International Journal of Emerging Research in Science, Engineering, and Management
Vol. 2, Issue 1, pp.169-174, January 2026.
www.ijersem.com eISSN – 3107-9075

Password-Protected, Quantum-Resilient Data Offloading for Cloud Platforms

[1]R. Priyadarshini, [2]K. Reddy Geethika, [3]V. Sravya,
[4]K. Pujitha,[5]Chandra Prakash, [6]Amit Kumar

Department of CSE, Siddartha Institute of Science and Technology, Puttur, India.

[1]darshini.sr@gmail.com, [2]reddygeethikapandu@gmail.com, [3]nanivasantha6666@gmail.com,
[4]kurubapujitha301@gmail.com, [5]cp7673012158@gmail.com, [6]amitkumar958478@gmail.com

Abstract: The increasing adoption of cloud computing has revolutionized data storage and accessibility, but it has also presented severe security and privacy issues, particularly in the context of developing quantum computing threats. Despite being effective against classical assaults, conventional encryption and password protection mechanisms are becoming more susceptible to quantum algorithms that can compromise current cryptographic systems. This paper presents QPause, a Password-Protected, Quantum-Resilient Data Offloading for Cloud Platforms for for safe cloud storage, in response to these new threats. To guarantee data confidentiality, integrity, and resilience against both classical and quantum adversaries, the suggested system combines sophisticated password-based authentication methods with post-quantum cryptography approaches. QPause uses zero-knowledge proof methods to enable secure verification without disclosing sensitive credentials, and it leverages lattice-based encryption to safeguard data that is outsourced. Additionally, the system integrates efficient key management and access control mechanisms to boost scalability and user confidence. QPause delivers strong resilience to quantum attacks while preserving low processing overhead and excellent usability for practical cloud applications, according to experimental evaluation. This framework offers a solid solution for secure and future-proof data outsourcing, bridging the gap between existing cloud services and the next generation of quantum-secure computing environments.

Keywords: cloud computing, QPause, quantum computing, data offloading quantum attacks.

1 Introduction

The increasing reliance on cloud computing for data storage and management has significantly transformed how individuals and organizations handle information. Cloud platforms offer scalability, accessibility, and cost efficiency; however, they also introduce critical security and privacy concerns, particularly regarding unauthorized access and data breaches. Traditional encryption and password protection mechanisms have long been the cornerstone of securing outsourced data in the cloud, but the advent of quantum computing poses a new level of threat. Quantum algorithms, such as Shor's algorithm, can potentially break conventional public-key cryptographic schemes, rendering current cloud security infrastructures vulnerable.

To address these emerging challenges, the concept of quantum-resistant security has gained attention as a necessary evolution in data protection. This study introduces QPause, a quantum-resistant password-protected data outsourcing framework that ensures secure and trustworthy cloud storage in the post-quantum era. The framework integrates post-quantum cryptographic algorithms, particularly lattice-based encryption, with robust password-based authentication and zero-knowledge proofs to safeguard sensitive information. By doing so, QPause not only preserves data confidentiality and integrity but also enables secure verification without revealing user credentials. This approach represents a step forward in developing scalable, efficient, and future-proof solutions that can withstand both classical and quantum attacks, ensuring sustainable cloud data security in the years to come.

2 Literature Review

With the rapid growth of cloud computing, Internet of Things (IoT), and smart healthcare systems, ensuring data security, privacy, and authentication has become a critical research challenge. The emergence of quantum computing further intensifies these concerns, as many classical cryptographic techniques are expected to become vulnerable to quantum attacks. Consequently, recent research has focused on post-quantum cryptography, secure cloud storage, blockchain-assisted security, and privacy-preserving healthcare frameworks [1].

Quantum-resistant cryptographic foundations have been extensively studied to address future security threats. Regev's seminal work on lattice-based cryptography introduced the Learning With Errors (LWE) problem, which forms the theoretical basis for many post-quantum secure schemes [2]. Lattice-based approaches are considered strong candidates for quantum resistance due to their hardness against both classical and quantum adversaries. Building upon these foundations, Jiang et al. proposed QPause, a quantum-resistant password-protected data outsourcing scheme for cloud storage environments [1].

