AI-Driven Explainable Monitoring Framework for Post-Quantum Cryptography (PQC) Migration in Multi-Cloud Environments

Sejal Shripad Bandewar, Guide: **Snehal Patil**
Department of Master of Computer Application
Dr. D. Y. Patil Institute of Master of Computer Application and Management, Akurdi
Pune, India

Abstract - Organizations are gradually replacing RSA and elliptic-curve cryptography with post-quantum cryptography (PQC) to prepare for the possibility that future quantum computers may break today's public-key methods. During this transition, classical and post-quantum techniques may operate together. This can affect handshake sizes, certificate chains and network timing. As a result, a security monitor trained on older traffic may mistake normal migration activity for an attack, while genuine threats may become harder to notice. This paper examines the issue by comparing published work on PQC migration, cryptographic performance and explainable intrusion detection. The reviewed studies mainly discuss migration planning, readiness and algorithm performance, while AI-based detection studies generally focus on ordinary network attacks. The comparison did not identify a study that directly investigates migration-related traffic changes as a source of false alerts. To address this gap, the paper puts forward a conceptual, migration-aware monitoring framework. It classifies events as normal activity, an expected migration-related change or a genuine anomaly, and uses feature attributions to explain each decision. The framework has not yet been implemented or experimentally tested; a plan for future evaluation is outlined. The study is intended to support further research and security monitoring during the transition to PQC.

Index Terms—Post-quantum cryptography, PQC migration, explainable AI, anomaly detection, multi-cloud security, SHAP.

I. INTRODUCTION

A. Background Information

A large part of secure communication over the internet relies on public-key techniques, including RSA and elliptic-curve cryptography. These methods depend on mathematical problems that are difficult for conventional computers to solve. However, Shor's algorithm showed that a sufficiently powerful quantum computer could solve some of these problems much more efficiently [1]. Although such a computer is not currently available, there is concern that attackers may collect encrypted information now and decrypt it later when the technology becomes practical. This is commonly known as the "store now, decrypt later" threat. It is particularly serious for information that must remain confidential for many years [2][3].

To prepare for this future risk, the National Institute of Standards and Technology (NIST) published its first post-quantum cryptography standards in 2024. These include ML-KEM for establishing shared keys [4], along with ML-DSA and SLH-DSA for digital signatures [5][6]. ML-KEM and ML-DSA are based on the CRYSTALS-Kyber and CRYSTALS-Dilithium designs [7][8]. Compared with elliptic-curve methods, these algorithms generally involve larger keys, ciphertexts and signatures. This means that the messages exchanged when two systems establish a secure connection can become larger or behave differently [9][7].

A complete changeover cannot usually happen all at once. Campbell estimates that enterprise PQC migration may take between five and fifteen years, or even longer, depending on the size and needs of an organization [2]. During this period, classical and post-quantum methods may need to work together in hybrid configurations. The challenge becomes more complicated in multi-cloud environments because cloud providers use different key-management services and may follow different migration schedules [10][11].

Security monitoring faces a related challenge. Machine-learning systems learn patterns from the network traffic used during training. When real-world traffic begins to differ from those patterns, detection performance can decline [12]. PQC migration can create exactly this type of change. Handshakes may become larger, certificate structures may be different and connection timing may shift, even when the activity is legitimate. A detector that is not aware of the migration may therefore raise alerts for normal changes.

B. Research Problem or Question

This situation creates a practical concern for organizations. A monitoring system trained before migration begins may generate many alerts when it encounters legitimate PQC-related traffic. Security analysts then have to spend time checking these alerts, and repeated false alarms can reduce their confidence in the monitoring system. At the same time, a real attacker could take advantage of the increased activity and uncertainty during a migration period. A useful monitoring approach should therefore recognize when a migration is taking place, distinguish approved changes from suspicious behaviour, and provide a clear reason for each decision. This paper is guided by the following research questions:

- RQ1. What do existing studies tell us about PQC migration and AI-based security monitoring, and how much do these two research areas overlap?
- RQ2. Do the reviewed studies leave a gap concerning network-traffic changes that occur specifically because of PQC migration?
- RQ3. What kind of framework could help address this gap while giving security analysts explanations they can understand?

