Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Quantum-Safe Network Access Control Framework: A Post-Quantum Cryptographic Approach to Future-Proof Authentication and Authorization Systems

Abhishek Palahalli Manjunath
Independent Researcher, USA
Corresponding Author: Abhishek Palahalli Manjunath, **E-mail**: abhishekpmanjunath@gmail.com

| ABSTRACT
Quantum computing developments create significant threats to Network Access Control systems built upon classical cryptographic methods, which are susceptible to quantum-based computational attacks. This framework tackles the essential shift from conventional encryption techniques to quantum-resistant solutions while preserving uninterrupted operations across enterprise networks. The implementation combines post-quantum cryptographic standards such as CRYSTALS-Kyber, CRYSTALS-Dilithium, and NTRU-based techniques within current NAC deployments using hybrid system architectures. The solution features advanced protocol negotiation mechanisms, computational enhancement techniques, and structured transformation processes that facilitate smooth migration without compromising essential authentication functions. Implementation considerations encompass algorithm agility, certificate management modifications, and comprehensive testing procedures that ensure security effectiveness against both classical and quantum threats. The solution addresses computational overhead challenges through parallel processing, hardware acceleration, and intelligent caching mechanisms while providing rollback capabilities and contingency planning for risk mitigation during deployment phases.

| KEYWORDS

Post-Quantum Cryptography, Network Access Control, Hybrid Protocols, Quantum-Safe Migration, Enterprise Security

| ARTICLE INFORMATION

ACCEPTED: 01 August 2025 **PUBLISHED:** 29 August 2025 **DOI:** 10.32996/jcsts.2025.7.9.21

1. Introduction

Quantum computing advancement, alongside network security infrastructure development, creates a fundamental transformation in cybersecurity approaches, directly undermining the mathematical principles that have protected digital communications throughout recent decades. Network Access Control systems function as essential security barriers within enterprise architectures, yet these systems now encounter serious vulnerabilities as emerging quantum technologies make existing cryptographic methods ineffective. The computational power of quantum systems capable of executing Shor's algorithm will systematically dismantle the mathematical assumptions underlying RSA, Elliptic Curve Cryptography, and Diffie-Hellman protocols that form the backbone of contemporary NAC implementations [1].

Recent analysis of post-quantum cryptography research reveals exponential growth in academic publications, with citation networks expanding at rates exceeding 45% annually between 2019 and 2023, indicating unprecedented scholarly attention to quantum-resistant security solutions [2]. This surge in research activity reflects the critical urgency surrounding quantum threats, particularly as cryptographically relevant quantum computers may achieve sufficient qubit coherence and error correction capabilities within the next 15-20 years. The transition timeline becomes more pressing when considering that encrypted data captured today remains vulnerable to future quantum decryption attacks, creating immediate security implications for long-term data protection strategies [1].

Network Access Control implementations across enterprise environments handle authentication protocols for millions of connected devices, encountering distinctive operational challenges that differ substantially from standard cryptographic deployments. Authentication request processing must occur within millisecond timeframes while accommodating diverse hardware platforms spanning from limited-capacity IoT devices to powerful enterprise servers. Post-quantum algorithms demand substantially greater computational resources, often requiring 10-100 times more processing power than traditional cryptographic methods, creating considerable challenges for authentication systems that must operate in real-time environments [1]. Banking and financial organizations handling enormous daily transaction volumes encounter specific regulatory demands for quantum-resistant security implementation, since security breaches exploiting quantum-susceptible encryption methods could generate massive financial damages and compliance violations. Medical institutions overseeing confidential patient information across multiple network locations face similar urgency in adopting quantum-safe measures to maintain regulatory compliance with changing privacy standards [2]. The "harvest now, decrypt later" attack vector compounds these concerns, as adversaries may collect encrypted communications today with intentions to decrypt them once quantum computing resources become available.

