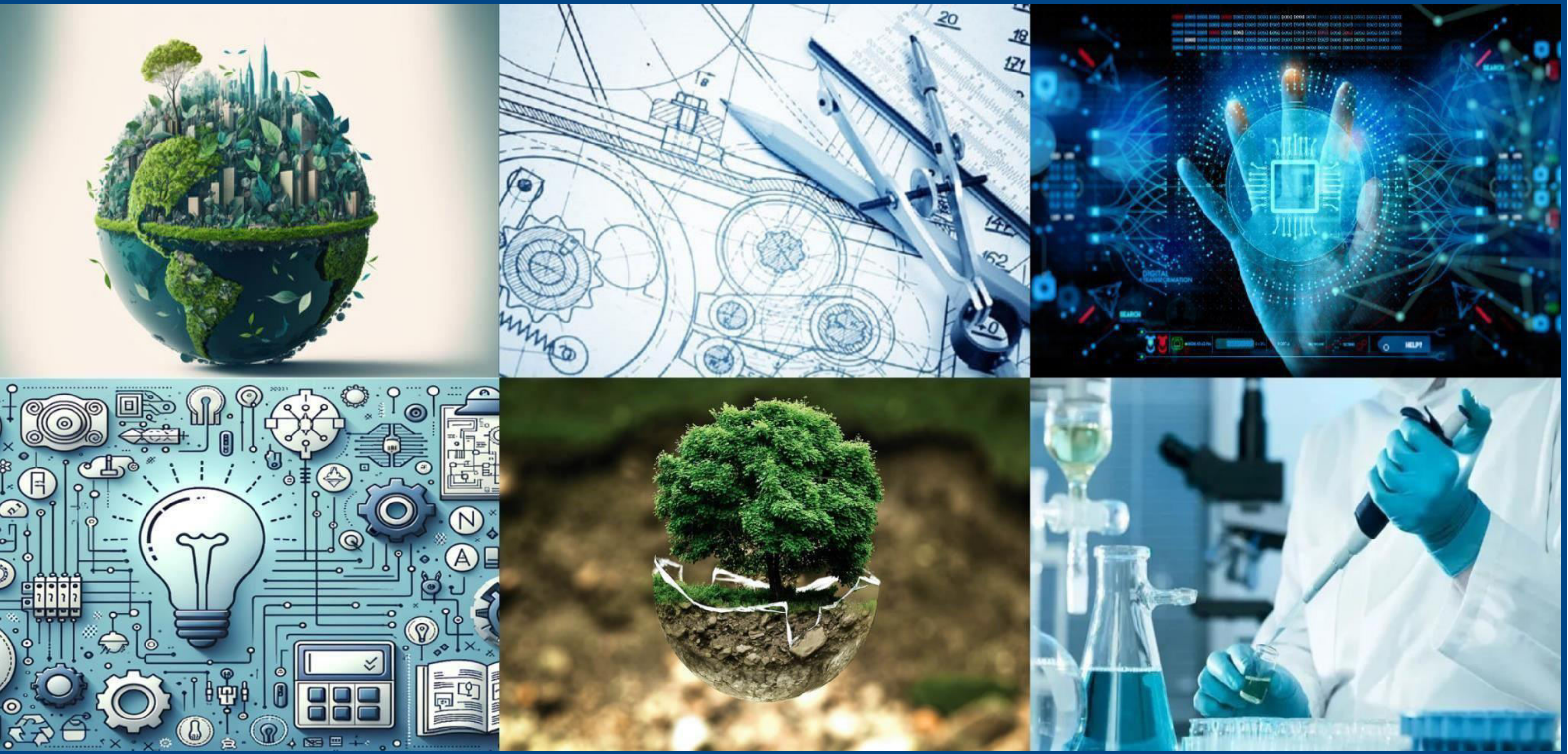
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

QPAUSE: QUANTUM-IMMUNE ACCESS CONTROL FOR SENSITIVE CLOUD STORAGE

N. Rajesh, Venkatesha S

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Cloud storage [1] efficiently manages large data volumes but raises serious security concerns, particularly in ensuring data owners retain control over outsourced information. Password-Protected Secret Sharing (PPSS [8], [11]) combines password authentication with secret sharing to secure data, enabling easy password-based access and protection against device failure. However, current PPSS [8], [11] methods lack resilience against post-quantum threats, creating a need for quantum-resistant solutions. We present QPause [12], [13], a lattice-based [13] quantum-resistant PPSS [8], [11] framework for cloud storage, offering round-optimal security against semi-honest and malicious adversaries. Formal proofs confirm its robustness against quantum-capable attackers, and performance analysis shows it outperforms existing approaches.

