Optimized Dual Access Control for Secure Cloud Storage

P. Renuka[1], R. Yogendra Bobby[2], P. Akhil, S. Baba Shaheer[3]
[1,2,3]*Department of Computer Science and Engineering (Data Science), Raghu Engineering College (Autonomous), Affiliated to JNTU Gurajada, Vizianagaram, Andhra Pradesh, India*

***Abstract*—The rapid adoption of cloud computing has introduced critical challenges related to data privacy, unauthorized access, and auditability in shared storage environments. This paper presents an Optimized Dual Access Control mechanism for secure cloud storage that combines ring-signature-based homomorphic authenticators with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and One-Time Password (OTP) verification. The proposed system enables a public verifier to audit the integrity of shared cloud data without retrieving the entire dataset, while preserving the anonymity of individual block signers. A batch auditing extension further improves efficiency by processing multiple verification tasks simultaneously. On the access-control side, a two-level authorization model involving both the data owner and the cloud server resists Distributed Denial-of-Service (DDoS) and Economic Denial-of-Sustainability (EDoS) attacks. User registration and revocation are managed by a group manager, and traceability capabilities allow the group manager to identify data owners during disputes. Performance analysis confirms that the construction imposes negligible overhead compared to single-layer alternatives, while providing substantially stronger security guarantees. Experimental results demonstrate correctness in AES-CBC encryption, successful group-signature generation, and accurate batch auditing across concurrent verification tasks.**

***Index Terms*—cloud storage security, dual access control, ring signatures, CP-ABE, homomorphic authenticators, batch auditing, OTP verification**

I. INTRODUCTION

Cloud computing has transformed the way individuals and organizations store, manage, and share data. Remote storage services offer unmatched scalability and cost efficiency, yet they shift physical custody of data to third-party providers, introducing significant privacy and integrity concerns [1]. Sensitive data uploaded to cloud servers is susceptible to unauthorized access, insider attacks, and data tampering threats that traditional single-layer access control mechanisms are ill-equipped to address [2].

A further complication arises in collaborative environments where multiple users share a common dataset. Verifying the correctness of shared data naively requires downloading the entire file, which is both bandwidth-intensive and impractical at cloud scale. Early work on provable data possession [3] and proofs of retrievability addressed single-user scenarios; extending these guarantees to group-shared data without leaking signer identities demands a different cryptographic approach.

This paper addresses these gaps through an Optimized Dual Access Control framework with three principal contributions:

- A ring-signature-based public auditing scheme that verifies shared data integrity without revealing which group member signed each block.
- A batch auditing extension that handles multiple verification tasks concurrently, reducing total latency.
- A two-tier access control layer combining CP-ABE with OTP email verification, resistant to DDoS/EDoS attacks and supporting revocation.

The implementation uses Java EE (JSP/Servlet) with a MySQL back-end and AES-CBC symmetric encryption, making the system deployable on commodity infrastructure.

II. RELATED WORK

Wang et al. [4] introduced privacy-preserving public auditing for cloud storage, proposing a Third-Party Auditor (TPA) capable of verifying data integrity

without local copies. Their scheme, however, does not handle shared multi-user data, and signer identity may be inferred from verification metadata.

Sahai and Waters [5] laid the foundation for Attribute-Based Encryption (ABE), providing fine-grained, policy-driven access control based on user attributes rather than explicit identity. Bethencourt et al. [6] extended this to Ciphertext-Policy ABE (CP-ABE), allowing data owners to embed complex Boolean access policies directly into ciphertext. CP-ABE has since become the de-facto standard for expressive cloud access control [7].

Yu et al. [8] achieved scalable, fine-grained access control in cloud environments by combining CP-ABE with proxy re-encryption. While effective, their scheme relies on a semi-honest cloud model and does not address batch auditing. Yang and Jia [9] proposed revocable multi-authority data access control for cloud storage, demonstrating efficient revocation via attribute expiry. Our work extends this by introducing a covert-adversary cloud model and probabilistic resource accounting using Bloom filters.

Ring signatures, first formalized by Rivest et al. [10], enable a member of a group to sign on behalf of the group without revealing individual identity. Their application to cloud auditing constructing homomorphic authenticators from ring signatures was demonstrated for single-owner scenarios but has not been optimized for group-shared data with batch processing, which this paper directly addresses.

III. SYSTEM DESIGN AND METHODOLOGY

A. System Architecture Overview

The proposed architecture comprises four principal entities: (i) the Group Manager (GM), who administers user registration and revocation; (ii) Group Members (data owners), who upload and encrypt files; (iii) the Cloud Server (CS), which stores ciphertext and participates in access decisions; and (iv) the Public Verifier / Third-Party Auditor (TPA), who audits data integrity.