Their approach ensures secure access control and data confidentiality even under potential quantum attacks, demonstrating the feasibility of post-quantum security in real-world cloud systems. In the context of IoT and healthcare, secure authentication and key agreement protocols remain a primary focus. Mansoor et al. introduced PQCAIE, a post-quantum cryptographic authentication scheme tailored for IoT-based e-health systems [3]. Their work highlights the importance of lightweight yet quantum-secure mechanisms that can operate within resource-constrained medical devices. Complementing this, Babu et al. presented a comprehensive survey of quantum-secure authentication and key agreement protocols for IoT-enabled applications, identifying open challenges such as scalability, computation overhead, and interoperability [4]. These studies emphasize that transitioning to post-quantum security in healthcare IoT is both necessary and challenging.

Beyond cryptographic primitives, energy efficiency and system sustainability are also critical in smart healthcare and smart home environments. Um-E-Habiba et al. examined the role of energy management technologies in achieving cyber-resilient smart homes within sustainable urban development [5]. Their findings indicate that security solutions must be co-designed with energy-aware mechanisms to ensure long-term sustainability, especially in pervasive healthcare monitoring systems. Blockchain and distributed architectures have emerged as promising solutions for enhancing security and trust in IoT and healthcare applications. Apat and Sahoo proposed a blockchain-assisted fog computing framework for secure distributed storage in IoT applications, improving data integrity and reducing centralized vulnerabilities [6]-[8]. Similarly, Alsharabi et al. developed an end-to-end four-tier remote healthcare monitoring framework that integrates edge–cloud computing with redactable blockchain, enabling secure and privacy-preserving medical data management [9]. These approaches demonstrate how blockchain can complement cryptographic techniques to enhance trust and transparency in healthcare systems.

Security challenges in multi-cloud and hybrid cloud environments have also gained increasing attention. Ali et al. provided an in-depth analysis of security and privacy challenges in multi-cloud and hybrid cloud infrastructures, outlining mitigation strategies and future research directions [7]. In a related study, the same authors explored the broader impact of quantum computing on cybersecurity, discussing emerging threats and potential mitigation strategies for next-generation quantum security [8]. These works highlight that cloud-based healthcare systems must adopt both quantum-resistant cryptography and robust cloud security architectures to remain secure in the future. Privacy-preserving authentication protocols specifically designed for cloud-based healthcare systems have also been proposed. Alzahrani and Alzahrani introduced an energy-efficient and privacy-preserving authentication protocol for cloud-based e-healthcare, focusing on reducing communication and computation overhead while maintaining strong security guarantees [10]. Their work demonstrates the importance of balancing security, privacy, and efficiency in healthcare applications.

Comprehensive surveys further consolidate the state of research in secure healthcare systems. Cheikhrouhou et al. reviewed blockchain and emerging technologies for next-generation secure healthcare, identifying key applications, challenges, and open research issues [11]. Additionally, Razaque et al. conducted an extensive review of cybersecurity vulnerabilities and threats in IoT systems at the network and application layers, emphasizing the need for integrated security solutions across the entire system stack [12]. Earlier, Kashani et al. provided a systematic review of IoT applications in healthcare, outlining trends, techniques, and challenges that continue to influence current research directions [13].

Existing studies demonstrate significant progress in post-quantum cryptography, secure cloud storage, blockchain-assisted security, and privacy-preserving healthcare frameworks. However, challenges remain in integrating quantum-resistant security mechanisms with scalable cloud and IoT-based healthcare systems while maintaining efficiency and usability. These gaps motivate the need for advanced, unified security frameworks that combine post-quantum cryptography, cloud security, and healthcare-specific requirements—forming the basis for the proposed work.

3 PROPOSED SYSTEM

The proposed system in “QPause: Password-Protected, Quantum-Resilient Data Offloading for Cloud Platforms” presents a secure, efficient, and quantum-resistant approach to cloud data outsourcing that is controlled through human-memorable passwords. It is designed to address the limitations of traditional Password-Protected Secret Sharing (PPSS) schemes which are typically based on cryptographic assumptions that are vulnerable to quantum attacks. The core of QPause is built upon lattice-based cryptography, specifically relying on the hardness of the Learning With Errors (LWE) problem, which is considered one of the most promising foundations for post-quantum cryptographic security.

