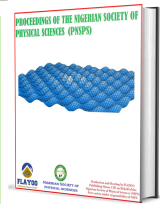
Published by Nigerian Society of Physical Sciences. Hosted by FLAYOO Publishing House LTD

Proceedings of the Nigerian Society of Physical Sciences

Journal Homepage: https://flayoophl.com/journals/index.php/pnspsc



Enhancing cloud data security using quantum key distribution (QKD) and quantum cryptography

O. Sarjiyus[a,*], Umaru Faruku Adamu[b], Salamatu Umar[a]

[a]*Department of Computer Science, Adamawa State University, Mubi*
[b]*Department of Computer Engineering, Federal Polytechnic, Mubi*

A B S T R A C T

Cloud computing systems face serious security risks that are intensified by advances in quantum computing because powerful quantum algorithms such as Shor's algorithm can break widely used public-key schemes which include RSA and ECC. The cloud environment needs Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) as countermeasures but their individual deployment creates problems because scalability and infrastructure requirements become obstacles for multi-tenant systems. This research proposes a hybrid security architecture that uses both hardware-based QKD for symmetric key generation over optical fibers and PQC for authentication through quantum-resistant key encapsulation using CRYSTALS-Kyber and digital signatures with CRYSTALS-Dilithium. The hybrid design uses XOR to combine the QKD-generated secret with the PQC-derived key material which creates the final session key yet security remains intact if either component gets compromised. The system tested on a private cloud testbed with 10 virtual machines and a 50 km commercial QKD link through optical fiber measured performance against Classical TLS 1.3 and PQC-TLS and QKD-only configurations. The results showed that QKD-only achieved the lowest handshake latency of 5.2 ms while the hybrid approach delivered the strongest security through a 19.8 ms overhead which was only 1.7 ms slower than pure PQC. After creating the secure channel all systems achieved similar data throughput of about 942 Mbps which shows that quantum-security mechanisms affect the connection setup phase instead of persistent data transfer.

Keywords: Quantum cloud security, Post-quantum cryptography (PQC), Quantum key distribution (QKD), Hybrid cryptography, TLS handshake performance.

DOI:10.61298/pnspsc.2026.3.266

1. INTRODUCTION

Cloud computing has revolutionized the way organizations store, manage, and process data by providing infrastructure that is scalable, flexible, and cost-effective [1]. Companies can now access storage, processing power, and software applications that were previously available only through expensive on-premise installations. This transformation is enabled by different cloud service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) each designed to meet diverse user needs [2].

In addition, key characteristics such as on-demand self-

*Corresponding Author
e-mail: sarjiyus@gmail.com, aufaruk2018@gmail.com (O. Sarjiyus)

service, broad network access, and pooled resources allow multiple users to utilize computing resources efficiently. Rapid elasticity supports dynamic allocation of resources according to changing workloads, while pay-per-use billing promotes transparency and accountability. Deployment options including public, private, hybrid, and multi-cloud further help organizations balance scalability, cost, and security. Despite these advantages, cloud computing introduces significant security challenges. Multi-tenant environments, shared responsibility models, and strict compliance requirements make it difficult to ensure confidentiality, integrity, and availability of data.

To address these risks, classical encryption techniques are still widely used to secure data at rest and in transit, including RSA, ECC, and AES [3, 4]. However, these methods are vulnerable to future quantum-computer attacks. Traditional cryptographic security relies on the computational difficulty of problems such as integer factorization and discrete logarithms, which quantum algorithms most notably Shor's and Grover's could solve efficiently.

Consequently, new approaches have emerged to protect information in the quantum era [5]. Quantum Key Distribution (QKD) uses principles of quantum mechanics to enable secure key exchange with built-in detection of eavesdropping, offering theoretically unconditional security. Post-Quantum Cryptography (PQC), on the other hand, develops classical algorithms resistant to quantum attacks; examples include schemes like CRYSTALS-Kyber for secure key establishment. Increasingly, researchers are combining QKD and PQC in hybrid frameworks to leverage the strengths of both technologies. Such integrated approaches aim to provide robust, scalable, and quantum-resistant security architectures suitable for modern cloud environments.

