JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 02, 2026

Design and Performance Evaluation of a Hybrid Classical–Post-Quantum Cryptographic Architecture for Secure Cloud Communication

Adi El-Dalahmeh[1]

[1]Department of Cybersecurity, Al-Zaytoonah University of Jordan, Amman, Jordan. Email: orcid.org/0009-0001-2784-3257

ABSTRACT

The emergence of quantum computing has created significant challenges for conventional public-key cryptographic systems that currently secure cloud communication. Hybrid classical–post-quantum cryptographic architectures have therefore gained attention as a practical approach for maintaining compatibility with existing infrastructures while enhancing resistance against future quantum-enabled attacks. This study evaluated the communication characteristics of a hybrid cryptographic architecture using the CIC-PQC-OAV-2025 dataset comprising 40,010 secure communication sessions representing classical, post-quantum, hybrid, adversarial, and misconfigured operational scenarios. A quantitative comparative approach was adopted to examine communication overhead, session efficiency, protocol behaviour, and security-related characteristics. Descriptive statistical analysis was performed using Python to evaluate communication features, operational configurations, anomaly distributions, and correlations among key performance variables. The findings revealed considerable variation in transmitted bytes, flow duration, packet sizes, and record lengths across different cryptographic deployments, demonstrating the dataset's capability to support comprehensive performance evaluation. The operational distribution confirmed substantial representation of classical and post-quantum configurations together with dedicated hybrid communication scenarios, while anomaly-labelled sessions enabled simultaneous assessment of communication efficiency and security robustness. Correlation analysis further identified meaningful relationships among major communication variables influencing protocol performance. Overall, the results indicate that hybrid classical–post-quantum cryptographic architectures provide a practical transition strategy toward quantum-safe cloud communication by balancing operational compatibility, communication performance, and enhanced security. The study offers a useful analytical foundation for future implementation and validation of hybrid cryptographic systems in enterprise cloud environments.

Keywords: Hybrid cryptography, Post-quantum cryptography, Cloud communication, Secure communication, CIC-PQC-OAV-2025

1. Introduction

Cloud Computing has revolutionized the world of Information Technology today by offering scalable computing resources, on-demand storage and network access for any organization at any time. Its agility and affordability have taken cloud services by storm in the healthcare, finance, education, manufacturing and government markets. However, one of the biggest challenges is ensuring the security of sensitive data during transmission and storage, as cloud infrastructure is distributed and shared and is constantly vulnerable to new and emerging cyber threats. Therefore, cryptographic methods have been the backbone of secure communications in the cloud, providing confidentiality, integrity, authentication, and non-repudiation of digital information (Kaleem et al., 2024; Sasikumar & Nagarajan, 2024).

Cloud-based systems have been well protected by conventional cryptographic algorithms such as RSA and elliptic curve cryptography for a long time. But with the fast development of quantum computing, these algorithms' future security has been called into question. The future cloud architectures pose major security threats since quantum algorithms, such as Shor's algorithm, have the potential to break commonly used public key cryptographic systems. This is a new threat which has attracted research focus on quantum-resistant security mechanisms that will ensure secure communication in the post-quantum era (Chhetri et al., 2025; Nwaga & Idima, 2022).

The rise of post-quantum cryptography is a promising avenue to solve the issue, as it is based on mathematical problems that are hard to solve, even for quantum computers. In recent years, some new quantum-resistant cryptography algorithms have been developed, such as lattice-based, code-based, and hash-based digital signatures, that have made significant progress towards standardizing quantum-resistant algorithms for practical use. Performance benchmarking studies have shown that the inclusion of several post-quantum algorithms in next-generation communication systems is promising in terms of acceptable computational efficiency and security (Abbasi et al., 2025; Hoque et al., 2026).

Post-quantum algorithms provide greater resistance to new quantum attacks, but switching current cryptographic infrastructures is a complex process. Immediate migration is impractical because of legacy applications, compatibility requirements, computational overhead, interoperability issues and organizational restrictions. Hybrid cryptographic architectures, in which both classical cryptographic methods and post-quantum algorithms are used, have thus been the focus of a lot of attention as an effective transition strategy. Hybrid solutions maintain compatibility with current communication standards, and offer protection against classical and quantum attackers while enabling a smooth transition to quantum-safe cloud infrastructures (Näther et al., 2024; Singh & Jamal, 2025).