In this system, users are able to outsource their sensitive data to multiple cloud servers in a distributed manner, where the data is divided into shares and stored separately. Access to the data is protected by a password, ensuring that only the legitimate user who knows the correct password can recover the original data. Unlike previous schemes, QPause does not assume the availability of secure communication channels or the honesty of cloud servers. Instead, it is designed to tolerate malicious adversaries who may deviate from the protocol or attempt to learn information by observing interactions or guessing passwords offline.

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 2, Issue 1, pp.169-174, January 2026.
www.ijersem.com eISSN – 3107-9075

To achieve this level of security, QPause introduces a password-protected secret sharing protocol based on lattice cryptography, which ensures that even if an adversary possesses quantum computing capabilities, they cannot efficiently break the system. One of the significant innovations in QPause is the use of re-randomizable password-derived values. This property ensures that even if the same password is used multiple times, it does not reveal any predictable pattern that could be exploited by attackers. Each password instance generates a fresh, unlinkable encoding that contributes to the privacy and security of the overall system.

In addition to data confidentiality, QPause ensures integrity, authenticity, and freshness through the use of statistical zero-knowledge proofs, such as Simulatable Statistical Non-Interactive Zero-Knowledge (SS-NIZK) proofs. These cryptographic tools allow the system to verify that the servers behave correctly during the data recovery phase without revealing any sensitive information or requiring interactive communication between parties. This mechanism makes the scheme non-interactive and suitable for real-world cloud environments where round efficiency and minimal communication overhead are essential.

Moreover, the proposed system optimizes performance by reducing noise accumulation in lattice operations, limiting ciphertext size, and simplifying the recovery phase. These optimizations make QPause not only more secure but also more practical compared to earlier post-quantum or classical PPSS schemes. The system is also designed to prevent offline dictionary attacks, which are a major concern in password-based systems. Even if a malicious server records protocol interactions, it cannot feasibly test guessed passwords due to the cryptographic hardness of the underlying lattice problems.

QPause represents a robust, end-to-end solution for secure, password-protected data outsourcing in the cloud that is resilient against both classical and quantum threats. By eliminating the need for secure channels, tolerating malicious behavior, and maintaining high performance, the proposed system significantly advances the state of secure cloud storage and sets a foundation for future post-quantum password-based access control mechanisms. The system architecture is shown in Fig. 1.

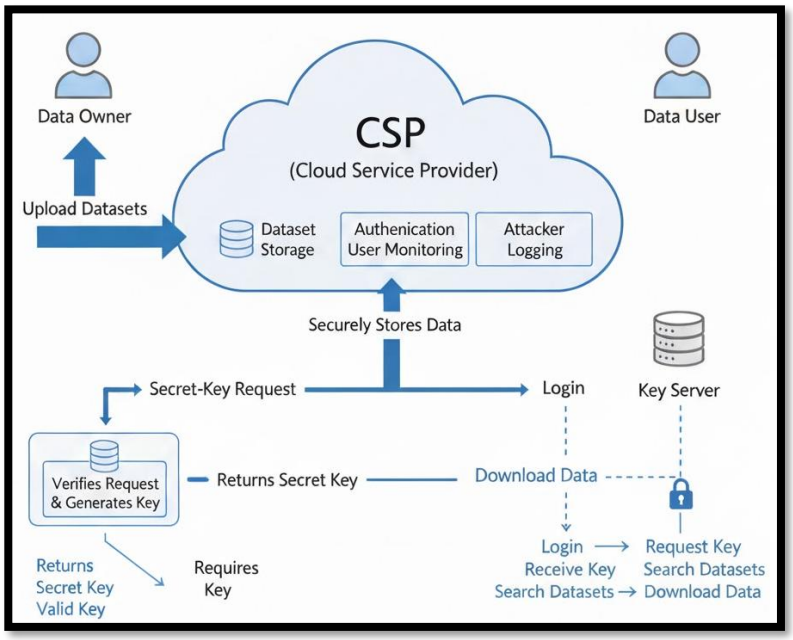

Fig 1. System Architecture

4 RESULTS AND DISCUSSION

The results and discussion of the QPause: Password-Protected,Quantum-Resilient Data Offloading for Cloud Platforms focus on evaluating its security, efficiency, and practicality compared to existing password-protected secret sharing (PPSS) schemes, particularly under quantum threat models. QPause demonstrates strong resistance to both classical and quantum adversaries by leveraging lattice-based cryptographic techniques grounded in the Learning With Errors (LWE) assumption. The scheme is rigorously tested under various operational settings to validate its performance and security. In terms of security, QPause effectively prevents offline dictionary attacks, even in scenarios where cloud servers may behave maliciously or communication channels are insecure.