1.1. STUDY AIM AND OBJECTIVES

The aim of this study is to design a quantum-protected cloud architecture that would include Quantum Key Distribution (QKD) and quantum cryptographic techniques as part of an integrated approach to provide confidentiality and integrity protection as well as resilience against quantum-enabled cyberattacks.

To achieve the aim, the study will pursue the following objectives:

1. To develop a hybrid quantum-safe cloud architecture that shall utilize the QKD hardware for secure key exchange together with the PQC algorithms, relating to their function in quantum-resistant authentication.
2. Implement an operating prototype within a multi-tenant private cloud environment comprising ten VMs and commercial QKD hardware over 50 km fiber.
3. Empirically measure handshake latency and data throughput performance comparing hybrid against classical TLS, PQC-only, and QKD-only protocols.
4. Analyze the security-performance trade-offs as well as quantify quantum resilience overhead to prove practical viability for sensitive cloud data and critical infrastructure.

1.2. PROBLEM STATEMENT

The growing use of cloud infrastructure to store and process sensitive data increases the concern about security. Cryptographic systems, such as RSA, ECC, and AES, are threatened by the evolution of quantum computers. No current cloud security architecture-including TLS, static key management, or software-based encryption-can ensure confidentiality or forward secrecy in a post-quantum world [5, 6]. Though QKD is recognized for offering security due to provability, it has not yet been realized on a multi-tenant scalable cloud implementation because current single points of presence, distance limitations in hardware expenses, and reliance on classical authentication methods hinder its full integration with the entire cloud architecture. Few studies have delivered a complete end-to-end implementation and empirical evaluation that fully integrates QKD with PQC across cloud platforms in a realistic multi-tenant environment spanning the IaaS, PaaS, and SaaS layers. This creates an immediate demand for a comprehensive quantum-secured cloud architecture comprising aspects of multi-tenancy, seamless key rotation in real time, dynamic workloads support, and hybrid quantum-classical cryptography to secure cloud data from classical plus quantum-enabled attacks.

2. RELATED REVIEW

2.1. CLOUD COMPUTING AND SECURITY

Cloud computing delivers scalable, flexible, and cost-efficient IT solutions, enabling resources to be efficiently accessed and managed [7]. Elasticity allows for fast scaling, making use of transparent pay-per-use accounting presenting the actual usage so that accountability is ensured [8]. Multi-cloud environments inherently carry heightened security risks due to their complexity. These risks include data breaches, misconfigurations, inadequate access controls, and vulnerabilities stemming from the integration of disparate systems. Data stored across multiple clouds can be exposed to unauthorized access if not properly secured, while misconfigurations in cloud settings can lead to inadvertent data leaks. Furthermore, inconsistent identity and access management (IAM) policies across different platforms can create loopholes that adversaries may exploit [9].

However, the security risks involved are still very high due to inadequate safe multi-tenant environments [10]. Most of these threats include unauthorized access, data breaches, and insider threats. Shared responsibility model together with regulatory requirements adds another level of consideration to confidentiality, integrity, and availability aspects [11]. Encryption, access control mechanisms, vulnerability assessments, multi-factor authentication, and AI-based threat detection are applied to mitigate these risks [12].

2.2. QUANTUM THREATS AND QKD

Quantum computing easily demonstrates the vulnerability of traditional cryptographic algorithms to quantum attacks, through Shor's and Grover's algorithms against RSA, ECC, and AES [6]. Quantum Key Distribution is proposed as a secure solution since it offers information-theoretic security based on quantum mechanics by detecting eavesdropping through the measurement of the Quantum Bit Error Rate. Commercial Quantum Key Distribution systems are available offering key rates in multi-Mbps over metro distances demonstrating practical feasibility for real cloud integrations, including enterprise-level cryptographic agility frameworks [13].