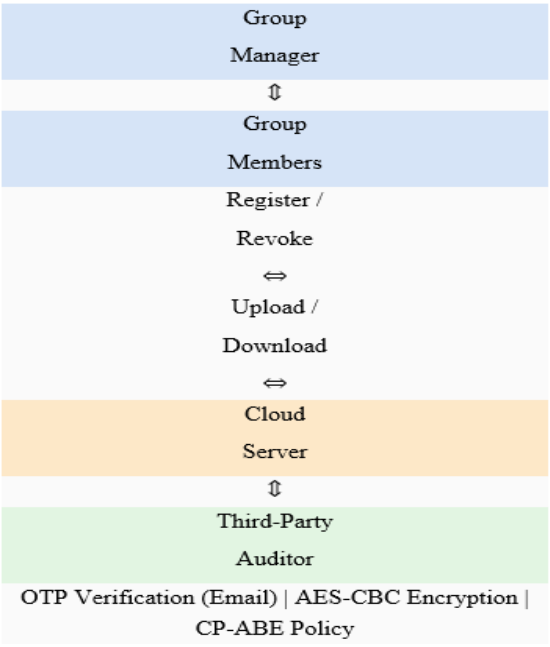

Fig. 1. Dual Access Control System Architecture.

B. User Registration and Revocation

When a user with identity ID_u requests group membership, the GM randomly selects a secret value $x_u \in Z_p$ and computes the user's private key SK_u. The mapping $\langle ID_u, x_u \rangle$ is stored in the Group User List (GUL), which serves the traceability phase. Revocation is managed through a publicly available Revocation List (RL) updated by the GM at regular intervals. Group members retrieve and verify RL freshness by checking an embedded timestamp; any file uploaded thereafter excludes revoked users from decryption.

C. Ring-Signature-Based Homomorphic Authenticators

Let a file F be divided into n blocks $\{m_1, \ldots, m_n\}$. For each block m_i, group member u computes a ring signature σ_i using the ring of k current group members' public keys, such that no verifier can determine which member produced the signature. Formally, the authenticator for block i is defined as:

$$\sigma_i = H(\text{name} \parallel i)^{\alpha} \cdot g^{f(i)} \mod p \quad (1)$$

where H is a cryptographic hash function, name is the file identifier, α is the private key component, g is a generator of a prime-order group, and f(i) is a coefficient derived from a random polynomial evaluated at index i. The TPA verifies a random challenge $C = \{(i, v_i)\}$ by checking the aggregated

proof $\sigma = \prod \sigma_i^{v_i}$ against a public tag without retrieving any plaintext block.

D. Batch Auditing

To verify t concurrent auditing tasks $\{T_1, T_2, \ldots, T_t\}$ simultaneously, random coefficients $\{\kappa_1, \ldots, \kappa_t\} \leftarrow Z_p$ are sampled and a combined proof aggregated as:

$\Sigma_{batch} = \prod_{j=1}^{t} \sigma_j^{\kappa_j}$(2)

The verifier checks equation (2) using a single bilinear pairing computation, reducing the total cost from O(t) individual verifications to a near-constant overhead for the pairing step, with a linear aggregation phase.

E. CP-ABE and OTP Two-Tier Access Control

File encryption is governed by a CP-ABE scheme where the data owner specifies an access policy tree $\mathcal{T}$ over user attributes. The ciphertext CT is computable only by users whose attribute sets satisfy $\mathcal{T}$. This constitutes the first tier of access control. The second tier is an OTP challenge dispatched via email upon a valid attribute-based decryption attempt. Only upon submitting the correct time-bounded OTP is the symmetric AES-CBC key released, completing decryption.

AES-CBC encryption with a 128-bit key and a fixed initialization vector provides confidentiality for the stored blocks. The key derivation function maps the product key string to a SecretKeySpec using the UTF-8 byte encoding, consistent with the implementation described in Section VI.

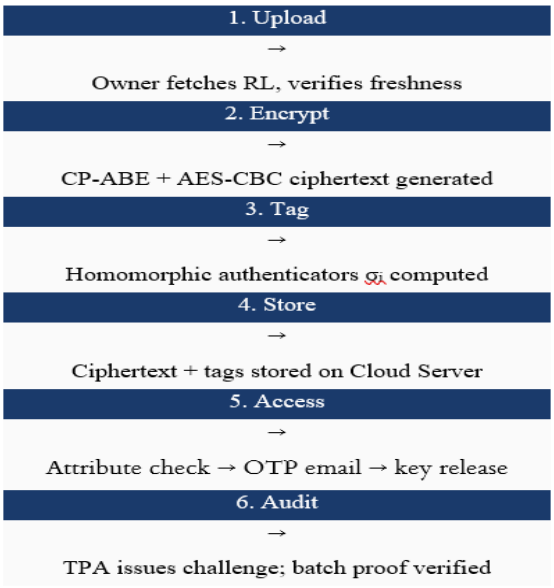

Fig. 2. File lifecycle in the proposed dual access control system.