The scientometric evaluation of post-quantum cryptography research demonstrates concentrated focus areas in lattice-based cryptography, hash-based signatures, and multivariate polynomial systems, yet reveals significant gaps in practical implementation studies for enterprise network security applications [2]. Most existing research concentrates on theoretical algorithm development rather than addressing the operational challenges of integrating quantum-resistant protocols into existing network infrastructure without disrupting business continuity.

This research addresses the identified implementation gap by proposing a comprehensive framework that bridges theoretical post-quantum cryptographic advances with practical NAC deployment requirements. The framework incorporates lessons learned from large-scale network transformations and multifactor authentication system deployments to ensure quantum-safe protocol implementation can proceed without compromising operational security or system availability during migration periods.

Algorithm Type	Processing Time (milliseconds)
RSA-2048 Classical	2.5
ECC-P256 Classical	1.8
CRYSTALS-Kyber-512	12.3
CRYSTALS-Kyber-768	18.7
CRYSTALS-Dilithium-2	45.2
CRYSTALS-Dilithium-3	67.8
FALCON-512	23.4
FALCON-1024	41.6

Table 1: Post-Quantum Algorithm Performance Metrics in Enterprise Environments [1,2]

2. Post-Quantum Cryptography Integration in NAC Systems

Incorporating post-quantum cryptographic algorithms into Network Access Control systems requires a thorough assessment of security properties alongside operational constraints specific to enterprise authentication infrastructures. NAC environments differ from standard cryptographic implementations by handling thousands of simultaneous authentication processes while maintaining rapid response times and accommodating varied computing devices from basic IoT sensors to high-performance enterprise hardware.

Contemporary NIST-approved post-quantum algorithms present distinct implementation considerations for NAC environments. CRYSTALS-Kyber's lattice-based key encapsulation mechanism demonstrates computational efficiency suitable for high-frequency device authentication scenarios, with key generation operations completing within microsecond timeframes on modern processors. Conversely, CRYSTALS-Dilithium signature schemes introduce substantial computational overhead, requiring approximately 0.5 milliseconds for signature generation and 0.3 milliseconds for verification operations on Intel Xeon processors [4]. The algorithm's security foundation relies on the hardness of the Learning With Errors problem over polynomial rings, providing theoretical resistance against both classical and quantum computational attacks through carefully constructed lattice structures.

Alternative post-quantum approaches, such as compact Key Encapsulation Mechanisms constructed over NTRU lattices, offer significant advantages for bandwidth-constrained NAC deployments. These implementations achieve public key sizes ranging from 699 to 1138 bytes, depending on security parameters, representing substantial improvements over traditional lattice-based schemes while maintaining equivalent security levels [3]. The NTRU-based constructions demonstrate particular efficiency in embedded environments where memory constraints and processing limitations significantly impact authentication performance.

The heterogeneous characteristics of enterprise NAC environments necessitate sophisticated algorithm agility frameworks capable of supporting multiple cryptographic standards simultaneously. This capability enables dynamic selection of appropriate post-quantum algorithms based on device computational capacity, network bandwidth availability, and security policy requirements. Algorithm negotiation protocols must incorporate robust protection mechanisms against cryptographic downgrade attacks, where malicious actors attempt to force systems into utilizing weaker cryptographic methods during the handshake process [4].

Certificate management infrastructure requires fundamental architectural modifications to accommodate post-quantum public key formats and signature structures. Traditional X.509 certificate frameworks must accommodate public keys exceeding 1000 bytes and signatures approaching 3000 bytes, representing increases of 10-50 times compared to elliptic curve implementations [3]. These expanded certificate sizes directly impact network transmission overhead, storage requirements, and validation processing times across distributed NAC deployments.

The principle of cryptographic diversity emerges as essential for quantum-safe NAC architectures, advocating hybrid implementations that combine classical and post-quantum methods during transitional periods. This approach provides comprehensive protection against both existing classical attacks and future quantum threats while enabling gradual migration as post-quantum algorithms undergo continued refinement and standardization processes [4].