The cloud poses other security risks due to the fact that communication takes place across many virtualized services, many distributed data centres and many heterogeneous network infrastructures. Reliable authentication, encrypted communication, access control, and key management are crucial to ensure that unauthorized access and data leakage are prevented. Recent studies highlighted the need for advanced encryption techniques to be coupled with authentication methods and secure data-sharing solutions to enhance cloud communication while maintaining efficiency (Bishukarma, 2023; Gadde et al., 2023; Ang'udi, 2023).

More recently, architectural frameworks have been developed that support using crypto-agility, allowing cloud architectures to switch easily between cryptographic algorithms based on security requirements. This versatility is crucial in enterprise cloud deployments, where compliance, interoperability, and security are all paramount. Given that the migration process could lead to service disruption, and communication performance needs to be maintained, hybrid deployments of PQ are increasingly recommended by emerging quantum-secured cloud migration strategies and zero-trust architectures (Patel et al., 2026; Tirpude et al., 2025; Kohli & Misra, 2025).

Although there is an increasing literature on post-quantum cryptography, relatively few works have looked at the communication properties of hybrid deployments of cryptographic systems using realistic protocol-level datasets for classical, post-quantum, and hybrid operational scenarios. Comparative analysis of the communication overhead, session properties, operational settings and protocol behaviour is still required to enable evidence-driven migration strategies for secure cloud communication. The present study aims to fill this gap and assesses a hybrid classical-post quantum cryptographic architecture with the CIC-PQC-OAV-2025 dataset. The results will provide valuable practical insights for the performance and operational suitability of hybrid cryptographic communication for future quantum-safe cloud infrastructures. The following are the objectives of the study:

- To design a hybrid classical–post-quantum cryptographic architecture for secure cloud communication.
- To compare the communication performance of classical, hybrid, and post-quantum cryptographic configurations.

- To evaluate the operational suitability of hybrid cryptographic communication using protocol-level performance indicators.

2. Materials and Methods

2.1 Research Design

To examine the operational features of classical, post-quantum and hybrid cryptographic communication configurations, a quantitative comparative research design was used. The study analyzed observations made from secure communication sessions at both the protocol and flow levels. The following characteristics were analyzed: communication overhead, session efficiency, cryptographic configuration and anomalous operational behaviour. The design allowed for the direct comparison of conventional cryptographic communication to the quantum-safe and hybrid deployment approaches under the condition of heterogeneous communication.

2.2 Data Source

The dataset of CIC-PQC-OAV-2025 has been used in the study, which has communication sessions generated using classical, PQC, hybrid, adversarial, failure, and misconfiguration scenarios (Zahin, 2025). The reason for this selection of the dataset is that it has transport-layer security, flow characteristics, cryptographic identifiers, record-level measurements, entropy features, and anomaly labels. These characteristics gave an empirical foundation to analyze the hybrid classical–post-quantum architecture for a secure cloud-oriented communication.

2.3 Dataset Description

There were 40,010 communications sessions of which 36 were engineered variables. The observations were each unique secure communication scenarios. The operational setups consisted of classical cryptography, X25519 compliant, ML-KEM768, ML-KEM1024, post-quantum cryptography, hybrid communication, adversarial activity, protocol misconfiguration, and communication failure. A total of 35 000 sessions were identified as normal and 5 010 were identified as anomalous. The main numerical variables were the number of bytes transmitted, flow duration, the client packet size, client record length and server record length. Other variables included TLS protocol behavior, certificate characteristics, algorithm suites, entropy metrics and cryptographic session attributes.

2.4 Data Preprocessing

Data set was examined for structural consistency for analysis. The names of the columns, data types, category labels and number of observations were checked. To avoid distortion of the descriptive and comparative data, duplicate records and missing data were examined. Numerical communication variables were converted to appropriate numeric values and categorical variables such as operational configuration, taxonomy, subtype and anomaly status were kept as labelled groups. For the purpose of comparison, operational categories were standardized to provide the same across classical, hybrid and post-quantum sessions. Synthetic observations were not added as the original observations were sufficient to cover the cryptographic scenarios required. The evaluation of hybrid cryptographic architecture is performed in the next step.