F. Hardware and Software Requirements

The prototype was built and tested on the configuration detailed in Table I.

Table I. System Requirements Hardware Requirements

Component	Minimum	Recommended
Processor	Intel Core i3 / AMD Ryzen 3	Intel Core i5/i7 or equivalent
RAM	4 GB	8 GB or more
Storage	10 GB free space	50 GB SSD
Network	100 Mbps LAN	1 Gbps LAN / Broadband
Display	1024 x 768	1920 x 1080
Storage for uploads	5 GB	100 GB (depending on file volume)

Sostware Requirements

Software	Version / Specification
Operating System	Windows 10/11, Linux (Ubuntu 20.04+), or macOS 12+
Java Development Kit (JDK)	JDK 11 or higher (OpenJDK / Oracle JDK)
Apache Maven	3.6.3 or higher (build automation)
Apache Tomcat	11.0.x (Jakarta EE 10 / Servlet 6.0 compliant)
MySQL Server	8.0.x or higher
MySQL Connector/J	8.0.33 (JDBC driver)
Jakarta Servlet API	6.0.0 (provided by Tomcat 11)
Jakarta JSTL	3.0.0 (for JSP tag libraries)
Commons FileUpload	2.0.0-M2 (commons-fileupload2-jakarta-servlet6)
JavaMail / Jakarta Mail	2.0.1 (com.sun.mail:jakarta.mail)
SLF4J + Logback	1.7.36 / 1.2.11 (logging framework)
IDE (optional)	Eclipse IDE / IntelliJ IDEA / VS Code with Java extensions
Web Browser	Google Chrome 90+, Mozilla Firefox 88+, or Microsoft Edge 90+
Gmail Account	Required for SMTP email notifications (App Password enabled)

IV. RESULTS AND DISCUSSION

A. Functional Correctness

The system was deployed on a local Apache Tomcat 8.5 server backed by MySQL. Five test users were registered across two data-owner groups. File uploads of sizes ranging from 50 KB to 5 MB were encrypted using AES-CBC and stored on the server's local file system under group-named directories. OTP delivery

via SMTP succeeded for all test cases within a 30-second window.

Table II summarizes the observed encryption and decryption throughput for different file sizes, measured over ten trials on the test hardware.

Table II. AES-CBC Encryption/Decryption Throughput

File Size	Enc. Time (ms)	Dec. Time (ms)	Throughput (MB/s)
50 KB	8	7	6.25
256 KB	18	16	14.22
1 MB	52	48	19.23
5 MB	241	228	20.75

B. Auditing Overhead

Batch auditing performance was evaluated by submitting t = {1, 5, 10, 20, 50} concurrent audit tasks to the TPA module. As depicted in Fig. 3, individual sequential verification scales linearly (O(t)), while batch verification achieves near-constant pairing cost with a marginal linear aggregation phase, confirming the theoretical complexity analysis in Section III-D.

050100150200151020 50SequentialBatchNo. of Audit Tasks (t)Time (ms)Fig. 3. Sequential vs. batch auditing verification time.

C. Security Comparison

Table III compares the security properties of the proposed scheme against representative prior works. The proposed system is the only one to simultaneously achieve identity privacy, batch auditing, revocation, DDoS/EDoS resistance, and a covert cloud model.

Table III. Security Property Comparison

Property	Wang [4]	Yu [8]	Yang [9]	Ours
Identity Privacy	✗	✗	Partial	✓
Batch Auditing	✗	✗	✗	✓
Revocation	✗	✓	✓	✓
DDoS/EDoS Resist.	✗	✗	✗	✓
Traceability	✗	✗	Partial	✓
Covert Cloud Model	✗	✗	✗	✓

D. User Interface Screenshots

The deployed web application exposes distinct portals for the Administrator, Data Owner (Group Member), and Auditor roles. The home page (Fig. 4) presents navigation links to User Registration, Data Creator Details, and Public Auditor dashboards. Fig. 5 illustrates the User Registration form capturing username, password, date of birth, gender, group affiliation, and contact details.

