RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES

DOI:10.5281/zenodo.22801991

Quantum Shield S3: A Hybrid Post-Quantum Encryption Framework with Self-Hosted Object Storage and Workflow Automation

Dr. Hiteshkumar M. Nimbark*[1], Ms. Hansiniba P. Jadeja[2], Mr. Dhruvraj Parmar[3]

[1*] *Gyanmanjari Innovative University, Bhavnagar, Gujarat, India, prof.nimbark@gmail.com*
[2] *Gyanmanjari Innovative University, Bhavnagar, Gujarat, India, hpjadeja@gmiu.edu.in*
[3] *Gyanmanjari Innovative University, Bhavnagar, Gujarat, India, research1@gmiu.edu.in*

Abstract: The growing transition toward post-quantum cryptography has created new challenges for institutions that must protect sensitive digital records over long periods of time. Universities, hospitals, legal offices, research centers, and public agencies need security architectures that address future cryptanalytic risks without sacrificing operational control or affordability. This paper presents Quantum Shield S3, a hybrid and self-hosted framework that combines ML KEM 768 for post-quantum key encapsulation, AES 256 GCM for bulk encryption, SHA-3 512 for supplementary integrity verification, MinIO object storage, and n8n workflow automation. The study does not introduce a new cryptographic primitive. Instead, it examines how standardized post-quantum tools can be integrated into a storage environment that supports data sovereignty, auditability, and crypto agility. Prototype findings show that the post-quantum component incurs a visible fixed cost for very small files, while the relative overhead becomes more limited for medium and large storage workloads. The paper argues that post-quantum migration should be understood not only as a technical upgrade but also as an institutional governance issue involving workflow accountability, infrastructure control, and long-term digital stewardship. Quantum Shield S3 is presented as a research prototype and a practical reference model for organizations preparing for future-ready storage security.

Keywords: Post-Quantum Cryptography, ML KEM 768, Institutional Data Protection, Self-Hosted Storage, Workflow Automation

Introduction

The long-term security of digital information is increasingly shaped by developments in quantum computing. For many years, institutions have relied on classical public key systems to secure communication channels, archives, and stored records. That confidence is now being reconsidered because sufficiently advanced quantum machines may eventually undermine the mathematical assumptions behind widely used public key schemes. Shor (1997) showed that integer factorization and discrete logarithm problems can be solved efficiently on a quantum computer, which places long-range pressure on cryptographic systems built around RSA and elliptic curve methods.

This concern becomes more serious in sectors where confidentiality must remain intact for many years. Medical files, legal records, financial archives, research data, and government documents often outlive the cryptographic tools originally used to protect them. The harvest now, decrypt later scenario captures this risk clearly. Under this model, adversaries collect encrypted data in the present and wait for future computational advances that may allow later decryption (Bernstein & Lange, 2017; ENISA, 2021). For institutions responsible for long-lived sensitive information, this means that present security decisions have future consequences.

The publication of post-quantum standards has changed the discussion from speculation to implementation. NIST formalized ML KEM in FIPS 203 and signaled that post-quantum migration should begin early because replacing vulnerable cryptographic dependencies across real systems takes time and planning (NIST, 2024a, 2024b). Public guidance from BSI, ENISA, and the National Cybersecurity Center of Excellence has similarly emphasized risk assessment, staged transition, and crypto agility rather than delayed action (BSI, 2021; ENISA, 2021; NCCoE, 2026).

Even with these developments, a significant gap remains between standardization and operational deployment. Much of the literature focuses on algorithm design, theoretical security, or protocol benchmarking. Less attention has been given to how standardized post-quantum methods can be combined with self-hosted storage, structured metadata, and automation workflows in an institutional setting. In practice, a future-ready security architecture must do more than encrypt data. It must also support auditability, storage governance, key lifecycle control, and operational repeatability.

