Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Operationalizing Post-Quantum Cryptography in Multi-Cloud Environments

Syed Mohiuddin Qadri
Senior Solutions Architect, Hewlett Packard Enterprise / Harrisburg University of Science and Technology, Harrisburg, PA, USA
Corresponding Author: Syed Mohiuddin Qadri**, E-mail:** me@syedqadri.com

| ABSTRACT

The emergence of quantum computing is a serious threat to traditional cryptographic algorithms, making it critical to transition to post-quantum cryptography (PQC). This work proposes a holistic conceptual and analytical framework for deploying PQC in multi-cloud environments where the complexity of different infrastructure, workloads and key management schemes pose significant security and efficiency problems. The proposed framework for crypto-agility follows a layered approach, with a cryptographic abstraction layer, a policy-based orchestration engine, a centralized hardware security module (HSM) management plane, and an ongoing monitoring module to facilitate a smooth transition from classical to hybrid and fully quantum-resistant cryptographic systems. He researches identifies and critically analyzes major challenges in deploying PQC technologies in multi-cloud environments, such as inter-cloud interoperability, computational complexity, latency, key management, and regulatory and compliance considerations. The framework tackles these challenges by incorporating hybrid cryptographic protocols that blend classic cryptographic algorithms with NIST-approved PQC algorithms, namely ML-KEM (FIPS 203) and ML-DSA (FIPS 204), to maintain backward compatibility and increase security against quantum-powered adversaries. Moreover, the framework proposes dynamic policy-driven algorithm selection to implement context-sensitive cryptographic enforcement based on sensitivity labels, security threats, and regulatory considerations. An experimental framework is proposed to assess the efficiency and scalability of PQC algorithms deployed in a multi-cloud environment, including metrics such as CPU usage, memory usage, latency and throughput with different workloads. Although this research is conceptual, it draws on previous benchmarking to discuss the securityperformance trade-offs associated with PQC. The results highlight the need for centralized trust anchors, crypto-agility and hybrid deployment models to address risks from cryptographic diversity and ensure the sustainability of security operations. This study advances the research on quantum-safe cloud security by offering a systematic, scalable and policy-oriented framework for PQC deployment. It provides practical guidance for businesses, cloud architects, and security professionals on how to safeguard against quantum vulnerabilities and ensure efficient operations in distributed systems by implementing quantum-safe cryptographic infrastructures.

| KEYWORDS

Post-Quantum Cryptography (PQC), Multi-Cloud Security, Crypto-Agility, ML-KEM, ML-DSA, Hybrid Cryptography, Hardware Security Module (HSM), Quantum-Safe Security, Cloud Computing, Key Management, Cryptographic Migration, Distributed Systems Security, Policy-Driven Security, Quantum Computing Threats 1.

| ARTICLE INFORMATION

ACCEPTED: 15 April 2026 **PUBLISHED:** 15 May 2026 **DOI:** 10.32996/jcsts.2026.5.7.2

Introduction

1.1 Background of Cloud Security

Cloud computing is now the foundation of digital systems, providing scalable and on-demand access to computing resources, storage and applications in a distributed manner. Security is crucial as businesses increasingly depend on public, private, and hybrid cloud environments for critical services, analytics and artificial intelligence applications. But this growth has brought about new security concerns, especially regarding the confidentiality of data, secure communication, and trust in distributed

environments. Current cloud security practices are largely dependent on classical cryptographic technologies such as RSA, Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES), which have been effective against traditional computational attacks.

1.2 Quantum Computing Threats

The advent of quantum computing represents a new era of computing, capable of solving mathematical problems that are intractable for classical computers. Quantum algorithms, like Shor's algorithm, show that popular public-key encryption algorithms, such as RSA and ECC, can be efficiently solved using large-scale quantum computers. While fault-tolerant quantum computers capable of large-scale quantum computing are still in development, there is a real concern about the "harvest now, decrypt later" model. Attackers could store encrypted data now and break it when quantum computing technology becomes available, thus affecting the long-term security of the data.

1.3 Post-Quantum Cryptography

Post-quantum cryptography (PQC) is a potential approach to mitigate quantum threats by designing quantum resistant cryptographic algorithms. The National Institute of Standards and Technology (NIST) has been driving standardization efforts, leading to the choice of quantum-resistant algorithms like ML-KEM and ML-DSA. These algorithms aim to be backward compatible and can replace or complement existing systems. But the shift to PQC is not a simple one-to-one substitution; it involves integration, performance analysis, compatibility, and other aspects, especially in large-scale cloud environments.

1.4 Issues in Multi-Cloud Environments

In multi-cloud environments, where companies use more than one cloud service provider (e.g., Amazon, Microsoft, Google), managing cryptography becomes more complex. They can be plagued by key management fragmentation, lack of uniform security policies and interoperability issues. Introducing PQC in multi-cloud environments presents several challenges, including higher computational demands, latency considerations, cryptographic algorithm compatibility, and cryptographic policy consistency across multiple platforms. Additionally, there are challenges in achieving consistent security and regulatory compliance across different jurisdictions.