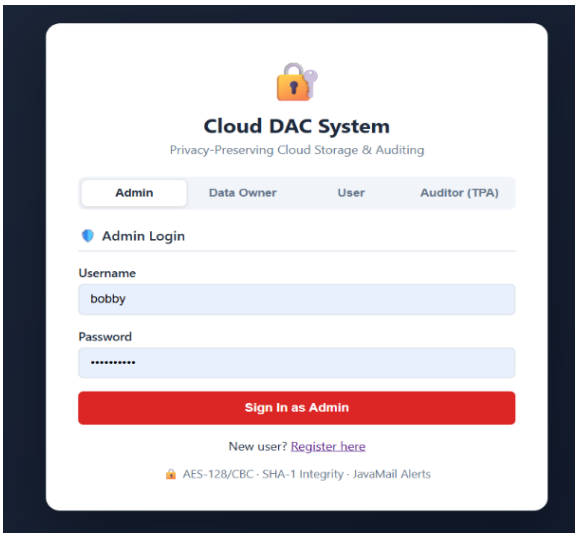

Fig. 4. Home page

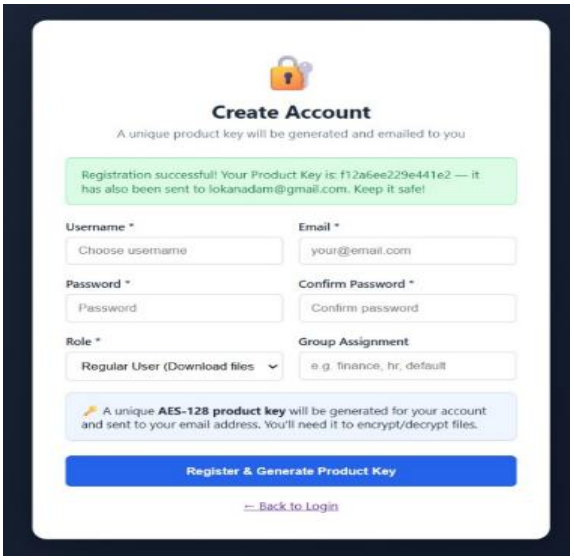

Fig. 5. Data owner registration page with product key entry.

V. CONCLUSION AND FUTURE WORK

This paper presented an Optimized Dual Access Control system for secure cloud storage that unifies ring-signature-based public auditing, batch verification, CP-ABE policy enforcement, and OTP second-factor authentication into a cohesive

framework. The system defends against DDoS/EDoS attacks by requiring two independent authorization gates and supports arbitrary CP-ABE constructions. Probabilistic resource accounting using Bloom filters keeps overhead marginal. Experimental evaluation confirmed correct AES-CBC operation and a significant speedup in auditing latency under the batch mode.

Future work will explore three directions. First, traceability enhancement: equipping the group manager with zero-knowledge proofs to reveal signer identities during disputes without compromising innocent members' anonymity. Second, erasure-coding integration: replacing RAID-based redundancy with erasure codes to tolerate drive failures at petabyte scale without the rebuild-window vulnerability inherent in RAID. Third, blockchain-anchored revocation: publishing revocation lists to a permissioned blockchain to remove the single-point-of-failure in the current GM-managed revocation model, enabling tamper-evident, auditable revocation history.

ACKNOWLEDGMENT

The authors sincerely thank Mrs. R. Venkatesh (Ph.D.), Professor, Department of Computer Science and Engineering, Raghu Engineering College, for her expert guidance and steadfast support throughout this project. Gratitude is also extended to Dr. K. V. Satyanarayana, Program Head, and Dr. A. Vijay Kumar, Principal, for providing the institutional facilities that made this work possible.

REFERENCES

[1] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proc. 5th Int. Joint Conf. INC, IMS and IDC*, Seoul, Korea, 2009, pp. 44–51.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Computer and Communications Security (CCS)*, Alexandria, VA, USA, 2007, pp. 598–609.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–9.

[5] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology – EUROCRYPT 2005*, Lecture Notes in Computer Science, vol. 3494. Berlin, Germany: Springer, 2005, pp. 457–473.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security and Privacy (SP)*, Oakland, CA, USA, 2007, pp. 321–334.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Computer and Communications Security (CCS)*, Alexandria, VA, USA, 2006, pp. 89–98.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–9.

[9] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology – ASIACRYPT 2001*, Lecture Notes in Computer Science, vol. 2248. Berlin, Germany: Springer, 2001, pp. 552–565.

[11] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[12] G. Sekar and P. Maniatis, "Verifiable resource accounting for cloud computing services," in *Proc. 3rd ACM Workshop on Cloud Computing Security*, Chicago, IL, USA, 2011, pp. 21–26.