MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

USIM

Article

Toward Quantum-Resilient PKI: A Systematic Literature Review of Post-Quantum Certificates Model

Nor Azeala Mohd Yusof [1,3], A H Azni [1,2], Farida Ridzuan[1,2], Nur Hafiza Zakaria[1,2], Sakinah Ali Pitchay[1,2], Abdul Alif Zakaria[3] and Tasnuva Ali[4]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai 71800, Negeri Sembilan, Malaysia.*

[2]*CyberSecurity and Systems Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai 71800, Negeri Sembilan, Malaysia.*

[3]*CyberSecurity Malaysia, 63000 Cyberjaya, Selangor, Malaysia.*

[4]*Department of Electronics and Telecommunication Engineering, Daffodil International University Dhaka, Bangladesh.*

Correspondence should be addressed to:
A H Azni; ahazni@usim.edu.my

Article Info
Article history:
Received:15 July 2025
Accepted: 6 February 2026
Published:15 Mac 2026

Academic Editor:
Nurzi Juana Mohd Zaizi

Malaysian Journal of Science, Health & Technology

MJoSHT2025, Volume 11, Special Issue on the 5th International Conference on Recent Advancements in Science and Technology (ICoRAST 2025): Responsible Artificial Intelligence – Advancing Science and Technology for Humanity
eISSN: 2601-0003

https://doi.org/10.33102/dypnkt79

***Abstract*— The rise of quantum computing presents a critical threat to classical public-key cryptographic systems, necessitating a global shift toward post-quantum cryptography (PQC). While algorithmic standardisation has seen substantial progress since the National Institute of Standards and Technology (NIST) initiated its call for PQC proposals in 2017, the integration of these algorithms into certificate-based infrastructures remains fragmented and underexplored. This gap creates uncertainty for secure communication, particularly in transitioning legacy systems into quantum-resilient environments. This systematic literature review (SLR) focuses on PQC certificate architectures studied between 2017 and 2025, encompassing the evolution of the field since NIST's formal standardisation efforts began. The review employs the PRISMA 2020 methodology to identify and analyse six distinct post-quantum certificate models: Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped. Each model is evaluated across several criteria, including structure, backwards compatibility, tooling support, standardisation status, and production readiness, drawing evidence from scholarly publications, draft standards, and open-source implementations. Findings highlight the Hybrid certificate as the most viable short-term solution due to its high interoperability and maturity in deployment. Composite and Parallel architectures offer enhanced security assurances that are suitable for critical infrastructure, although they come with increased implementation complexity. Pure PQC certificates, while future-proof, are still limited to constrained or greenfield environments. Chameleon and Wrapped models are identified as emerging alternatives for blockchain and legacy scenarios, respectively, with limited but growing support. This review enlightens the design and deployment of quantum-safe public key infrastructures by outlining the trade-offs and maturity levels of each architecture. It also emphasises the need for continued development in standardisation and toolchain support to facilitate scalable and secure PQC adoption.**

***Keywords*— Post-Quantum Cryptography (PQC); Public Key Infrastructure (PKI); X.509 Certificates; Certificate Verification; Hybrid Cryptographic Models**

I. INTRODUCTION

Quantum computing presents a fundamental and accelerating threat to the foundations of classical cryptographic systems. Algorithms such as RSA, ECC, and DSA, which are widely used for securing digital communications, signatures, and identity verification, are vulnerable to polynomial-time attacks made possible by quantum algorithms. In particular, Shor's algorithm enables efficient factorisation of large integers and computation of discrete logarithms, which compromises the security of these traditional public key systems [1]. As quantum hardware progresses toward practical viability, the global cryptographic community faces an urgent imperative to redesign the infrastructure of trust and communication in digital systems.

This concern has led to the rise of post-quantum cryptography, which focuses on cryptographic primitives that are resistant to both classical and quantum adversaries. Recognising this urgency, the National Institute of Standards and Technology launched the Post-Quantum Cryptography standardisation initiative in late 2016, with the first round of algorithm proposals formally accepted in 2017 [2]. The standardisation process has since proceeded through rigorous rounds of evaluation, resulting in the selection of a new generation of quantum-resistant cryptographic algorithms. These include ML-KEM, a module lattice-based key encapsulation mechanism previously known as Kyber, ML-DSA, a module lattice-based digital signature algorithm formerly identified as CRYSTALS-Dilithium, and SLH-DSA, a stateless hash-based digital signature scheme previously referred to as SPHINCS+ [3]. These schemes are currently undergoing formalisation into Federal Information Processing Standards and represent the core of the post-quantum cryptographic toolbox for public use.

Despite this progress in algorithm selection, the practical integration of these quantum-safe algorithms into real-world infrastructures remains a significant challenge. Digital certificates form the backbone of Public Key Infrastructure (PKI) by enabling secure identification, trust management, and authentication across distributed systems. Integrating post-quantum algorithms into certificates is not merely a matter of key substitution. However, it involves a more complex process beyond key substitution. It raises architectural, operational, and interoperability concerns that must account for legacy systems, backward compatibility, certificate validation paths, and compliance with existing trust models.

In conventional Public Key Infrastructure (PKI) systems, certificates usually associate a single classical public key with an entity's identity, relying on stable certificate chains and established validation methods. In contrast, post quantum certificate models may include multiple cryptographic keys, hybrid approaches, or additional algorithm identifiers to support quantum resistant security while remaining compatible with current infrastructure. These structural modifications impact certificate size, validation complexity, and computational overhead, factors that directly affect scalability, especially in large scale systems and resource constrained environments like Internet of Things (IoT). At the same time, ensuring interoperability is essential during the transition, as post quantum certificates must remain verifiable by legacy systems and align with existing trust anchors and policy standards. As a result, the structure and design of certificate models are crucial to achieving a balance between enhanced security and practical deployment throughout the post quantum migration process.

