5] [12] [7].
8. **Test & validate.** Establish quantum-safe CI pipelines with interop suites; run chaos/rollback drills; monitor cert issuance volumes to avoid outages [18] [19] [20].

Category	Score
Inventory	80
Agility	70
Hybrid TLS	60
PKI Updates	65
IoT Readiness	50
Compliance	75



Year	Estimated Migration Cost (% of IT Budget)
2025	10
2027	25
2029	30
2031	55
2034	75
2037	95





VI. RESEARCH AND OPEN PROBLEMS

Even though there has been a lot of advancement in the area of cryptography that is secure against quantum computers (PQC) and creating standards, there are still some problems that need to be solved:

A. Security Guarantees and Simplifications

Most PQC methods depend on security assumptions that haven't been around for very long, like the Learning with Errors (LWE) problem based on lattices or structured codes. Even though people think these problems can't be solved by quantum computers, we need better security proofs, studies that try to break the code, and constant testing against new quantum algorithms to be sure in the long run.

B. Attacks Through Hidden Channels and Implementations

Even if PQC methods are mathematically correct, they can be broken by attacks that use physical means,

such as looking at power usage, injecting errors, or finding information from the computer's structure. Creating implementations that can resist these hidden channel attacks and still work well on regular computer processors and small IoT devices is still a popular topic of study.

C. Creating Mixed Protocols

During the changeover, mixed methods that use both regular and PQC algorithms are very important. However, making sure that past communications stay private, keeping message sizes small, and stopping middle boxes from becoming outdated are still unsolved problems. It is especially important to find the right mix between security and speed in mixed TLS, IPsec, and QUIC systems.

D. PKI and Ability to Grow the Infrastructure

Big key and certificate sizes create risks for public key infrastructures, cell phone networks, and embedded systems that have limited resources. We need research into certificate formats that don't take up much space, ways to efficiently cancel certificates, and plans for spreading them in a way that can be expanded.

E. Security of Quantum Key Distribution (QKD)

QKD promises security based on information theory, but actual systems can still be attacked by blinding detectors, using Trojan horses, and timing attacks. We still don't have official frameworks and certified defenses for QKD hardware, which makes people less confident in using it widely.

F. Ease of Use and Migration Tools

Aside from just the basic cryptographic parts, changing over also needs tools for developers, testing environments, and studies on how easy it is to use. Research into automatically finding cryptographic elements, flexible libraries, and easy-to-use programming interfaces will be very important to cut down on deployment mistakes and speed up adoption.

VII. CONCLUSION

Quantum computing presents both challenges for cybersecurity that will take time to solve and those that need attention right away. Even though quantum computers that are large enough to be useful don't exist yet, there are computer programs like Shor's and Grover's that could break current public-key systems and some basic encryption methods once these computers are developed. The risk of someone collecting encrypted data now with the intention of decrypting it later makes it even more important for groups to start getting ready now, especially if they are in charge of important data that needs to be kept safe for a long time.

Groups that set standards, including NIST, NSA, ETSI, and IETF, have started working hard to create new encryption methods that can withstand quantum computers and plans for switching over to them. However, there are still technical and practical problems, like bigger keys and signatures, incorporating them into current systems, and hardware limits in places where resources are limited. Because of this, the switch needs to be done in steps and managed carefully to avoid causing problems while making sure things stay secure in the long run.

This paper focused on three very important things: creating lists of all the encryption methods being used, having the ability to quickly change encryption methods, and using a mix of old and new solutions while switching over. Groups that do these things will be ready to use the new encryption standards as soon as they are finished and be able to keep up with changing rules. In the end, it is important to plan ahead and work together to switch over, so that important systems, communication methods, and data stay safe when quantum computers become common.

REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comput.*, 1997. (SIAM Ebooks)

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th ACM STOC*, 1996. (ACM Digital Library)

[3] "Grover's algorithm," Wikipedia, accessed Sep. 17, 2025. (Wikipedia)

[4] NIST, "Post-Quantum Cryptography | CSRC," Aug. 2024. (FIPS 203/204/205) (NIST Computer Security Resource Center)

[5] NSA, "Post-Quantum Cybersecurity Resources / CNSA 2.0," Mar. 2025. (NSA)

