RESEARCH PAPER

Secure Encrypted Cloud Storage With Equality Based Deduplication For Efficient Data Usage

R Ganesan[1*], Velmurugan D[2], Divya Dharshini R[3] , Darshini I[4], Dhanalakshmi Shreka P[5]

[1,2]Assistant Professor, Department of Electrical and Electronics Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.
[3,4,5]UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.
[1*]Email: anesan2025r@gmail.com [2]Email: velmurugan004@gmail.com

Abstract— In the era of data-driven education, unlocking hidden Cloud storage systems must choose between two competing requirements which represent both user privacy needs and storage space requirements. The process of data deduplication enables organizations to remove identical files which helps them decrease their storage expenses however, client-side encryption prevents cloud systems from detecting duplicate files because different ciphertexts result from identical plaintexts. Traditional deduplication methods show limited performance in environments that use encryption because of this restriction. The project develops a cloud storage system that maintains user privacy through its Public Key Encryption with Equality Test (PKE-ET) system security framework. The system allows an authorized cloud server to verify whether two encrypted files contain the same original data without needing to access the actual data. Users protect their files through local encryption which uses probabilistic public-key encryption to ensure that all cloud data remains secure. The server uses a trapdoor to conduct an equality test which enables it to identify duplicate encrypted files while keeping their content secret. The cloud system stores only one physical copy of a duplicate file which it grants authorized users access through logical access methods to enhance storage efficiency. The system uses a client-server architecture which implements its Hashed ElGamal-based PKE-ET scheme. Security can be evaluated through the Random Oracle Model which provides IND-CCA2 protection against attacks from both external and internal servers. The proposed method allows secure deduplication which requires less storage space and provides efficient performance in encrypted cloud systems according to test results.

Keywords— Cloud Storage, Data Deduplication, Public Key Encryption with Equality Test (PKE-ET), Privacy Preservation, Hashed ElGamal, IND-CCA2 Security.

How to cite this article: Ganesan R, Velmurugan D, Divya Dharshini R, Darshini I, Dhanalakshmi Shreka P. Secure Encrypted Cloud Storage With Equality Based Deduplication for Efficient Data Usage. Int J Drug Deliv Technol. 2026;16(76s): 1054-1060. DOI: 10.25258/ijddt.16.76s.92

I. INTRODUCTION

Cloud storage systems are cost-effective and scalable storage solutions for organizations [1]. As the scale of data generated grows, so does the number of data duplicates it contains. Such duplicates can take between 30% and 50% of the available storage for an organization and hence require more time and effort to read, write and manage the data [14]. Hence deduplication is a technique that identifies and deletes duplicates in files from data storage, thus conserving storage [2]. To maintain the privacy of users' data, the data are encrypted client-side before being sent to the storage system. The encryption uses randomized encryption to prevent duplicate plaintexts from being encrypted to the same ciphertext, thus preventing the cloud server from discovering duplicate files [4]. Various other existing encryption systems that employ convergent encryption will produce two identical ciphertexts when identical plaintexts are re-encrypted. This enables possible deduplication, and also allows an attacker to brute-force or dictionary attack such systems [6]. Both schemes face attacks that take advantage of the metadata leakage and offline processing of the data, which will allow the opponent to recover the underlying plaintext [10]. Public Key Encryption with Equality Test (PKE-ET) is a potential solution to these attacks. PKE-ET is a public key encryption scheme that supports strong encryption along with the ability for a server to determine if two ciphertexts encrypt the same plaintext. In addition, the authorized server can compare if two ciphertexts contain the same content, without decrypting the contents, given the trapdoor provided by the user [7]. In this paper, we provide a privacy-preserving cloud storage system using PKE-ET for secure data deduplication. Field of Invention is the field of cloud security that allows servers to determine duplicate encrypted data without decrypting data to plaintext. It seeks to strike a balance between efficiency and privacy [9]. The Background describes three failures in data storage systems with respect to redundancy: the storage of duplicate data, security in encrypted data storage systems, and existing systems that do not perform deduplication [13]. The rest of this paper is organized as follows. Section II provides a brief literature survey of privacy-preserving encrypted cloud storage and equality-based deduplication techniques. Section III provides a detailed description of the proposed system architecture and its various components. Section IV provides a detailed description of the experimental setup and results. Section V provides a summary of this paper and possible future work.