KEYWORDS: PPSS [12], [13] [8], [11], Cloud Storage, Quantum-Resistant Security

I. INTRODUCTION

The rapid adoption of cloud storage services has transformed the way individuals and organizations manage their data, offering scalable capacity, flexible access, and reduced infrastructure costs [5]. Despite these advantages, outsourcing data to third-party cloud providers inevitably raises critical security and privacy concerns, as sensitive information becomes vulnerable to unauthorized access, corruption, and loss of control. Ensuring that data owners can securely store, manage, and retrieve their outsourced data without relying entirely on the trustworthiness of service providers remains a key challenge. Password-Protected Secret Sharing (PPSS [12], [13] [8], [11]) has emerged as a promising cryptographic paradigm that integrates password authentication with secret sharing techniques [4], [5], [8], [10], [11]. By leveraging human-memorizable passwords [13], PPSS [12], [13] [8], [11] enables secure data management and resilience against device failure without requiring users to store or maintain complex cryptographic keys. However, most existing PPSS [12], [13] [8], [11] schemes are designed for classical computational environments and fail to address the emerging security threats posed by quantum computing. With advancements in quantum algorithms [10], [12], many widely used cryptographic primitives, such as RSA and ECC, are expected to become vulnerable, rendering traditional PPSS [12], [13] [8], [11] models inadequate in the post-quantum era.

II. LITERATURE SURVEY

We propose SPADE [4], an encrypted data deduplication scheme that eliminates key management issues and resists compromised key servers. It uses a proactivization mechanism to periodically replace key servers, a password-hardening protocol against dictionary attacks, and layered password-based encryption and authentication, enabling secure access using only passwords [13]. Analyses and experiments confirm SPADE [4]'s provable security and high efficiency.

a. EXISTING SYSTEM

Password-based authentication [6], [7] is widely used despite its security and usability flaws. Password-Protected Secret Sharing (PPSS [12], [13]) enables users to encrypt [8], [11] data locally, split encryption keys among multiple servers, and retrieve them with only a password. While effective, existing PPSS [12], [13] schemes rely on traditional cryptographic assumptions, making them vulnerable to quantum attacks [10], [12]. Lattice-based approaches exist but are either insecure against certain attacks or lack a quantum-resistant password-protected outsourcing solution.

b. PROPOSED SYSTEM

We propose QPause [12], [13], a quantum-resistant password-protected data outsourcing scheme for cloud storage based on Learning With Errors (LWE). QPause [12], [13] extends PPSS [8], [11] with quantum-secure primitives, re-randomized passwords, low-noise decryption, and structured noise to enhance security. It uses temporary key pairs to prevent eavesdropping [10], [12] and SS-NIZK proofs for computation validity. QPause [12], [13] achieves compactness, robustness, and superior performance compared to existing schemes, with formal security proofs under established models.

III. SYSTEM ARCHITECTURE

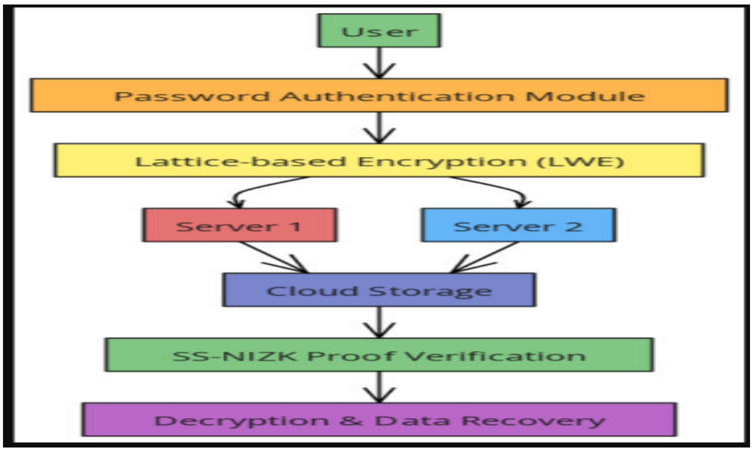

User
Password Authentication Module
Lattice-based Encryption (LWE)
Server 1
Server 2
Cloud Storage
SS-NIZK Proof Verification
Decryption & Data Recovery