This paper addresses that gap by presenting Quantum Shield S3, a hybrid post-quantum storage framework that integrates ML KEM 768, AES 256 GCM, SHA-3 512, MinIO object storage, and n8n workflow automation. The contribution of this work lies not in inventing a new primitive, but in demonstrating how existing standardized and open tools can be assembled into a practical reference architecture. The paper pursues three objectives. First, it presents the design of a self-hosted post-quantum storage framework suitable for institutional evaluation. Second, it analyzes the performance profile of the prototype across different file sizes. Third, it interprets the framework as a socio-technical model that connects cryptography with governance, traceability, and long-term data stewardship.

Literature Review

Post-quantum cryptography has moved from a specialized research area into a strategic field of infrastructure planning. Bernstein and Lange (2017) argued that quantum-resistant migration cannot wait until the threat fully materializes, because large-scale security transitions are slow and depend on legacy systems as well as institutional processes. Lattice-based cryptography emerged as one of the strongest candidates for this transition because it combined theoretical depth and practical adaptability. Lyubashevsky et al. (2013) contributed important foundational work on learning with errors over structured rings, while later research translated those ideas into practical mechanisms for key establishment and encapsulation.

A major step in this development was the standardization of ML KEM. NIST finalized FIPS 203 to define the Module Lattice Based Key Encapsulation Mechanism and standardized parameter sets for ML KEM 512, ML KEM 768, and ML KEM 1024 (NIST, 2024a). Earlier technical work on Kyber, which forms the basis for the standardized mechanism, had already demonstrated the feasibility of lattice-based encapsulation in practical settings (Ducas et al., 2018; Basso et al., 2021). NIST's formal adoption of ML KEM gave institutions a clearer basis for migration planning and signaled that implementation should no longer be treated as a distant research topic (NIST, 2024b).

Policy-oriented guidance has also stressed that post-quantum transition should not be framed as a simple one-time swap. ENISA (2021) described the transition as a matter of anticipatory risk reduction and long-term preparedness. BSI (2021) emphasized crypto agility and explicitly recommended hybrid approaches where practical, since institutional systems often need transitional models rather than abrupt replacement. The NCCoE project on migration to post-quantum cryptography similarly treats the problem as one of identifying vulnerable dependencies across hardware, software, and services and then moving toward quantum-resistant alternatives through staged implementation (NCCoE, 2026).

Applied performance studies reinforce the importance of context. Alkim et al. (2016) and Paquin et al. (2020) showed that post-quantum cryptographic operations often introduce fixed costs that are most noticeable in small payload or handshake-dominated environments. In larger application settings, however, those costs may become a smaller proportion of total runtime. This distinction is especially relevant for storage systems, where the dominant workload often involves file handling, transfer, and persistence rather than repeated lightweight exchanges.

At the same time, the operational side of post-quantum storage remains underexplored. Real security infrastructures depend on more than encryption algorithms. They also require

audit trails, metadata discipline, access control boundaries, key version tracking, and repeated administrative routines. MinIO provides a self-hosted S3-compatible object storage environment that is well suited for studying these issues outside proprietary cloud dependence (MinIO, 2026). n8n offers a self-hosted workflow platform capable of automating scheduled and event-driven tasks in a transparent and customizable form (n8n, 2026). Bringing these tools together with standardized post-quantum cryptography creates an opportunity to examine post quantum transition not merely as a cryptographic problem, but as an institutional systems problem.

Methodology

This study adopts an applied design and prototype evaluation approach. The purpose is to investigate how standardized post-quantum cryptography can be embedded into a manageable storage architecture that institutions can understand, operate, and adapt. The design of Quantum Shield S3 was guided by five principles: post-quantum readiness, self-hosted control, workflow automation, auditability, and modularity.