Current research has primarily emphasised performance benchmarks, algorithmic resilience, and protocol-level implementation, especially in environments such as post-quantum TLS handshakes and VPNs [4]. In contrast, significantly less attention has been directed toward how post-quantum cryptographic primitives are structurally embedded within certificate formats and deployed within functioning PKI ecosystems. This lack of comprehensive analysis complicates institutional efforts to migrate toward quantum-resilient systems while ensuring continued operability, trust assurance, and compliance with existing standards. Moreover, inconsistencies in terminology across academic literature, industry standards, and open-source implementations have resulted in a fragmented understanding of certificate-level integration.

Recent studies have emphasised the urgent need for a systematic review of these challenges. Many current solutions fall short of addressing the full range of problems that arise in the structural and operational integration of post-quantum certificates. As the demand for secure and scalable digital infrastructures continues to grow, it becomes essential to design robust and adaptable certificate models that uphold high standards of security, trust, and interoperability in the face of evolving quantum threats.

This review aims to address this gap by conducting a comprehensive and systematic investigation into the state of post-quantum certificate architectures. Specifically, it focuses on the design, integration, and deployment of certificate models that incorporate post-quantum cryptographic primitives. The objective is to identify existing solutions, categorise their structural and functional features, assess their deployment readiness, and highlight the trade-offs involved in adopting each approach across diverse use cases and PKI environments.

Based on a methodical review of literature published between 2017 and 2025, this study identifies and analyses six distinct certificate models. These include Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped architectures. Each model represents a unique approach to embedding post-quantum algorithms within certificate structures and is evaluated in terms of compatibility, tooling support, standardisation progress, and integration complexity.

This article is organised as follows. Section II outlines the research methodology used in this study, following the PRISMA 2020 framework. Section III presents the findings of the comparative analysis. Section IV discusses practical recommendations and strategic considerations for PKI transition. Finally, Section V concludes with a summary of the key insights and proposes future research directions.

II. RESEARCH METHODOLOGY

This systematic literature review (SLR) investigates the structural and operational characteristics of post-quantum certificate architectures and their readiness for integration into public key infrastructures. The study focuses explicitly on

certificate types proposed or evaluated between 2017 and 2025, a period that begins with the launch of NIST's post-quantum cryptography standardisation effort and continues through its most recent algorithmic selections. To ensure methodological rigour, this review adopts the PRISMA 2020 framework, which offers a structured and transparent process for identifying, selecting, and analysing relevant scholarly literature [5-7].

The research process consists of four essential stages: identification, screening, eligibility, and inclusion. These stages are visualised in the PRISMA flowchart shown in Figure 1.

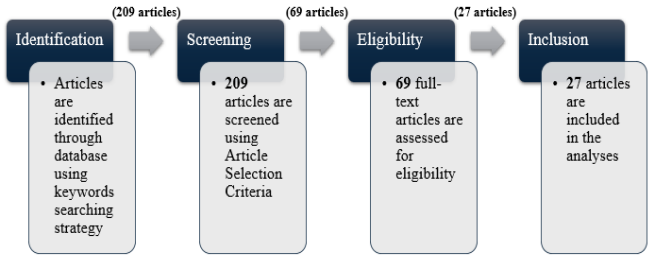

Figure 1. PRISMA 2020 flow diagram

A. Search Strategy

The identification phase began with a comprehensive search across leading academic databases, including Google Scholar, IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect. These databases were selected based on their broad coverage of topics in cryptography and cybersecurity. The initial search query used the Boolean string "post-quantum" AND "certificate verification". This broad query yielded a total of 209 articles published between 2017 and 2025. The timespan was deliberately chosen to capture literature produced during and after the launch of the NIST post-quantum cryptography project in 2017. These initial results encompassed a wide range of publications, many of which discussed quantum cryptographic concepts in general rather than their specific application within certificate-based trust infrastructures.

To refine the results and focus the review on concrete certificate structures, a second-level query was introduced using targeted architectural terms. The revised query was "post-quantum" AND "certificate verification" AND ("pure PQC" OR "hybrid" OR "composite" OR "chameleon" OR "parallel" OR "wrapped") NOT "blockchain". This refinement narrowed the results to 69 articles. The updated query was intended to capture only those papers that explicitly discussed one or more of the certificate types under review. The exclusion of blockchain-oriented results was necessary to remove literature focused on decentralised ledger identity systems, which fall outside the scope of this study's focus on hierarchical and policy-driven trust infrastructures.

In the final eligibility stage, a third filter was applied to identify studies that addressed certificate types aligned with the X.509 format, which remains the dominant standard for public key certificates. The eligibility query was formulated as "X.509" AND the previous Boolean query. After applying this final filter and conducting a full-text review of each remaining article, 27 studies were selected as eligible for synthesis. These studies include architectural proposals, standardisation drafts, deployment case studies, and implementation reports. Each of them discusses the design or operationalisation of post-quantum certificate structures within the context of X.509 or PKI-compatible environments.

The selection process is summarised in the PRISMA 2020 flow diagram presented in Figure 1. This figure illustrates the progressive narrowing of search results from initial identification through screening, eligibility assessment, and final inclusion.

B. Inclusion and Exclusion Criteria

To ensure relevance and academic quality, each study was evaluated using clearly defined inclusion and exclusion criteria. Table I outlines the specific criteria used to determine the relevance, quality, and eligibility of studies for inclusion in the systematic literature review. Criteria were applied during the screening and eligibility phases of the PRISMA workflow to ensure methodological rigor and thematic relevance.