C. Significance of the Research

This issue matters because false alerts take up analysts' time and can weaken confidence in automated security tools. Missing a real attack during a migration period can also have serious consequences. Since PQC migration is expected to continue over several years [2], the monitoring challenge is likely to remain relevant for a considerable time. From a research perspective, this paper identifies an area that receives limited attention in the literature reviewed. The work is also connected to the Sustainable Development Goals, particularly SDG 9, which focuses on resilient infrastructure, and SDG 16, which supports trustworthy institutions. Secure and properly monitored digital systems contribute to both goals. It is important to clarify that this paper is conceptual: it reviews published research and proposes a framework, but does not implement the framework or present experimental results.

II. Literature Review

A. Overview of Relevant Literature

1) PQC Migration and Readiness Planning: Hasan et al. introduce a migration-planning framework that starts by identifying an organization's cryptographic assets and the dependencies between them. They demonstrate the approach through three case studies [13]. Näther et al. review research on software migration to PQC and report that the available migration approaches are still developing [14]. Campbell discusses the possible migration timelines for organizations of different sizes and explains the store-now-decrypt-later concern [2]. Campagna, LaMacchia and Ott also describe the readiness issues organizations need to consider [3]. More recent work looks at ways to assess readiness. QUASAR presents a strategic architecture with a scoring method [15], while Erlemann et al. combine a knowledge graph and a language model to calculate an explainable enterprise-readiness score using Shapley-value decomposition [16]. Dubey and Varshney study PQC readiness across 32,011 internet domains and report that 49.3% support hybrid post-quantum key exchange [17].

Cloud-focused studies also examine how PQC can be introduced into existing services. Lichani et al. describe a hybrid classical-and-PQC encryption approach for protecting data stored in the cloud [10]. Rajkumar et al. combine cloud security posture management with PQC to support secure data transmission [11]. Overall, this group of studies approaches migration through planning, readiness measurement or system design. The studies reviewed do not examine how security-monitoring tools behave while the migration itself is taking place.

2) PQC Algorithms and Performance: The Kyber [7] and Dilithium [8] designs form the basis of important NIST PQC standards [4][5]. Research on post-quantum TLS also considers the performance impact of these algorithms. For example, Zheng et al. report that their ML-KEM optimization can make handshakes up to 1.64 times faster when AVX-512 instructions are used [9]. Such work shows that handshake performance remains an important engineering concern. These studies, together with Stallings' textbook [18], help explain the technical changes that occur during PQC adoption. However, they do not investigate how those changes may affect security monitoring.

3) Explainable AI for Intrusion Detection: Ali and Kostakos combine a random-forest anomaly detector with SHAP and LIME explanations, and provide a language-model interface intended to assist analysts [19]. Ahmed et al. present HAEnID, an explainable hybrid-ensemble approach, and report accuracy of 97–98% on CIC-IDS2017 [20]. Abdulganiyu et al. introduce HeXAI-AttentionCPS, which uses an attention-based LSTM with SHAP and is evaluated using TON_IoT [21]. Mia et al. discuss how analysts can use overlapping SHAP plots to understand false-positive and false-negative results [22]. These studies focus on general

intrusion detection rather than on traffic changes caused by a particular technology migration.

4) Traffic Shift and Detector Accuracy: Mousavipour et al. present NetSight, a method designed to identify and respond to changes in network-traffic distributions without requiring manual relabelling [12]. Their work supports the idea that changes in traffic patterns can reduce the effectiveness of intrusion detectors. However, it considers distribution shift as a general issue and does not specifically examine PQC migration as the reason for that shift.

5) Related Work in Cloud and Quantum Security: Other research explores quantum-inspired data placement for multi-cloud workflows [23], quantum key distribution for secure access to cloud data [24], and the use of PQC to protect Internet of Things devices [25]. These studies demonstrate the wider interest in security for cloud, edge and quantum-era systems. However, they do not address the monitoring of network activity during a PQC migration.

B. Key Theories or Concepts

Hybrid cryptography. During the transition to PQC, a secure connection may use a conventional cryptographic method together with a post-quantum method. This arrangement is intended to maintain protection if one of the methods is later found to be vulnerable. It can also produce larger handshake messages and changes to certificate structures [9][7].

Concept drift. Machine-learning detectors work best when the traffic they encounter is reasonably similar to the data used during training. If network behaviour changes, the number of false-positive and false-negative results may increase [12].