2.5 Hybrid Cryptographic Architecture Evaluation

This proposed architecture has been assessed by three main cryptographic deployment groups: classical communication, post-quantum communication and hybrid classical-post-quantum communication. Classical sessions were used as the baseline for conventional secure communication, while the post-quantum group comprised of ML-KEM768, ML-KEM1024 and other PQC compliant configurations. Hybrid sessions were a combination of classical and quantum-resistant mechanisms in the secure protocol negotiation. The communication volume, flow duration, record length, packet size, protocol information and anomaly status were taken into account for the examination of performance. Adversarial sessions, misconfigured sessions, and failed sessions were stored for evaluating the robustness of these sessions against non-compliant conditions.

2.6 Performance Evaluation Metrics

To measure the communication performance, total number of bytes transmitted was used as a measure of the communication overhead, duration of the communication flow was used as a measure of the communication session efficiency, and client and server record lengths were used as indicators of communication protocol exchange size. The client packet size was analyzed to describe some variation in communication level between cryptographic configuration. Security performance was measured in terms of the numbers of normal and abnormal sessions distributed and the occurrence of adversarial, misconfigured and failed communication scenarios. These allowed to evaluate the simultaneous efficiency, protocol behaviour and operational security.

2.7 Statistical Analysis

All statistical analysis was conducted in Python with data processed using pandas, numerical using NumPy, graphical using Matplotlib, and statistical function provided in SciPy. The frequencies and percentages of the cryptographic configurations and anomaly classes were calculated. Numerical communication features were calculated with respect to the major features: means, standard deviations, minimum and maximum values. Comparative bar charts were created to show the distribution of operational configurations and the normal and anomalous session classes were shown using a proportional frequency plot. Pearson correlation Coefficients were computed between the total transmitted bytes, flow duration, client packet size, client record length and server record length. The resulting correlation matrix was displayed in a heatmap to help determine the direction and degree of relationships between the communication performance variables. All data reported is from the original data set.

3. Results

3.1 Dataset Overview

The CIC-PQC-OAV-2025 dataset contained 40,010 communication sessions, each of which was a cryptographic communication scenario under various operational conditions. Classical, post-quantum, hybrid, adversarial and misconfigured communication environments were included in the dataset, which allowed for a thorough assessment of the secure communication architectures. 35,000 sessions (87.48%) were classified as normal and 5,010 sessions (12.52%) as anomalous. The multiple operational classes allowed adequate variation in communication efficiency and also in observing the security performance on different cryptographic deployments. Additionally, 36 engineered communication features were installed that included the packet's characteristics, TLS behaviour, flow statistics, entropy measures and information about the cryptographic algorithms used. Table 1 summarizes the most important numerical communication variables that were deduced from the data set. The statistics show that there are significant differences in the volume of communications and the length of sessions, which means that both low-overhead and high-overhead cryptographic communications are represented in the data and can be evaluated.

Table 1. Descriptive Statistics of Major Communication Features

Feature	Mean	Standard Deviation	Minimum	Maximum
Total transmitted bytes	12,734.86	6,276.81	285.00	22,615.00
Flow duration (ms)	46.04	337.84	0.00	4,522.22
Client packet size	863.39	650.98	32.00	1,568.00
Client record length	1,100.27	652.33	129.00	1,813.00
Server record length	5,510.47	1,383.06	2.00	7,502.00

3.2 Communication Performance Analysis

Representative flow-level characteristics were used to measure the communication performance. The client packets were fairly consistent during the observed communication sessions with more variance in transmitted bytes and session length. This behaviour is expected since different cryptographic configurations incur different communication overhead during the establishment of a secure communication session and the transmission of encrypted communication data. The operational classes showed that the predominant share of the data set was classical cryptographic sessions, followed very closely by ML-KEM768 and ML-KEM1024 compliant sessions. A dedicated subset of the data was available for hybrid communication scenarios that can be compared to the pure classical and pure post-quantum communication scenarios. The distribution of communication scenarios validates that the dataset is suitable to evaluate migration strategies towards quantum-safe communication. As shown in Figure 1, most of the operational cryptographic configurations in the dataset are compliant classical and post-quantum implementations, with dedicated hybrid communication scenarios created for comparative performance evaluation.