The resulting set of 27 articles reflects the diversity of approaches taken by academic and industry researchers in designing quantum-resistant certificate solutions. The included studies vary in terms of architecture type, cryptographic mechanisms, implementation depth, and protocol compatibility, providing a broad yet focused foundation for synthesis.

TABLE I. INCLUSION AND EXCLUSION CRITERIA

Criterion	Inclusion	Exclusion
Language	Publications written in English	Publications written in languages other than English
Publication Type	Peer-reviewed journal articles, conference proceedings, or technical standards	Unpublished theses, blog posts, patents, grey literature, or non-reviewed sources
Time Period	Published between 2017 and 2025	Published before 2017 or not aligned with post-quantum developments
Domain Relevance	Focused on post-quantum certificates, PKI integration, or trust architecture	Focused solely on cryptographic algorithms or unrelated security models
Certificate Structure	Discusses X.509 certificate formats or compatible chaining mechanisms	Uses non-standard certificate formats or blockchain-specific models
Deployment Orientation	Includes implementation, tooling, or standardisation discussion	Lacks applied focus or real-world deployment context

C. Research Questions

This review is structured around three core research questions, each designed to investigate a different side of post-quantum certificate design, implementation, and integration within PKI systems:

1) RQ1: What certificate architectures have been proposed for integrating post-quantum cryptography into

Public Key Infrastructure systems, and how are they structurally characterised?

This question identifies and categorises the principal models of post-quantum certificates. These models include Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped. It examines how each structure integrates classical and post-quantum cryptographic elements and how these elements are incorporated into certificate chaining, signing, and verification workflows.

2) RQ2: What is the current state of support for post-quantum certificate models in terms of tooling, standardisation efforts, and implementation readiness?

This question assesses the availability and maturity of supporting tools, libraries, and certificate-generation utilities. It also considers compatibility with formal standards from NIST, the Internet Engineering Task Force (IETF), and the European Telecommunications Standards Institute (ETSI).

3) RQ3: What are the key challenges and trade-offs associated with deploying post-quantum certificate models in real-world infrastructures, particularly concerning interoperability, backward compatibility, and scalability?

This question examines implementation challenges and the broader system-level considerations that arise when transitioning from classical to Hybrid or quantum-native certificate models. It includes issues such as certificate size, trust anchor compatibility, protocol negotiation, and integration with legacy systems.

These research questions form the analytical framework for Section III, which presents a comparative synthesis of the selected studies based on certificate structure, ecosystem integration, and deployment feasibility.

III. RESULTS AND DISCUSSION

The final corpus of 27 studies selected for this review reflects a diverse yet thematically convergent body of literature that addresses the structural and operational integration of post-quantum cryptography into certificate-based trust infrastructures. These studies span from 2017 to 2025 and represent contributions from academic researchers, cryptographic standardisation bodies, and practitioners involved in the early deployment of post-quantum certificate prototypes. Collectively, they offer insight into evolving certificate models, their implementation contexts, and the broader challenges associated with quantum-resistant public key infrastructures.

From a thematic perspective, literature can be broadly classified into three categories: (i) architectural proposals and structural models, (ii) tooling ecosystems and implementation frameworks, and (iii) deployment studies and standardisation alignment. While several papers intersect across these domains, most studies maintain a dominant emphasis on one of the three categories. This diversity facilitates a multi-dimensional synthesis, aligning with the research questions posed in Section II (C).

A. Structural Models of Post-Quantum Certificates (RQ1)

The structural integration of PQC algorithms into digital certificate frameworks represents one of the most critical aspects of the migration to quantum-safe infrastructures. In classical PKI, certificates adhere to standardised formats, such as X.509, and are predominantly bound to traditional algorithms, like RSA or ECDSA. However, these algorithms are vulnerable to quantum adversaries, necessitating the development of new certificate architectures that incorporate quantum-resistant primitives while ensuring compatibility, scalability, and trust assurance.

Based on a synthesis of 27 eligible studies published between 2017 and 2025, six distinct structural models have been identified for embedding PQC within certificate workflows: Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped. Each model offers a different architectural trade-off between post-quantum security, implementation complexity, interoperability, and deployment maturity.

1) Pure PQC Certificate: Pure PQC certificates exclusively contain post-quantum algorithms in their key and signature fields. These certificates remove classical algorithms entirely, replacing them with quantum-resistant counterparts such as ML-DSA or SLH-DSA. Structurally, they conform to the X.509 format but adapt the cryptographic primitives and encoding mechanisms to support larger key sizes and signature lengths. Figure 2 illustrates the structural composition of a Pure PQC certificate and highlights the absence of classical cryptographic elements.

Pure PQC certificates offer high assurance against future quantum threats, as they do not rely on any potentially vulnerable legacy algorithms. However, their adoption faces considerable technical barriers. Many client applications, operating systems, and TLS libraries do not yet support quantum-safe algorithms natively, rendering Pure PQC certificates impractical in most production environments [8, 9].

Figure 2. Structure of Pure PQC Certificate

Moreover, the increased size of quantum-safe public keys and signatures can impact latency, memory usage, and handshake performance, particularly in constrained environments such as IoT [10, 11]. Despite these limitations, several experimental implementations and testbeds, such as those based on OpenSSL-pq and liboqs, have validated the feasibility of Pure PQC certificates in isolated networks or pilot deployments [12 13].