1.6 Aim and Objectives

The main aim of this research is to establish a systematic and scalable approach for implementing post-quantum cryptography in multi-cloud settings. To achieve this aim, the study has the following objectives:

- To understand the vulnerabilities of existing cryptographic systems to quantum computing
- To explore the design and operational constraints of PQC in a multi-cloud environment
- To develop a crypto-agility strategy for deployment and selection of hybrid cryptographic implementations
- To assess the impact of PQC on performance using specific measures like latency, throughput, and processing time
- To offer guidelines for secure and efficient transition to the next generation of cloud communications

2. Literature Review

2.1 Classical Cryptography

Modern information security relies on classical cryptography for secure communications, data confidentiality, and authentication. This mainly comprises symmetric algorithms like the Advanced Encryption Standard (AES) and asymmetric algorithms like RSA and Elliptic Curve Cryptography (ECC). Symmetric-key cryptography allows efficient encryption of data, and asymmetric-key cryptography enables secure key exchange, digital signatures, and authentication. These schemes are used in combination to provide confidentiality, integrity, and authenticity in protocols like Transport Layer Security (TLS). While these cryptographic techniques are safe against computational attacks on classical computers, their security relies on mathematical problems that may be solved in the presence of quantum computers.

2.2 Attacks on RSA, ECC, and Diffie–Hellman

Public-key cryptosystems are vulnerable to a disruptive attack from quantum computing. Shor's Algorithm shows that factoring integers and computing discrete logarithms (the basis of the security of RSA, ECC and Diffie-Hellman respectively) can be done in polynomial time on a quantum computer. This makes conventional key exchange and digital signature schemes vulnerable to

quantum computers. By comparison, symmetric cryptographic schemes are less vulnerable; Grover's Algorithm offers a quadratic increase in speed, which can be countered by longer keys (e.g., AES-256). The advent of the "harvest now, decrypt later" attack also increases the need to move towards quantumresistant cryptography.

2.3 Post-Quantum Cryptography Standards\

Post-quantum cryptography (PQC) seeks to create cryptography algorithms that remain secure against both classical and quantum attacks. The National Institute of Standards and Technology (NIST) has overseen an international process for the standardization of PQC algorithms over several years. This process has resulted in the adoption of a number of algorithms, evaluated for security, performance and practicability. PQC standards aim to be integrated with current communication protocols, allowing a smooth transition from traditional systems without the need for a complete overhaul. These standards are essential for interoperability, compliance and long-term security.

2.4 ML-KEM, ML-DSA and SLH-DSA

Key standardized PQC algorithms include ML-KEM (Module-Lattice Key Encapsulation Mechanism), ML-DSA (Module-Lattice Digital Signature Algorithm) and SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). ML-KEM, based on CRYSTALS-Kyber, is used for key agreement and provides high security with reasonable efficiency. ML-DSA, a variant of CRYSTALS-Di lithium, delivers secure digital signatures that ensure authenticity and integrity. SLH-DSA, based on SPHINCS+, is a hash-based digital signature that focuses on long-term security and few assumptions about algebraic structures. These digital signatures vary in computational efficiency, key lengths and signature sizes, and need to be taken into account in cloud systems.

2.5 Crypto-Agility in Cloud Systems

Crypto-agility is the capability of a system to change cryptographic mechanisms to protect against changes in threat or vulnerability, or to comply with regulatory changes. Crypto-agility is critical in the cloud because of constantly evolving technology and the decentralized architecture of the cloud. This allows seamless transitions between cryptographic algorithms with minimal service disruption. Crypto-agility mechanisms include abstraction, policybased orchestration and key management. These enable systems to adopt hybrid cryptographic systems, leveraging both traditional and PQC algorithms during the transition period. But implementing crypto-agility is hindered by legacy system interdependencies, standardization and performance costs.

2.6 HSMs and Key Management in Multi-Cloud

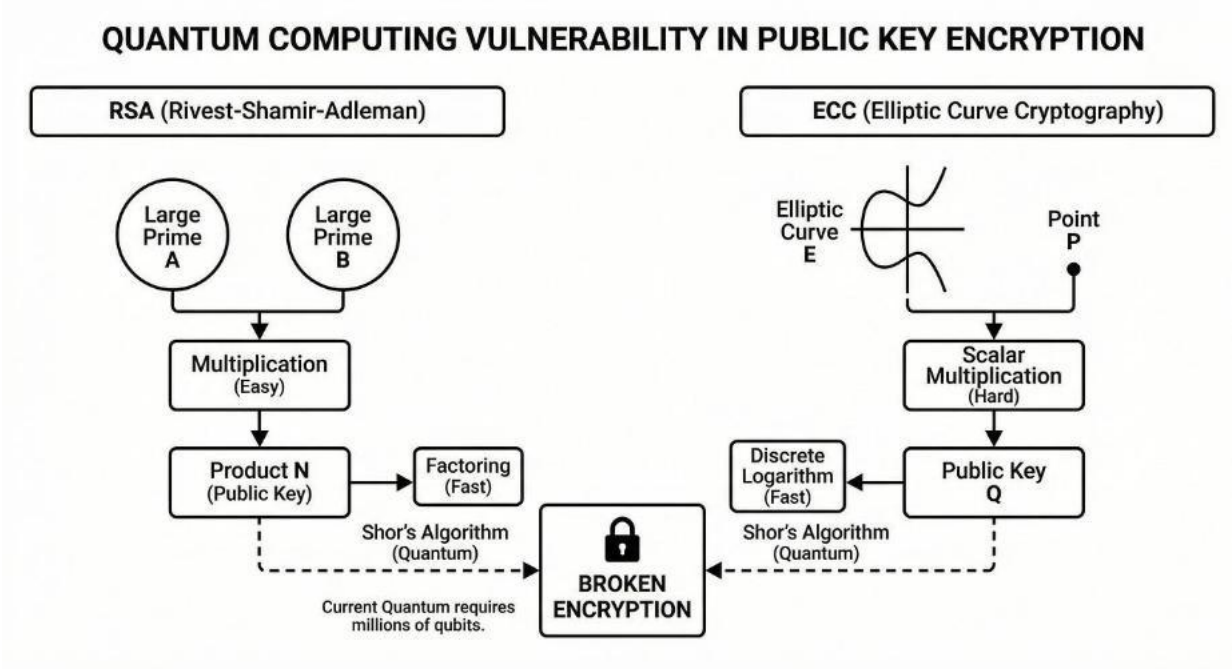
Hardware Security Modules (HSMs) play an essential role in key management, cryptographic processing, and trust provisioning in cloud computing. HSMs in multi-cloud offer a central trust root to maintain security across multiple providers. Contemporary cloud services provide managed HSMs, but these are typically proprietary, resulting in diverse key management approaches. In multi-cloud environments, key management involves secure key generation, distribution, rotation and revocation, and integration with identity and access management. PQC adds complexity to key management due to increased key sizes and computational costs, requiring scalable and interoperable key management.