The framework is organized into five layers. The first is an application interface implemented with FastAPI. This layer receives storage requests and exposes encryption and retrieval functions through a structured API. The second is the cryptographic engine, which performs ML KEM 768 encapsulation and decapsulation together with AES 256 GCM encryption and decryption. A supplementary SHA-3 512 digest is also generated for verification and audit purposes. The third layer is the storage backend, implemented through MinIO as a self-hosted S3-compatible repository. The fourth layer is a lightweight SQLite metadata store used for timestamps, object paths, integrity records, and key version tracking. The fifth layer is n8n, which automates recurring operational tasks such as upload-triggered encryption, periodic integrity checks, audit reporting, and key rotation review.

The use of ML KEM 768 was chosen for its balance of performance and security within the standardized ML KEM family. Open Quantum Safe documents ML KEM 768 with a public key length of 1184 bytes, a secret key length of 2400 bytes, a ciphertext length of 1088 bytes, and a shared secret length of 32 bytes (Open Quantum Safe, 2026b). These values are practically relevant because they affect storage overhead as well as processing time.

The encryption workflow follows a hybrid model. First, ML KEM 768 encapsulates a shared secret using the recipient's public key. Second, that shared secret is used in AES 256 GCM to protect the file payload. Third, a SHA-3 512 digest is computed over selected cryptographic artifacts and metadata fields. This digest is not treated as a replacement for the authentication already provided by AES GCM. Instead, it functions as an additional verification record for audit logs, workflow validation, and integrity review.

Encrypted objects are stored under a structured path that includes tenant or organizational unit identity, temporal organization, and an object identifier. Metadata associated with each object includes the digest value, the encryption timestamp, and the key version identifier. This structure was selected because institutional security requires procedural visibility in addition to confidentiality. A system is easier to govern when administrators can reconstruct what happened, when it occurred, and which key generation or workflow state was involved.

Performance evaluation relied on prototype measurements collected across file sizes ranging from one kilobyte to one gigabyte. The tests were performed in a single-machine environment with co-located services. Although this setup does not represent distributed production conditions, it is sufficient for analyzing relative overhead patterns and assessing whether the design is plausible for institutional storage workloads.

Table and figures

Table 1. Functional Layers of Quantum Shield S3

Layer	Component	Technology	Main Role
Interface	Application service	FastAPI	Receives requests and returns auditable responses
Cryptography	Key encapsulation	ML KEM 768 via liboqs	Establishes post-quantum shared secrets
Cryptography	Bulk Encryption	AES 256 GCM	Protects file confidentiality and authenticity
Verification	Supplementary digest	SHA-3 512	Supports audit comparison and integrity checks
Storage	Object backend	MinIO	Stores encrypted objects in a self-hosted environment
Metadata	Local record store	SQLite	Maintains timestamps, key versions, and workflow logs
Automation	Workflow engine	N8n	Schedules verification, reporting, and key management

Table 2. Prototype Latency Comparison

File Size	Classical Balance	Hybrid Prototype	Relative Overhead
1KB	0.5 ms	1.2 ms	about 140 percent
1 MB	12 ms	14 ms	about 16.7 percent
10 MB	120 ms	125 ms	about 4.2 percent
100 MB	1.2 s	1.25 s	about 4.2 percent
1 GB	12 s	12.5 s	about 4.2 percent

The layered design illustrates how cryptographic functions, storage operations, and administrative workflows can be combined into a unified architecture without relying entirely on proprietary cloud infrastructure. This modularity also allows future substitutions if organizational policies, compliance conditions, or implementation guidance change.