Explainability and SHAP. SHAP uses Shapley values from cooperative game theory to estimate how much each input feature contributes to a model's prediction. This helps an analyst understand which features influenced an alert and whether they increased or reduced its score [19][22].

Store now, decrypt later. This term describes the risk that encrypted information collected today could be decrypted in the future when sufficiently capable quantum computers become available. It is one of the main reasons organizations are preparing to move to PQC [2][3].

C. Summary of Key Findings from the Literature Review

- Research on PQC migration mainly discusses planning, readiness assessment, measurement and the performance of cryptographic algorithms [13][9][2][17][14][15][16].
- Studies of explainable detection mostly examine general-purpose intrusion-detection systems and their ability to identify network attacks [19][20][21][22].
- Earlier work recognizes that changes in traffic patterns can affect detector performance [12]. However, the reviewed studies do not connect this issue directly to changes caused by cryptographic migration.
- A review published in 2026 observes that PQC and AI-based threat hunting have largely been examined as separate topics, and that research bringing them together remains limited [26].

III. Research Gap

The comparison of the literature points to four areas where further work is needed:

1) Weak Link Between PQC Migration and Security Monitoring: Most of the available studies discuss migration planning separately from intrusion detection. Because these topics are usually considered on their own, organizations have limited guidance on how a monitoring system should interpret network activity while PQC migration is underway.

2) Lack of a Common Method for Studying Migration Traffic: The reviewed research does not provide a shared dataset or evaluation approach for distinguishing normal changes in PQC or hybrid handshakes from genuinely malicious activity.

3) Insufficient Explanation of Approved Migration Changes: Current explainable-AI approaches generally focus on showing why a system considers an event suspicious. Less attention is given to explaining why unusual traffic may be legitimate because it is part of an authorized migration.

4) Uncertain Impact on Detection Performance: Further investigation is needed to determine how larger handshakes, updated certificate chains and timing changes influence false alarms and the ability to detect real attacks.

Taken together, these gaps suggest the need for a monitoring approach that takes the migration schedule and context into account while also explaining its decisions. Future evaluation could combine established public network-traffic datasets with simulated PQC migration traffic [9], [12], [20], [26], [7].

IV. Methodology

A. Research Design

This research follows a qualitative approach based on published literature and is organized into two stages. First, relevant studies are compared to identify areas of overlap and gaps in the existing work. Second, a conceptual monitoring framework is developed by linking each identified gap to a proposed design feature. The study is not an experiment: it does not involve human participants, collect primary experimental traffic or train a machine-learning model.

B. Data Collection Methods

The analysis is based on secondary information collected from research sources available through IEEE Xplore, SpringerLink, Nature (Scientific Reports), Frontiers, MDPI and arXiv. Search phrases included terms such as "post-quantum cryptography migration," "hybrid TLS," "explainable intrusion detection," "SHAP anomaly detection," "concept drift network intrusion" and "PQC multi-cloud." The foundational algorithm publications date from 1994 and 2018, while the other sources mainly fall between 2020 and 2026. No new experimental dataset was collected for this conceptual paper. For future testing, simulated traffic could be generated using open-source PQC tools and studied alongside public network-traffic datasets such as CIC-IDS2017 and TON_IoT.

C. Sample Selection

The literature review includes 27 sources: 23 research publications, books and foundational papers, three NIST standards, and one description of an open-source project. Sources were selected when they addressed PQC migration or performance, explainable or drift-aware intrusion detection, or the basic principles of post-quantum cryptography. Vendor content and commentary without a technical focus were left out. Fourteen sources were directly relevant to the comparison matrix in Table I. The remaining references were used to provide background and explain key concepts.

D. Data Analysis Techniques

- Thematic grouping: The selected studies were organized into four themes: PQC migration and readiness, cryptographic performance, explainable intrusion detection, and changes in network-traffic patterns.
- Comparison matrix: The fourteen directly relevant studies were assessed using four criteria decided before the comparison. These were whether a study covered PQC or migration, whether it addressed AI-based monitoring or intrusion detection, whether it included explainability, and whether it examined traffic changes caused by migration. Each classification was based on the stated scope and contribution of the source.
- Gap-to-design mapping: Each gap identified through the review was linked to a corresponding part of the proposed framework, as summarized in Table II.

V. Results

A. Presentation of Findings

Table I presents the results of comparing the fourteen directly relevant studies against the four selected criteria.