Fig 3.1 System Architecture

IV. METHODOLOGY

a. Overview and Design Goals

QPause [12], [13] enables password-only control of outsourced data, secure even against quantum-capable adversaries. It combines password-protected secret sharing (PPSS [8], [11]) with lattice-based [13] post-quantum primitives in a round-optimal protocol without secure channels. User [5], [11]s encrypt data locally, split the encryption key across key servers, and recover it using only a password. Goals include robustness under realistic password distributions, compact ciphertexts independent of server count (via SS-NIZK [10] thresholdizing), and secure threshold decryption with hidden shares.

b. System and Threat Model

The system includes a data owner, cloud storage (CS) for ciphertexts, and N key servers (KS) where any t+1 can recover the key. Adversaries [6] may eavesdrop, modify, or inject messages, corrupt up to t KS, and possess quantum capabilities. QPause [12], [13] ensures key/data confidentiality, share privacy, resistance to offline password guessing [5], [10], and robust recovery despite active attacks.

c. Cryptographic Foundations

QPause [12], [13] relies on Learning With Errors (LWE) over lattices, immune to known quantum attacks [10], [12]. Keys are protected via LWE-based encryption, and PPSS [8], [11] is adapted to lattices: the key is secret-shared among KS, gated by a password-derived value. Features include re-randomizable password masking, low-norm interpolation, and structured noise to hide shares. SS-NIZK proofs over lattice commitments provide active security and keep ciphertext size independent of N.

d. Architecture and Protocol Flow

The protocol has setup, outsourcing, and recovery phases, with optional key rotation/share refresh. User [5], [11] software handles cryptography, KS run lightweight lattice operations, and CS stores only ciphertexts. Communication uses ordinary channels secured with ephemeral lattice keys [9], [10] and SS-NIZK [10] tags.

V. DESIGN AND IMPLEMENTATION

The system consists of four main modules: Cloud Service Provider (CSP [9]), Key Server [10] (KS), Data Owner [4], [8], and User [5], [11].

1) Cloud Service Provider (CSP [9]) – Handles authorization, global visibility, and security analytics. Manages token issuance/validation, dataset metadata views, dashboards for suspicious activities, system operation analytics, password attack reports, and audit logs.

2) Key Server [10] (KS) – Manages threshold key shares and partial decryptions with proof verification. Provides rate-limiting, quorum health monitoring, and secure handling of operations without revealing raw keys.

3) Data Owner [4], [8] – Manages the dataset lifecycle, including client-side encryption, key share creation, upload to CSP [9]/KS, dataset catalog viewing, and key/share rotation or revocation.

4) User [5], [11] – Accesses protected datasets using only a password via the QPause [12], [13] recovery process. Modules include:

- *My Profile* – View/update credentials, login history, and alerts.
- *Request Secret Key* – Perform round-optimal, quantum-secure key recovery with KS quorum.
- Download Datasets – Fetch encrypted datasets from CSP [9], decrypt if key is recovered, and maintain download history.

Data Flow: Owners encrypt datasets, store ciphertext in CSP [9], and masked shares in KS. User [5], [11]s are authorized by CSP [9], recover keys via KS quorum, and decrypt datasets locally. CSP [9] dashboards provide system-wide monitoring and attack analytics.

VI. OUTCOME OF RESEARCH

This research presents QPause [12], [13], a quantum-resistant password-protected data outsourcing scheme that overcomes the limits of existing PPSS [8], [11] models in the post-quantum era. Built on lattice-based [13] cryptography and the Learning With Errors (LWE) assumption, QPause [12], [13] secures outsourced datasets against classical and quantum attacks [10], [12] without requiring secure channels. Using SS-NIZK proofs and ephemeral key pairs, it ensures robustness, compactness, and protection from eavesdropping. Structured noise and low-norm interpolation prevent share leakage, while re-randomized passwords keep masked shares indistinguishable from random values. Performance tests show reduced computation and communication costs in recovery compared to existing schemes. Fully integrated CSP [9], Key Server, Data Owner [4], [8], and User [5], [11] modules enable secure management, controlled access, real-time attack monitoring, and complete auditability.