[6] NSA, "CSfC Post-Quantum Cryptography Guidance Addendum 1.0 (Draft)," Apr. 2025. (NSA)
[7] ENISA, "Post-Quantum Cryptography: Current State and Quantum Mitigation," Mar. 2024. (ENISA)
[8] NIST, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," Aug. 2024. (NIST)
[9] NSA, "NSA Releases Future Quantum-Resistant Algorithm Requirements for NSS (CNSA 2.0)," Sep. 2022. (NSA)
[10] ETSI, TR 104 016 V1.1.1, *Quantum-Safe Migrations and Migration Planning*, 2024. (ETSI)
[11] NIST, "What is Post-Quantum Cryptography? (HNDL explanation)," Aug. 2024. (NIST)
[12] NIST IR 8547 (IPD), *Transition to Post-Quantum Cryptography*, Nov. 2024. (NIST Publications)
[13] CISA, *Preparing Critical Infrastructure for Post-Quantum Cryptography*, 2022. (CISA)
[14] CCCS (Canada), *Preparing your organization for the quantum threat to cryptography*, Feb. 2025. (Canadian Centre for Cyber Security)
[15] NIST IR 8545, *Status Report on the Fourth Round of the NIST PQC Process*, Mar. 2025. (NIST Publications)
[16] CISA, *Cybersecurity Strategic Plan FY2024-2026*, Jan. 2025. (CISA)
[17] IETF, *Hybrid Key Exchange in TLS 1.3* (draft-ietf-tls-hybrid-design-10), Apr. 2024. (IETF)
[18] IETF PQUIP WG, "State of Protocols and PQC," GitHub, accessed Sep. 17, 2025. (GitHub)
[19] ETSI, TR 103 965 V1.1.1, *Impact of Quantum Computing on Cryptographic Security Proofs*, Oct. 2024. (ETSI)
[20] ETSI, TR 103 967 V1.1.1, *Impact of Quantum Computing on Symmetric Cryptography*, Jan. 2025. (ETSI)
[21] I. Gerhardt *et al.*, "Full-field implementation of a perfect eavesdropper on a QKD system," *Nat. Commun.*, 2011. (Nature)
[22] Nature News, "Hackers blind quantum cryptographers," Aug. 2010. (Nature)
[23] E. Diamanti *et al.*, "Practical challenges in quantum key distribution," *npj Quantum Information*, 2016. (Nature)
[24] K. Yoshino *et al.*, "QKD with an efficient countermeasure against detector blinding," *npj Quantum Information*, 2018. (Nature)
[25] R. Kumar *et al.*, "Experimental vulnerability analysis of QKD based on attack constructions," *Sci. Rep.*, 2021. (Nature)
[26] E. R. Zaka, S. M. Mushtaher Uddin, M. A. Hayat, A. Murtaza, S. A. Haiderand C. lal Beejal, "AI-Driven Cybersecurity for IoT–Cloud Ecosystems", Physical Education, Health and Social Sciences, vol. 3, no. 3, Sep. 2025, doi: 10.5281/zenodo.17079810.
[27] M. Siddiqui, H. M. A. Siddiqui, S. Hussain, Dr. Muhammad Faseeh Ullah Khan, Syed Faraz Aliand M. A. Hayat, "INTERACTION OF FINANCIAL LITERACY IN IMPULSIVE BUYING BEHAVIOR THEORY", Remittances Review, vol. 9, no. 3, pp. 780–802, 2024, doi: 10.5281/zenodo.17079478.
[28] M. A. Hayat, S. A. Ahmed, S. Fatima, E. F. Irfan, M. O. Nizamaniand A. Khalil, "TINY MACHINE LEARNING (TINYML) ADVANCEMENTS FOR INTELLIGENT BATTERY-POWERED IOT SENSORS", TINY MACHINE LEARNING (TINYML) ADVANCEMENTS FOR INTELLIGENT BATTERY-POWERED IOT SENSORS, vol. 3, no. 8, pp. 818–832, Aug. 2025, doi: 10.5281/zenodo.16932733.
[29] M. A. Hayat, S. Ahmed, M. R. K. Khan, E. M. Zaka, E. F. Irfanand E. R. Zaka, "Blockchain-Secured Iot Framework for Smart Waste Management in Urban Environments", The Critical Review of Social Sciences Studies, vol. 3, no. 3, Aug. 2025, doi: 10.5281/zenodo.17079639.
[30] Muhammad Ahsan Hayat, "The Role of HR in Managing Robotic Process Automation (RPA) Displacement Anxiety among Employees," The Critical Review of Social Sciences Studies, vol. 3, no. 3, pp. 1-20, 3 8 2025.
[31] Muhammad Ahsan Hayat, "HR Beyond the Office: Leveraging AI to Lead Distributed Teams and Cultivate Organizational Culture in the Age of Remote and Hybrid Work," ACADEMIA International Journal for Social Sciences (AIJSS), vol. 4, no. 3, pp. 1-20, 2025.