TABLE I. COMPARISON OF DIRECTLY RELEVANT STUDIES AGAINST FOUR CRITERIA

Ref.	**Research focus**	Coverage and relevance to this research
[13]	Hasan et al. (2024)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[19]	Ali and Kostakos (2023)	PQC/migration: No; AI/IDS: Yes; explainability: Yes; migration-related traffic analysis: No.
[12]	Mousavipour et al. (2025)	PQC/migration: No; AI/IDS: Yes; explainability: No; migration-related traffic analysis: No.
[20]	Ahmed et al. (2024)	PQC/migration: No; AI/IDS: Yes; explainability: Yes; migration-related traffic analysis: No.
[9]	Zheng et al. (2024)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[10]	Lichani et al. (2026)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[2]	Campbell (2025)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.

Ref.	Research focus	Coverage and relevance to this research
[17]	Dubey and Varshney (2026)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[21]	Abdulganiyu et al. (2026)	PQC/migration: No; AI/IDS: Yes; explainability: Yes; migration-related traffic analysis: No.
[14]	Näther et al. (2024)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[22]	Mia et al. (2024)	PQC/migration: No; AI/IDS: Yes; explainability: Yes; migration-related traffic analysis: No.
[15]	Weinberg (2025)	PQC/migration: Yes; AI/IDS: No; explainability: No; migration-related traffic analysis: No.
[16]	Erlemann et al. (2026)	PQC/migration: Yes; AI/IDS: No; explainability: Yes*; migration-related traffic analysis: No. The explanation is for readiness scoring, not traffic monitoring.
[26]	Mohamed and Taherdoost (2026)	PQC/migration: Yes; AI/IDS: Yes (conceptual); explainability: not specified; migration-related traffic analysis: No (identified as an open area).
Summary	**Fourteen directly relevant sources**	PQC/migration: 9/14; AI/IDS: 6/14; explainability: 5/14; migration-related traffic analysis: 0/14.

* In this comparison, explainability for readiness scoring is not treated as explainability for traffic monitoring. “n/s” means that the reviewed source does not specify the point. References [18], [3], [11], [23], [24], [25] and [1], [7], [8] provide background information and are not included in the comparison scoring.

Of the fourteen directly relevant sources, nine discuss PQC or migration, six cover AI-based monitoring or intrusion detection, and five include an explainability element. Only one source, the conceptual review by Mohamed and Taherdoost, considers both migration and AI-based monitoring [26]. That review itself describes the combination as an area that has not yet been explored in depth. None of the fourteen studies examines traffic changes specifically caused by migration.

B. Data Analysis and Interpretation

The comparison shows a consistent difference between the two research areas. PQC migration studies explain how organizations can prepare for, assess and carry out the transition. Intrusion-detection studies focus on developing accurate and explainable models for more general network conditions. The two groups therefore address different parts of the problem. One possible explanation is that the NIST standards were released in 2024 [4][5], leaving limited time for researchers to study the effects of actual deployment on security monitoring. This is an interpretation of the publication pattern, rather than a conclusion directly established by the sources.

C. Support for Research Questions

- RQ1. The reviewed literature falls mainly into two groups: studies about PQC migration and studies about explainable intrusion detection. One conceptual review discusses the connection between these areas [26].
- RQ2. Based on the sources included in this review, a gap is present. None of the fourteen directly relevant studies examines traffic changes caused by PQC migration, and the 2026 review also identifies this intersection as underexplored [26].
- RQ3. The proposed design in Section V.D offers a conceptual response to the identified gap. Table II links each framework component to the issue it is intended to address.

D. Proposed Framework

The proposed framework contains seven stages, as shown in Fig. 1. Its main purpose is to provide the monitoring system with information about an approved PQC migration. With this context available, the system can avoid treating every unusual migration-related change as a possible attack.