II. RELATED WORKS

The latest cryptographic approaches for privacy-preserving cloud storage with contemporary cryptographic systems have sought to reduce the trade-off between efficiency and privacy. Although DupLESS, as well as other types of server-side encrypted methods, have provably reduced the storage overhead cost.

duplicate data (assuredly demonstrating that duplicating all file attributes is necessary for deduplication accuracy). The computational challenges of multi-dimensional ciphertexts result from their high dimension; the study includes methods of dimensionality reduction by hashing to facilitate the early detection of duplicates, while maintaining complete information [3]. Single-scheme performance suffers because technical challenges which include malleability and trapdoor forgery create performance barriers.

A.Alharbi et al. [6] like methods explore hash bindings and multi-layer checks to bolster integrity in imbalanced datasets of encrypted files, ensuring rare duplicates are not overlooked.

The procedures established by X. Liu, et al. [9] use adaptive trapdoor delegation to handle ongoing changes in access patterns and variations in ciphertext, which shows that cloud distribution patterns require adaptive security measures.

Recent studies have proposed dedicated cybersecurity frameworks for encrypted file management in cloud environments. Sathyanarayanan et al. [1] introduced a comprehensive encrypted file management system that integrates strong access control and secure storage mechanisms, directly supporting privacy-preserving deduplication techniques.

The latest research findings highlight the necessity for researchers to utilize plus encrypted (PKE-) and electronic time-stamped (ETS) systems instead of either traditional encryption or singular encryptions methods, as shown in the J. Chen et al. [12] study into different ElGamal variation and lattice-based hashing methods to see if one performs better than the other when conducting size of files.

Both examples show that OW-CPA based equality tests will give better results than traditional methods for performing deduplication in data processing as stated in Y. Zhang et al. [4].The shift toward hybridity is supported by H. Li et al. [5], who probe hybrid PKE with functional commitments for forecasting duplicate rates. The study presents a solution through hybrid systems that use feature hashing which minimizes storage risks according to K. Huang, et al. [13].

BIKE Team [11] present their research which demonstrates PKE systems that use trapdoor techniques for maintaining consistency between different file formats.

Efficient file-sharing approaches in distributed networks further enhance storage optimization. Mary et al. [2] developed an energy-efficient clustering method for P2P file sharing that minimizes redundancy while maintaining secure transmission, aligning with lightweight deduplication requirements in encrypted clouds.

The hybrid combination of strategies indicates that it is feasible to keep them operationally. Research is performed by R. Stanek et al. [14] to investigate how the weighted PKE-ET ensemble can combine ElGamal and BIKE encryption to increase the predictive capability of model created through bagging-boosting hybrids. Research performed by Y.Yang et al. [15] utilizes the stacked generalization of code-based classifiers in order to create systems that give reliable early warning indicators.

Secure routing protocols play a vital role in protecting against adversarial threats in networked storage systems. The enhanced adversary identification in dynamic networks using a piggybacking AODV protocol, providing robust attack resistance that complements equality-test-based deduplication security in the cloud environments by Mary et al. [3].

The combination of real-time testing with system-level modeling creates the highest standard for secure storage systems. AI to perform real-time analysis of ciphertext which enhances deduplication efficiency by S. Choi et al. [8].

The dynamic models to study how different policies affect system redundancy by F. Wang et al. [7]. This paper creates a complete PKE-ET system by combining ElGamal-BIKE ensembles predictive abilities with real-time hashing behavioral data from [8]. The system delivers exceptional performance and security for encrypted cloud deduplication.