2.7 Existing Commercial Solutions

There are some commercial offerings that cover some aspects of cryptographic management and quantum readiness in the cloud. Large cloud providers provide key management tools like AWS Key Management Service, Azure Key Vault and Google Cloud Key Management, which offer encryption, key storage and access control features. Thirdparty services like Hashi Corp Vault, Thales Group Cipher Trust and IBM Quantum Safe solutions provide enhanced cryptographic capabilities. Although these environments support key lifecycle management and, in some cases, early engagement with PQC, they do not necessarily offer multi-cloud crypto-agility solutions and standards for hybrid cryptography deployment.

2.8 Research Gaps

While considerable research has been conducted on PQC and cloud security, there are still some gaps. First, there is a need for holistic frameworks that integrate PQC, crypto-agility and multi-cloud interoperability. Second, much of the current research has a theoretical focus on cryptographic design but lacks consideration of real-world implementation issues like performance, latency and scalability. Third, there is a lack of research on policy-based cryptographic management and migration approaches for distributed systems. Finally, there is a lack of focus on translating research into practice, especially in integrating PQC with enterprise needs. Closing these gaps is critical for secure, scalable and quantum-proof cloud computing in the future.



3. Methodology

3.1 Research Design

This research employs a conceptual and analytical research design with structured benchmarking references, rather than empirical studies. This study draws on academic literature, uniform PQC standards and publicly released performance reports to provide a scalable approach for post-quantum cryptography (PQC) in multi-cloud settings, as well as to evaluate its effectiveness. The design adopts a system-level perspective, addressing architecture modeling, security evaluation and performance considerations. Rather than performing large-scale deployment trials, the research uses verified benchmark results and simulation hypotheses to enable accurate and technically sound conclusions. This approach is suitable due to the rapidly changing landscape of PQC technologies and the lack of production-level quantum-safe cloud platforms.

3.2 Analytical Framework

Our analytical framework draws on a model of a crypto-agile architecture that facilitates the dynamic integration and orchestration of cryptographic algorithms in a distributed cloud environment. The framework is comprised of four main components:

- Cryptographic Abstraction Layer Offers a consistent API to integrate traditional and PQC algorithms without code changes
- Policy-Driven Orchestration Engine Allows adaptive choice of algorithms according to policies including data criticality, regulation, and risk
- HSM Control Plane Provides a central trust point for key management (generation, storage, lifecycle) in the cloud
- Monitoring and Compliance Module Monitors cryptographic practices, identifies threats and provides audit support and compliance

This layered design facilitates hybrid cryptographic integration, enabling classical algorithms to co-exist with PQC schemes like ML-KEM and ML-DSA for backward compatibility and smooth transition.

3.3 Multi-Cloud Scenario Definition

The research presents a typical multi-cloud scenario involving a number of cloud service providers and workloads. The scenario includes:

- Public cloud services (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform)
- Containerized applications deployed through orchestration tools (e.g., Kubernetes)
- Decentralized data transfers between nodes of the cloud with secure communication

- Centralized and decentralized key management setups

We consider hybrid cryptographic communication, which involves classical key exchange protocols to be complemented by PQC-based key encapsulation (for example, ML-KEM) to achieve quantum security. This scenario mirrors real-world enterprise deployments with a need for interoperability and scalability.

3.4 Security and Performance Criteria

The research proposes a set of security and performance criteria to evaluate the proposed framework:

Security Criteria

- Quantum-resistant (as per NIST PQC guidelines)
- Key confidentiality and integrity
- Key management (generation, distribution, rotation, revocation)
- Adherence to regulatory or data protection standards
- Defense against "harvest now, decrypt later" attacks

Performance Criteria

- Latency: Time taken for cryptographic tasks (key establishment, handshake)
- Throughput: Secure transactions per unit time
- CPU Utilization: Processing load with PQC algorithms
- Memory Usage: Effect of increased key sizes and ciphertexts
- Scalability: Performance under a cloud environment with multiple nodes Such metrics offer a comprehensive assessment of both security and performance.