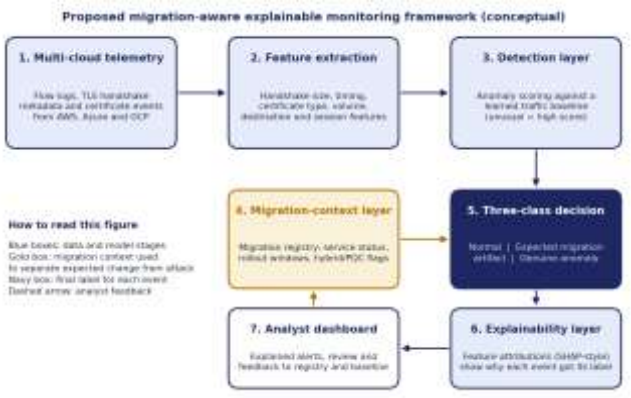


Fig. 1. Proposed migration-aware explainable monitoring framework (conceptual).

- Multi-cloud telemetry. Network flow records, TLS handshake details and certificate-related events are gathered from the different cloud providers. The information is then converted into a common format so it can be examined consistently.
- Feature extraction. Relevant details are taken from the collected telemetry, including handshake size, connection timing, certificate type, traffic volume, destination information and session characteristics.
- Detection layer. An anomaly detector compares each event with an established traffic baseline and assigns an anomaly score. At this stage, the detector does not yet consider whether a migration is taking place, allowing it to represent the behaviour of a conventional monitoring system.
- Migration-context layer. A migration registry stores details about services scheduled to move to hybrid or PQC mechanisms. It includes the planned rollout period and the traffic changes expected during that period. This registry provides the additional context that a standard detector may not have.
- Three-class decision. Each event is placed into one of three categories: normal, expected migration artifact or genuine anomaly. If unusual activity belongs to a registered service and occurs within its approved migration window, it can be treated as an expected migration artifact. Activity that does not match the registered context is sent for further investigation.
- Explainability layer. SHAP-style feature contributions are used to show which input details influenced the decision. Analysts can compare these reasons with the information recorded in the migration registry.
- Analyst dashboard and feedback. Analysts review the explanations attached to alerts. Any corrections or confirmed findings can then be used to update the migration registry and improve the traffic baseline.

TABLE II. MAPPING OF FRAMEWORK COMPONENTS TO THE GAPS FOUND

Framework component	Research gap addressed	**Related sources**
Migration-context layer	Without migration information, a detector may interpret approved migration-related changes as suspicious activity.	[13], [12], [2]
Three-class decision	A simple normal-or-attack classification does not account for unusual activity that is expected during an approved migration.	[12], [20]
Explainability layer	Analysts need an understandable reason for every classification, particularly when activity is marked as an expected migration change.	[19], [20], [21], [22]
Multi-cloud telemetry	Cloud providers use different logging and key-management arrangements, and their migration schedules may not match.	[10], [11]
Evaluation plan	The reviewed studies do not measure the false alerts that may be triggered by migration-related traffic.	[12], [26]

E. Illustrative Scenario

The examples below are hypothetical and are included only to demonstrate the intended operation of the framework. They are not based on real organizational data.

- Event A. A payment gateway hosted in one cloud is scheduled to move to hybrid key exchange. Once the rollout begins, its handshake messages become larger and its certificate chain changes. A conventional detector, which has no information about the migration, reports an increase in unusual activity. The proposed framework checks the migration registry, confirms that the service is within its approved rollout period and labels the events as “expected migration artifact.” Its explanation identifies handshake size and

certificate type as the main factors, which are consistent with the planned changes.

- Event B. An internal machine starts communicating with an unfamiliar external address at unusual times. The connections use standard handshakes but show an unexpected volume of traffic. Since the migration registry contains no matching entry, the framework labels the event as a "genuine anomaly." The explanation highlights the unusual destination, timing and traffic volume.
- Event C. An attacker attempts to imitate the handshake patterns associated with a hybrid migration, but the activity comes from a service that is not listed in the migration registry. Because the registry check does not find an approved migration entry, the event is escalated for investigation. This example also highlights a limitation: the framework depends on the migration registry being accurate and kept up to date.

F. Evaluation Plan for Future Validation

The framework has not yet been validated; the following steps are proposed for future work. Normal and attack-related baseline traffic could be assembled from public datasets such as CIC-IDS2017 and TON_IoT, which have been used in earlier studies [20][21]. Hybrid and PQC handshake traffic could then be generated with open-source tools such as the Open Quantum Safe library [27]. The proposed framework could be compared with a conventional detector that does not receive migration context. Three measures are suggested: the false-positive rate on migration traffic, the rate at which genuine attacks are detected, and the practical usefulness of the explanations to security analysts.