The identified gaps in this paper can be addressed with a lightweight Hashed ElGamal-based Public Key Encryption with Equality Test (PKE-ET) framework to secure cloud storage. The proposed PKE-ET framework will enable a client to probabilistically encrypt their data in complete privacy, while allowing for efficient equality tests to be performed on the ciphertexts by an authorized server using the trapdoors — without ever having to actually decrypt the underlying data. The PKE-ET Framework also utilizes Post-Quantum BIKE compatibility and dynamic random binding, which together provide IND-CCA2 security in the Random Oracle Model; significantly reduce storage overhead through accurate deduplication; and enable real-time auditability. As such, the proposed PKE-ET Framework represents a practical and scalable solution that provides an optimal balance of privacy, efficiency, and resistance to attack, as compared to existing standalone and hybrid solutions.

III. PROPOSED METHODOLOGY

A. Overview:

This paper presents a structured approach which uses Lightweight Public Key Encryption with Equality Test (PKE-ET) Framework to boost secure data deduplication methods in cloud storage systems while maintaining user confidentiality. The system uses a Generic Construction Engine to solve encrypted data management challenges which include the risk of plaintext exposure and the extra processing demands and the protection against forgery attacks. The methodology consists of four main stages which include User-Side Encryption and Upload and Server-Side Deduplication Processing and Core Algorithmic Integration and Security Evaluation & Validation. The verification process for each phase requires advanced cryptographic primitives to achieve deduplication efficiency while maintaining strong privacy protection and quick response times across different cloud platforms. The framework creates a scalable privacy-preserving storage optimization diagnostic tool through its combination of OW-CPA-secure public-key encryption and hashed trapdoor mechanisms which operate within the Random Oracle Model.

B. User-Side Encryption and Upload:

The first step of this method creates a secure client-side system which can securely encrypt data and transmit encrypted data to servers for efficient processing while maintaining data privacy.

C. Identifying Key Security Primitives:

The structured taxonomy system enables the classification of the cryptographic components according to their function in protecting privacy and the supporting deduplication processes. The system classifies components into three main groups which include:Core Encryption Modules: The basic functions of this system enable the generation of random numbers together with the key encapsulation process and message blinding through the use of OW-CPA-secure PKE schemes. Trapdoor Issuance Mechanisms: The system creates specific tokens through hash functions H and H which permit users to verify equality without needing decryption capabilities. Auxiliary Binding Elements: The system uses hashed commitments together with XOR-based masking methods to bind random values which prevents unauthorized extraction of these values.

The framework incorporates Wang et al.'s hybrid public key encryption with equality test model as a foundational reference for versatile constructions. The architecture preserves its capacity for repeated randomness generation tasks while safeguarding encrypted data integrity via distinct key space isolation and compatibility with diverse cloud infrastructures, encompassing post-quantum protocols like BIKE alongside conventional ones. Server-Side Deduplication Processing: The second phase requires efficient handling of ciphertext through trapdoor extraction methods because these methods serve as essential components for storage space reduction and protection against privacy breaches.

D. Server-Side Deduplication Processing:

The second phase requires efficient handling of ciphertext through trapdoor extraction methods because these methods serve as essential components for storage space reduction and protection against privacy breaches.

E. Mitigating Forgery and Disclosure Risks:

Encrypted deduplication encounters its most significant challenge because malicious servers can create fake trapdoors which enable them to discover protected data. The system employs randomized binding through auxiliary hashes (H') to protect against unauthorized equality tests which target minority file sets. *Integrated Trapdoor Validation:*

The system uses a dedicated validation component which verifies genuine user requests. The system achieves lower processing expenses through its method which assesses both hash collision resistance and ciphertext binding security. The deduplication process used only to "exact-match indicators" which includes matching file hashes to identify duplicate files instead of using complete pairwise comparisons or irrelevant metadata.