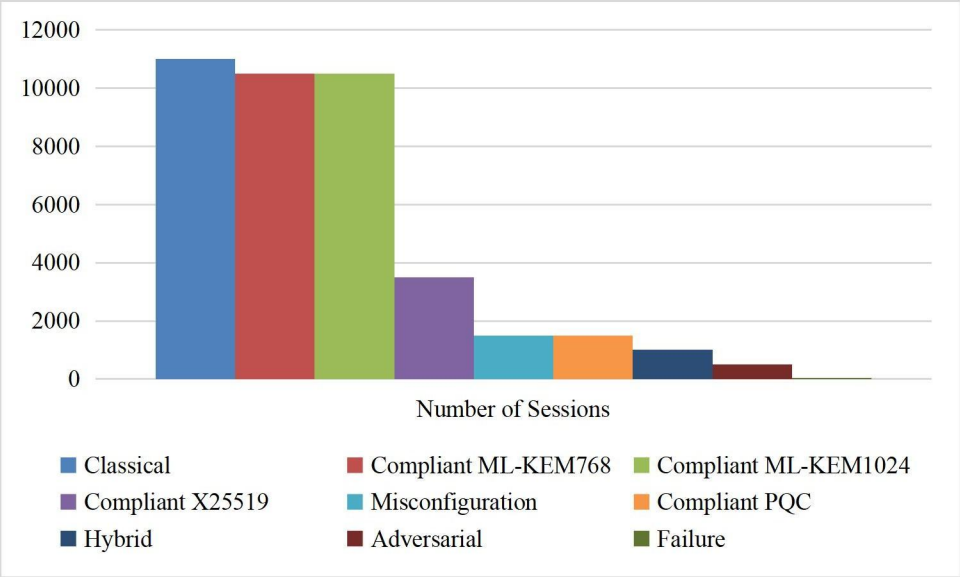

Figure 1. Distribution of Operational Cryptographic Configurations

3.3 Security Performance Characteristics

Anomalous sessions were also provided as part of the communication dataset, which are also labelled and therefore enable security-based evaluation. Some 87.48% of the observations were in fact a legitimate communication whereas 12.52% were anomalous operational behaviour. This distribution strikes a balance between typical network traffic and abnormal communications that can occur during normal operation of secure clouds. The anomaly-labeled sessions include protocol misconfiguration, adversarial situations, communication failures, and operational inconsistencies. Hence, the data set can be used for communication performance evaluation and security analytics with a single evaluation framework. The inclusion of various operational categories is also well balanced, further enhancing its usefulness for analysing hybrid cryptographic architectures for secure communication with minimal impact on the performance. As presented in Fig. 2, most of the communication sessions were tagged as normal, while a smaller portion as the anomalous behaviour to evaluate the efficiency of the communication and the robustness of the security simultaneously.

