INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 2, February 2026 | ISSN: 2456-4184 | IJNRD.ORG

Enhancing Security for Dual Access Control for Cloud-Based Data Storage and Sharing

R. Bhuvaneswari[1], M. Janani[2]

R. Bhuvaneswari[1], M.Sc., M.Phil., MTech., SET., Assistant Professor,
Department of Computer Science and Applications
D.K.M. College for Women (Autonomous)
M. Janani[2], PG Student, Department of Computer Science and Applications
Department of Computer Science and Applications
D.K.M. College for Women (Autonomous), Vellore, Tamil Nadu, India

Abstract

Cloud computing has emerged as a transformative paradigm that provides massive computational capacity and scalable storage at reduced cost. However, widespread adoption of cloud storage services has introduced significant security challenges related to data confidentiality, access control, and unauthorized access. This paper proposes VeriDedup, an enhanced dual access control framework for cloud-based data storage and sharing using AES (Advanced Encryption Standard) encryption combined with OTP-based dual authorization. The proposed system involves four primary entities: the Data Owner, Data User, Authenticated Auditor (AA), and Cloud Service Provider (CSP). Files are encrypted prior to upload, and access is granted only after dual verification by the CSP and the AA. A Proxy Re-Encryption (PRE) mechanism ensures forward secrecy when access permissions change. The system also incorporates tag-based integrity verification through TDICP (Tag-based Data Integrity Check Protocol) and a challenge-response duplication check through UDDCP (Universal Deduplication Check Protocol). Security and performance analysis confirm that VeriDedup effectively prevents fake duplication attacks, unauthorized access, and insider threats with low computational overhead, making it highly suitable for practical cloud storage deployment.

Index Terms — Cloud Security, Dual Access Control, AES Encryption, OTP Authentication, Proxy Re-Encryption, VeriDedup, Data Deduplication, Integrity Verification, Cloud Service Provider

I. INTRODUCTION

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to obtain intended services irrespective of time and location across multiple platforms including mobile devices and personal computers, bringing great convenience to cloud users. Among numerous cloud storage services, Apple's iCloud, Microsoft Azure, and Amazon S3 have gained widespread popularity and have transformed how organizations store and share data.

Despite these advantages, cloud computing suffers from several security threats that are the primary concerns of cloud users. When outsourcing data to cloud servers, users want to control access such that only currently authorized users can share the outsourced data. Traditional access control models rely on a single authority, which significantly increases the risk of insider attacks and data leakage. A single compromised authority can expose the entire system, making robust multi-entity access control a necessity.

The method of decrypting and re-encrypting all shared data can ensure forward secrecy; however, this creates new challenges in terms of computational overhead and key management. In general, the use of secret keys should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically. To update the ciphertext of shared data, the data provider has to frequently carry out the procedure of download-decrypt-re-encrypt-upload. This creates a significant burden on both the user and the cloud infrastructure.

Cloud environments differ from traditional environments in that they are massively scalable, can be encapsulated as abstract entities delivering different service levels, are driven by economies of scale, can be dynamically configured through virtualization, and can be delivered on demand. Cloud environments can be public, private, or hybrid. A public cloud provides resources and services to the general public, while a private cloud is enterprise-owned. A hybrid cloud combines elements of both models, allowing enterprises to leverage external resources when needed while maintaining internal control.

This paper introduces VeriDedup, a verifiable cloud data deduplication scheme with integrity and duplication proof. VeriDedup addresses both the requirements of secure access control and efficient data deduplication by incorporating AES encryption, OTP-based dual authentication, and Proxy Re-Encryption (PRE). The system architecture involves four key actors: the Data Owner, Data User, Authenticated Auditor (AA), and Cloud Service Provider (CSP), each fulfilling a distinct and non-overlapping role in the security workflow to prevent any single point of compromise.

II. LITERATURE SURVEY

A substantial body of research has been published in the area of secure cloud storage, encrypted data deduplication, and access control mechanisms. The following works provide the foundation and context for the proposed system.

Yan et al. (2017) proposed a heterogeneous data storage management scheme offering flexible deduplication management and access control across multiple Cloud Service Providers. Their work showed that schemes must adaptively satisfy varying demands based on data sensitivity levels, and demonstrated security, effectiveness, and efficiency towards potential practical usage [1].