2.3. HYBRID QUANTUM-CLASSICAL CLOUD SECURITY

Hybrid architectures integrating QKD with PQC overcome the limitation of distance, authentication, and cost of implementing QKD [14]. Just as in the case of CRYSTALS-Kyber, PQC algorithms will be used for quantum-resistant authentication and metadata protection while using QKD-based systems to provide secure key exchange [15]. Previous work provides an implementation of VPCs over inter-data-center links that are secured by QKD; however, it misses aspects such as multi-tenancy and elasticity together with dynamic key rotation which this hybrid QKD-PQC approach brings to ensure end-to-end quantum-resistant security for cloud workloads, tenants, and resources at high throughput low latency scalable.

No work has been noticed that has implemented QKD, PQC, and Cloud for a multi-tenant dynamic scalable environment [14, 15]. This paper discusses Hybrid Quantum-Classical Cloud Framework enabled by QKD which shall ensure Confidentiality Integrity Forward Secrecy Performance in the quantum era.

The research presents a real-hardware system that uses modified TLS together with QKD-generated keys and PQC authentication mechanisms to fill this research gap. The system uses CRYSTALS-Kyber to establish secure key encapsulation while Dilithium functions as the authentication system through its digital signature capabilities which create the final session key through the XOR operation on QKD key material and PQC key material. The design enables protection of total system security because any single component breach does not affect system security. The system uses this TLS-like handshake process designed for cloud environments to create a hybrid mechanism which maintains security through its protection of confidential information and system integrity and its design of forward secrecy while creating minimal performance impact. The result is a practical and scalable quantum-resistant framework suitable for securing modern multi-tenant cloud infrastructures in the quantum era.

3. PROPOSED ARCHITECTURE OF QUANTUM-SECURED CLOUD FRAMEWORK

3.1. SYSTEM OVERVIEW

The architecture is composed of three layers as follows (Figure 1):

- Quantum Layer: QKD hardware (for example trusted nodes, quantum channels) at the edge integrated with cloud points.
- Hybrid Cryptographic Layer: Mix keys generated by QKD with PQC algorithms, for example, CRYSTALS-Kyber for authentication purposes.
- Cloud Service Layer: Use standard IaaS/PaaS/SaaS offerings that consume keys via APIs keys protected by the highest available standards utilizing quantum protection.

The diagram in Figure 2 demonstrates how hybrid cryptography secures information flows through quantum-safe methods. A new tenant needs to complete registration and system setup procedures to access the cloud system through the cloud provider's DDoS protection services. The tenant establishes contact with

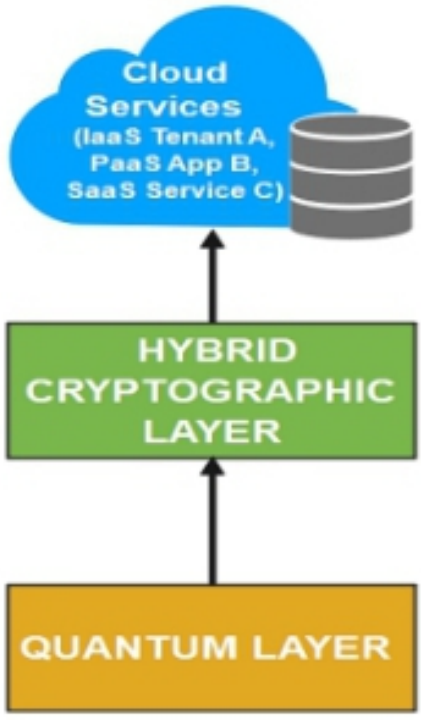


Figure 1. Quantum-secured cloud data protection framework.