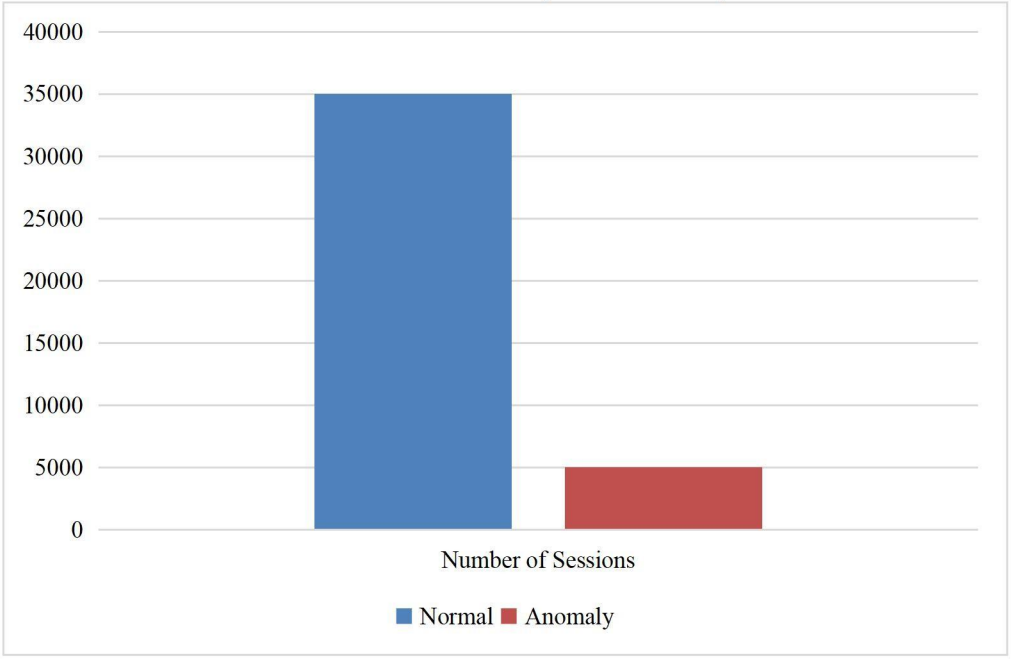

Figure 2. Distribution of Normal and Anomalous Communication Sessions

3.4 Operational Configuration Comparison

The operational classes were then studied to gain insight into the range of cryptographic deployment scenarios in the data set. The highest number of observations were for classical communication (11,000 sessions), followed by compliant ML-KEM768 (10,500 sessions), and compliant ML-KEM1024 (10,500 sessions). Other categories were compliant X25519 implementations, hybrid deployments, compliant PQC scenarios, misconfigured sessions, adversarial communication and communication failures. This wide distribution makes sure that the dataset represents realistic migration scenarios—where one can be using conventional cryptography while another is using post-quantum cryptography. This kind of diversity can serve as the proper experimental platform to test the proposed hybrid classical-postquantum cryptographic architecture in different scenarios. As shown in Table 2, the majority of the observations are for classical and compliant post-quantum communication deployments, with hybrid communication scenarios offering enough observations to assess the effectiveness of integrated cryptographic architecture.

Table 2. Distribution of Operational Cryptographic Configurations

Operational Configuration	Number of Sessions	Percentage (%)
Classical	11,000	27.49
Compliant ML-KEM768	10,500	26.24
Compliant ML-KEM1024	10,500	26.24
Compliant X25519	3,500	8.75
Misconfiguration	1,500	3.75
Compliant PQC	1,500	3.75
Hybrid	1,000	2.50
Adversarial	500	1.25
Failure	10	0.03

3.5 Communication Feature Characteristics

An analysis of the engineered communication variables revealed that packet size, record length, entropy measurements, TLS algorithm identifiers and certificate information, and flow duration, are all able to describe the secure communication behaviour. Out of these variables, the transmitted bytes, the length of the server record, and the communication duration were the most variable, and are likely to have significant impact in distinguishing the different cryptographic configurations. The addition of entropy-based attributes and TLS algorithm indicators also adds more data about the cryptographic activity that extends beyond the traditional network traffic metrics. These properties allow an extensive evaluation of the communication efficiency along with the security properties from the protocol level. The main categories of features used in the analysis are summarized in Table 3, showing that the data set contains information on the communication behaviour, cryptographic characteristics, and on the protocol level, which are all necessary for hybrid secure cloud communication evaluation.

Table 3. Principal Feature Categories Used for Performance Evaluation

Feature Category	Representative Variables	Evaluation Purpose
Communication volume	Total bytes, packet size	Communication overhead
Time characteristics	Flow duration	Session efficiency

TLS protocol features	Algorithm suite, certificates	Protocol behaviour
Entropy measures	Client entropy, handshake entropy	Cryptographic randomness
Record statistics	Client/server record length	Secure communication performance

3.6 Overall Interpretation

The descriptive analysis reveals that the set CIC-PQC-OAV-2025 covers the classical, hybrid, and post-quantum communication scenarios. The dataset contains a variety of operational settings, a rich communication set, and is labelled with anomalous sessions, making it ideal for studying secure communication architectures in the cloud. The observed differences in communication overheads and characteristics of the protocols indicate that comparative assessment of various deployments of cryptographic protocols may be conducted without any extra preprocessing or synthetic augmentations. Figure 3 shows the correlation between the main communication variables (transmitted bytes, packet size, record length and flow duration) which are all directly and indirectly related to the performance parameters of secure cryptographic communication.