VI. Discussion

A. Interpretation of Results

The comparison indicates that research on cryptographic migration and research on explainable intrusion detection have largely developed as separate areas. This separation creates a practical difficulty. An organization may follow published migration guidance [13][2][15] and use an explainable detection model [20][21], yet still have little research-based direction on how the two should operate together. The framework presented here is an initial conceptual design for bringing migration information into security monitoring. Its effectiveness will need to be assessed through future testing.

B. Comparison with Existing Literature

This result is in line with the 2026 review, which describes the connection between PQC and AI-based threat hunting as an area that remains largely unexplored [26]. The proposal also extends the discussion of network-traffic shift in [12]. That work considers how a detector can respond to unexpected changes in traffic, whereas a cryptographic migration is a planned change that can be recorded in advance. A migration registry could therefore provide useful context that a general drift-detection method may not have. Existing explainable detectors [19][20][21][22] use explanations mainly to show why an event appears malicious. In the proposed framework, explanations would also help show why an unusual event is considered an expected part of an approved migration. Readiness approaches [15][16] focus on preparation and planning, while this framework is intended to support monitoring during live migration activity.

C. Implications and Limitations of the Study

1) Implications: Migration teams and security teams should exchange information about planned rollout dates and the services involved, because these details can help monitoring systems interpret unusual traffic. However, organizations should not simply turn off or broadly suppress alerts during migration periods. Doing so could give attackers an opportunity to operate with less scrutiny. For researchers, the findings point to the need for shared datasets and consistent evaluation methods for monitoring during PQC migration.

2) Limitations: The study has several limitations, which should be considered when interpreting its findings.

- The proposed framework is conceptual and has not been implemented or tested. Its expected benefits therefore remain to be demonstrated.
- The review includes a limited set of sources and was completed by one reviewer. Studies were classified according to the topics and contributions described by their authors; their underlying datasets and results were not independently re-analysed.
- Some references are preprints and may not have completed formal peer review [19][12][9][17][22][15][16][24][25].
- The proposed approach relies on the migration registry containing correct and current information. An attacker may also try to imitate

traffic patterns associated with an approved migration.

- PQC and AI-based security research are developing quickly, so some of the gaps identified in this paper may be addressed by new work in the near future.

VII. Conclusion

A. Summary of Key Findings

The reviewed research on PQC migration and explainable AI-based intrusion detection is substantial. However, none of the sources examined directly studies how migration-related changes in network traffic may confuse a security monitor. The 2026 review by Mohamed and Taherdoost reports a similar lack of connection between the two areas [26]. In response, this paper proposes a conceptual framework that supplies migration context to anomaly detection, separates expected migration activity from genuine threats, and provides explanations for its decisions.

B. Contributions to the Field

- A comparison of PQC migration and explainable intrusion-detection studies using four consistent criteria.
- A seven-stage conceptual monitoring framework that includes a migration-context registry and a three-category event decision.
- A proposed evaluation approach, including comparison measures and baseline data sources, for future empirical research.

C. Recommendations for Future Research

- Empirical validation: Develop a working version of the framework and evaluate it using simulated hybrid traffic together with public intrusion-detection datasets. Compare its results with a detector that does not use migration context.
- Field studies: Examine real PQC migration activity across different cloud environments to understand how network traffic changes in practice.
- Analyst studies: Assess whether explanations for expected migration-related events help analysts make decisions more confidently and respond more efficiently.
- Practitioner surveys: Gather views from security and migration professionals about how monitoring is currently handled during migration periods.
- Wider scope: Explore whether the same approach can be adapted to other major changes in network protocols and cryptographic technologies.

VIII. References

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proc. 35th Annu. Symp. Found. Comput. Sci. (FOCS), 1994, pp. 124–134.

[2] R. Campbell, “Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks,” Computers, vol. 15, no. 1, Art. no. 9, 2026, doi: 10.3390/computers15010009.

[3] M. Campagna, B. LaMacchia, and D. Ott, “Post quantum cryptography: Readiness challenges and the approaching storm,” Computing Community Consortium white paper, 2020.

[4] National Institute of Standards and Technology, “Module-lattice-based key-encapsulation mechanism standard,” FIPS 203, Aug. 2024.

[5] National Institute of Standards and Technology, “Module-lattice-based digital signature standard,” FIPS 204, Aug. 2024.