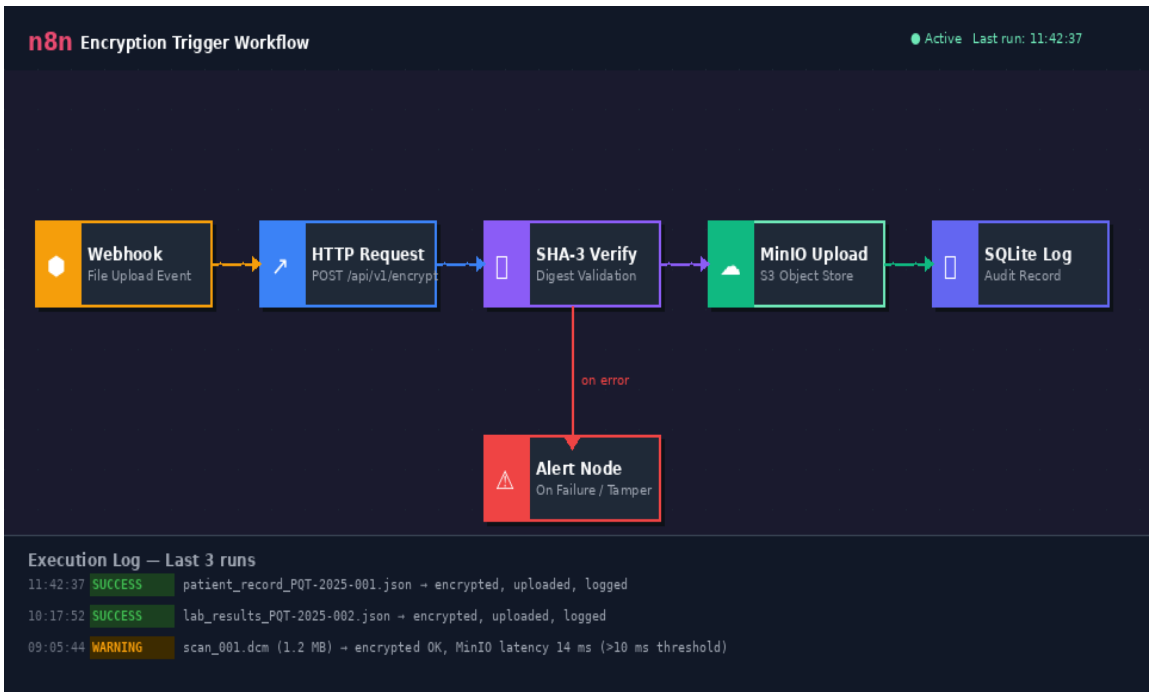

Figure 1. Conceptual architecture of Quantum Shield S3 showing client upload, encryption service, cryptographic engine, MinIO storage, SQLite metadata logging, and n8n workflow automation

Results and Discussions

The prototype results show a clear difference between small file and large file behaviour. For very small objects, the fixed cost of post-quantum key encapsulation is a large part of the total runtime. That is why the relative overhead at one kilobyte is high. For larger objects, however, the encryption and storage tasks dominate a greater share of the workflow, so the encapsulation cost becomes proportionally smaller.

The most defensible reading of the benchmark results is that the hybrid layer becomes operationally modest for files from about ten megabytes upward. The one-megabyte case still shows a visible increase and should not be described as negligible. This distinction is important because careful interpretation improves the credibility of the paper. Rather than making broad claims, the study shows that the practical value of post-quantum storage depends on workload context.

From an institutional perspective, the significance of the framework extends beyond timing figures. First, the use of MinIO supports data sovereignty by allowing organizations to keep encrypted objects within self-controlled infrastructure rather than relying fully on external cloud storage. Second, the use of n8n improves workflow consistency by automating routine protective actions such as logging, verification, and scheduling. Third, the preservation of metadata and digest values strengthens auditability by making it easier to review system behaviour and reconstruct security events.

These advantages are especially relevant in environments where digital trust is not only a technical matter but also an administrative and ethical one. A university, hospital, or public institution cannot assess a security architecture solely by asking whether the cipher is strong. It must also ask whether the system can be governed responsibly, whether workflows are traceable, and whether staff can verify that sensitive records are handled consistently. In this sense, post-quantum migration is part of a broader question of institutional stewardship.

The study also has limitations. The overall hybrid system is not supported by a new formal security proof. The benchmark environment is single-node and co-located, so the results should not be generalized directly to distributed storage clusters. Workflow fault

recovery under interruption or partial execution requires further testing. The implementation also depends on evolving software libraries such as liboqs, which Open Quantum Safe positions as an important tool for experimentation and integration, though not as a substitute for every form of regulatory certification (Open Quantum Safe, 2026a, 2026b).