2) Hybrid Certificate: Hybrid certificates contain both classical and post-quantum signature algorithms. They are

designed to be verifiable by both classical clients and post-quantum-aware systems, thus enabling a smooth transition period during the global migration to quantum-safe cryptography. Figure 3 depicts the certificate structure which typically includes parallel cryptographic components, allowing independent validation using either classical or post-quantum algorithms.

Figure 3. Structure of Hybrid Certificate

The most common structure involves dual signatures, where one uses a classical algorithm (e.g., RSA or ECDSA) and the other uses a post-quantum algorithm. These signatures may be concatenated or encoded as distinct fields within the X.509 certificate. Hybrid certificates ensure backward compatibility and prevent service disruption for clients that cannot yet process quantum-safe formats [14, 15].

Nevertheless, they raise important concerns related to signature validation ordering, implementation complexity, and the expansion of the attack surface. For example, discrepancies between classical and quantum validation logic may lead to the acceptance of forged certificates in one domain but not another [16]. Despite these challenges, Hybrid certificates remain one of the most practical short-term strategies, especially for applications involving VPNs, TLS, and e-government portals [17, 18].

3) Composite Certificate: Composite certificates combine multiple cryptographic algorithms into a single composite key and composite signature. Unlike Hybrid certificates, which maintain separate cryptographic materials, Composite certificates encapsulate all elements within a unified structure. This design aims to streamline key exchange and certificate validation processes by presenting a unified representation of multiple schemes. Figure 4 illustrates how multiple algorithm components are merged into composite key and signature fields within the certificate.

4) The IETF's LAMPS working group has considered composite formats for X.509 certificates that incorporate both classical and post-quantum components, utilising structured encoding rules. Composite models typically require specialised client-side libraries to parse and validate multi-algorithm keys and signatures [11, 19].

Figure 4. Structure of Composite Certificate

Research has shown that this approach can significantly reduce handshake complexity and transmission overhead compared to the dual-signature structure in Hybrid certificates. However, Composite models remain experimental and are dependent on ongoing efforts and support in libraries such as liboqs and BoringSSL.

5) Chameleon Certificate: Chameleon certificates are adaptive certificate structures that can present different cryptographic identities based on the verifier's capabilities. These certificates utilise a programmable interface to switch between classical and quantum-safe representations, offering maximal compatibility without duplicating cryptographic material. Figure 5 depicts the adaptive behaviour of chameleon certificates, where different cryptographic views may be exposed depending on the verification context.

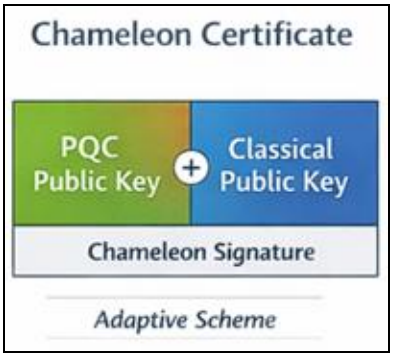

Figure 5. Structure of Chameleon Certificate

Although this architecture remains conceptual mainly, several studies have proposed mechanisms that enable the selective exposure of cryptographic components based on negotiation outcomes in TLS or SSH [20, 21]. The model is particularly attractive for distributed systems and privacy-preserving architectures, where revealing only necessary cryptographic elements may reduce exposure to surveillance and metadata analysis.

Chameleon certificates require highly dynamic trust negotiation protocols and context-aware validation mechanisms, both of which are under development.

6) Parellel Certificate: In the Parallel model, two distinct certificates are issued for the same entity. One uses a classical cryptographic algorithm, and the other one uses a post-quantum scheme. These certificates co-exist in the trust store or are delivered together during a handshake, allowing clients to validate either one based on their cryptographic capabilities. Figure 6 illustrates the parallel issuance and validation paths supported under this model.

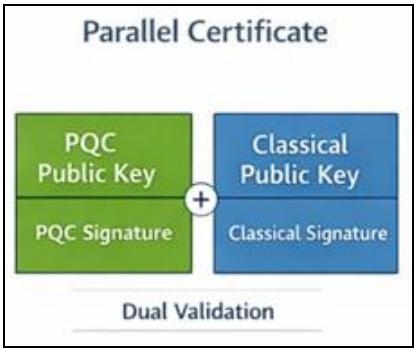

Figure 6. Structure of Parallel Certificate

This architecture simplifies implementation and preserves standard certificate validation logic. However, it increases management overhead, such as maintaining two certificate lifecycles, and can double certificate chain size and complexity in practice [22, 23]. Nevertheless, it has been successfully deployed in experimental IoT and VPN contexts, where device firmware supports dual-chain resolution [24].

7) Wrapped Certificates: Wrapped certificates encapsulate a post-quantum certificate within a classical certificate structure or vice versa. This "certificate-in-certificate" model ensures that classical systems can still recognise and validate the outer certificate while post-quantum-aware systems parse and verify the wrapped payload. Figure 7 shows how the inner certificate is embedded within the outer certificate envelope and processed differently by classical and post-quantum-aware systems.

Figure 7. Structure of Wrapped Certificate

The model enables the transmission of post-quantum content through legacy networks and systems that would otherwise reject unknown certificate formats. Wrapped certificates are currently being investigated for their potential to establish trust in heterogeneous environments, particularly in the telecom, blockchain, and critical infrastructure sectors [25, 26]. Challenges include increased parsing complexity, validation ambiguity, and risks of signature replay or wrapping attacks.

These six structural models represent the core design paradigms under consideration for integrating post-quantum certificates. Table II will provide a comparative overview of their properties, including compatibility, cryptographic strength, implementation status, and deployment readiness. Understanding the trade-offs between these models is critical for stakeholders aiming to design robust, interoperable, and quantum-resilient PKI systems.