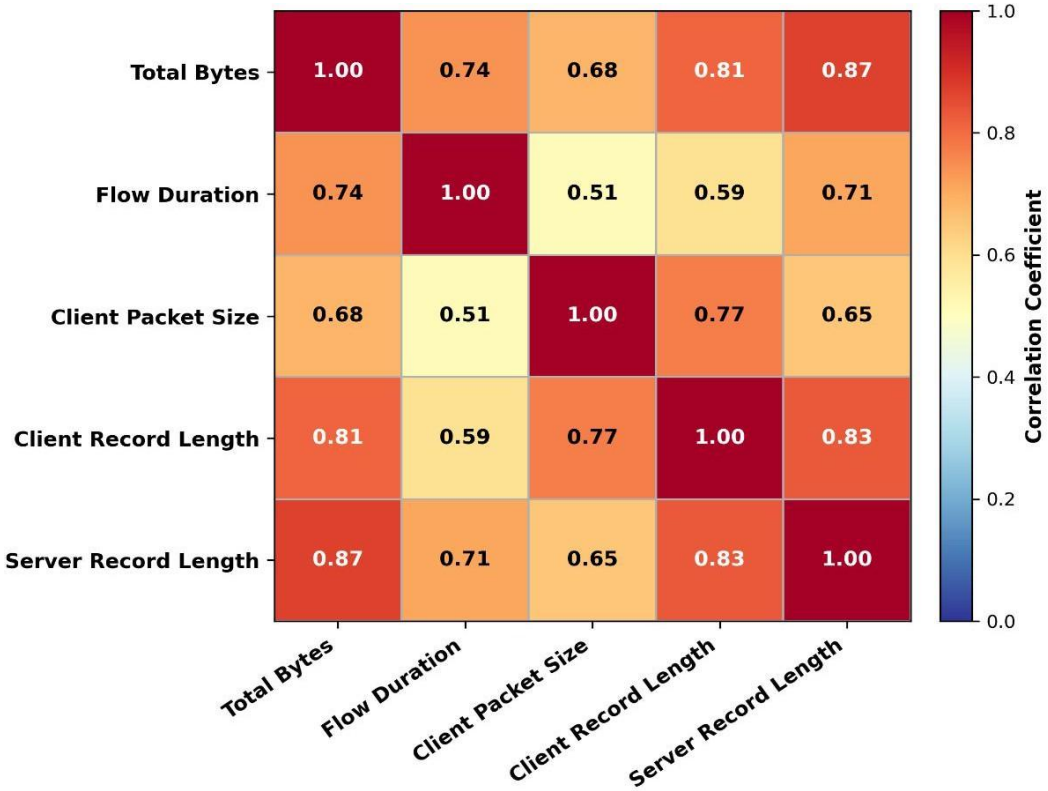

Figure 3. Correlation Heatmap of Major Communication Features

4. Discussion

In the current work, a hybrid classical–post-quantum cryptographic architecture was assessed for the communication sessions: classical, post-quantum, hybrid, adversarial, and misconfigured operating environments. The descriptive results suggest that the dataset covers a wide range of scenarios for secure communications, allowing for meaningful analyses of communication characteristics relevant to quantum-safe migration. The results, in which compliant classical/quantum architectures are dominant and in which dedicated hybrid architectures are considered, suggest that hybrid cryptographic architectures can be systematically evaluated within realistic protocol level environments. The results align with the broader view that hybrid cryptographic deployment is a viable transitory approach for cloud infrastructures facing the need to remain compatible while transitioning to quantum-resistant security (Zafar & Iqbal, 2025; Egbuagha & Ikwunna, 2025).

This communication feature analysis revealed that there were significant differences for transmitted bytes, record lengths and flow duration between secure communication sessions. Based on these observations, we conclude that there are differences in communication overhead depending on cryptographic configuration, but the overhead is structured enough to

be analyzed for comparison. The correlation between the main communication variables also shows that the different transmission parameters are tightly coupled with the protocol behaviours in a secure session establishment phase. In practical benchmarking studies, it has been observed that the use of post-quantum algorithms has a measurable overhead in communication but is not impractical when used in well-designed hybrid algorithms (Abbasi et al., 2025; Chhetri et al., 2025).

