International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at wwwijsred.com

RESEARCH ARTICLE OPEN ACCESS

Quantum-Resilient Cryptographic Frameworks for Post-Quantum Cloud and Edge Computing

Aswathy P S
Department of Computer Science, Narayanaguru college of engineering
Email: ps.aswathy.nair15@gmail.com

----------**********----------

Abstract

The rapid advancement of quantum computing introduces unprecedented security threats to modern cloud and edge computing infrastructures. Classical public-key cryptographic algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC) are fundamentally vulnerable to quantum attacks enabled by Shor's algorithm. As a result, the confidentiality, integrity, and authenticity of data stored and processed in distributed systems are at serious risk.

Post-quantum cryptography (PQC) aims to develop cryptographic algorithms that are resistant to both classical and quantum adversaries. This paper presents a comprehensive quantum-resilient cryptographic framework designed specifically for post-quantum cloud and edge computing environments. The framework integrates post-quantum cryptographic primitives, hybrid cryptographic approaches, crypto-agile architectures, and secure key management mechanisms.

The proposed framework addresses performance constraints, scalability requirements, and deployment challenges in heterogeneous environments. A detailed discussion of security threats, architectural components, performance considerations, and future research directions is provided. The proposed approach enables long-term security and supports a smooth transition toward quantum-safe distributed computing systems.

Keywords

Post-Quantum Cryptography, Quantum Security, Cloud Computing, Edge Computing, Crypto Agility, Quantum-Resilient Frameworks

----------**********----------

1. Introduction

Cloud computing and edge computing have emerged as fundamental paradigms for delivering scalable computing, storage, and real-time data processing services. These technologies support a wide range of applications including healthcare analytics, financial systems, smart cities, industrial automation, and Internet of Things (IoT) ecosystems.

Security in cloud and edge environments relies heavily on cryptographic mechanisms for secure communication, authentication, access control, and data protection. However, the rapid progress of quantum computing poses a serious threat to these cryptographic foundations. Quantum algorithms such as Shor's algorithm can efficiently solve problems that form the basis of widely used public-key cryptosystems.

In addition, Grover's algorithm reduces the effective security of symmetric cryptographic algorithms, necessitating larger key sizes. Cloud and edge systems are particularly vulnerable due to long-term data storage and large-scale distributed communication. This paper proposes a quantum-resilient cryptographic framework that ensures long-term security while maintaining performance and scalability.

2. Related Work

Significant research efforts have focused on developing post-quantum cryptographic algorithms to counter quantum-enabled attacks. Lattice-based cryptography has gained attention due to its strong

security assumptions and computational efficiency. Hash-based and code-based cryptographic schemes also provide promising quantum resistance.

Hybrid cryptographic approaches combining classical and post-quantum algorithms have been proposed to support gradual migration. Existing cloud security frameworks primarily depend on classical cryptography and lack crypto-agility. Edge computing research often prioritizes low latency and resource efficiency, leaving long-term cryptographic resilience underexplored.

Despite these advancements, comprehensive frameworks that jointly address cloud and edge computing security in the post-quantum era remain limited. This paper aims to bridge this research gap.

3. Quantum Threat Model

Quantum computers exploit quantum mechanical principles such as superposition and entanglement to perform computations that are infeasible for classical computers. Shor's algorithm enables polynomial-time factorization and discrete logarithm computation, rendering RSA, Diffie–Hellman, and ECC insecure.

Grover's algorithm provides a quadratic speedup for brute-force attacks against symmetric cryptographic systems. As a result, symmetric encryption and hash functions require increased key sizes to maintain equivalent security levels.

Cloud infrastructures store vast volumes of sensitive data for long durations, making them vulnerable to harvest-now, decrypt-later attacks. Edge devices often operate with limited computational and energy resources, further increasing their exposure to quantum threats.

4. Post-Quantum Cryptographic Primitives

Lattice-based cryptography relies on the hardness of mathematical problems such as Learning With Errors (LWE) and Short Integer Solutions (SIS). Algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium have been selected by NIST for standardization.

Hash-based cryptographic schemes such as SPHINCS+ offer strong security guarantees based solely on cryptographic hash functions. While highly secure, these schemes incur large signature sizes and increased communication overhead.

Code-based cryptography, including McEliece variants, has demonstrated long-term resistance to quantum attacks. However, large public key sizes limit their applicability in resource-constrained edge environments.

5. Proposed Quantum-Resilient Framework

The proposed quantum-resilient framework integrates post-quantum cryptographic mechanisms into cloud and edge computing infrastructures using a modular and crypto-agile design.

The framework consists of a post-quantum secure communication layer, hybrid cryptographic engine, crypto-agility abstraction layer, quantum-resilient key management infrastructure, and an edge optimization module.

This architecture ensures secure communication, authentication, and data storage while enabling dynamic algorithm migration and system scalability.

6. Hybrid Cryptographic Deployment

Hybrid cryptographic deployment combines classical and post-quantum algorithms to ensure backward compatibility and enhanced security during the transition phase.

Hybrid TLS handshakes allow systems to negotiate both classical and post-quantum keys, providing protection against quantum attacks while maintaining interoperability with legacy systems.

7. Crypto Agility and Key Management

Crypto agility refers to the ability of a system to dynamically replace cryptographic algorithms without significant architectural changes.

The proposed framework incorporates a crypto-agile key management infrastructure supporting automated key rotation, algorithm migration, secure storage, and policy enforcement.

8. Performance and Deployment Considerations

Edge computing environments are constrained by limited computational power, memory, and energy resources. Efficient PQC deployment requires lightweight algorithms and optimization techniques.

Cloud environments demand scalability, multi-tenant isolation, and distributed key management. Hardware acceleration and computation offloading play a critical role in maintaining performance.

9. Challenges and Future Directions

Despite advancements in post-quantum cryptography, challenges remain including increased key sizes, communication overhead, lack of mature PQC hardware, and evolving standards.
Future research should focus on lightweight PQC algorithms, hardware accelerators, cross-platform interoperability, and real-world benchmarking.

10. Conclusion

This paper presented a comprehensive quantum-resilient cryptographic framework for post-quantum cloud and edge computing environments. By integrating post-quantum primitives, hybrid cryptographic techniques, and crypto-agile architectures, the framework ensures long-term security against quantum-enabled threats.
The proposed approach supports scalable, secure, and future-proof distributed computing systems.

References

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of FOCS, 1994.
NIST, Post-Quantum Cryptography Standardization Project, 2022.
D. J. Bernstein et al., Post-Quantum Cryptography, Nature, 2017.
A. Alabdulatif et al., Quantum-safe security for cloud computing, IEEE Access, 2020.