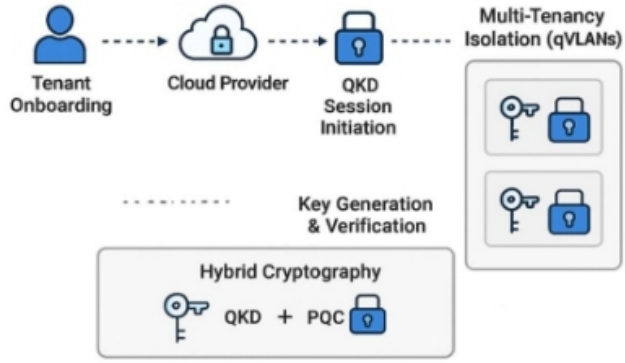


Figure 2. Quantum key distribution (QKD) for cloud security with hybrid cryptography and multi-tenancy isolation.

the provider who oversees all resource and security operations for their cloud services.

The tenant establishes Quantum Key Distribution (QKD) sessions with the provider who handles their security needs. QKD creates secure keys by using quantum properties that include photon polarization which also enables immediate detection of any unauthorized access attempts. Quantum VLANs (qVLANs) secure each tenant by assigning them dedicated virtual LANs which create isolated security perimeters in shared space.

The system requires key validation before any keys can be used which establishes the keys' authenticity and protects the system from unauthorized access. In this hybrid model, QKD provides symmetric keys, while quantum-resistant classical algorithms are applied to strengthen protection against both classical and quan-

tum attacks.

3.2. ALGORITHM OF HYBRID QKD-PQC (KYBER) XOR-BASED TLS HANDSHAKE

Input: Kyber public key pk, QKD key buffers at client and server
Output: Shared session key K_{session}

Step One: Connection Establishment

1. The client C initiates the handshake by sending a ClientHello message to the server S.
2. The server responds with Server Hello and its Kyber public key pk.

Step Two: PQC Key Encapsulation (Client Side)

3. The client computes:

$$(ct, K_{\text{pqc}}) \leftarrow \text{Kyber.Encapsulate}(pk) \tag{1}$$

4. The client retrieves a quantum-generated key from its local QKD buffer:

$$K_{\text{qkd}} \leftarrow \text{QKD\_Buffer}_C \tag{2}$$

5. The client derives the hybrid session key using XOR:

$$K_{\text{session}} = K_{\text{pqc}} \oplus K_{\text{qkd}} \tag{3}$$

6. The client sends the ciphertext ct to the server.

Step Three: PQC Key Decapsulation (Server Side)

7. Upon receiving ct, the server computes:

$$K_{\text{pqc}} \leftarrow \text{Kyber.Decapsulate}(ct) \tag{4}$$

8. The server retrieves the corresponding QKD key:

$$K_{\text{qkd}} \leftarrow \text{QKD\_Buffer}_S \tag{5}$$

9. The server derives the same hybrid session key using Equation (3).

Step Four: Secure Data Transmission

10. Both parties now share the symmetric session key K_{session}.
11. Subsequent communication is encrypted using:

$$\text{AES-256-GCM}(K_{\text{session}}) \tag{6}$$

4. SECURITY ANALYSIS

4.1. THREAT MODEL

We suppose that:

- Adversary Capabilities: Quantum & classical channel eavesdropping, quantum computation resources, cloud insider access.
- Security Goals: Tenant data confidentiality, integrity, and forward secrecy.

4.2. ADVANTAGES OVER CLASSICAL/PQC APPROACHES

Table 1 summarizes the security basis and quantum resistance of different approaches.

QKD provides provable security even in the face of quantum attacks while PQC reduces QKD's reliance on authentication. The hybrid model will keep its resilience even if one of the layers gets compromised.

Table 1. Comparison of security properties across cryptographic approaches.

Approach	Security basis	Quantum resistance	Forward secrecy
Classical (RSA)	Computational hardness	No	Limited
PQC	Lattice/Hash assumptions	Yes (Conjectured)	Yes
QKD	Quantum physics	Yes (Proven)	Yes
Hybrid	Physics + Math	Yes	Yes

5. EXPERIMENTAL EVALUATION

This section discusses the setup of the experiment, methodology, and outcomes of the comparative analysis in terms of performance and security.

