Migration Strategies from Traditional Cryptography to Post-Quantum Cryptography in Cloud Systems

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Divya, S., and Bagavathi Lakshmi R. "Migration Strategies from Traditional Cryptography to Post-Quantum Cryptography in Cloud Systems." *Shanlax International Journal of Arts, Science and Humanities,* vol. 13, no. 3, 2026, pp. 254–61.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i2-Feb.10284

S. Divya
Research Scholar, Vels Institute of Science,Technology & Advanced Studies (VISTAS) Pallavaram, Chennai

Dr. R. Bagavathi Lakshmi
Guide /Associate Professor
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai

Abstract

Cloud systems urgently need to switch to Post-Quantum Cryptography (PQC) since the majority of traditional cryptographic algorithms will become vulnerable due to the looming danger of quantum computing. The methodical approaches for switching from conventional cryptography (such as RSA and ECC) to PQC algorithms established by the National Institute of Standards and Technology (NIST) are examined in this study. We look at performance bottlenecks, cloud-native issues, migration phases customized for service-oriented architectures, hybrid deployment models that blend classical and quantum-resilient algorithms, and backward compatibility techniques. The trade-offs between security and performance are demonstrated through experimental research in a cloud setting, with a focus on protocol support, adaptive key management, and incremental migration. Our research aims to help security engineers and cloud architects implement PQC in practice while preserving scalability, compliance, and service quality.

Keywords: Quantum-Resistant, Post-Quantum Cryptography (PQC), Cloud Security, Migration Strategy, Cryptographic Transition, PQC Adoption, Hybrid Cryptosystems, Performance Evaluation.

Introduction

Introduction Cloud computing is now a key part of modern digital systems, supporting important services in areas like finance, healthcare, education, and government. These cloud platforms use traditional encryption methods such as RSA, ECC, AES, and SHA to keep data safe during communication and storage.But the rise of large quantum computers is a big risk for these encryption methods. Shor's algorithm can quickly solve math problems that traditional encryption relies on, like factoring large numbers and solving discrete logarithms. This means RSA and ECC could be broken. Grover's algorithm also makes symmetric encryption less secure by making brute-force attacks faster. The need to move to quantum-safe

algorithms is even more urgent because of the "Harvest Now, Decrypt Later" strategy. This means attackers could collect encrypted data today and decrypt it later once quantum computers are powerful enough. This paper suggests a clear plan for moving cloud systems from old encryption methods to new quantum-resistant algorithms approved by NIST.

Background and Related Work

Traditional Cryptography in Cloud Systems

- Cloud systems usually rely on:
- RSA for sharing keys and signing digital documents
- ECC for quick and secure login checks
- AES-128 or AES-256 for keeping data safe
- TLS rules for making sure data is sent securely over the internet

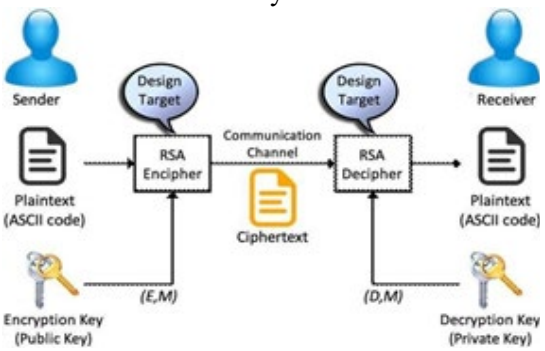

Figure 2.1

Emergence of Post-Quantum Cryptography The quantum factoring algorithm developed by Peter Shor showed that RSA and ECC can be broken quickly, in a time that grows polynomially with the size of the problem. Also, Lov Grover presented a method that speeds up brute-force attacks by a square factor, which affects symmetric cryptography systems.

To address these threats, the National Institute of Standards and Technology (NIST) started the Post-Quantum Cryptography (PQC) Standardization Project in 2016. This effort led to the approval of several algorithms that can resist attacks from both classical and quantum computers, including: CRYSTALS-Kyber (used for key exchange) CRYSTALS-Dilithium (used for digital signatures) FALCON (used for digital signatures) SPHINCS+ (based on hash functions for digital signatures)

These algorithms are built on mathematical problems that are thought to be hard for both classical and quantum computers to solve, such as: Learning With Errors (LWE) Module-LWE Hash-based construction methods The rise of PQC represents a major change from relying on number-theoretic problems for security to using lattice-based and hash-based security models.