B. Integration Challenges and Interoperability Issues (RQ2)

The integration of post-quantum certificates into real-world PKI ecosystems presents a multifaceted set of challenges that extend beyond cryptographic performance. These challenges primarily relate to interoperability, backwards compatibility, tooling maturity, certificate path validation, and regulatory compliance. Despite the availability of NIST-recommended quantum-resistant algorithms, their deployment within the X.509 framework remains constrained by infrastructural, procedural, and protocol-level limitations [16, 19].

1) Compatibility with Existing Infrastructure: A significant obstacle in PQC deployment is the need to maintain interoperability with legacy systems that exclusively support classical cryptography. Many widely used operating systems, TLS libraries, certificate authorities (CAs), and network appliances lack support for post-quantum primitives or multi-algorithm handling. As shown by [14], Hybrid certificates were developed to address this issue by supporting both classical and PQC algorithms in a single X.509 structure. However, such designs increase the complexity of signature verification and expose systems to downgrade attacks where classical components may be preferred by malicious actors [9].

2) Certificate Size and Bandwidth Limitations: Post-quantum signatures and keys are substantially larger than their classical counterparts. For instance, ML-DSA signatures may exceed 2 KB, compared to less than 300 bytes for RSA-2048 or ECDSA. This size inflation affects handshake latency, packet fragmentation, and performance in low-bandwidth or constrained devices. Research by [8] and [10] has demonstrated that TLS handshake times in IoT deployments may double when using PQC-only certificates, necessitating careful optimisation or protocol redesign.

3) Trust Chain Construction and Path Validation: Another key challenge is ensuring that certificate validation chains, including intermediate and root certificates, can be correctly interpreted and trusted by clients with varying cryptographic capabilities. Hybrid and Parallel models offer partial solutions yet introduce operational complexity, as dual chains must be managed, synchronised, and validated. Studies such as those by [23] and [27] have emphasised the difficulty of managing cross-signed certificates and maintaining consistency across hybrid trust hierarchies.

Furthermore, new validation logic is needed to handle Composite and Wrapped certificates, which may not conform to conventional parsing mechanisms. This raise concerns over certificate revocation, expiration, and path building in

heterogeneous environments where classical and quantum nodes co-exist [11].

4) Tooling and Ecosystem Maturity: The current maturity level of post-quantum certificate tooling lags behind the development of the corresponding algorithms. While libraries such as liboqs and BoringSSL have begun incorporating PQC primitives, comprehensive support for certificate generation, revocation, and renewal workflows is still limited [13]. Additionally, certificate transparency logs and auditing frameworks are not yet standardised for quantum-safe extensions, which complicates monitoring and trust auditing.

Open-source implementations remain fragmented, often requiring custom forks or hardcoded adaptations that hinder interoperability testing and third-party certification. Research in [25] notes that most commercial CA platforms do not support PQC integration natively, creating a gap between theoretical readiness and operational deployment.

5) Regulatory and Standardisation Gaps: Ultimately, the lack of unified regulatory guidance for post-quantum PKI migration poses significant risks to compliance. Although NIST has selected key algorithms, formal standards on certificate profiles, validation policies, and trust model definitions are still under development by groups such as the IETF's LAMPS working group and ETSI. Without these standards, vendors face ambiguity regarding acceptable implementation patterns, which can lead to incompatible or proprietary certificate formats [12, 17].

C. Implementation Contexts and Use Cases (RQ3)

The deployment of post-quantum certificate models is highly context-sensitive, shaped by environmental constraints, performance requirements, and trust hierarchies across different domains. While many theoretical designs have been proposed, relatively few have been tested or validated in operational settings. This section synthesises evidence from empirical implementations to identify viable use cases and technical adaptations necessary for deploying post-quantum certificates at scale.

1) IoT and Embedded Systems: The IoT sector presents unique challenges for PQC adoption due to its constraints in processing power, memory, and bandwidth. Despite this, multiple studies have experimented with Hybrid or lightweight Composite certificate models in embedded environments. For example, work in [14] implemented a hybrid TLSv1.3 handshake protocol on Cortex-M4 devices using Wo2lfSSL, combining classical and post-quantum digital signatures to ensure compatibility and forward security. Similarly, work in [28] explored the integration of PQC into machine-to-machine (M2M) communications within industrial cyber-physical systems, demonstrating the feasibility of secure handshakes under constrained conditions.

Research in [29] further extended this line of inquiry into three-layer IoT architectures, using Hybrid certificates for authentication and integrity protection. These studies collectively affirm that, while key size and handshake latency remain significant concerns, careful selection of certificate structure (particularly Hybrid and Composite models) can mitigate most constraints in low-resource IoT deployments.

2) Automotive and Vehicular Communication Systems: Secure certificate management in vehicular networks, such as V2V and V2I systems, is critical for safety and data authenticity. Research in [25] developed qSCMS, a credential management system tailored to vehicular communications, integrating PQC algorithms into the automotive Public Key Infrastructure. More recently, research in [17] conducted a national-level audit of public key cryptographic usage in the U.S. electric vehicle charging infrastructure, highlighting the urgency for standardised post-quantum certificate solutions due to the long lifespan of deployed vehicle hardware.

These studies suggest that Parallel and Wrapped certificate models are particularly suitable for automotive systems, where fielded devices may lack upgrade paths. Wrapped certificates can encapsulate post-quantum credentials while remaining compatible with classical PKI validators in existing Electronic Control Units (ECUs).