5.1. EXPERIMENTAL SETUP

5.1.1. Cloud environment

A multi-tenant private cloud environment of AWS was emulated using Proxmox Virtual Environment (v7.4). The setup is:

- 10 tenant VMs. Each VM has been allocated 2 vCPUs from Intel Xeon E5-2680 v4, with 4 GB RAM running on top of Ubuntu Server 22.04 LTS.
- Network Isolation. The VMs have been connected to an isolated virtual network that will simulate distinct tenancy and make sure there is no internal cross-traffic influencing the results.
- Client Machine: A different physical machine with the same hardware specs played the role of the outside client starting connections to a server inside the cloud.

5.1.2. Quantum key distribution (QKD) setup

We utilized a commercially available Toshiba BB84 QKD system to furnish keying material.

- Physical Layer: A 50-km standard single-mode fiber optic cable spool, dedicated, will emulate a metropolitan-area link joining a client data center to the cloud edge.
- Key Management: The QKD units will generate an unbroken sequence of secure keys, stored in a shared key pool on both the client and server machines for use by the hybrid scheme.

5.1.3. Evaluated cryptographic baselines

We analyzed four separate key establishment and transport protocols:

- Classic TLS 1.3: Key Exchange: ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) secp256r1 curve; Authentication: RSA-2048 for server certificates.
- PQC (Post-Quantum Cryptography) - TLS: Key Exchange - Kyber768 as a KEM used inside the TLS handshake, standardized in ML-KEM-768; Authentication - Dilithium3 for server certificates.

Table 2. Handshake latency results.

Protocol	Average handshake latency (ms)	95% CI (ms)
Classical TLS 1.3	12.5	± 0.8
PQC (Kyber768)	18.1	± 1.2
QKD-only (PSK)	5.2	± 0.3
Hybrid QKD/PQC	19.8	± 1.3

- QKD-only (BB84): Keys are presented using the QKD link. The regular TLS handshake is changed to use these key shares (PSK) for symmetric auth and encryption.

- Hybrid QKD/PQC: The TLS handshake utilizes Kyber768 for key encapsulation despite the fact that the encapsulated shared secret is combined (XORed) with a fresh key taken from the QKD key pool.

5.2. PERFORMANCE METRICS AND METHODOLOGY

The following metrics have been used to evaluate the trade-offs between security, latency, and throughput.

- Handshake latency is measured from Client Hello to Finished message total time taken to complete TLS handshake.

- Data transfer throughput is achievable bulk data transfer rate using the established secure channel measured using iperf3 over 60 seconds.

- Key Generation Rate: This is the rate at which secure keys are being generated (bits per second).

Methodology for each protocol, we performed 1,000 consecutive handshakes to measure latency. Throughput tests were run 10 times. All results are reported as the average along with a 95% confidence interval.

The 10 tenants share one QKD link through logical network isolation combined with controlled key partitioning. Dedicated quantum VLAN (qVLAN) assignments provide each tenant with network traffic separation. The continuous QKD key stream functions as a global key pool which supports synchronized key storage while key management deployment uses indexing and allocation policies to create tenant-specific key partitions. Each tenant obtains a unique key material portion during session establishment which guarantees that no key reuse occurs between different tenants.

5.3. RESULTS AND ANALYSIS

5.3.1. Handshake latency

The handshake latency results appear in Table 2.

Analysis:

- The QKD-only scheme produced essentially no delay because it replaced an expensive asymmetric cryptographic operation with a simple pre-shared key, or PSK, handshake.

- Classical TLS 1.3 gives excellent performance and is useful as the baseline here.