[6] National Institute of Standards and Technology, “Stateless hash-based digital signature standard,” FIPS 205, Aug. 2024.

[7] J. Bos et al., “CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM,” in Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P), 2018, pp. 353–367.

[8] L. Ducas et al., “CRYSTALS-Dilithium: A lattice-based digital signature scheme,” IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 1, pp. 238–268, 2018.

[9] J. Zheng, H. Zhu, Z. Song, Z. Wang, Y. Zhao, et al., “Faster post-quantum TLS 1.3 based on ML-KEM: Implementation and assessment,” arXiv:2404.13544, 2024.

[10] A. Lichani, R. Nouara, and N. Belala, “Post-quantum ready hybrid encryption for cloud data-at-rest,” in Smart Applications in Healthcare, Precision Farming and Transportation (ICSA 2025), A. Chaoui, S. Chikhi, R. Capilla, and M. Djoudi, Eds., Lecture Notes in Networks and Systems, vol. 1883. Cham, Switzerland: Springer, 2026, pp. 59–71, doi: 10.1007/978-3-032-19929-4_6.

[11] N. Rajkumar, K. K. Kumar, M. Gokul, and S. Durai, “Post-quantum cryptography security with

CSPM for secure data transmission in cloud environments," in Proc. ICUIS, IEEE, 2024.

[12] E. Mousavipour, A. Dimanchev, and M. Ghaderi, "Shift detection and adaptation for network intrusion detection," arXiv:2508.15100, 2025.

[13] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," IEEE Access, vol. 12, pp. 23427–23450, 2024, doi: 10.1109/ACCESS.2024.3360412.

[14] C. Näther, D. Herzinger, S.-L. Gazdag, J.-P. Steghöfer, S. Daum, and D. Loebenberger, "Migrating software systems toward post-quantum cryptography: A systematic literature review," IEEE Access, 2024.

[15] A. I. Weinberg, "Preparing for the post quantum era: Quantum ready architecture for security and risk management (QUASAR): A strategic framework for cybersecurity," arXiv:2505.17034, 2025.

[16] R. Erlemann, C. C. Morris, and S. Sathe, "Full-stack knowledge graph and LLM framework for post-quantum cyber readiness," arXiv:2601.03504, 2026.

[17] V. M. Dubey and G. Varshney, "Measurement study of post-quantum readiness of Internet: 2026," arXiv:2606.16473, 2026.

[18] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2023.

[19] T. Ali and P. Kostakos, "HuntGPT: Integrating machine learning-based anomaly detection and explainable AI with large language models (LLMs)," arXiv:2309.16021, 2023.

[20] U. Ahmed, Z. Jiangbin, A. Almogren, S. Khan, M. T. Sadiq, A. Altameem, and A. U. Rehman, "Explainable AI-based innovative hybrid ensemble model for intrusion detection," J. Cloud Comput., vol. 13, 2024.

[21] O. H. Abdulganiyu, O. Fadi, Y. Moukafih, T. Ait Tchakoucht, Y. K. Saheed, J. E. Chukwuere, and S. Yau, "Explainable attention-based few-shot LSTM for intrusion detection in imbalanced cyber-physical system networks," Sci. Rep., 2026.

[22] M. Mia, M. M. A. Pritom, T. Islam, and K. Hasan, "Visually analyze SHAP plots to diagnose misclassifications in ML-based intrusion detection," arXiv:2411.02670, 2024.

[23] Z. Brahmi and R. Derouiche, "EQGSA-DPW: A quantum-GSA algorithm-based data placement for scientific workflow in cloud computing environment," J. Grid Comput., 2024, doi: 10.1007/s10723-024-09771-5.

[24] S. V. V. Lakshmi and Z. H. Choudhury, "Secure data access in cloud environments using quantum cryptography," arXiv:2506.10028, 2025.

[25] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the future Internet of Things with post-quantum cryptography," arXiv:2206.10473, 2022.

[26] N. Mohamed and H. Taherdoost, "The convergence of post-quantum cryptography and AI-driven threat hunting: A review of quantum-resilient defense frameworks," Front. Commun. Netw., 2026, doi: 10.3389/frcmn.2026.1816116.

[27] Open Quantum Safe Project, "liboqs: C library for quantum-resistant cryptographic algorithms." [Online]. Available: https://openquantumsafe.org