3.5 Benchmarking Approach

While the full experimental setup is not covered in this work, a benchmarking model is proposed for future experimentation. The benchmarking framework is founded on tools and models such as:

- Open Quantum Safe (labors) for PQC algorithms
- OpenSSL 3.x supporting hybrid cryptography
- Network testing software (e.g., iperf3) for network performance
- Containerized environments for simulating multi-cloud workloads

The benchmarking process is used to compare:

- Traditional cryptographic operations (e.g., key exchange based on ECDH)
- Hybrid cryptographic operations (e.g., ECDH + ML-KEM)
- PQC-only configurations

Throughput, average time to complete a handshake, CPU cycles and overhead of the size of the data are measured under various workloads. The research provides references to other benchmark results in support of its analysis and anticipated performance trade-offs.

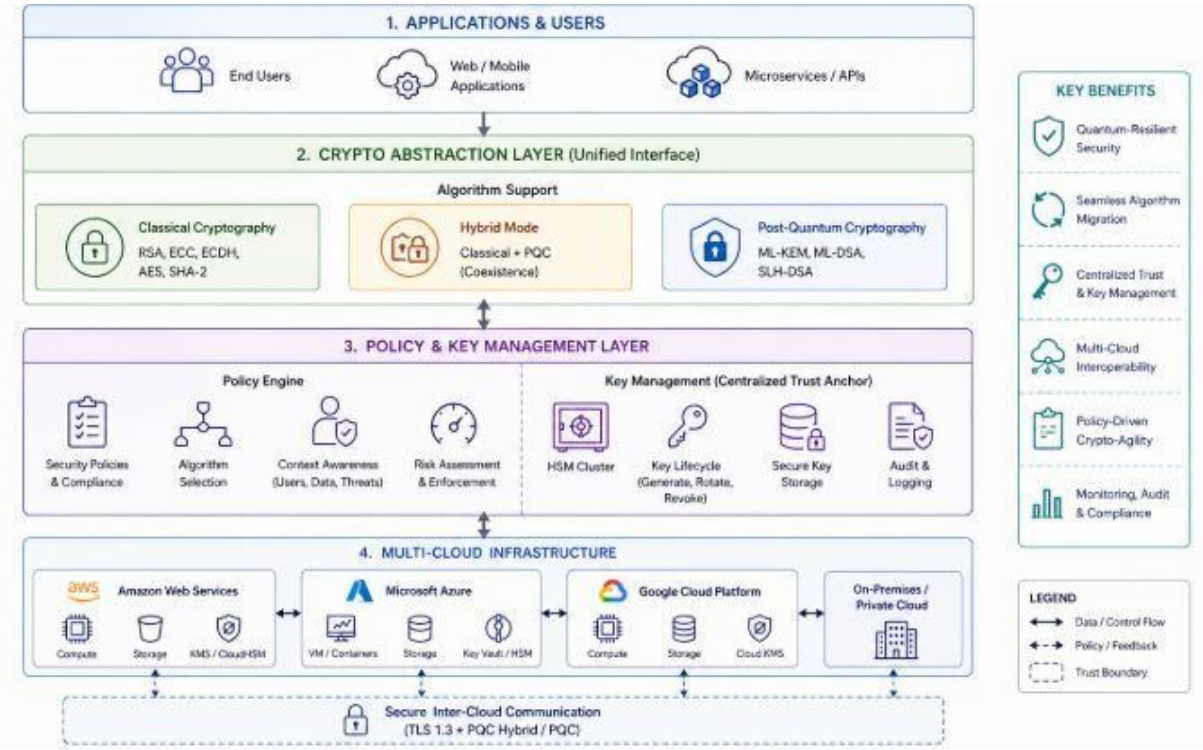
3.6 Caveats

There are a number of limitations to this study:

The study is not fully empirically validated: The work is conducted using analytical modeling and existing benchmarks, rather than new large-scale experiments

- Evolving PQC standards: Changes in PQC algorithms and implementation may impact future use
- Multi-cloud setup assumptions: The environment is defined as a typical example and might not reflect all deployment scenarios
- Performance variability: Results may vary based on hardware, cloud provider settings and workloads
- Vendor-neutral approach: The methodology is vendor-independent and does not focus on proprietary solutions

Despite these challenges, the approach offers a systematic and realistic framework for addressing PQC integration issues and informing empirical studies.



4. Proposed Crypto-Agility Framework

4.1 Framework Overview

Our proposed crypto-agility framework aims to support the smooth migration from traditional cryptography to postquantum cryptography (PQC) in multi-cloud settings. It uses a layered and modular approach that separates the application from the cryptographic operations, enabling dynamic security adaptation to changing needs and quantum security risks .The framework comprises seven key elements: a crypto-abstraction layer, policy engine, hybrid algorithm orchestration component, hardware security module (HSM) control plane, monitoring and cryptographic inventory component, integration with the Cryptographic Bill of Materials (CBOM) and migration state machine. These components together offer complete crypto-agility, supporting interoperability, scalability and future-proofing of security for cloud environments.