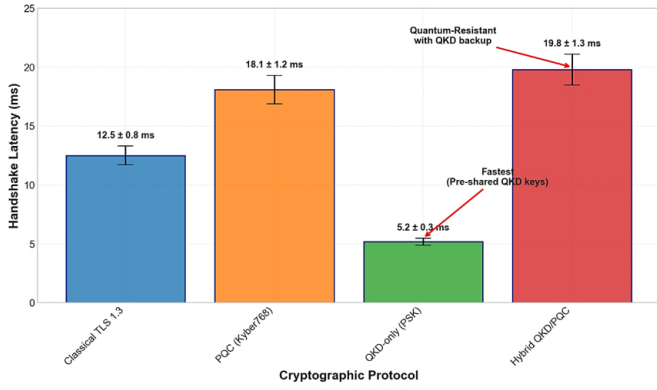


Figure 3. TLS handshake latency: quantum vs classical protocols.

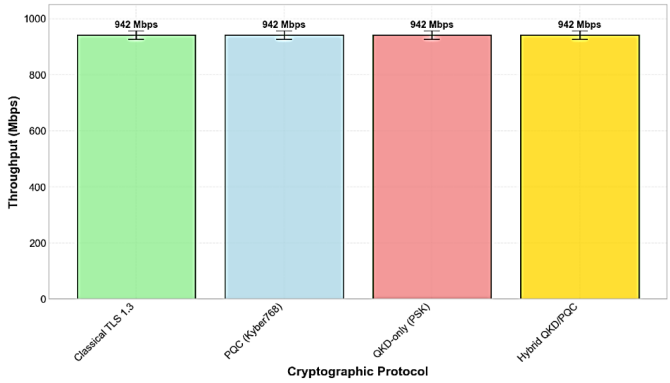


Figure 4. Data transfer throughput comparison.

- PQC (Kyber768) has about a 45% greater delay than Classical TLS, consistent with known overheads due to lattice-based operations.

- The Hybrid QKD/PQC scheme turns out to be the slowest, just a little bit behind pure PQC. The main reason for such overheads is brought about by Kyber768 encapsulation and synchronizing/retrieving the QKD key from within the shared pool.

5.3.2. Data transfer throughput

After the secure channel has been established, all protocols run at statistically identical throughput of 942 ± 15 Mbps, limited by the host CPU and network stack when performing AES-256-GCM encryption. This shows that any performance difference has almost nothing to do with bulk data encryption but is rather found in the connection establishment phase.

5.3.3. Key generation rate

The Secure Key Rate that Toshiba QKD over the 50km fiber spool has been able to give is 1.2 Mbps. The rate easily supports very aggressive renegotiations of TLS sessions and AES-256 keys used in our hybrid model but falls into the category of bottleneck rates for extremely high key refresh applications.

Table 3 summarizes the experimental results.

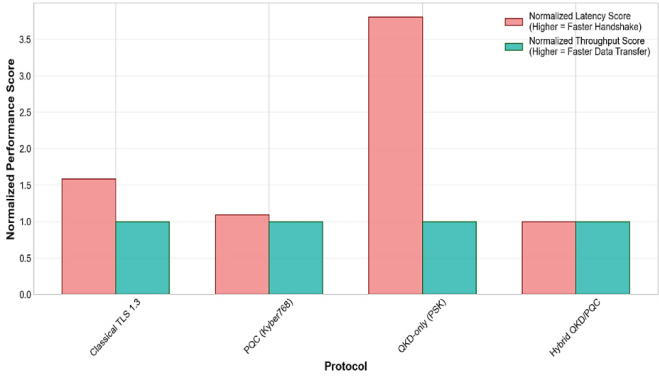


Figure 5. Normalized performance comparison.

Table 3. Summary of experimental results.