Related Work on Migration Strategies

A. Crypto-Agility Frameworks

Recent studies focus on crypto-agility, which lets systems easily switch cryptographic methods without needing big changes. Key areas of interest include: Using modular cryptographic libraries Adding abstraction layers in TLS systems Developing configurable key management systems Crypto-agility is seen as a key part of preparing for the transition to quantum-safe cryptography.

B. Hybrid Cryptographic Approaches

Many researchers suggest using hybrid cryptography during the transition period, combining classic and PQC algorithms. Hybrid TLS handshakes include: ECDHE along with Kyber RSA paired with Dilithium for dual signatures These methods help maintain compatibility with older systems while adding quantum resistance. Tests show some extra delay but also significant security improvements.

C. Cloud-Specific PQC Deployment Studies

Various studies highlight unique challenges in deploying PQC in cloud environments, such as: Handling the large-scale reissuance of certificates Managing multi-tenant infrastructure limitations Dealing with performance issues from larger key sizes Impact on bandwidth and storage usage Research shows that lattice-based schemes increase the size of handshakes but are still practical for large cloud operations.

D. Risk Models and "Harvest Now, Decrypt Later"

Security experts introduced the "Harvest Now, Decrypt Later" (HNDL) threat model, which stresses the need to move to PQC quickly to protect long-term sensitive data. Studies suggest focusing on: Government records Financial transaction data Healthcare information This research supports the idea of moving to PQC in a planned, step-by-step way rather than waiting for a crisis.

Gaps in Existing Research

Even though there's a lot of research on PQC algorithms, some issues remain: Few frameworks that can handle full migration for major cloud providers Not enough testing of performance in real-world multi-cloud setups No widely accepted models for integrating PQC into cloud-native systems Little attention to following regulations during the transition Most research looks at the security of the algorithms themselves, not how they work in real cloud environments.

Research Contribution Positioning

This paper builds on previous work by: Suggesting a structured, multi-phase model for moving to PQC in cloud systems Combining crypto-agility, hybrid deployment, and compliance considerations Analyzing how performance and security balance in large cloud environments Designing a layered architecture that can help with the practical transition to PQC The background and related work show that while PQC algorithms are moving toward official standards, there's still important work needed to develop effective strategies for cloud migration.

Cloud-Specific Challenges in PQC Migration

Moving from old encryption methods like RSA and ECC to Post-Quantum Cryptography (PQC) in cloud systems is difficult because of how big and complex cloud environments are.

Performance Overhead

PQC uses bigger keys and needs more computing power than traditional encryption. This can cause: - Slower network connections because of bigger handshake processes - More storage space needed - Higher use of computer processors in busy cloud services

Hybrid Compatibility

While switching to PQC, cloud systems need to work with both old and new encryption methods. This means: - More complicated communication protocols, like during TLS setup - Need to keep old systems working with new ones - More testing and checking to make sure everything works.

Key Management Complexity

Cloud Key Management Services (KMS) have to deal with: - Different types of keys - More storage for larger keys - Securely changing keys across many different locations - Updating hardware security modules (HSMs) and secure areas adds more work

Multi-Tenant and Distributed Architecture

Cloud systems run in many different regions and use changing virtual machines. Making sure: - PQC is properly set up everywhere - Keys are copied securely - There is no interruption in service is tough when dealing with large numbers of users and systems

Standards and Compliance Gaps

PQC is still being developed into standards. Without clear rules and certifications, it's hard to use PQC in cloud systems that need to follow strict regulations.

Proposed Migration Framework

This section introduces a clear and flexible approach for moving from older encryption methods like RSA and ECC to Post-Quantum Cryptography in cloud systems. The plan is built to keep security strong, operations running smoothly, and meet legal requirements throughout the changeover.

A. Cryptographic Asset Discovery and Risk Assessment

The first step is to find and list all cryptographic assets used in the cloud setup. This includes things like TLS certificates, VPN connections, encrypted storage, identity and access control systems, APIs, and connections with outside services.A full risk check is done to:

Find out which algorithms are weak, like RSA, ECC, and Diffie-Hellman.

Check how long data needs to stay secure, considering the risk of someone storing data now and decrypting it later.

Group workloads based on how sensitive the data is and what rules apply.

Decide which parts of the system need to be updated first based on how risky they are.

The result of this step is a plan to move to new encryption methods that fits with security and compliance goals.