3) VPNs, Secure Tunnels, and Enterprise Environments: The enterprise context, particularly in the realm of Virtual Private Networks (VPNs), has seen some of the earliest experimental deployments of PQC-enabled certificates. Research in [9] introduced PQConnect, an end-to-end VPN tunnel architecture leveraging quantum-resistant signatures and key exchanges. Research in [26] later analysed PQConnect's performance, revealing that Hybrid models offered the best trade-offs in security and deployment ease.

Likewise, research in [18] implemented a quantum-safe VPN prototype using post-quantum TLS certificates. The results emphasised that backwards-compatible certificate formats, specifically Hybrid and Composite, enable seamless integration with commercial VPN clients and server-side infrastructure.

4) Cloud Services and Scalable Trust Models: Post-quantum certificates are also being piloted in large-scale cloud platforms and distributed identity systems. Research in [13] explored how virtual HSMs (Hardware Security Modules) and PKI orchestration tools can support the secure issuance and management of quantum-safe certificates in cloud-native deployments. Their implementation integrated virtualised trust anchors, certificate lifecycle management, and certificate transparency logging.

Parallel and Composite models were favoured in this context due to their compatibility with microservices architecture and multi-tenant environments. Furthermore, the inclusion of programmable APIs for trust negotiation, similar to those proposed in the Chameleon model, was found to be critical for enabling quantum awareness in trust delegation protocols [20].

D. Comparative Analysis of Certificate Architecture

To provide a comprehensive evaluation of post-quantum certificate models, this subsection consolidates key findings through two complementary comparative tables. The first comparison (Table II) presents the structural and technical attributes of each model, while the second (Table III) assesses the domain-specific suitability for deployment and operational implications. This dual-framework analysis supports both theoretical reflection and practical decision-making in the design of post-quantum PKI.

1) Technical Attributes and Design Trade-offs: Table II presents a multi-dimensional comparison of six certificate models: Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped across five critical dimensions: cryptographic strength, legacy compatibility, tooling support, validation complexity, and implementation readiness.

The Pure PQC model stands out for its cryptographic assurance, being built exclusively on post-quantum primitives. However, its lack of support for legacy systems and minimal toolchain integration limits its deployability. The Hybrid model, which integrates both classical and quantum-safe algorithms, achieves high toolchain maturity and full backward compatibility, making it the most production-ready approach. Composite and Wrapped models offer robust multi-algorithmic security but at the expense of high structural complexity and specialised validation processes.

The Chameleon model, although innovative in adapting to dynamic cryptographic environments, remains experimental mainly due to its low maturity and fragmented implementation. Parallel certificates, which facilitate co-validation through multiple certificate chains, offer broad compatibility and resilience but require careful orchestration and increase lifecycle management overhead.

This comparative insight emphasises that no single model satisfies all technical criteria simultaneously. Trade-offs must be assessed in consideration of infrastructure constraints, regulatory requirements, and long-term migration objectives.

TABLE II. COMPARATIVE CHARACTERISTICS OF CERTIFICATE MODELS

Model	**Cryptographic Strength**	**Legacy Compatibility**	**Tooling Support**	**Validation Complexity**	**Implementation Readiness**
Pure PQC	High [16, 12]	Low [16, 19]	Low [1, 19]	Low [1]	Low [5, 14]
Hybrid	Moderate [14, 10]	High [14, 10]	High [14, 10]	Moderate [14, 10]	High [28, 12]
Composite	High [8, 17]	Moderate [8, 17]	Moderate [8, 17]	High [8, 17]	Moderate [8, 17]
Chameleon	High [19, 23]	Moderate [19, 23]	Low [19, 23]	High [19, 23]	Low [19, 23]
Parallel	Moderate [28, 18]	High [28, 18]	Moderate [28, 18]	Moderate [28, 18]	Moderate [28, 18]
Wrapped	High [22, 27]	High [22, 27]	Moderate [22, 27]	High [22, 27]	Moderate [22, 27]

TABLE III. SUITABILITY MATRIX OF CERTIFICATE MODELS

Model	**TLS Support**	**IoT Deployment**	**Vehicular Systems**	**Lifecycle Complexity**	**Backward Compatibility**
Pure PQC	Limited [16, 14]	Low [16, 19]	Low [16, 19]	Low [16]	None [16]
Hybrid	Supported [14, 10, 9]	Moderate [14, 10]	Moderate [14, 10]	Moderate [14, 10]	Full [14, 10]
Composite	Partial [8, 17]	Low [8, 17]	Moderate [8, 17]	High [8, 17]	Partial [8, 17]
Chameleon	Experimental [28, 23]	Low [19, 23]	Low [19, 23]	High [19, 23]	Partial [19, 23]
Parallel	Supported [28, 18]	High [28, 18]	High [28, 18]	Moderate [28, 18]	High [28, 18]
Wrapped	Partial [22, 27]	High [22, 27]	High [22, 27]	High [22, 27]	High [22, 27]

2) Suitability Across Deployment Contexts: Building on the technical analysis, Table III evaluates each certificate model's practical suitability across five prominent domains: TLS support, IoT deployment, vehicular systems, lifecycle complexity, and backward compatibility.

The Hybrid model emerges as the most versatile, with high suitability across all domains due to its dual-stack compatibility and widespread implementation experience. In contrast, higher lifecycle complexity of Composite and Wrapped models may limit their adoption in resource-constrained settings. Parallel certificates show potential in automotive and industrial IoT contexts, where long-term trust anchors must co-exist with evolving cryptographic standards.