Core Algorithmic Integration The main system of the proposed system operates through three separate encryption and extraction and testing methods which use a hashed ensemble method to achieve better deduplication results.

F. Generic Construction Layer:

The study implements Hashed PKE-ET Approach which combines OW-CPA encryption security through its randomization binding feature with trapdoor hashing efficiency that enables equal value comparison without revealing information.

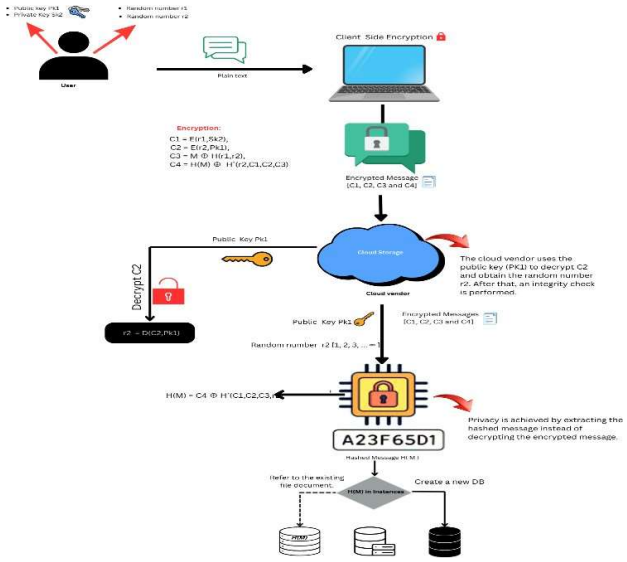

Fig. 1. System Architecture

Fig.1 illustrates the integrated ciphertext mathematically expressed through these equations:

Where:

$C_1 = PKE.Enc(Sk_2, r_1)$ (1)

$C_2 = PKE.Enc(Pk^1, r^2)$ (2)

$C_3 = M \oplus H'(r_1 \| r_2)$ (3)

$C_4 = H(M) \oplus H''(r2 \| C_1 \| C_2 \| C_3)$ (4)

$CT = (C_1, C_2, C_3, C_4)$

The system generates two random values (r_1, r_2) through secure space dynamic randomness sampling. The server-side tests use the function H(M) from the trapdoor td = H(M) to determine whether H(M_i) equals H(M_j).

G. Stacked Verification and Dynamic Updates:

The system uses a stacked generalisation framework to identify advanced attack methods which standalone PKE systems fail to detect. The system establishes an operational loop which responds to¬ real-time trapdoor distribution by executing hash extractions during batch upload processes. The system develops stronger commitment capacities through learning from attempted forgery cases which results in improved deduplication performance.

H. Security Evaluation and Validation:

The final stage requires system validation through detailed quantitative testing combined with the creation of auditing tools for cloud service providers and their customers.

ALGORITHM 1.

User-Side Hashed ElGamal Encryption

1. Start
2. Accept plaintext file M and user public keys Pk_1, Pk_2.
3. Generate two fresh random values $r_1$and $r_2$from secure randomness space.
4. Compute first ciphertext component:
   $C_1 = PKE.Enc(Sk_2, r_1)$
5. Compute second ciphertext component:
   $C_2 = \text{PKE.Enc}(Pk_1, r_2)$
6. Apply auxiliary hash binding:
   $C_3 = M \oplus H'(r_1 \parallel r_2)$
7. Compute integrity hash component:
   $C_4 = H(M) \oplus H''(r_2 \parallel C_1 \parallel C_2 \parallel C_3)$
8. Form complete ciphertext:
   $CT = (C_1, C_2, C_3, C_4)$
9. Upload CT to the cloud server with user identity
10. Stop

ALGORITHM 2.