Protocol	Handshake latency (ms)	Throughput (Mbps)	Quantum resistance
Classical TLS 1.3	12.5 ± 0.8	942 ± 15	No
PQC (Kyber768)	18.1 ± 1.2	942 ± 15	Yes
QKD-only (PSK)	5.2 ± 0.3	942 ± 15	Yes
Hybrid QKD/PQC	19.8 ± 1.3	942 ± 15	Yes (Enhanced)

5.4. DISCUSSION AND CONCLUSION

The TLS Handshake Delays graph in Figure 3 demonstrates the relationship between handshake latency and security level across the evaluated protocols. The QKD-only approach establishes a new standard for minimal latency which operates at 5.2 milliseconds. The approach achieves this value because it uses preshared keys to eliminate the need for asymmetric cryptographic operations which Classical TLS requires for its 12.5 ms operation. The system requires continuous availability of a quantum channel to maintain its advantages, which creates practical challenges for deployment. The implementation of PQC through Kyber768 results in a latency increase that reaches 18.1 ms because lattice-based cryptography requires more computing resources than optimized classical systems. The hybrid QKD/PQC approach shows only a modest increase beyond pure PQC, reaching about 19.8 ms, with an additional overhead of approximately 1.7 ms. The small increase in QKD and PQC usage provides stronger and more resilient security.

All protocols reach a throughput of 942 ± 15 Mbps after the secure channel has been established according to the data transfer performance analysis shown in Figure 4. Handshake-related overhead does not interfere with bulk data transmission according to this evidence. System factors such as CPU performance and AES-256-GCM encryption efficiency determine the maximum throughput which can be achieved. The initial handshake cost gets distributed across the entire duration of long-lived connections which include streaming and large file transfers and persistent sessions. The study demonstrates that quantum-resistant cryptographic mechanisms can be operated in high-bandwidth applications without causing data transfer performance degradation.

Figure 5 enables a latency and throughput comparison which shows the performance security trade-off between multiple systems. While the QKD-only approach delivers the fastest handshake, all protocols maintain similar throughput levels. The selection of a quantum-safe solution requires decision-makers to evaluate two main factors which include handshake latency and security strength. The hybrid model achieves better security because it needs only minimal operational speed which remains unchanged from its basic PQC system.

The results show that quantum-resistant cloud architectures create an explicit conflict between improving performance and establishing security. The QKD-only approach provides the best latency but is limited by its dependence on continuous quantum link availability. The hybrid QKD/PQC model introduces a slightly higher handshake delay but delivers robust protection against both current classical attacks and future quantum threats. The dual-layer design protects security functions from vulnerabilities unless one system function becomes nonoperational. Security-critical cloud systems can handle the 1.7 ms additional overhead which security systems require to establish session keys through the QKD key rate.

The hybrid QKD/PQC approach secures cloud communications during the quantum era by providing a practical and future-proof solution. The system delivers resilient security through its strong security system which maintains performance during connection setup. The system protects sensitive multi-tenant cloud data which has a long lifespan through its secure data transfer capabilities.

5.5. LIMITATIONS AND FUTURE WORK

The study shows promising results but it has several existing limitations. The experimental setup tests a single QKD link which extends through a 50 km fiber spool but this only demonstrates a limited aspect of actual cloud environments which span multiple locations across large distances. The QKD key generation rate (1.2 Mbps) needs to be increased because its current value becomes a limiting factor for applications which need continuous key updates and require very high scalability. The prototype system functions inside a private cloud environment which is controlled but its deployment in actual environments will face new problems because of network changes and hardware malfunctions and the need to connect with current cloud orchestration systems.

The upcoming research will develop the architecture to work with multiple QKD links while testing its compatibility with upcoming quantum repeater technology to solve distance problems. Researchers need to study key management systems which handle multiple tenants in large environments to build adaptive key distribution systems and create systems for quick data synchronization. The hybrid model needs to expand its capabilities to fully support TLS standardization while researchers should test its performance with actual cloud computing workloads to achieve practical deployment. The investigation of new PQC algorithms together with dynamic crypto-agility mechanisms will enhance security and flexibility for organizations which face changing quantum threat environments.

DATA AVAILABILITY

The data will be available on request from the corresponding author.

References

[1] P. Varshney & Y. Simmhan, ‘‘Characterizing application scheduling on edge, fog and cloud computing resources’’, Software: Practice and Experience **50** (2020) 558. https://doi.org/10.1002/spe.2699.