4.2 Crypto Abstraction Layer

The cryptographic abstraction layer is a single interface between applications and cryptographic schemes. The main purpose is to abstract away complexity of algorithms and allow transparent switching of cryptographic algorithms without changing the application code.

Key features include:

- Unified Cryptographic API
- Provides basic operations like encryption, decryption, signing, verification and key exchange
- Algorithm Agnosticism
- Supports multiple families of algorithms, such as:
- Classical: RSA, ECC, AES
- Hybrid: Classical + PQC combinations

- PQC: ML-KEM, ML-DSA, SLH-DSA
- Pluggable Architecture
- Supports external cryptographic libraries (OpenSSL, liboqs) and hardware devices

- Provider Abstraction
- Abstracts applications away from vendor's solutions (cloud KMS, HSMs, third-party providers)

This provides portability and flexibility, which is the basis for crypto-agility.

4.3 Policy Engine

The policy engine is the brain of the framework, making decisions on which cryptographic settings are to be used based on context and regulations.

Core capabilities include:

1. Context Awareness
    a. Assesses data classification, user, location, device and threat
2. Policy-as-Code Implementation
    a. Implements cryptographic policies using declarative rules (e.g., YAML, Rego), allowing them to be automated
3. Risk Assessment and Scoring
    a. Assesses security levels of operations and recommends cryptographic solutions
4. Dynamic Algorithm Selection
    a. Dynamic use of classical, hybrid or PQC algorithms based on policy settings
5. Compliance Enforcement

a. Helps meet standards like NIST, FIPS and data privacy requirements

The policy engine allows adaptive security, ensuring cryptographic choices are context-sensitive and future-proof.

4.4 Hybrid Algorithm Orchestration

This component oversees the interaction and integration of classical and PQC algorithms.

Key functionalities include:

- **Hybrid Mode Execution**
  Combines classical algorithms (e.g., ECDH) with PQC mechanisms (e.g., ML-KEM) to provide dual-layer security
- **Dynamic Mode Switching**
  Supports three operational modes:

  Classical-only

  Hybrid (Classical + PQC)

  PQC-only

- **Handshake Negotiation Support**
  Enables hybrid key exchange in protocols such as TLS 1.3
- **Performance Optimization**
  Selects optimal algorithm combinations based on system constraints
- **Fallback and Fail-Safe Mechanisms**
  Ensures continuity in case of algorithm failure or incompatibility

This is essential for phased migration, to reduce operational impact and improve security.

4.5 HSM Control Plane

The HSM control plane is the foundation of the framework, providing a trustworthy key management service across multiple cloud providers.

Core responsibilities include:

- **Secure Key Generation and Storage**
  Keys are generated and stored within tamper-resistant HSMs

- **Key Lifecycle Management**
  Includes key rotation, revocation, versioning, and expiration
- **Access Control Enforcement**
  Implements role-based and attribute-based access control (RBAC/ABAC)
- **Multi-Cloud Integration**
  Connects with cloud-native HSM services and on-premises HSM clusters
- **Audit and Logging**
  Maintains secure logs for compliance and forensic analysis

This module centralizes key management to avoid fragmentation and instill uniform security policies.

4.6 Monitoring and Inventory
The monitoring component offers real-time insights into cryptographic activities and assets, facilitating risk mitigation.

Key capabilities include:

- **Cryptographic Asset Inventory**
  Tracks algorithms, keys, certificates, and cryptographic libraries across systems
- **Real-Time Monitoring**
  Observes cryptographic usage and detects anomalies
- **Weakness Detection**
  Identifies outdated or vulnerable algorithms (e.g., RSA-1024)
- **Alerts and Notifications**
  Generates alerts for policy violations or security risks
- **Reporting and Dashboards**
  Provides insights into cryptographic posture and compliance status

This module supports **observability and governance**, which are essential for large-scale deployments.

4.7 CBOM Integration The system includes a Cryptographic Bill of Materials (CBOM) to keep track of cryptographic elements.

CBOM elements include:

- Cryptographic algorithms and versions
- Key management modules
- Certificates and keys
- Cryptographic dependencies and providers
- Compliance and standardization status

Integration Workflow

- Discovery and scanning of cryptographic assets
- CBOM generation and enrichment
- Validation against policies and standards
- Continuous monitoring and updates

Benefits

- Improved transparency and traceability
- Enhanced vulnerability management
- Automated compliance reporting
- Better risk assessment and decision-making

CBOM integration represents a **novel contribution**, bridging software supply chain security with cryptographic governance.

5. Implementation Strategy

5.1 Classical-Only Baseline

The proposed framework is implemented with the deployment of a classical cryptography baseline, which represents the current configuration of most enterprise cloud systems. In this setting, secure communication is based on classical cryptographic mechanisms, such as elliptic curve Diffie–Hellman key exchange, elliptic curve digital signature algorithms or RSA for authentication, and Advanced Encryption Standard for symmetric encryption. Transport layer security protocols like TLS 1.2 and TLS 1.3 are applied to secure communication and are at the heart of modern cloud security implementation. This baseline is important as it enables security and performance comparisons to be made between the baseline and the post-quantum cryptographic mechanisms. It also allows the discovery of cryptographic dependencies, mission-critical systems, and assets that need to be prioritized for migration.