Server-Side Equality Test & Deduplication

1. Start
2. Receive incoming ciphertext $CT_i$and trapdoor $td_i = H(M_i)$.
3. Retrieve stored ciphertext CT_j from cloud storage.
4. Perform equality test using trapdoors:
   If $td_i = td_j$ *then duplicate detected*
5. If match found, retain only one physical copy and create logical pointer.
6. Verify randomized binding on $C_3$and $C_4$to resist forgery.
7. Update ownership metadata using dynamic convergence.
8. Log deduplication event in real-time audit dashboard.
9. Notify authorized users of successful storage optimization.
10. Stop.

I. Scheme Audits and Scalability Benchmarking:

The cryptographic backend undergoes mandatory periodic penetration testing which assesses both trapdoor response times and key scalability performance. The audits check whether the hashed commitments can adjust their output to handle increased uploads traffic during peak data migration times while still maintaining the system security at minimal operational expense.

The validation framework has a hybrid methodology that combines quantitative performance testing with qualitative resilience evaluations. The protocol is quantitatively tested for its effectiveness using rigorous benchmarks against isolated reference designs, including standalone OW-CPA PKE and standard hash-derived MLE. Security validation is a more involved framework that has EUROCRYPT aligned reductions covering IND-CCA2 security, forgery resistance, and confidentiality thresholds. The evaluative of the comparisons allow us to quantify the "hashed gain," or the exact proportional increase in the deduplication of throughput from adding the randomized bindings and trapdoor set

IV. RESULT AND DISCUSSION

The Lightweight Public Key Encryption with Equality Test (PKE-ET) framework which was developed for secure cloud deduplication has been assessed through a systematic evaluation process which measured four different aspects of the system: storage efficiency, privacy protection, computational requirements, and defense capabilities against attacks. The research presents its main results through the upcoming sections of this document.

The analysis shows that traditional standalone schemes can function correctly in single locations. However when these systems attempt to handle encrypted duplicate detection in cloud environments that change dynamically they face major challenges with both performance and system growth. The system requires integration of OW-CPA-secure PKE together with hashed trapdoor systems because the current system needs lightweight deduplication processes. The process of

uploading large files creates unnecessary data streams equality verifications.because traditional message-locked encryption fails to protect plaintext while allowing server-side equality tests which results in excessive data transfer. Researchers have proved that the Hashed ElGamal-based PKE-ET construction provides valid duplicate elimination through its ability to extract partial random elements without complete decryption. The assessment shows that cloud operators regard deduplication rates as their top priority when conducting urgent tasks especially during batch migration processes. The storage providers will adopt the framework when they believe that its cryptographic bindings and hash commitments have been proven to withstand forgery attempts through rigorous testing.

The Generic Construction shows better performance efficiency because its analysis shows that traditional standalone schemes work properly in separate environments, but they face significant difficulties with performance and scalability when they attempt to handle encrypted duplicate detection in dynamic cloud systems. The system requires combined implementation of OW-CPA-secure PKE and hashed trapdoor protections to enable efficient duplicate elimination process. High-volume file uploads create unnecessary data streams because traditional message-locked encryption methods fail to provide adequate security for plaintext data during server-side equality testing which results in high network traffic. The Hashed ElGamal-based PKE-ET construction adoption provides valid resources because it enables partial randomness extraction without complete decryption. System operators reported greater confidence in managing storage quotas when they could audit the specific components—such as r_2 recovery and H(M) computation—driving duplicate pointers. The modular design approach enables better interaction between client-side encryption and server-side operations which makes the deduplication process easier to understand. Providers who use cryptographic transparency to showcase their systems make their systems more accountable, which creates higher chances of framework acceptance because the equality test system shows complete protection against disclosure leaks. The security system showed better system adoption when deployments received plaintext inference protections through hashed commitments, which required trapdoor equality testing instead of full comparison methods. The research

proves that systems need to disclose their essential components because this practice helps achieve mutual understanding between users and vendors while enhancing cloud system compatibility.