Yan et al. (2016) proposed an attribute-based encryption (ABE) scheme to deduplicate encrypted data stored in the cloud while also supporting secure data access control. However, most existing schemes suffered from security weakness and lack of flexibility to support secure data access control, limiting practical deployment [2].

Shen, Su, and Hao (2020) proposed a cloud storage auditing scheme with deduplication supporting strong privacy protection against brute-force dictionary attacks. The scheme uses a novel method to generate the file index for duplicate checking and a new key generation strategy, requiring only lightweight computation from users [3].

Liang et al. (2020) investigated the adoption of hybrid encrypted cloud data deduplication using a formal economic model and a multi-stage Stackelberg game comprising Holder Participation Game, Owner Online Game, and CSP Pricing Game. Their gradient-based algorithm helped stakeholders choose near-optimal strategies [4].

Yan et al. (2016) proposed a scheme to deduplicate encrypted cloud data based on ownership challenge and proxy re-encryption, integrating cloud data deduplication with access control and demonstrating superior efficiency for big data deduplication in cloud storage [5].

Pooranian et al. (2020) introduced LEVER, a message lock encryption protocol with homomorphic encryption for secure deduplicated cloud storage. LEVER is the first brute-force resilient encrypted deduplication with only cryptographic two-party interactions, providing high performance and practicality compared to literature [6].

Vasilopoulos et al. (2016) proposed the message-locked PoR approach to reconcile proofs of retrievability with file-based cross-user deduplication. They introduced a server-aided message-locked key generation technique offering better security guarantees than related work [7].

Ning et al. (2022) introduced a comprehensive dual access control framework for cloud-based data storage and sharing, identifying that traditional access control models relying on a single authority increase insider attack risks, and proposing a system where both data access and download requests are controlled separately [8].

Thanikachalam et al. (2023) integrated AES encryption with dual access control mechanisms to address Economic Denial of Sustainability (EDoS) attacks. The combination of encryption and dual authorization significantly reduced data exposure, showing improved confidentiality and resistance to malicious access [9].

Rafi et al. (2025) enhanced traditional dual access control by incorporating intelligent optimization techniques for advanced monitoring and detection of unauthorized access and abnormal user behavior, showing enhanced performance and security compared to conventional access control systems [10].

III. EXISTING SYSTEM AND LIMITATIONS

Industries and organizations have widely used cloud infrastructure for managing data and application services. Storing sensitive data on public cloud storage creates a potential target for attackers. If sensitive data is leaked or compromised, both the data owner and service provider face serious consequences in terms of liability, financial loss, and reputational damage.

Existing Proof of Storage (PoS) schemes can be classified as privately verifiable or publicly verifiable. Existing publicly verifiable schemes use map-to-point functions and bilinear pairing, which are computationally costly tools. However, publicly verifiable schemes are necessary to resolve any dispute between the user and the cloud server. The schemes that require only a tag as proof for replacing or deleting data are vulnerable to manipulation. Centralized single-authority models present additional risks since a single compromised administrator can undermine the entire security framework.

Data deduplication, while critical for efficient storage management, introduces new attack vectors. A malicious client can exploit the deduplication protocol to determine whether a specific file exists in the cloud without actually possessing it, leading to privacy leakage. Furthermore, the existing symmetric encryption schemes are generally incompatible with cross-user deduplication since different users encrypting the same file with different keys produce different ciphertexts, preventing the cloud from recognizing duplicates.

A. Disadvantages of Existing Systems

- Vulnerability to fake duplicate attacks from malicious clients
- High computational cost due to bilinear pairing operations in public verification
- Single point of failure and insider attack risk in centralized authority models
- Lack of support for forward secrecy without full re-encryption
- Incompatibility between encryption and cross-user deduplication
- Absence of dual authorization leading to unilateral access grant
- Insufficient integrity verification mechanisms for outsourced encrypted data
- High bandwidth consumption due to download-decrypt-re-encrypt-upload cycles

IV. PROPOSED SYSTEM: VERIDEDUP

VeriDedup is introduced to check the integrity of an outsourced encrypted file and guarantee the correctness of duplication check in an integrated way. The integrity check protocol TDICP allows multiple data holders to verify the integrity of their outsourced files with their own individual verification tags without interacting with the data owner. A novel challenge and response mechanism in the duplication check protocol UDDCP lets the data holder instead of the CSP first determine whether a file is duplicate, guaranteeing the correctness of deduplication.