[2] V. Topno, T. Kundu & M. K. Dehury, ‘‘Role of quantum computing in government and the defence sector’’, in *Digital technologies in modelling and management: insights in education and industry*, Igi Global, 2024, pp. 296–312. https://doi.org/10.4018/978-1-6684-9576-6.ch015.

[3] M. K. Yousif, Z. E. Dallalbashi & S. W. Kareem, ‘‘Information security for big data using the NTRU encrypt method’’, Measurement: Sensors **27** (2023) 100738. https://doi.org/10.1016/j.measen.2023.100738.

[4] G. Yousif, S. Alhayali, S. Wahhab & Z. Hussain, ‘‘Secure data in the cloud with a robust hybrid cryptographic approach’’, Journal of Electrical Systems **20** (2024) 2450. https://doi.org/10.52783/jes.2018.

[5] A. Kumar, C. Ottaviani, S. S. Gill & R. Buyya, ‘‘Securing the future internet of things with post-quantum cryptography’’, Security and Privacy **5** (2022) e200. https://doi.org/10.1002/spy2.200.

[6] F. Barrett-Danes & F. Ahmad, ‘‘Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024)’’, Discover Applied Science **7** (2025) 1083. https://doi.org/10.1007/s42452-025-07322-5.

[7] A. Priyadarshini, S. P. Abirami, M. A. Ahmed & B. Arunkumar, ‘‘Quantum-enhanced cybersecurity analysis and medical image encryption in cloud IoT networks’’, Optical and Quantum Electronics **56** (2024) 4. https://doi.org/10.1007/s11082-023-06018-7.

[8] D. Dhinakaran, L. Srinivasan, S. M. Udhaya Sankar & D. Selvaraj, ‘‘Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things: an extensive analysis’’, Quantum Information and Computation **24** (2024) 227. https://doi.org/10.26421/QIC24.3-4-3.

[9] S. R. Julakanti, N. S. K. Sattiraju & R. Julakanti, ‘‘Multi-cloud security: strategies for managing hybrid environments’’, Neuro Quantology **20** (2022) 10063. https://doi.org/10.48047/nq.2022.20.11.nq67000.

[10] S. M. J. Abdalwahid, B. F. Ibrahim, S. H. Ismael & S. W. Kareem, ‘‘A new efficient method for information security in Hadoop’’, Qalaai Zanist Journal **7** (2022) 1115. https://doi.org/10.25212/lfu.qzj.7.2.42.

[11] U. Nauman, Y. Zhang, Z. Li & T. Zhen, ‘‘Q-ECS: quantum-enhanced cloud security with attribute-based cryptography and quantum key distribution’’, Research Square Preprint (2024). https://doi.org/10.21203/rs.3.rs-4006533/v1.

[12] H. T. Nguyen, M. Usman & R. Buyya, ‘‘iQuantum: a toolkit for modeling and simulation of quantum computing environments’’, Software: Practice and Experience **54** (2024) 1141. https://doi.org/10.1002/spe.3331.

[13] D. Sikeridis, D. Ott, S. Huntley, S. Sharma, V. K. Dhanasekar, M. Bansal, A. Kumar, U. N. Anwitha, D. Beveridge & S. Veeraswamy, ‘‘ELCA: introducing enterprise-level cryptographic agility for a post-quantum era’’, Cryptology ePrint Archive, Paper 2023/1539 (2023). https://eprint.iacr.org/2023/1539.

[14] A. I. Saiyed, ‘‘Hybrid quantum-classical cryptographic protocols: enhancing security in the era of quantum supremacy’’, Spectrum of Research **5** (2025) 1. http://spectrumofresearch.com//index.php/sr/article/view/12/12.

[15] A. L. Tariq, A. Atta, U. Farooq, N. Anwar, M. Asim & N. Tabassum, ‘‘Quantum-inspired cryptography protocols for enhancing security in cloud computing infrastructures’’, Statistics, Computing and Interdisciplinary Research **6** (2024) 19. https://doi.org/10.52700/scir.v6i1.149.