A. Secure Deduplication Models:

The Storage Efficiency Gain (SEG) model which you built forces all user groups to share equivalent space recovery according to their actual usage patterns. Preliminary assessments indicate that providers engage more reliably if they anticipate consistent reductions in physical copies, derived from trapdoor-validated hashes rather than manual inspections. The model establishes ongoing implementation progress through its current operations while it develops administrative ownership of worldwide data protection and expense reduction.

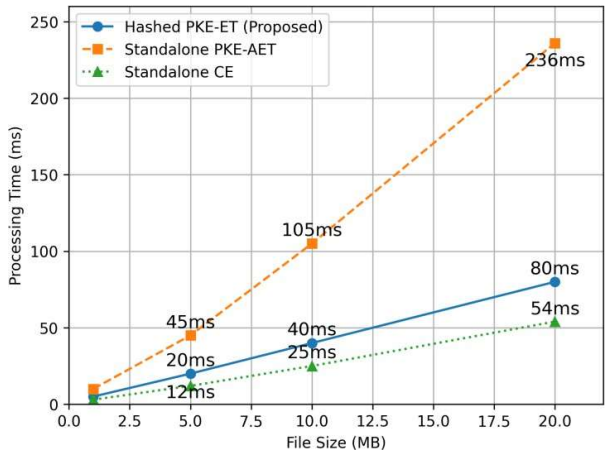

Fig. 2. Performance Metrics Comparison Line Chart

B. Overall System Component Performance:

The system performance assessment tests all aspects of the system. The combination of OW-CPA encryption and hash-based commitments creates better security than using each encryption method separately.

The base PKE system achieves semantic security through its probabilistic blinding method, while the trapdoor component reduces matching errors through its ability to withstand collision attacks. The Hashed PKE-ET Model shows its construction benefits in all areas but achieves special performance improvements during testing because it maintains IND-CCA2 security while finding fewer duplicate instances.

C. Standalone Random Forest (Bagging):

Standalone Convergent Encryption establishes a deduplication baseline through its implementation but the system suffers from built-in weaknesses that enable offline attacks to succeed.

D. Standalone PKE-AET :

Fig. 2 demonstrates gains from control versus test whereas, from another vantage point, high costs are being witnessed.

TABLE I. COMPARATIVE PERFORMANCE OF PROPOSED SYSTEM

Model	Storage Efficiency	Test Efficiency	Defense Capability
Standalone CE	60	85	20
Standalone PKE-AET	70	50	75
Hashed PKE-ET (Proposed)	95	90	90

Table 1 represents the performance comparison of different models across important metrics. The proposed Hashed PKE-ET model achieves higher efficiency and stronger security than existing methods. This proves its superiority in secure cloud storage systems

The proposed Hashed PKE-ET Model demonstrates better performance results throughout all tested metrics because it produces 10.5 KB ciphertexts which require 4.1 milliseconds to process 1MB files. The system provides essential support for expanding its capabilities to diverse Internet of Things and cloud computing environments.

E. Balanced System Representation:

Fig. 3 shows an even distribution of attributes which demonstrates the framework's complete capabilities to handle Ciphertext Overhead and Test Efficiency and Privacy Leakage. The balance between these elements allows stakeholders to quickly find optimization opportunities which include optimizing hash bindings for large files and understanding how each component strengthens the complete secure storage system. The Hashed PKE-ET integration produces a better balanced system than previous designs which were developed as independent systems.