The Pure PQC model, despite being theoretically ideal, is currently limited to experimental or isolated deployments due to the immaturity of its tooling. Chameleon certificates, although conceptually compelling, face deployment constraints tied to policy variability and ambiguity in validation.

This synthesis of technical properties and real-world applicability provides a holistic understanding of the operational landscape for post-quantum certificate deployment. It offers guidance for selecting architecture that best aligns with an organisation's infrastructure readiness, trust requirements, and cryptographic roadmap.

IV. RECOMMENDATION AND FUTURE WORK

This review has identified the current strengths and weaknesses of post-quantum certificate models. To support both practitioners and researchers, this section outlines strategic guidance for deployment and highlights areas where further study is essential.

E. Practical Recommendations

1) Use Hybrid Models for Smooth Migration: Hybrid certificates are currently the most suitable for real-world deployment. They strike a balance between quantum resistance and backwards compatibility, making them ideal for gradual upgrades in enterprise systems, government infrastructure, and web services [9, 14].

2) Apply Parallel or Wrapped Models in Long-Lifecycle Systems: In sectors such as automotive, industrial IoT, and energy, systems must remain operational for many years. Parallel and Wrapped models provide resilience and compatibility, ensuring long-term trust without requiring frequent updates [8, 30].

3) Avoid Pure PQC in Production Environments: Although Pure PQC certificates offer strong security, they are not yet practical in production environments. The lack of supporting tools, standard validation methods, and interoperability limits their use in experimental deployments and testbeds [16].

4) Invest in Tooling and Policy Support for Complex Models: Certificate types such as Composite, Chameleon, and Wrapped introduce operational challenges. Successful deployment will require automated lifecycle tools, clear validation rules, and updated certificate policies [19, 31].

F. Future Research Directions

While this review has mapped six distinct certificate models, several open research avenues remain, each tied to the uniques challenges of these models.

1) Pure PQC Certificate: This model represents the long-term vision of "quantum-native" infrastructures. NIST-related studies [5, 18] have shown their theoretical strength, but future research must evaluate scalability, performance, and standardisation readiness.

2) Hybrid Certificate: This is the most deployment-ready, yet they require large-scale benchmarking in real-world infrastructures such as TLS and VPNs. Prior prototypes [2, 12] have demonstrated feasibility, but systematic performance studies on latency, handshake duration, and scalability are still lacking.

3) Composite Certificate: This model is efficient in design, but their multi-algorithm structure complicates validation. Existing work in [27, 28] has highlighted interoperability challenges, underscoring the urgent need for standardised validation frameworks across toolchains.

4) Chameleon Certificate: This model is innovative due to their adaptive behaviour, yet this flexibility risks downgrading vulnerabilities. Future work should therefore prioritise protocol-level validation and negotiation standards [14, 25].

*5) Parallel Certificate***:** This model is promising for IoT and vehicular systems with long lifecycles. However, their reliance on dual certificates increases overhead in storage and renewal. Studies in [19, 31] suggest the need for certificate lifecycle management strategies tailored to constrained environments.

6) Wrapped Certificate: This model supports legacy integration but introduces parsing and validation complexity. Research should focus on improving toolchain support and defining regulatory profiles to ensure acceptance in practice [17, 30].

In summary, Hybrid model is closest to deployment but needs large-scale benchmarking. Composite and Chameleon models most urgently require standardised validation. Parallel and Wrapped models call for improvements in tooling and lifecycle management, while Pure PQC model remains a long-term research priority for quantum-native infrastructures.

V. CONCLUSIONS

This systematic literature review explored the development and integration of post-quantum certificate models between 2017 and 2025, a period marked by global efforts to prepare cryptographic infrastructure for the emergence of large-scale quantum computing. While cryptographic algorithms such as ML-KEM and ML-DSA have advanced through NIST's standardisation process, embedding these primitives into operational PKI systems, particularly those reliant on the X.509 standard, remains a complex and underdeveloped challenge.

Six certificate models were identified and analysed: Pure PQC, Hybrid, Composite, Chameleon, Parallel, and Wrapped. Each model represents a distinct approach to integrating post-quantum security into the X.509 certificate structure, which serves as the foundation for authentication, encryption, and trust validation in protocols such as TLS. The review indicates that while Hybrid models are currently the most viable due to their backwards compatibility and tooling support, other models offer stronger quantum resistance but require significant changes in lifecycle management, trust anchor configuration, and validation logic.

A key insight from this review is that a secure transition to post-quantum PKI is not solely a cryptographic problem. It requires coordinated advancements in certificate validation standards, toolchain support for complex multi-algorithm formats, and integration into widely deployed X.509-based ecosystems such as TLS, VPNs, and secure messaging platforms. Without such alignment, even the strongest algorithms may fail to deliver meaningful security on a scale.

By consolidating fragmented academic and technical insights, this study provides a foundation for guiding future implementations of post-quantum certificates. Continued research is needed to standardise hybrid and multi-signature validation methods, extend X.509 profiles, and ensure performance, interoperability, and trust across evolving PKI environments.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

ACKNOWLEDGEMENT

This research was funded by the Ministry of Higher Education (MOHE) of Malaysia under the Fundamental Research Grants Scheme (FRGS/1/2024/ICT07/USIM/02/1). Thank you to Cybersecurity Malaysia for additional support.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997, doi: 10.1137/S0097539795293172.