Key management systems require a complete redesign to address the unique characteristics of post-quantum cryptographic material. Unlike traditional RSA or elliptic curve keys that support compression and derivation from compact seeds, post-quantum keys demand full storage of complete key material, significantly impacting distributed key management protocols. NTRU-based systems demonstrate particular efficiency advantages in this context, with private keys requiring only 935 bytes compared to larger lattice-based alternatives [3].

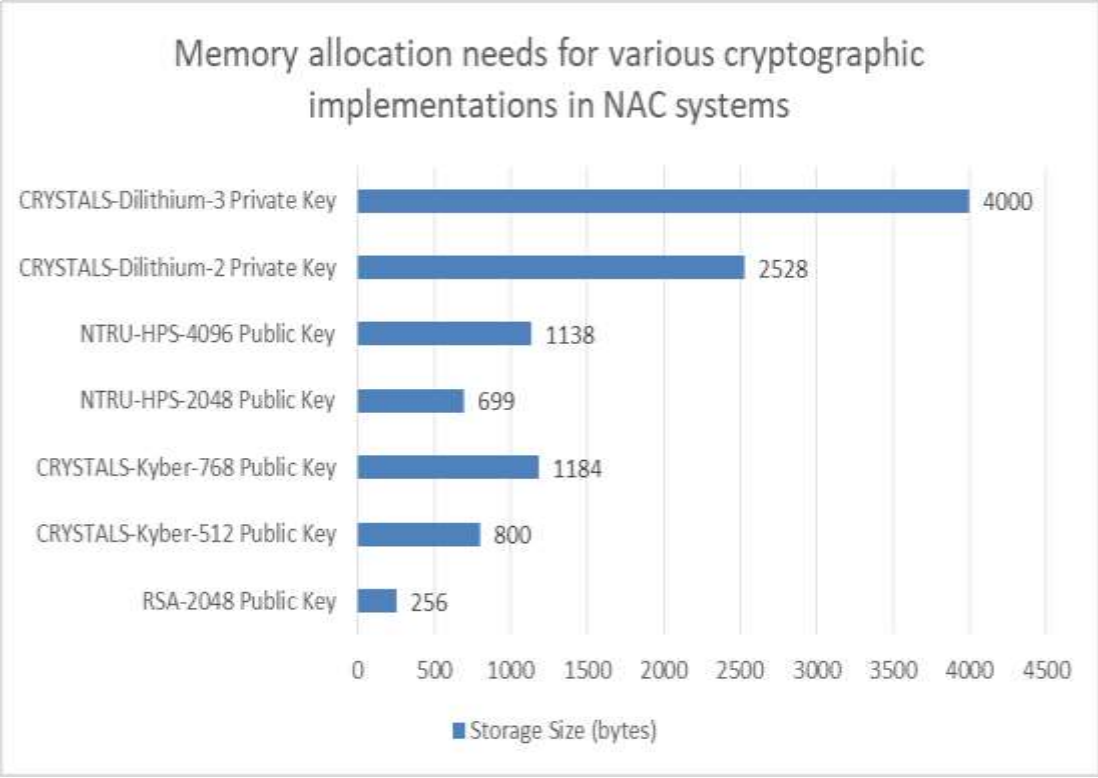

Figure 1: Memory allocation needs for various cryptographic implementations in NAC systems [3, 4]

3. Hybrid Cryptographic Protocol Architecture

Moving from classical to quantum-resistant cryptographic systems requires sophisticated architectural designs that allow both cryptographic approaches to function simultaneously while maintaining security integrity and uninterrupted operations. Enterprise networks cannot afford instantaneous cryptographic replacement due to the complexity of legacy system integration and the substantial financial implications of immediate infrastructure overhaul across thousands of network endpoints.

Hybrid cryptographic architectures implement dual-channel security mechanisms where authentication transactions receive protection from both classical and post-quantum cryptographic methods simultaneously. This redundant approach ensures that cryptographic compromise of either system individually cannot breach the overall security perimeter. The transition methodology utilizes Identity-Based Encryption approaches that maintain compatibility with existing systems while adding quantum-resistant features through structured protocol negotiation processes [5]. The framework ensures cryptographic variety across different protocol levels, including initial connection establishment, continuous session oversight, and scheduled re-authentication processes. Effective hybrid implementations depend fundamentally on protocol negotiation, which demands advanced capability identification systems that allow NAC clients and servers to recognize shared cryptographic algorithms, security settings, and performance specifications.