B. Hybrid Cryptographic Enablement

To keep things working smoothly and avoid breaking old systems, the process uses a mix of old and new encryption methods during the changeover.In this part:

Old and new encryption methods run at the same time.Both types of encryption are used together in secure communication tools like TLS.Software used for encryption and cloud tools are updated to support new, stronger encryption methods.Tests are done to make sure everything works with older systems and third-party tools.This mixed approach helps avoid problems from future computer power while keeping the current setup working.

C. Cloud Infrastructure and Key Management Adaptation

The move needs changes to how cloud security is set up, especially parts that manage keys, like Key Management Services (KMS) and Hardware Security Modules (HSMs).Key actions are: Making sure new encryption types and bigger key sizes work.Updating how keys are stored, copied, and backed up. Changing rules about how often keys are changed and how they're handled over time. Allowing the system to quickly switch to new encryption methods if needed. This step makes sure key management stays strong and can handle large cloud environments.

D. Phased Deployment and Performance Optimization

Because cloud systems are big, the move happens step by step. Deployment plans include: Focusing on the most risky or important parts first. Putting new changes in one area or part of the system at a time.Checking how fast the system works, how much data it can handle, and how well connections are made.Testing how much extra work the new encryption causes and making sure resources are used well.A test rollout, where a small part of the system is changed first, is suggested to keep things running smoothly and check performance.

E. Full PQC Enforcement and Legacy Decommissioning

Once everything is ready and works well together, old encryption methods are stopped. This stage involves: Turning off old methods like RSA and ECC for key exchanges.

Using only new encryption methods that can handle future computer power. Updating legal and certification documents. Checking security with independent experts. The end goal is a cloud system that can handle future threats from powerful computers.

F. Design Principles of the Framework

The plan follows these main ideas: Flexibility to quickly switch to new encryption standards as they come. Support for old systems while changing to new methods. Designed to work well in large, shared cloud environments. Making sure services keep running without interruptions. Following new rules for strong encryption that are coming out.

Hybrid Cloud Migration Architecture

To make the switch from old cryptography methods like RSA and ECC to new Post-Quantum Cryptography (PQC) safe and manageable, a Hybrid Cloud Migration Architecture (HCMA) is suggested. This setup helps move things step by step, keeps older systems working with new ones, and avoids big disruptions in both public and private cloud setups.

A. Layered Hybrid Integration

This architecture mixes old and new security methods across different parts of the cloud:-

- Application Layer: Uses PQC-ready APIs and libraries that can switch between different encryption methods as needed.-
- Transport Layer: Combines traditional and PQC methods for secure data transfer using a mixed TLS setup.
- Data Storage Layer: Slowly moves encryption keys to be protected using PQC techniques
- Identity and Access Management (IAM) Layer: Uses PQC for signing in and creating secure tokens.
- Key Management Layer: Has a system that can handle both old and new key types, allowing for generating, storing, and updating keys as needed.

B. Phased Deployment Model

The move to PQC happens in three steps:

1. Hybrid Enablement: Both old and new encryption methods work at the same time.
2. Priority Migration: Important tasks that are at higher risk are fully switched to PQC.
3. Classical Decommissioning: Older encryption methods are turned off after they are confirmed to be safe to remove.

C. Performance and Governance Considerations

The system includes ways to test performance, manage keys across different locations, check compliance with rules, and have backup plans in case something goes wrong. These features help make the process scalable, meet legal standards, and keep things running smoothly.

Security Analysis

The proposed migration plan improves cloud security by dealing with weaknesses in old encryption methods that could be broken by quantum computers. Traditional systems like RSA and ECC can be cracked using quantum computing techniques, but Post-Quantum Cryptography (PQC) uses math problems that are hard for both regular and quantum computers to solve.

While moving to PQC, a mix of old and new encryption methods is used, offering double protection. This ensures security as long as at least one method is still safe. This helps prevent the risk of attackers collecting encrypted data now and breaking it later. Also, this approach works with existing systems, so there's no need to replace everything at once.

The system keeps important security features like keeping data secret, making sure it hasn't been changed, and confirming the sender's identity. It uses PQC for exchanging keys and creating digital signatures. Also, the system allows for easy updates and changing keys, which makes it safer over time.

Performance Evaluation

This section evaluates the performance impact of migrating from traditional cryptography to Post-Quantum Cryptography (PQC) in cloud environments.

A. Evaluation Metrics

The migration strategy is checked using these measures:Time to create keysTime to encrypt and decrypt dataTime taken for a secure connection to startUse of computer processor and memoryExtra data sent over the network because of encryption and key sizeHow much data can be processed when many users are using the system at the same timeThese measures show how well the system works in real cloud environments.