5.2 Classical and PQC Hybrid Deployment

To ensure a smooth and secure migration to quantum-safe solutions, the framework proposes a hybrid deployment approach that combines classical cryptographic algorithms with post-quantum techniques. Here, classical key exchange protocols coexist with PQC-based methods, ensuring security is not compromised even if one system is compromised. This layered approach enables compatibility with legacy systems while also incorporating quantum resilience. Hybrid deployment is well suited to tackling long-term security threats such as the "harvest now, decrypt later" attack, by providing security against both existing and future threats. This approach ensures a smoother transition and enables testing under realistic conditions for performance assessment.

5.3 ML-KEM Key Encapsulation

In the hybrid approach, ML-KEM is the main method for key establishment. ML-KEM, a lattice-based key encapsulation scheme standardized as part of the NIST PQC project, offers robust quantum security and is compatible with existing protocols. In secure handshake protocols, ML-KEM collaborates with traditional key exchange methods to derive secrets, thus strengthening the security of the communication link. While ML-KEM brings increased computational costs and ciphertext expansion compared to traditional key exchange schemes, these come at the tradeoff of enhanced security against quantum attacks. The incorporation into protocols like TLS 1.3 highlights its suitability for use in cloud-based systems.

5.4 ML-DSA for Digital Signatures

The framework uses ML-DSA as a post-quantum solution for authentication and integrity assurance. ML-DSA is based on lattice-based cryptography and offers strong resistance against quantum attacks, supporting critical operations such as certificate verification, API signing and code signing. In transitional stages, ML-DSA can be used in combination with other signature schemes to provide compatibility and trust relationships. Despite the algorithm's larger signature sizes and slower verification, its security features mean that it could be used in the long term in settings where the authenticity of data needs to be maintained over longer durations.

5.5 Policy-as-Code for Algorithm Selection

Another key component of the approach is the adoption of policy-as-code for automated and contextual cryptographic decision-making. Instead of manual configuration, the framework specifies cryptographic policies in a declarative manner, enabling them to be evaluated at runtime. The policies take into account data classification, compliance standards, performance considerations and threat data to choose the optimal cryptographic mechanism. This logic is implemented within the policy engine, enabling consistent policy enforcement across distributed systems and eliminating the potential for human error. This also improves auditability, as policies can be versioned and reviewed, ensuring cryptographic practices are compliant with corporate governance standards.

5.6 Confidential Computing Integration

To enhance cryptographic security, the framework also incorporates confidential computing techniques that use trusted execution environments. These offer hardware-enforced isolation for cryptographic operations, allowing cryptographic processes to be secured even against trusted system components or cloud providers. The framework ensures that key management and policy enforcement functions are executed in secure enclaves, reducing the threat of data exposure in use. This is essential in multi-cloud deployments, where trust boundaries span multiple environments. Thus, the use of confidential computing improves security by protecting data in storage, transit, and during processing.

5.7 Rollback and Migration Controls

The framework's approach to rollback and migration control mechanisms accounts for the challenges and risks in transitioning to post-quantum cryptography. These controls are in line with the migration state model described in the previous section, allowing organizations to transition through various stages while ensuring system stability. In cases of performance issues, incompatibilities, or security policy violations, the framework supports rollback to stable points. This guarantees that the migration process is reversible without disruption. Moreover, integration of checkpoints is provided during migration to assess system performance and security. The framework's automation combined with controlled supervision facilitates a safe and controlled evolution towards quantum-resistant cryptographic systems.

6. Evaluation and Discussion

6.1 Security Benefits

Our crypto-agility framework offers numerous security benefits by countering both existing and future cryptographic vulnerabilities. The framework's use of hybrid cryptographic schemes provides defense against both classical and quantum attacks. The use of post-quantum cryptographic schemes (ML-KEM and ML-DSA) enhances key exchange and digital signatures, minimizing the potential impact of classical schemes falling compromised. Additionally, the centralization of trust entities using hardware security modules protects cryptographic keys and reduces risks in distributed systems. The approach also prevents long-term attacks, specifically the "harvest now, decrypt later" threat, by securing sensitive information with quantum-resistant technologies. In summary, the integration of crypto-agility, hybrid deployment and central governance forms a secure and adaptable security framework that can respond to security threats.

6.2 Performance Overhead

While post-quantum cryptography enhances security, it comes at the cost of performance. PQC keys and operations are often larger and more complex than their classical counterparts, impacting performance. Hybrid systems, which run classical and PQC algorithms in parallel, also incur additional computational overhead due to double encryption operations. This is especially pronounced in high-throughput or low-latency applications. But the architecture addresses these concerns through algorithm selection and policy-based optimization, enabling organizations to meet security and performance goals. Hence, the performance overhead associated with improved security is acceptable if supported by suitable orchestration. 6.3 Latency and CPU Implications

PQC has a considerable impact on the latency and the CPU load, particularly in cryptographic handshakes. Cryptographic key encapsulation operations, such as ML-KEM, introduce extra operations and, as a consequence, increase the time required for the handshake compared to traditional key exchange protocols. Likewise, post-quantum digital signature verification consumes more resources, thus increasing CPU load. In multi-cloud environments, these impacts could be exacerbated by network effects and load balancing. However, the framework provides solutions to these issues by supporting hybrid and targeted deployment of quantum-resistant mechanisms, allowing highperformance systems to function effectively and seamlessly adapt to quantum-resistant security. As hardware advances and efficient implementations emerge, these performance impacts are likely to diminish.