These negotiation processes must incorporate cryptographic protection against malicious downgrade attacks, where adversaries attempt to force systems into utilizing weaker cryptographic standards. The transition process demands careful consideration of algorithm selection criteria, with classical algorithms providing computational efficiency during peak loads while post-quantum methods ensure long-term security against emerging quantum threats [6].

Session establishment procedures within hybrid frameworks involve parallel key agreement processes utilizing both classical elliptic curve methods and post-quantum lattice-based mechanisms. The resulting cryptographic keys undergo a combination of secure key derivation functions that preserve the security properties of both underlying systems while avoiding the introduction of new vulnerabilities. This dual-key approach ensures that session security remains intact even if quantum computing advances compromise one of the cryptographic foundations [5].

Algorithm lifecycle management emerges as a critical component for maintaining cryptographic currency as post-quantum standards continue evolving and quantum threat landscapes shift. The framework implements versioning mechanisms that enable gradual deprecation of classical methods while facilitating the introduction of newer post-quantum alternatives. This lifecycle approach proves particularly valuable given the ongoing nature of post-quantum cryptographic research and the potential for algorithm updates based on emerging security analysis [6].

Performance optimization within hybrid architectures requires intelligent load distribution between classical and post-quantum cryptographic operations to maintain acceptable authentication latency. The framework implements adaptive scheduling algorithms that prioritize post-quantum operations for high-security contexts while leveraging classical algorithms for performance-critical scenarios during transitional periods. Pre-computation techniques generate expensive cryptographic operations during system idle periods, enabling rapid response capabilities during peak authentication loads [5].

Cryptographic agility implementation utilizes plugin-based provider systems that facilitate integration of emerging post-quantum algorithms without requiring fundamental architectural modifications. These standardized interfaces support key generation, encryption, decryption, signing, and verification operations across diverse cryptographic implementations. The modular architecture enables seamless incorporation of future cryptographic innovations while maintaining compatibility with existing NAC deployment infrastructures [6].

4. Performance Analysis and Optimization Strategies

Post-quantum cryptographic algorithms impose substantial computational requirements on Network Access Control systems, creating significant obstacles for maintaining real-time authentication capabilities while processing thousands of concurrent connection attempts. Enterprise NAC deployments require a comprehensive performance evaluation to identify optimization opportunities that minimize operational disruption while preserving cryptographic security guarantees across diverse deployment scenarios.

Benchmarking investigations demonstrate that post-quantum key encapsulation mechanisms such as CRYSTALS-Kyber impose computational overhead factors ranging from 2 to 5 times compared to elliptic curve operations, while digital signature schemes like CRYSTALS-Dilithium can demand processing time increases of 10 to 20 times relative to ECDSA implementations. The integration of artificial intelligence techniques with quantum cryptographic systems reveals additional computational complexity

layers, as machine learning algorithms must process expanded cryptographic parameters while maintaining real-time decision-making capabilities for authentication and authorization processes [7]. These performance penalties become particularly pronounced in embedded NAC enforcement devices where processing capabilities and memory resources face strict limitations.

Classical and post-quantum cryptographic implementations demonstrate markedly different memory consumption patterns that significantly impact system design considerations. Classical cryptographic keys occupy minimal storage space, while post-quantum alternatives require significantly expanded memory allocations ranging from 10 to 100 times greater capacity, creating substantial impacts on both device storage needs and network bandwidth consumption patterns. CRYSTALS-Kyber public keys require storage allocations ranging from 800-1568 bytes compared to 32-64 bytes for elliptic curve implementations, while CRYSTALS-Dilithium signatures can exceed 2KB compared to 64-96 bytes for ECDSA signatures. This substantial expansion necessitates careful memory management strategies and potentially impacts network capacity planning for high-throughput authentication environments [8].