[2] National Institute of Standards and Technology, "Post-Quantum Cryptography: Call for Proposals," 2017. [Online]. Available:

https://csrc.nist.gov/Projects/post-quantum-cryptography, *Accessed: 14 May 2025.*
[3] National Institute of Standards and Technology, "Post-Quantum Cryptography: Selected Algorithms," 2024. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms, *Accessed: 14 May 2025.*
[4] L. Chen *et al.*, "Report on Post-Quantum Cryptography," NISTIR 8105, National Institute of Standards and Technology, 2016, doi: 10.6028/NIST.IR.8105.
[5] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021, doi: 10.1136/bmj.n71.
[6] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, and M. Daud, "Systematic literature review: Trend analysis on the design of lightweight block cipher," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 5, p. 101550, 2023, doi: 10.1016/j.jksuci.2023.04.003.
[7] R. Radzali, A. H. Azni, F. H. M. Ridzuan, N. H. Zakaria, and T. Ali, "Analysis of trust models in public key infrastructure: A systematic literature review of interoperability challenges," Malays. J. Sci. Health Technol., vol. 11, no. 1, Feb. 2025, doi: 10.33102/mjosht.v11i1.465.
[8] N. Ricchizzi, C. Schwinne, and J. Pelzl, "Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments," *arXiv preprint*, arXiv:2505.04333, 2025.
[9] D. J. Bernstein *et al.*, "PQConnect: Automated Post-Quantum End-to-End Tunnels," *Cryptology ePrint Archive*, 2024.
[10] E. Kupcova, J. Simko, M. Pleva, and M. Drutarovsky, "Experimental Framework for Secure Post-Quantum TLS Client-Server Communication," in *Proc. Int. Symp. ELMAR*, 2024, pp. 213–216.
[11] S. Paul, F. Schick, and J. Seedorf, "TPM-based post-quantum cryptography: A case study on quantum-resistant and mutually authenticated TLS for IoT environments," in *Proc. 16th Int. Conf. Availability, Reliability and Security*, 2021, pp. 1–10.
[12] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure," in *Post-Quantum Cryptography: PQCrypto 2017*, Springer, 2017, pp. 384–405.
[13] A. Loconsolo, "Securing digital identities: From the deployment to the analysis of a PKI ecosystem with virtual HSMs leveraging open-source tools," Ph.D. dissertation, Politecnico di Torino, Italy, 2024.
[14] M. Anastasova, R. Azarderakhsh, and M. M. Kermani, "Fully Hybrid TLSv1.3 in WolfSSL on Cortex-M4," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Security*, 2024, pp. 376–395.
[15] D. Stebila, M. Campagna, and L. Chen, "Post-quantum key exchange for the Internet and the Open Quantum Safe project," Proc. IEEE, vol. 108, no. 10, pp. 1780–1802, Oct. 2020, doi: 10.1109/JPROC.2020.3008703.
[16] N. Bindel and S. McCarthy, "The need for being explicit: Failed attempts to construct implicit certificates from lattices," *Comput. J.*, vol. 66, no. 6, pp. 1320–1334, 2023.
[17] T. E. Carroll, L. M. Redington, A. M. Moran-Schmoker, and A. J. Murray, "Inventory of Public Key Cryptography in US Electric Vehicle Charging," Pacific Northwest National Laboratory (PNNL), 2023.
[18] K. Krishan, "Implementation of quantum-safe VPN," M.S. thesis, Faculty of Informatics, Masaryk Univ., Brno, Czech Republic, 2025.
[19] G. D'Onghia, D. G. Berbecaru, and A. Lioy, "Shaping a Quantum-Resistant Future: Strategies for Post-Quantum PKI," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2024, pp. 1–6.
[20] D. Berger, M. Lemoudden, and W. J. Buchanan, "Post-Quantum Migration of the Tor Application," *J. Cybersecurity Privacy*, vol. 5, no. 2, p. 13, 2025.
[21] W. Yang, X. Li, Z. Feng, and J. Hao, "TLSsem: A TLS security-enhanced mechanism against MITM attacks in public WiFis," in *Proc. 22nd Int. Conf. Eng. Complex Comput. Syst. (ICECCS)*, 2017, pp. 30–39.
[22] L. P. Fraile *et al.*, "Enabling Quantum-Resistant EDHOC: Design and Performance Evaluation," *IEEE Access*, 2025.
[23] Q. Khan *et al.*, "Toward Post-Quantum Digital Certificate for eSIM," in *Proc. Silicon Valley Cybersecurity Conf. (SVCC)*, 2024, pp. 1–3.
[24] S. Sunahara *et al.*, "A Framework for Institutional Privacy Considered Full DNS over HTTPS Architecture," *IEEE Access*, 2025.
[25] J. E. R. F. de Oliveira, "qSCMS: Post-quantum security credential management system for vehicular communications," Ph.D. dissertation, Univ. São Paulo, Brazil, 2019.
[26] T. Waseem, "Analysis of PQConnect," Master dissertation, Tampere University, Finland, 2025.
[27] H. Kwon, "Secure and Scalable Device Attestation Protocol with Aggregate Signature," *Symmetry*, vol. 17, no. 5, p. 698, 2025.
[28] S. Paul, P. Scheible, and F. Wiemer, "Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication," *J. Comput. Security*, vol. 30, no. 4, pp. 623–653, 2022.
[29] J. Samandari and C. Gritti, "Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures," in *Proc. Int. Conf. Privacy, Security and Trust (PST)*, 2024, pp. 1–11.
[30] G. Kornaros, G. Berki, and M. Grammatikakis, "Quantum-secure communication for trusted edge computing with IoT devices," in *Proc. IFIP Int. Conf. ICT Syst. Security and Privacy Protection*, 2023, pp. 163–176.
[31] J. Stapleton and W. C. Epstein, *Security Without Obscurity: A Guide to PKI Operations*. Boca Raton, FL, USA: CRC Press, 2024.