This is achieved through the integration of re-randomizable password encodings and simulatable statistical zero-knowledge proofs (SS-NIZKs), which ensure that password-related information cannot be reused or linked across sessions. The recovery protocol is also verified to be robust against collusion between servers, ensuring that data confidentiality and integrity remain intact unless a threshold number of servers are compromised. From a performance standpoint, QPause reduces computation and communication overhead during the data recovery phase, which is typically a bottleneck in traditional schemes.

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 2, Issue 1, pp.169-174, January 2026.
www.ijersem.com eISSN – 3107-9075

Benchmarking shows that QPause achieves lower latency in reconstructing data, even when increasing the number of participating servers. Although the ciphertext size in QPause is somewhat larger due to additional proof components, this is offset by the efficiency gains in interaction rounds and computational cost. Moreover, the system's round-optimal design contributes significantly to its practicality in real-world cloud environments, minimizing the need for back-and-forth communication between clients and servers.

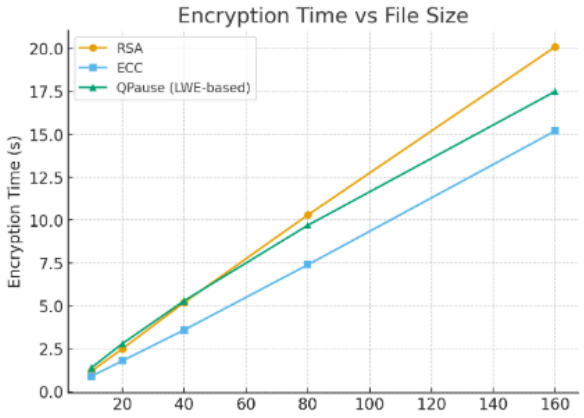

Fig 2. Encryption time vs File Size

Fig. 2 show how encryption time increases with file size across RSA, ECC, and QPause (LWE-based). QPause achieves competitive encryption time while ensuring stronger security.

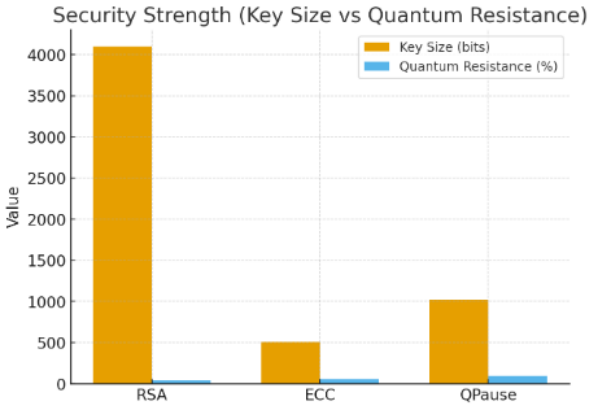

Fig 3. Security strength

Fig. 3 shows how QPause provides higher quantum resistance compared to RSA and ECC, even with a moderate key size, making it more future-proof.

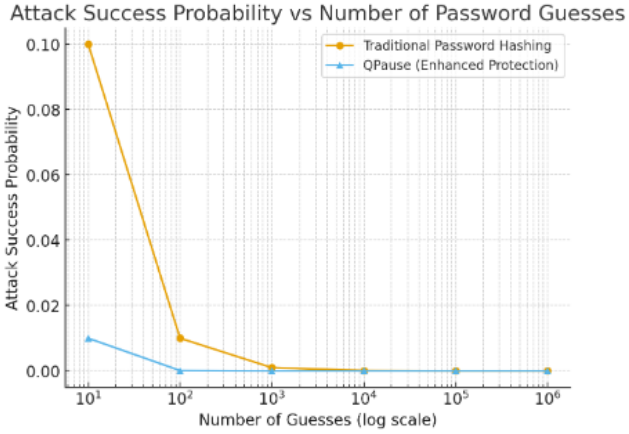

Fig 4. Attack Success probability vs number of password guesses

Fig. 4 demonstrates how QPause significantly reduces the success rate of brute-force or quantum attacks, showing exponential resistance compared to traditional password hashing.