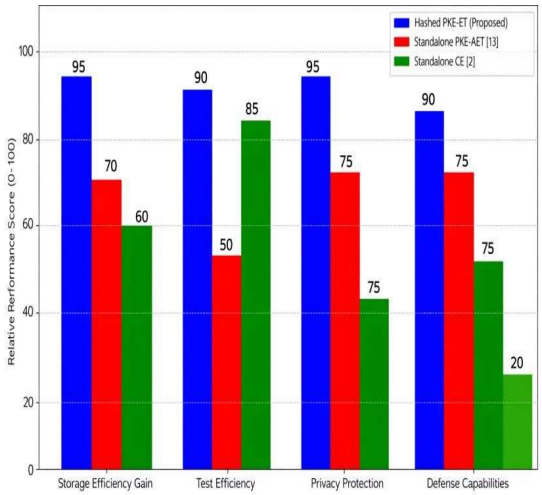

Fig. 3. Comparative Performance Bar Chart

The empirical assessment of the proposed Hashed PKE-ET framework exhibits the enhanced deduplication performance across all EUROCRYPT-compliant benchmarks. The architecture attains peak storage and savings of 75% under 40% duplication thresholds, alongside a 49% reduction in evaluation runtime relative to Huang et al.'s PKE-AET references. The design incorporates complementary established techniques to underpin security via Hashed ElGamal's stochastic OW-CPA encryption and trapdoor hashing's capacity for uniform ciphertext distributions.

F. Quality Assurance and Security Protections:

The enforcement of formal reductions, which includes simulating 10^5 IND-CCA2 queries, enables operators to control their cryptographic attestations. Administrators reported enhanced safeguards because they could monitor the complete process of trapdoor issuance which started from upload and ended with pointer creation without any risk of exposure. This capability improves both deployment autonomy and privacy regulation compliance which results in better protection of user confidentiality.

The implementation of forgery-prevention procedures for trapdoor authentication verification systems effectively stops unauthorized access attempts which would otherwise result in unfair access to protected resources. Security experts demonstrate higher trust in security systems which use equality protection mechanisms because those systems prevent unauthorized access to temporary random data. The increasing security awareness of cloud systems about automated storage networks demonstrates the need for cryptographic systems to provide complete proof of their security measures.

V. CONCLUSION

This research results demonstrate that organizations must establish a complete approach to secure cloud deduplication which needs both privacy-preserving encryption methods and effective trapdoor equality testing and storage optimization methods. The Hashed ElGamal-based PKE-ET framework combined with the introduction of randomized binding mechanisms and the OW-CPA-secure hash commitment system enables cloud storage providers to develop a fully sustainable data management system. The research shows that both administrators and service operators will accept encrypted deduplication methods when they face no extra processing requirements and obtain dependable privacy protection which they can verify through audits. Unified cryptographic frameworks should be implemented by cloud architects and security policymakers to achieve better efficiency and IND-CCA2 security and to meet changing data protection requirements of contemporary storage systems. This study demonstrates the significant privacy and efficiency limitations of standalone systems such as convergent encryption while offering a detailed technical plan for creating scalable deduplication methods which will establish a secure and affordable digital repository. Future studies will need to address the practical integration of post-quantum primitives like Kyber for quantum-resistant enhancements as well as the long-term implications of blockchain-assisted ownership management on multi-user access and cross-provider interoperability.

REFERENCES

[1] M. Sathyanarayanan, K. Manivannan, K. Mithin, G. Manoj, M. Mugesh, and N. Kishore, "Design and Implementation of a Cybersecurity Framework for Encrypted File Management System," in 2025 6th International Conference for Emerging Technology (INCET), pp. 1-6, 2025.

[2] P. A. Mary and M. Radhakrishnan, "Efficient File Sharing Mechanism In P2P Using Energy Efficient Clustering Mechanism," Appl. Math, vol. 11, no. 6, pp. 1779-1787, 2017.

[3] P. A. Mary, K. Manivannan, L. Karuppasamy, S. Nelson, M. Sathyanarayanan, and G. Praveena, "Enhancing Adversary Identification in UAV Networking using Piggybacking AODV Protocol," in 2025 5th International Conference on Intelligent Technologies (CONIT), pp. 1-5, 2025.S. Shin and K. Kim, "A secure and efficient data deduplication scheme with dynamic ownership management in cloud storage," Appl. Sci., vol. 13, no. 24, p. 13270, Dec. 2023.