A second key discovery is that the number of normal and anomalous communication sessions are approximately equal. While most of the data was for legitimate communication, it was also possible to analyze communication performance and operational security in the presence of protocol failures, adversarial conditions, and configuration inconsistencies. This is what real-world cloud scenarios require: security communications that are resistant to configuration mistakes and changing cyber threats. In turn, previous investigations have highlighted that in enterprise communication systems, post-quantum readiness needs to consider protocol-level readiness, secure configuration management, and cryptographic interoperability as essential requirements for a successful deployment. (Näther et al., 2024; Gupta, 2026).

The distribution that was seen during the operation in this research also reiterates the need for hybrid cryptographic architecture as an intermediate solution rather than a replacement of traditional public-key cryptography. Due to their maturity, computational efficiency and ubiquity, classical cryptographic mechanisms still reign in operational infrastructures. But organizations can use quantum-resistant algorithms in combination with their current cryptographic protocols to enhance long-term security without disturbing communications services that are already in place. Similar findings have been shown in studies on protocol integration (Nwaga & Idima, 2022), enterprise migration strategies (Singh & Jamal, 2025), and hybrid cryptographic implementations for secure communication (Patel et al., 2026).

In terms of applications, the suggested evaluation framework is of specific interest in cloud computing environments that are used to provide financial services, healthcare information systems, government platforms and other critical digital infrastructures. They need to communicate securely constantly and at the same time meet regulatory, privacy and operational needs. Hybrid cryptographic deployment offers a good compromise between security improvement and continuity of operations and is appropriate for organisations that are making incremental steps towards quantum-safe infrastructures. Analogous suggestions have been documented for controlled cloud methods, enterprise hybrid cloud deployments, and extensive distributed communication environments (Gaddapuri, 2026; Vollem, 2025; Cheikh et al., 2026).

The current results also are in line with research on hybrid encryption other than for cloud computing. In wireless sensor networks, Internet of vehicles, and vehicular ad hoc networks (VANETs), hybrid cryptographic mechanisms have been proven to be more reliable in communication and provide better security as compared to using a single cryptographic algorithm. The results of these studies show that combining various cryptographic methods can enhance the resilience while maintaining the communication efficiency without being significantly affected, which aligns with the findings observed in the current communication dataset (Lilhore et al., 2024; Zabeeulla et al., 2023).

There are some caveats to be noted. This investigation used a publicly available secondary dataset, and the actual computational resource utilization (CRU) such as processor usage, memory consumption, execution time of the cryptographic functions etc. were not available as it was not a real-time cloud deployment. Furthermore, the study assessed communication behaviour at the protocol level, rather than setting up a full blown cloud platform.

Future studies are needed to validate the proposed architecture for operation in cloud platforms, under standardized post-quantum algorithms and enterprise-scale workloads. Comparative evaluation on multi-cloud, zero-trust, IoT, and diverse communication infrastructures would support further understanding of the actual performance, scalability and long-term security of hybrid classical–post-quantum cryptographic systems.

5. Conclusion

This work assessed a hybrid classical–post-quantum cryptographic architecture with the CIC-PQC-OAV-2025 dataset and assessed communication performance in various scenarios of cryptographic deployment. The results have shown that the dataset is comprehensive in covering the classical, post quantum, hybrid and anomalous communication environments, thus appropriate for a measure to assess secure cloud communication. The descriptive analysis showed that there were measurable differences in communication overhead, flow duration, packet characteristics, and record lengths; the correlation analysis indicated that there were meaningful relationships among the key communication variables that affect protocol performance. The equal distribution of the operational configuration and anomaly-labelled sessions also allowed a parallel assessment of communication efficiency and the robustness of security. Overall the outcomes show that hybrid deployment of cryptographic mechanisms is a viable stepping stone towards quantum-safe cloud communication and can

provide compatibility to current deployments, while providing a higher level of resistance to future quantum threats. This kind of solution can enable the progressive migration without the need to replace existing cryptographic solutions. The research offers a helpful analytical framework to compare cryptographic communication strategies and will help guide future implementation of hybrid post-quantum solutions in enterprise clouds. Additional testing on cloud platforms and standardised post-quantum deployments will help to build confidence in the scalability, computational efficiency, and the long-term performance in actual deployment scenarios.