VII. RESULT AND DISCUSSION

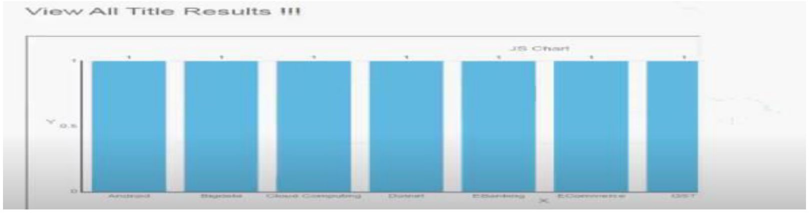


Fig 7.1. Bar Graph

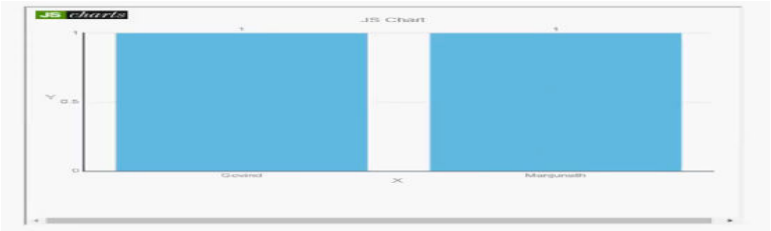


Fig7.2. Bar graph for Result

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The experimental evaluation of QPause [12], [13] demonstrates its superior performance and robustness compared to existing password-protected secret sharing (PPSS [8], [11]) schemes, particularly in the post-quantum security context. Under two parameter configurations designed for 128-bit post-quantum security, QPause [12], [13] consistently outperformed Roy et al.'s lattice-based [13] PPSS [8], [11] in both computation and communication overhead during the recovery phase. The re-randomization password technique, coupled with clear-denominator interpolation and structured noise injection, effectively maintained decryption correctness while preventing leakage of server-side shares. Security proofs under the Zipf [10], [12] password distribution model confirmed resilience against offline password guessing [5], [10], key mismatch, and signal leakage attacks, even with up to ttt corrupted key servers. Additionally, the use of simulation-sound non-interactive zero-knowledge proofs (SS-NIZK [10]) ensured strong active security without secure channels, resulting in a compact, round-optimal protocol with practical recovery latency.

VIII. CONCLUSION

QPause [12], [13] successfully delivers a quantum-resistant, password-protected data outsourcing framework for cloud storage, addressing the limitations [8], [11], [12] of prior PPSS [8], [11] schemes. By integrating lattice-based [13] cryptography, re-randomization password masking, clear-denominator interpolation, and SS-NIZK [10] proofs, the system achieves strong security against both classical and quantum adversaries while maintaining efficiency and usability. Experimental results validate its superiority in computation, communication, and robustness under realistic password distributions, proving it as a scalable and reliable solution for secure data management in the post-quantum era.

REFERENCES

1.D. Rydning, J. Reinsel, and J. Gantz, "The digitization of the world from edge to core," *Framingham: Int. Data Corporation*, vol. 16, pp. 1–28, 2018.
2.M. B. Hui, "Cloud services may become the biggest source of DDoS [2] attacks," 2019.[Online].Available:https://www.freebuf.com/fevents/203988.html
3. M. Andrey, "Building a distributed network in the cloud: Using amazon EC2 to break passwords [13]?," 2017, [Online]. Available:https://blog.elcomsoft.com/2017/08/breaking-passwords-in-the-cloud-using-amazon-p2-instances.
4. Y. Zhang, C. Xu, N. Cheng, and X. Shen, "Secure password-protected encryption key for deduplicated cloud storage systems," IEEE Trans. Dependable Secure Comput., vol. 19, no. 4, pp. 2789–2806, Jul./Aug. 2022.
5. P. Das, J. Hesse, and A. Lehmann, "DPaSE: Distributed password-authenticated symmetric encryption," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2022, pp. 682–696.
6. V. Mangipudi, U. Desai, M. Minaei, M. Mainack, and K. Aniket, "Uncovering impact of mental models towards adoption of multi-device crypto-wallets," 2022. [Online].Available:https://eprint.iacr.org/2022/075
7. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2010, pp. 136–149.
8. A. Bagherzandi, S. Jarecki, N. Saxena, and Y. Lu, "Password-protected secret sharing," in *Proc. Int. Symp. Inf. Theory Appl.*, 2011, pp. 433–444.
9. "Google cloud key management service," 2018. [Online]. Available: https://cloud.google.com/kms/.pdf
10.S. Jarecki, H. Krawczyk, and J. Resch, "Updatable oblivious key management for storage systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 379–393.
11. S. Jarecki, A. Kiayias, and H. Krawczyk, "Highly-efficient and composable password-protected secret sharing," in *Proc. IEEE Eur. Symp. Secur. Privacy*, 2016, pp. 276–291.
12. D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," in *Proc. Annu. Cryptol. Conf.*, 2013, pp. 410–428.
13. M. Klooß, A. Lehmann, and A. Rupp, "(R)CCA secure updatable encryption with integrity protection," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2019, pp. 68–99.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com