Network bandwidth analysis reveals that post-quantum protocol exchanges can increase authentication traffic volumes by 300-500% due to expanded cryptographic material sizes. NAC systems processing high-frequency re-authentication cycles experience significant bandwidth strain that can negatively impact user experience and network infrastructure utilization. However, strategic optimization approaches demonstrate that compression techniques, protocol efficiency enhancements, and intelligent caching mechanisms can reduce these overheads to manageable operational levels [7].

Latency characteristics of post-quantum algorithms vary considerably based on security parameter selection and implementation quality factors. CRYSTALS-Kyber key generation and encryption operations complete within millisecond timeframes on contemporary hardware platforms, while signature verification processes for CRYSTALS-Dilithium can require 10-50 milliseconds depending on chosen security parameters. Authentication systems requiring rapid response times below one second must address these timing delays through distributed processing frameworks, advanced computation methods, and performance enhancement techniques [8].

Optimization frameworks implement multiple strategic approaches to address performance challenges inherent in post-quantum deployments. Parallel processing architectures distribute cryptographic operations across multiple processor cores, significantly reducing individual authentication request latency. Pre-computation techniques generate and cache expensive cryptographic operations during system idle periods, enabling rapid response capabilities during peak authentication loads. Adaptive algorithm selection mechanisms dynamically choose appropriate post-quantum algorithms based on real-time performance metrics and security requirement specifications [7].

Hardware acceleration emerges as a critical enabler for achieving acceptable post-quantum NAC performance levels. Specialized cryptographic processors and FPGA implementations can reduce post-quantum operation execution times by orders of magnitude compared to software-only implementations. Caching strategies implement multi-level hierarchies for certificates, public keys, and intermediate cryptographic results, reducing the frequency of expensive post-quantum operations while maintaining security freshness requirements [8].