B. Comparative Analysis

When compared to old methods like RSA and ECC, PQC methods usually have:Larger keys and signaturesMore data sent during secure connectionsA little more work needed to process dataHowever, the speed of symmetric encryption isn't greatly affected. Using a mix of encryption methods adds a bit of delay because of two key exchanges, but it still works well in large cloud systems.

C. Scalability Considerations

Testing shows that:Adding more computers can handle higher processing needs.Better PQC software reduces delays.The ability to switch between different algorithms helps adjust performance as needed.

Compliance and Governance

Successful migration to Post-Quantum Cryptography (PQC) in cloud systems needs strong compliance and governance. Cloud providers must make sure that the switch to new cryptography follows changing cybersecurity rules, data protection laws, and industry standards.

A centralized governance system should set which algorithms are allowed, allow for easy changes in algorithms, and focus on high-risk tasks first for migration. It's important to keep track of security through ongoing monitoring, logging activities, and regular security checks to stay transparent and accountable.

Policies based on risk should help in gradually replacing old, weak algorithms while keeping services running smoothly.

In the end, good compliance and governance make sure that using PQC is secure, follows standards, and stays legal in cloud environments where things are spread out.

Implementation Case Study (Hypothetical)

To demonstrate the feasibility of the proposed migration framework, a hypothetical case study is considered for a multi-region cloud service provider hosting financial and healthcare applications.

A. Initial Environment

The cloud infrastructure uses:

- RSA-2048 and ECC for TLS key exchange
- AES-256 for data encryption
- Centralized Key Management Service (KMS)
- Multi-tenant microservices architecture

B. Migration Process

The provider adopts a phased hybrid strategy:

- Assessment Phase: Cryptographic inventory identifies vulnerable RSA/ECC dependencies.
- Hybrid Deployment: TLS is upgraded to support classical + PQC key exchange.
- KMS Upgrade: PQC key generation and storage support are integrated.
- Priority Migration: Financial transaction services migrate fully to PQC.
- Decommissioning: Standalone classical key exchange is disabled after validation.

C. Observed Outcomes

- Slight increase in TLS handshake latency during hybrid phase.
- Increased key storage requirements due to larger PQC keys.
- No service downtime due to phased deployment.
- Enhanced resilience against future quantum threats.

Open Research Challenges

- Performance Optimization
- Standardization and Interoperability
- Secure Hybrid Design
- Scalable Key Management
- Compliance and Governance Models

Figure 10

Conclusion

The fast progress of quantum computing poses a big danger to traditional encryption methods like RSA and ECC, which are the main way modern cloud systems keep data safe. To deal with this new risk, this paper suggests a clear and step-by-step plan to move towards Post-Quantum Cryptography (PQC) that works well in cloud environments where many users share the same system.

This plan focuses on using both old and new encryption together, making it easy to switch algorithms as needed, managing keys efficiently at scale, improving performance, and following strict security rules. A step-by-step rollout helps keep the system working smoothly while slowly making it more resistant to quantum attacks.

While PQC brings some challenges in terms of computing power and system design, thoughtful planning, using a mix of old and new systems, and ongoing checks can make the transition both safe and practical. Future work should aim to improve how well PQC works, set common standards for different systems, and test it in real-world situations on a large scale.

In the end, moving to PQC early is important to keep data private, ensure it stays accurate, and maintain trust in cloud systems as we enter the post-quantum era.

References

1. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS), 1994, pp. 124–134.
2. L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proc. 28th Annual ACM Symposium on Theory of Computing (STOC), 1996, pp. 212–219.
3. National Institute of Standards and Technology (NIST), “Post-Quantum Cryptography Standardization,” NIST IR 8413, 2022.
4. D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.
5. J. Bos et al., “CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM,” in Proc. IEEE European Symposium on Security and Privacy, 2018.
6. L. Ducas et al., “CRYSTALS–Dilithium: Digital signatures from module lattices,” IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018.
7. A. Langley, M. Hamburg, and S. Turner, “Post-Quantum TLS,” Internet Engineering Task Force (IETF) Draft, 2020.
8. M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?” IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
9. ETSI, “Quantum-Safe Cryptography and Security,” ETSI White Paper No. 8, 2015.
10. N. Bindel et al., “Hybrid key exchange in TLS 1.3,” IACR Cryptology ePrint Archive, 2019.
11. S. Fluhrer et al., “Guidelines for migrating to post-quantum cryptography,” NIST Draft Report, 2020.
12. C. Peikert, “A decade of lattice cryptography,” Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016.