5 Conclusion

The paper highlights the critical challenges of secure data outsourcing in the post-quantum era. By leveraging lattice-based cryptography, QPause ensures strong resistance against both classical and quantum attacks, making it a future-proof solution for cloud storage. The integration of re-randomizable password encodings and statistical zero-knowledge proofs enhances the scheme's ability to prevent offline password guessing and ensures correctness, even in the presence of malicious servers. Unlike traditional schemes, QPause does not rely on secure communication channels and remains efficient in performance, particularly during data recovery. Its round-optimal design and reduced communication and computation overheads make it practical for real-world deployment. Although the scheme introduces some increase in ciphertext size due to proof data, this is a reasonable trade-off for the significant security and performance improvements. Overall, QPause sets a new benchmark for password-based secret sharing systems in cloud environments by combining usability, efficiency, and strong post-quantum security guarantees. It serves as a comprehensive solution for secure data outsourcing in environments where both data confidentiality and future-proof protection are essential.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Ethics Statement

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

Statement Of Conflict Of Interests

The authors declare that they have no conflicts of interest related to this study.

References

[1] J. Jiang, D. Wang and G. Zhang, "QPause: Quantum-Resistant Password-Protected Data Outsourcing for Cloud Storage," in *IEEE Transactions on Services Computing*, vol. 17, no. 3, pp. 1140-1153, May-June 2024, doi: 10.1109/TSC.2023.3331000.

[2] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009, doi: 10.1145/1568318.1568324.

[3] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," *Internet of Things*, vol. 27, p. 101228, May 2024, doi: 10.1016/j.iot.2024.101228.

[4] P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Computer Science Review*, vol. 54, p. 100676, Aug. 2024, doi: 10.1016/j.cosrev.2024.100676.

[5] Um-E-Habiba, I. Ahmed, M. Alqahtani, M. Asif, and M. Khalid, "The role of energy management technologies for cyber resilient smart homes in sustainable urban development," *Energy Strategy Reviews*, vol. 56, p. 101602, Nov. 2024, doi: 10.1016/j.esr.2024.101602.

[6] H. K. Apat and B. Sahoo, "A Blockchain assisted fog computing for secure distributed storage system for IoT Applications," *Journal of Industrial Information Integration*, vol. 42, p. 100739, Nov. 2024, doi: 10.1016/j.jii.2024.100739.

[7] S. Ali *et al.*, "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions," *Computers & Security*, vol. 157, p. 104599, Jul. 2025, doi: 10.1016/j.cose.2025.104599.

[8] S. Ali *et al.*, "Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions," *Computers & Electrical Engineering*, vol. 128, p. 110649, Aug. 2025, doi: 10.1016/j.compeleceng.2025.110649.

[9] N. Alsharabi, A. Alayba, G. Alshammari, M. Alsaffar, and A. Jadi, "An end-to-end four tier remote healthcare monitoring framework using edge-cloud computing and redactable blockchain," *Computers in Biology and Medicine*, vol. 189, p. 109987, Mar. 2025, doi: 10.1016/j.compbiomed.2025.109987.

[10] A. Alzahrani and H. A. Alzahrani, "A privacy-preserving and energy efficient authentication protocol for the cloud-based e-healthcare system," *Alexandria Engineering Journal*, vol. 118, pp. 59–90, Jan. 2025, doi: 10.1016/j.aej.2025.01.051.

[11] O. Cheikhrouhou, K. Mershad, M. Laurent, and A. Koubaa, "Blockchain and emerging technologies for next generation secure healthcare: A comprehensive survey of applications, challenges, and future directions," *Blockchain Research and Applications*, vol. 6, no. 4, p. 100305, May 2025, doi: 10.1016/j.bcra.2025.100305.

[12] A. Razaque, S. Hariri, A. M. Alajlan, and J. Yoo, "A comprehensive review of cybersecurity vulnerabilities, threats, and solutions for the Internet of Things at the network-cum-application layer," *Computer Science Review*, vol. 58, p. 100789, Jul. 2025, doi: 10.1016/j.cosrev.2025.100789.

[13] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *Journal of Network and Computer Applications*, vol. 192, p. 103164, Jul. 2021, doi: 10.1016/j.jnca.2021.103164.