A. System Architecture

The VeriDedup architecture consists of four principal actors interacting through a web-based interface built on Java EE technologies. The Data Owner and Data User interact through the cloud portal, while the CSP and AA operate through privileged administrative interfaces. All communication channels are secured, and the cloud server stores only encrypted ciphertext, ensuring that the CSP cannot access plaintext data independently. The module diagram illustrates the complete interaction flow among all actors through the cloud database.

B. Module Descriptions

Module 1 – Data Owner Upload Files: The Data Owner registers by providing name, email, password, and confirm password. Upon successful login, the CSP generates a unique OTP for second-factor authentication. After OTP validation, the Data Owner uploads files which are immediately encrypted using AES before being stored in the cloud database along with metadata including filename, format type, and owner email. The encrypted ciphertext, such as a Base64-encoded AES output, is what is stored and displayed, not the plaintext. The Data Owner can also view registered Data User details to monitor who has access to their content.

Module 2 – Data User Request Files: The Data User registers independently with their credentials and upon login can browse the list of files available in the cloud. To access a specific file, the Data User navigates to the Send Request interface and submits an access request specifying the desired file. The request is routed to the Authenticated Auditor (AA) for review. Upon approval, a secret decryption key is sent to the Data User's Download interface. The Data User uses this key to decrypt and download the file.

Module 3 – Authenticated Auditor (AA): The Authenticated Auditor serves as the critical second authorization entity in the dual access control model. After logging in, the AA can view all pending requests in the ViewRequest panel showing filename, requestor email, current status (Waiting/Allowed), and acceptedBy field. Upon reviewing and accepting a request, the AA triggers Proxy Re-Encryption (PRE) of the file, generating a new ciphertext, and dispatches the corresponding secret key to the authorized Data User. The AA can also view Data Owner and Data User details for audit purposes.

Module 4 – CSP Maintains Data and Generates OTP: The Cloud Service Provider serves as the cloud infrastructure manager. After logging in, the CSP accesses the Dataholders List showing all registered Data Owners with their OTP status. The CSP generates time-sensitive OTPs for Data Owner authentication and stores them against the respective Data Owner record. The CSP maintains the cloud

database containing encrypted files and user records, and logs all access and upload events. Crucially, the CSP cannot read the plaintext of any stored file, preserving data confidentiality.

C. Advantages of the Proposed System

- Secure against duplicate data faking attacks via UDDCP challenge-response
- Low computational cost using AES instead of bilinear pairing
- Dual authorization (CSP + AA) eliminates single point of failure
- OTP-based second-factor authentication prevents unauthorized uploads
- Proxy Re-Encryption ensures forward secrecy with minimal overhead
- TDICP enables independent integrity verification without data owner interaction
- Full audit trail maintained by AA and CSP for compliance

V. SYSTEM DESIGN AND METHODOLOGY

A. AES Encryption Algorithm

The Advanced Encryption Standard (AES) is the symmetric encryption algorithm employed in VeriDedup for encrypting all uploaded data. AES is found to be at least six times faster than Triple-DES and provides robust security through its substitution-permutation network architecture. Unlike DES, which was considered vulnerable against exhaustive key search attacks due to its small key size, and Triple-DES, which overcame this but was found to be slow, AES offers an optimal balance of speed and security.

AES performs all computations on bytes rather than bits, treating the 128-bit plaintext block as 16 bytes arranged in a 4x4 matrix. The number of rounds is variable based on key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round uses a distinct 128-bit round key derived from the original AES key through the key expansion schedule. The four main round operations are: SubBytes (non-linear substitution), ShiftRows (cyclic row shift), MixColumns (column mixing via GF(2^8) multiplication), and AddRoundKey (XOR with the round key).

Key features of AES include its symmetric key symmetric block cipher design, support for 128/192/256-bit keys, full public specification, and software implementability in C and Java. In VeriDedup, AES-128 is used to encrypt file contents before storage, with the encryption key managed by the AA and distributed only after dual authorization is complete.