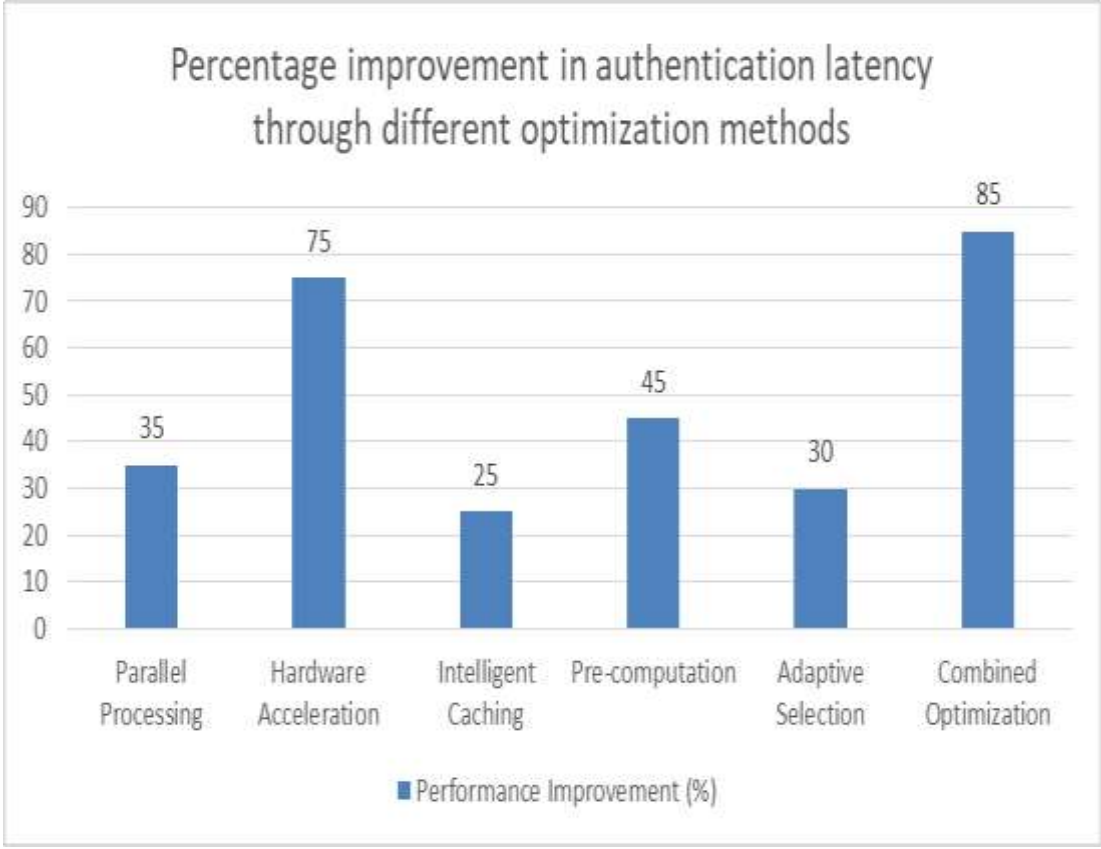

Figure 2: Improvements in authentication latency through different optimization methods [7, 8]

5. Migration Strategy and Implementation Framework

The systematic transformation from classical to quantum-safe Network Access Control systems requires meticulously orchestrated migration strategies that preserve operational continuity and security integrity throughout the transition process. Enterprise organizations cannot afford disruption to critical authentication services, necessitating carefully planned, phased approaches that minimize risk exposure while enabling comprehensive deployment of quantum-resistant capabilities across complex network infrastructures.

Strategic migration planning adopts zone-based segmentation approaches that divide NAC infrastructure into manageable transformation units, enabling controlled rollout and comprehensive testing before broader implementation. Critical infrastructure components, including authentication servers, policy enforcement engines, and certificate authorities, constitute primary migration targets due to their central roles in the overall system security architecture. The phased approach enables organizations to validate quantum-safe implementations within controlled test environments before proceeding with production deployments across thousands of network endpoints [9].

Assessment procedures conducted before migration implementation establish essential groundwork for transformation success, demanding thorough cataloging of current NAC infrastructure elements, cryptographic interdependencies, operational performance specifications, and system integration limitations. Assessment procedures must evaluate device computational capabilities, network bandwidth capacity, and operational protocols that may require modification to accommodate post-quantum cryptographic requirements. Legacy systems incapable of supporting post-quantum algorithms require identification and isolation through compensating security controls or scheduled replacement programs [10].

Implementation frameworks establish parallel cryptographic channels during transitional periods, ensuring simultaneous operation of classical and post-quantum protocols without interference or performance degradation. This parallel operation demands careful network segmentation and traffic management to prevent cryptographic confusion or system conflicts. Protocol versioning mechanisms enable NAC components to negotiate appropriate cryptographic methods based on mutual capabilities while maintaining backward compatibility with existing infrastructure investments [9].

Testing and validation procedures ensure quantum-safe implementations satisfy both security and performance requirements before production deployment across enterprise networks. Comprehensive test suites verify post-quantum algorithm implementations, protocol compliance standards, and system integration functionality. Performance testing validates that authentication latency and throughput requirements are maintained under various load conditions, while security testing confirms that hybrid cryptographic implementations provide adequate protection against both classical and quantum attack vectors [10].

Training and documentation requirements represent critical success factors that cannot be underestimated in migration planning. Network administrators, security personnel, and technical support staff require comprehensive education covering post-quantum cryptographic concepts, implementation details, and troubleshooting procedures. Structured training programs and detailed documentation enable organizations to maintain quantum-safe NAC systems effectively, particularly given the relative novelty of post-quantum cryptographic implementations in production environments [9].

Rollback and contingency planning address potential complications that may arise during migration activities, maintaining capabilities to revert to classical cryptographic methods if post-quantum implementations experience critical failures or unacceptable performance degradation. Rollback capabilities require careful state management and protocol versioning to ensure seamless transitions in either direction. Contingency procedures include alternative authentication methods and emergency access protocols that remain functional during migration activities [10].