6.4 Key Lifecycle Management

Key lifecycle management is a vital aspect of secure cryptography, and our proposed framework improves this capability through coordinated and automated key management. The proposed framework's use of a consolidated HSM control plane facilitates standardized procedures for generating, distributing, rotating and revoking keys across various cloud vendors. This centralized model eliminates silos and provides transparency of cryptographic processes, allowing organizations to apply consistent security policies. The incorporation of policy-based controls also enhances lifecycle management and supports automation to eliminate potential errors. The structured nature of the framework is crucial in managing larger keys and increasing complexity introduced with PQC, ensuring scalability and manageability at large deployment scales.

6.5 Vendor-Neutral Multi-Cloud Support

One of the key advantages of the proposed framework is its vendor neutrality, allowing it to function across different cloud providers. Through the abstraction of cryptographic operations and separation of provider-specific details, the framework is not tied to proprietary systems and can work across different providers. This feature is crucial for multicloud deployments, where companies aim to avoid vendor-specific solutions and ensure security across multiple providers. The adoption of standardized APIs and centralized policy enforcement mechanisms enables cryptographic functions to be consistently managed across different platforms. This approach enables scalable and adaptable deployments, allowing for flexibility in response to technological and business needs while maintaining security.

6.6 Comparison with Existing Solutions

the proposed framework offers several key differences when compared with existing solutions including AWS Key Management Service, Azure Managed HSM, as well as third-party platforms such as Hashi Corp Vault, Thales Group Cipher Trust, and Qu Secure. Existing cloud services offer secure key management and encryption but are often siloed to their respective providers, leading to challenges in managing security across multiple clouds. Third-party solutions provide greater integration, and more sophisticated key management capabilities; but their capabilities for postquantum cryptography and crypto-agility is either limited or still in development. However, the framework focuses on abstracting cryptography, dynamic algorithm switching, and seamless integration of PQC. The integration of CBOM-based cryptographic inventory and migration state machine also sets it apart from others by offering improved transparency and a well-defined migration process for quantum security. Although commercial products center on operational security, the framework builds on this by offering a look ahead to the quantum future.

6.7 Practical Adoption Barriers

While the framework has significant benefits, there are some practical barriers to its adoption. The first, and most obvious, is the potential inefficiency of PQC algorithms, which may hinder their deployment in time-critical applications. Furthermore, the absence of standardized practices and tooling for integrating PQC schemes can make adoption more challenging. Compatibility with existing systems not built to accommodate hybrid or quantum-resistant cryptography may also pose challenges. The deployment of policy as code and orchestration demands a level of organizational readiness, which may not always be present.

Moreover, regulatory frameworks may be uncertain and compliance requirements may be evolving, especially in sectors with stringent data privacy regulations. The adoption of emergent technologies like confidential computing and CBOM brings implementation challenges that need to be addressed. Overcoming these challenges will require ongoing research, industry partnerships and the establishment of standards and best practices.

Conclusion

Summary of Findings

This study has examined the growing necessity of transitioning from classical cryptographic systems to post-quantum cryptography in the context of multi-cloud environments. It has shown that while traditional cryptographic mechanisms remain effective against current computational threats, they are fundamentally vulnerable to the capabilities of emerging quantum computing technologies. The analysis highlights that multi-cloud infrastructures introduce additional complexity in cryptographic management due to fragmentation, interoperability challenges, and distributed trust boundaries. Within this context, the study demonstrates that a structured, crypto-agile approach is essential for ensuring both immediate and long-term security. The findings further indicate that hybrid cryptographic deployment, combined with centralized policy enforcement and key management, provides a practical pathway for mitigating quantum risks while maintaining operational continuity.

Research Contribution

The primary contribution of this research lies in the development of a comprehensive crypto-agility framework tailored for multi-cloud environments. Unlike existing approaches that focus either on theoretical cryptographic models or vendor-specific implementations, this study bridges the gap by proposing a unified, scalable, and vendor-neutral architecture. The framework introduces several novel elements, including the integration of a cryptographic abstraction layer, a policy-driven orchestration engine, and a centralized HSM control plane to support consistent and adaptive cryptographic management. Additionally, the incorporation of a Cryptographic Bill of Materials enhances visibility into cryptographic assets, while the migration state machine provides a structured and actionable roadmap for transitioning to post-quantum systems. Together, these contributions advance the field by offering both conceptual clarity and practical applicability.

Practical Implications

From a practical perspective, the proposed framework provides organizations with a clear strategy for preparing their cryptographic infrastructure for the quantum era. By enabling dynamic algorithm selection and supporting hybrid deployment models, the framework allows enterprises to incrementally adopt post-quantum cryptography without disrupting existing operations. Its vendor-neutral design ensures compatibility across diverse cloud platforms, reducing the risk of lock-in and supporting flexible deployment strategies. Furthermore, the integration of policy-ascode and centralized key management enhances governance, compliance, and operational efficiency. These capabilities are particularly valuable for industries that handle sensitive data and require long-term security guarantees, such as finance, healthcare, and critical infrastructure. The

framework therefore offers a practical foundation for organizations seeking to future-proof their security architectures in an increasingly complex and distributed computing landscape.