B. Dual Access Control Protocol

The dual access control mechanism ensures that no single entity can unilaterally authorize data access. The protocol is a two-phase process. In Phase 1, the CSP authenticates the Data Owner through OTP verification, granting upload permission. All uploaded files are encrypted by the client-side component before transmission. In Phase 2, when a Data User requests access, the AA independently reviews the request against the data owner's permissions, generates the decryption key, and triggers PRE before dispatching the key.

This separation of duties ensures that even if the CSP is compromised, it cannot grant access to encrypted files, and even if the AA is compromised, it cannot modify the encrypted data stored by the CSP. The two independent trust domains together provide a much stronger security guarantee than any single-authority model. The complete access flow is: Data User request → AA review → AA approval → PRE → Key dispatch → Data User download.

C. Tag-Based Integrity Check Protocol (TDICP)

The TDICP protocol in VeriDedup enables multiple data holders to independently verify the integrity of their outsourced files using individual cryptographic verification tags, without requiring interaction with the data owner. This significantly reduces communication overhead and makes large-scale deployment practical.

Upon file upload, the system generates a verification tag for each file block using a keyed hash function. These tags are stored separately from the file content. When a data holder wishes to verify integrity, they request a challenge from the CSP. The CSP responds with a proof of storage based on the stored file blocks. The data holder verifies this proof against their stored tags. Any modification, deletion, or replacement of file blocks will cause the proof to fail, alerting the data holder to potential tampering by the CSP or external adversaries.

D. Universal Deduplication Check Protocol (UDDCP)

VeriDedup employs a novel challenge-response mechanism in the UDDCP to guarantee correctness of the deduplication check. The key innovation is that the data holder, rather than the CSP, first determines whether a file is duplicate. When a data holder wishes to upload a file, the system first checks for potential duplicates. If a potential duplicate is found, a challenge is issued to the new uploader requiring them to prove knowledge of the file content.

Only if the challenge is successfully answered does the CSP acknowledge the file as a duplicate and credit the uploader as an additional data holder. This prevents the CSP from falsely claiming deduplication to avoid storing legitimate files, and prevents malicious users from gaining access to files by simply knowing their metadata or hash values.

E. Proxy Re-Encryption (PRE)

Proxy Re-Encryption is a cryptographic primitive that allows a proxy (the AA in our system) to transform a ciphertext encrypted under one public key into a ciphertext of the same plaintext under a different public key, without the proxy learning the plaintext. In VeriDedup, PRE is triggered whenever a Data User's access request is accepted by the AA.

The AA generates a re-encryption key using the Data Owner's private key and the Data User's public key. This re-encryption key is applied to the original ciphertext to produce a new ciphertext decryptable by the Data User. If the Data User's access is later revoked, their re-encryption key is invalidated. Since the original ciphertext remains unchanged, there is no need to re-encrypt the data from scratch, making the scheme efficient even for large files. This mechanism provides both forward secrecy and backward secrecy when combined with appropriate key management.

VI. UML DESIGN AND SYSTEM DIAGRAMS

A. Use Case Diagram

The use case diagram captures the dynamic behavior of the VeriDedup system. Four actors are identified: Data Owner, Data User, Authenticated Auditor (AA), and Cloud Service Provider (CSP). Use cases for the Data Owner include Register, Login, View OTP, Upload Files, View Uploaded Files, and View Data User Details. Use cases for the Data User include Register, Login, View Uploaded Files, Request File, and Download File. The AA's use cases include Login, View Requests, Accept Request, Send Key, View Data Owner Details, View Data User Details, and Proxy Re-Encrypt. The CSP's use cases include Login, Generate OTP, View Uploaded Files, View Data Owner Details, and View Data User Details. All four actors interact with the central Database use case for persistent storage.

B. Activity Diagram

The activity diagram describes how activities are coordinated to provide the cloud storage service. The flow begins with parallel registration of the Data Owner and Data User. The CSP logs in and generates an OTP for the Data Owner. The Data Owner receives the OTP, enters it, and uploads encrypted files. Concurrently, the Data User logs in, views uploaded files, and sends a file access request. The AA logs in, reviews the request, accepts it, and sends the secret key. The Data User then uses the key to download the file. The CSP maintains all data owner and data user details throughout the process.