Even with these limitations, the framework contributes a practical reference design. Its originality lies not in inventing a new primitive but in showing how standardized post quantum encryption can be tied to self-hosted storage and automated governance in a form that institutions can realistically study and adapt.

Equations

The core processing logic can be summarized as follows:

$$(C_{kem}, K) = \text{ML-KEM-768.Encaps}(pk) \quad (1)$$

$$(C_{sym}, T_{gcm}) = \text{AES-256-GCM.Encrypt}(K, nonce, P) \quad (2)$$

$$D = \text{SHA3-512}(C_{kem} \parallel C_{sym} \parallel T_{gcm} \parallel metadata \quad (3)$$

In Equation (1), a shared secret and key encapsulation ciphertext are generated from the recipient public key. In Equation (2), the shared secret is used to encrypt the plaintext file with AES 256 GCM. In Equation (3), a supplementary digest is created for metadata-based verification and audit review.

Conclusions

This paper presented Quantum Shield S3 as a hybrid post-quantum storage framework that combines ML KEM 768, AES 256 GCM, SHA-3 512, MinIO, and n8n within a self-hosted architecture. The prototype results show that post-quantum key encapsulation introduces a clear fixed cost for very small files, while the relative burden becomes much lower for medium and large storage workloads.

The broader contribution of the study lies in its institutional perspective. Post-quantum migration is not merely a cryptographic replacement exercise. It is also a governance challenge involving infrastructure control, workflow accountability, data sovereignty, and long-term stewardship of sensitive records. By linking standardized cryptography with storage metadata and automation, Quantum Shield S3 offers a practical reference design for institutions that want to explore future-ready security without losing operational visibility.

References

Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange: A new hope. In *Proceedings of the 25th USENIX Security Symposium* (pp. 327–343). https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim

Basso, A., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2021). *CRYSTALS Kyber algorithm specifications and supporting documentation* (Version 3.02). https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. https://doi.org/10.1038/nature23461

Bundesamt für Sicherheit in der Informationstechnik. (2021). *Migration to post-quantum cryptography*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Kyber: A CCA secure module lattice based key encapsulation mechanism. In *2018 IEEE European Symposium on Security and Privacy* (pp. 353–367). https://doi.org/10.1109/EuroSP.2018.00032

European Union Agency for Cybersecurity. (2021). *Post-quantum cryptography current state and quantum mitigation.* https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

FastAPI. (2026). *FastAPI documentation.* https://fastapi.tiangolo.com/

Federal Register. (2024, August 14). Announcing issuance of Federal Information Processing Standards FIPS 203, FIPS 204, and FIPS 205. https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. *Journal of the ACM, 60*(6), Article 43. https://doi.org/10.1145/2535925

MinIO. (2026). *MinIO documentation*. https://docs.min.io/

n8n. (2026). *Self hosting n8n*. https://docs.n8n.io/hosting/

National Cybersecurity Center of Excellence. (2026). *Migration to post-quantum cryptography.* https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

National Institute of Standards and Technology. (2024a). *Module lattice based key encapsulation mechanism standard* (FIPS 203). https://csrc.nist.gov/pubs/fips/203/final

National Institute of Standards and Technology. (2024b, August). *NIST releases first 3 finalized post-quantum encryption standards*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Open Quantum Safe. (2026a). *liboqs.* https://openquantumsafe.org/liboqs/

Open Quantum Safe. (2026b). *ML KEM algorithm datasheet*. https://openquantumsafe.org/liboqs/algorithms/kem/ml-kem.html

Open Quantum Safe Project. (2026). *liboqs GitHub repository.* https://github.com/open-quantum-safe/liboqs

Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In J. Ding & R. Steinwandt (Eds.), *Post-quantum Cryptography* (pp. 72–91). Springer. https://doi.org/10.1007/978-3-030-44223-1_5

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172