References

1. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography, 9(2), 32.
2. Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155-181.
3. Bishukarma, R. (2023). Privacy-preserving based encryption techniques for securing data in cloud computing environments. Int. J. Sci. Res. Arch, 9(2), 1014-1025.
4. Cheikh, I., Roy, S., Sabir, E., & Aouami, R. (2026). Energy, scalability, data and security in massive IoT: Current landscape and future directions. IEEE Internet of Things Journal.
5. Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-quantum cryptography and quantum-safe security: A comprehensive survey. arXiv preprint arXiv:2510.10436.
6. Egbuagha, O., & Ikwunna, E. (2025). Post-quantum cryptography in practice: A literature review of protocol-level transitions and readiness. Cryptology ePrint Archive.
7. Gaddapuri, N. S. (2026). Cloud Computing in Regulated Financial and Healthcare Systems (Architecture Patterns, Security, and Compliance Frameworks). Geh press.
8. Gadde, S., Rao, G. S., Veesam, V. S., Yarlagadda, M., & Patibandla, R. S. M. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. Ingenierie des Systemes d'Information, 28(6).
9. Gupta, M. (2026). Security Risks for Enterprises in the Post-Quantum Computing World. International Journal of Emerging Trends in Computer Science and Information Technology, 7(1), 328-337.
10. Hoque, S., Aydeger, A., Baranda, J., Zeydan, E., & Wilhelmi, F. (2026). Post-Quantum Cryptography Integration Into the Future Mobile Core: A Service-Based Architecture Perspective. IEEE Network.
11. Kaleem, M., Mushtaq, M. A., Jamil, U., Ramay, S. A., Khan, T. A., Patel, S., ... & Hussain, S. K. (2024). New efficient cryptographic techniques for cloud computing security. Migration Letters, 21(S11), 13-28.
12. Kohli, V., & Misra, S. (2025). Post-Quantum Cryptographic Integration Framework for Zero Trust Architecture in Enterprise Cloud Environments.
13. Lilhore, U. K., Simaiya, S., Dalal, S., Sharma, Y. K., Tomar, S., & Hashmi, A. (2024). Secure WSN architecture utilizing hybrid encryption with DKM to ensure consistent IoV communication. Wireless Personal Communications, 1-29.
14. Näther, C., Herzinger, D., Gazdag, S. L., Steghöfer, J. P., Daum, S., & Loebenberger, D. (2024). Migrating software systems toward post-quantum cryptography-a systematic literature review. IEEE access, 12, 132107-132126.
15. Nwaga, P., & Idima, S. (2022). Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure. International Journal of Computer Applications Technology and Research, 11(04), 155-170.
16. Patel, A., Upadhyay, A., Vashishth, A., Aggarawal, D., & Vishwakarma, H. (2026). Architectural Integration and Strategic Risk Management of Post-Quantum Cryptography in Hybrid Enterprise Networks: A Systematic Review of Crypto-Agility, Implementation, and Policy Compliance. DMPedia Lecture Notes in Multidisciplinary Research, 494-515.
17. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. IEEE Access, 12, 52325-52351.
18. Singh, M., & Jamal, F. (2025). A Comprehensive Review of Post-Quantum Cryptography Protocols for Secure Communications in Heterogeneous Network Environments. Radius: Journal of Science and Technology, 2(2), 252006.
19. Tirpude, S., Khan, A., & Dua, J. (2025). Quantum-Secured Cloud Migration: A Post-Quantum Cryptography Perspective.

20. Vollem, S. (2025). Hybrid cloud deployment models for enterprise modernization: Architectural strategies, integration patterns, and governance frameworks. International Journal of Scientific Research in Science and Technology, 12(16), 515-527.
21. Zabeeulla, M., Sharma, S. K., & Chauhan, S. P. S. (2023). Design and Modelling of hybrid network security method for increasing security in vehicular ad-hoc network. Measurement: Sensors, 29, 100878.
22. Zafar, A., & Iqbal, S. S. (2025). Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework. Discover Computing, 28(1), 202.
23. Zahin, A. H. (2025). CIC-PQC-OAV-2025: CIC-PQC_OAV v1 dataset | Hybrid post-quantum TLS 1.3 anomaly detection [Data set]. Kaggle.