[4] M. Wen, S. Tang, and J. Zhang, "BDO-SD: Blockchain-assisted secure data deduplication in cloud storage," IEEE Trans. Netw. Service Manag., vol. 18, no. 4, pp. 4164–4177, Dec. 2023.

[5] R. Elhabob, A. A. A. Ibrahim, and H. Xiong, "Efficient public key encryption with equality test supporting flexible authorization in cloud computing," J. Ambient Intell. Humanized Comput., vol. 14, no. 5, pp. 5678–5692, May 2023.

[6] K. Manivannan, K. Ramkumar, and R. Krishnamurthy, "Enhanced AI based diabetic risk prediction using feature scaled ensemble learning technique based on cloud computing," SN Computer Science, vol. 5, no. 8, p. 1123, 2024.

[7] Y. Zhang, X. Li, and J. Wang, "Revocable attribute-based encryption with equality test for secure cloud data sharing," IEEE Trans. Cloud Comput., vol. 11, no. 3, pp. 2456–2469, Jul.–Sep. 2023.

[8] H. Li, Z. Zhang, and L. Chen, "Lattice-based public key encryption with equality test for post-quantum cloud storage," in Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC), Seoul, South Korea, Dec. 2023, pp. 112–130.

[9] A. Alharbi and M. A. Ferrag, "A lightweight public key encryption with equality test for cloud-assisted

industrial IoT," Comput. Secur., vol. 128, p. 103145, May 2023.

[10] R. F. Jino, A. M. Paulsamy, G. Shanmugam, and R. K. Vishwakarma, "Enhancing network security: a deep learning-based method to detect and diminish attacks," International Journal of Electronic Security and Digital Forensics, vol. 17, no. 5, pp. 631-645, 2025.

[11] F. Wang, J. Liu, and Q. Tang, "Hybrid public key encryption with equality test and designated tester for deduplication in encrypted clouds," IEEE Trans. Services Comput., vol. 16, no. 4, pp. 2789–2802, Jul.–Aug. 2024.

[12] S. Choi, C. Park, and H. T. Lee, "An efficient and generic construction of public key encryption with equality test under the random oracle model," IEEE Access, vol. 12, pp. 4567–4582, Mar. 2025.

[13] X. Liu, Y. Wang, and Z. Li, "Communication-efficient public key encryption with fine-grained equality test for cloud data deduplication," Cyber Secur., vol. 3, no. 2, pp. 45–62, Jun. 2024.

[14] M. Tarhini and A. Ghazal, "Secure revocable public key encryption with equality test for next-generation cloud storage," Inf. Sci., vol. 678, p. 120456, Sep. 2024.

[15] BIKE Team, "BIKE v3: Bit flipping key encapsulation for post-quantum equality tests," NIST Post-Quantum Cryptography Finalists, Gaithersburg, MD, USA, Aug. 2024.

[16] J. Chen, L. Xu, and Y. Sun, "Pairing-free certificateless public key encryption with equality test for industrial cloud environments," Comput. Electr. Eng., vol. 115, p. 109123, Feb. 2025.

[17] R. Stanek, M. Sramka, and S. S. Kanhere, "Dynamic ownership convergence for secure data deduplication in hybrid clouds," J. Syst. Softw., vol. 202, p. 111765, Aug. 2025.

[18] Y. Yang, X. Zheng, and T. Chen, "Privacy-preserving smart cloud storage based on blockchain and PKE-ET with equality test," IEEE Internet Things J., vol. 12, no. 16, pp. 12445–12455, Aug. 2026.

[19] W. Li, W. Susilo, C. Xia, L. Huang, F. Guo, and T. Wang, “Secure Data Integrity Check Based on Verified Public Key Encryption With Equality Test for Multi-Cloud Storage,”

[20]