Future Research Directions

While this study provides a structured approach to post-quantum cryptographic integration, several areas remain open for further investigation. Future research should focus on conducting large-scale empirical evaluations to quantify the performance impact of PQC algorithms across diverse cloud environments and workloads. The development of optimized implementations and hardware acceleration techniques will be critical for reducing latency and computational overhead. Additionally, further exploration of automated policy frameworks and machine learningdriven risk assessment models could enhance the adaptability of crypto-agile systems. The integration of emerging standards and technologies, including advanced confidential computing and real-time cryptographic monitoring tools, also presents opportunities for extending the framework. As quantum computing continues to evolve, ongoing research will be essential to refine and validate approaches that ensure secure, scalable, and sustainable cryptographic systems.

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]. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. https://doi.org/10.1038/nature23461

[2]. Buchmann, J., Dahmen, E., & Schneider, M. (2008). Merkle signatures for long-term security. In *Public Key Cryptography (PKC)* (pp. 1–20). Springer.

[3]. Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NIST IR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

[4]. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALSDilithium: A lattice-based digital signature scheme. In *IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 238–255). IEEE.

[5]. Hülsing, A., Rijneveld, J., Song, F., & Schwabe, P. (2018). SPHINCS+: Stateless hash-based signatures. In *Advances in Cryptology – EUROCRYPT* (pp. 3–33). Springer.

[6]. Koblitz, N., & Menezes, A. (2015). A riddle wrapped in an enigma: Post-quantum cryptography. *IEEE Security & Privacy, 13*(6), 34–42.

[7]. Liu, F., Shu, J., & Chen, H. (2018). Hybrid cloud security: A survey. *IEEE Access, 6*, 71452–71473. https://doi.org/10.1109/ACCESS.2018.2878023

[8]. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (SP 800-145). National Institute of Standards and Technology.

[9]. National Institute of Standards and Technology. (2024). *Post-quantum cryptography standardization*. https://csrc.nist.gov/projects/post-quantum-cryptography

[10]. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science, 10*(4), 283–424. https://doi.org/10.1561/0400000074

[11]. Rogaway, P. (2015). The moral character of cryptographic work. *IACR Cryptology ePrint Archive*.

[12]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (SP 800-207). National Institute of Standards and Technology.

[13]. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE.

[14]. Vaudenay, S. (2018). *A classical introduction to cryptography: Applications for communications security*. Springer.

[15]. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2020). Enabling secure and efficient cloud computing. *IEEE Cloud Computing, 7*(2), 34–42.

[16]. Zhang, L., Chen, X., & Li, J. (2022). Crypto-agility in cloud systems. *Future Generation Computer Systems, 128*, 85–97. https://doi.org/10.1016/j.future.2021.09.010

[17]. Amazon Web Services. (2024). *Post-quantum cryptography strategy*. https://aws.amazon.com/security/postquantum-cryptography/

[18]. Google Cloud. (2023). *Encryption and key management architecture*. https://cloud.google.com/security/encryption

[19]. Microsoft. (2023). *Azure Managed HSM documentation*. https://learn.microsoft.com/azure/keyvault/managed-hsm/

[20]. HashiCorp. (2023). *Vault: Secrets management*. https://www.hashicorp.com/products/vault

[21]. Thales Group. (2023). *CipherTrust data security platform*. https://cpl.thalesgroup.com

[22]. QuSecure. (2024). *Post-quantum cryptography solutions*. https://www.qusecure.com

[23]. IBM Research. (2024). NIST PQC standards overview. https://research.ibm.com/blog/nist-pqc-standards

[24]. ETSI. (2022). *Quantum-safe cryptography and security*. https://www.etsi.org

[25]. Bernstein, D. J., Schwabe, P., & others. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice KEM. In *IEEE European Symposium on Security and Privacy* (pp. 353–367).

[26]. Aljahdali, A. O. (2025). Hybrid quantum encryption frameworks using ML-KEM and ML-DSA. *Journal of Information Security*.

[27]. Chen, A. C. H. (2025). NIST PQC algorithms and QRNG integration. *arXiv preprint arXiv:2507.21151*.

[28]. Chhetri, G., & Sharma, P. (2025). Post-quantum cryptography and quantum-safe security: A survey. *arXiv preprint arXiv:2510.10436*.

[29]. Faval, R. A., et al. (2026). PQC integration in next-generation networks. *arXiv preprint arXiv:2603.28626*.

[30]. Chhetri, R., et al. (2026). Benchmarking ML-KEM and ML-DSA on IoT devices. *arXiv preprint arXiv:2603.19340*.

[31]. Egbuagha, O. (2025). Post-quantum cryptography in practice. *IACR ePrint Archive*.

[32]. Olushola, A. (2025). Authenticated PQC session protocols using ML-KEM and ML-DSA. *Frontiers in Physics*.

[33]. Cherkaoui, I. (2026). Quantum-resistant zero-trust architectures. *Scientific Reports*.

[34]. Mastercard. (2025). *Migration to post-quantum cryptography*. https://www.mastercard.com