Monitoring and metrics collection enable continuous assessment of migration progress and system performance throughout the transformation process. Comprehensive logging and monitoring systems track cryptographic algorithm utilization, performance metrics, and security events, providing visibility for proactive issue identification and optimization opportunities while generating evidence of successful quantum-safe implementation for compliance and audit requirements [9].

Risk Category	Mitigation Success (%)
Legacy System Compatibility	78
Performance Degradation	85
Security Vulnerability	92
Operational Disruption	73
Training Requirements	68
Rollback Necessity	95
Compliance Achievement	89

Table 2: Enterprise Migration Risk Mitigation Effectiveness [9, 10]

6. Conclusion

The Quantum-Safe Network Access Control Framework represents a critical advancement in preparing enterprise security infrastructures for the quantum computing era. This comprehensive solution successfully bridges the gap between theoretical post-quantum cryptographic developments and practical implementation requirements in production environments. The hybrid architectural technique enables organizations to maintain operational continuity while systematically transitioning from vulnerable classical cryptographic methods to quantum-resistant alternatives. Performance optimization strategies effectively address computational overhead concerns associated with post-quantum algorithms, ensuring that authentication latency remains within acceptable bounds for real-time enterprise operations. The systematic migration paradigm provides organizations with structured pathways for transformation that minimize risk exposure while maximizing security benefits. Implementation of cryptographic diversity principles through hybrid protocols ensures protection against both current classical attacks and future quantum threats during transitional periods. The framework's emphasis on algorithm agility and modular design enables adaptation to evolving post-quantum standards and emerging cryptographic innovations. Organizations adopting this framework will achieve quantum-safe NAC capabilities while preserving existing infrastructure investments and maintaining compliance with evolving regulatory requirements in the post-quantum landscape.

Funding: This research received no external funding
Conflicts of interest: The authors declare no conflict of interest
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] Basil H and Mohammad Ali. (2025). Analyzing the research impact in post quantum cryptography through scientometric evaluation, *Springer Nature, Apr. 2025*. [Online]. Available: https://link.springer.com/article/10.1007/s10791-025-09507-3

[2] Fabian S and Muhammad I Al H. (2025). Efficient Implementation of CRYSTALS-KYBER Key Encapsulation Mechanism on ESP32, arXiv, Mar. [Online]. Available: https://arxiv.org/html/2503.10207v1

[3] Kanza C D. (2024). Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process, *MDPI*. [Online]. Available: https://www.mdpi.com/2227-7080/12/12/241

[4] Krishnamoorthy N. (2024). Post-Quantum Cryptography: Securing Future Communication Networks Against Quantum Attacks, ResearchGate. [Online]. Available: https://www.researchgate.net/publication/386476602_Post-Quantum_Cryptography_Securing_Future_Communication_Networks_Against_Quantum_Attacks

[5] Latika R D. (2025). Advanced Techniques in Post-Quantum Cryptography for Ensuring Data Security in the Quantum Era, *Panamerican Mathematical Journal, 2025*. [Online]. Available: https://internationalpubls.com/index.php/pmj/article/view/2097/1318

[6] Léo D. (2017). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme, IACR Transactions on Cryptographic Hardware and Embedded Systems [Online]. Available: https://eprint.iacr.org/2017/633.pdf

[7] Minati R & Hema D. (2025). Quantum powered credit risk assessment: a novel approach using Hybrid Quantum-Classical Deep Neural Network for Row-Type Dependent Predictive Analysis, EPJ Quantum Technology - Springer Open. [Online]. Available: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-025-00323-8

[8] Petar R. (2024). Artificial intelligence and quantum cryptography, *Journal of Analytical Science and Technology - Springer Open, 2024*. [Online]. Available: https://jast-journal.springeropen.com/articles/10.1186/s40543-024-00416-6

[9] Thiago L A and Ricardo C. (2024). Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption, MDPI. [Online]. Available: https://www.mdpi.com/1424-8220/24/22/7300

[10] Zhichuang L. (2024). Compact and efficient KEMs over NTRU lattices, ScienceDirect. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0920548923001095