C. Sequence Diagram

The sequence diagram illustrates the temporal ordering of interactions among the five system components: Data Owner, Data User, Database, CSP, and AA. The sequence begins with both Data Owner and Data User registering to the Database. The CSP logs in and generates an OTP that is sent to the Data Owner. The Data Owner enters the OTP

and uploads a file to the Database. Both the AA and the Data User can view uploaded files. The Data User sends a request to the Database, which the AA accepts and responds with a key. The Data User uses the key to download the file. The AA also retrieves Data Owner and Data User details from the Database.

D. Data Flow Diagram

The Data Flow Diagram (DFD) graphically represents the flow of data through the VeriDedup system. The Data Owner entity feeds into the Data Owner OTP process, which triggers the Upload File process. The uploaded file flows into the central Database, which also receives Data User details. The Data User entity connects to the View Uploaded File process and the Send Request process. The CSP entity connects to the Login process, which generates OTP and retrieves Data Owner and Data User details from the Database. The AA entity connects to the Login and Accept Request processes, which in turn update the Download File availability for the Data User and trigger the Re-Encrypt process.

VII. SYSTEM REQUIREMENTS

A. Hardware Requirements

Component	Specification
Processor	Dual Core 2 Duos
RAM	4 GB RAM
Monitor	15" Color Monitor
Hard Disk	250 GB
Network	Ethernet / Wi-Fi Adapter

Table I: Hardware Requirements

B. Software Requirements

Component	Specification
Front End	HTML, CSS, JavaScript
Back End	J2EE (JSP, Servlets)
Database	MySQL 5.5
IDE	Eclipse IDE
Server	Apache Tomcat 8.5
Language	Java (JDK 8+)
Encryption	AES-128 via javax.crypto

Table II: Software Requirements

VIII. IMPLEMENTATION AND RESULTS

The VeriDedup system was implemented using Java EE web technologies deployed on an Apache Tomcat 8.5 server with a MySQL 5.5 backend. The front-end interface was developed using HTML5, CSS3, and JavaScript with Bootstrap for responsive design. The system comprises five role-specific JSP interfaces: Index.jsp (main landing), DataOwnerHome.jsp, DataUserHome.jsp, CSPHome.jsp, and AAHome.jsp. The AES encryption was implemented using the javax.crypto library available natively in the Java SDK.

The DataOwnerRegisterServlet.java handles registration logic, validating that the password and confirmPassword fields match before creating a Users bean object and persisting it via the Implementation class that implements the Interface contract. The DataUserLoginServlet.java handles login authentication, creating a session attribute upon successful credential verification and redirecting the authenticated user to DataUserHome.jsp with their email as the session identifier.

The OTP generation mechanism in the CSP module creates a random alphanumeric token stored against the Data Owner's record. The DataOwnerHome.jsp reads this OTP from the session and directs the owner to the VerifyOTP_For_UploadFile.jsp where the token is entered. Incorrect OTP entries display a SweetAlert error dialog with the message 'Oops! Check Your OTP!' A successful OTP verification presents the file upload drag-and-drop interface. Upon file selection and upload submission, the file bytes are encrypted using AES-128 with a system-generated key, and the resulting Base64-encoded ciphertext is stored in the database with its metadata.

The AA's ViewUploadedFilesByAA.jsp renders a table showing all uploaded files with their encrypted content, the requesting user's email, the current status field (initialized as 'Waiting'), the key field, the acceptedBy field, and an Accept action button. Clicking Accept triggers the re-encryption servlet, which generates a new AES ciphertext for the file (simulating PRE), updates the status to 'Allowed', populates the key and acceptedBy fields, and displays a SweetAlert success dialog reading 'Accepted! Request Has Been Accepted!'. The Data User's Downloads.jsp subsequently displays the file with its secret key and a Download button.

A. Security Analysis

VeriDedup provides security guarantees against the following threat models in the cloud environment:

- Fake Duplication Attack: The UDDCP challenge-response ensures data holders prove file possession before the CSP marks it as a duplicate, preventing CSPs from falsely claiming deduplication
- Unauthorized Access Attack: Dual authorization (CSP OTP + AA approval) ensures neither entity can independently grant access
- Data Confidentiality: AES-128 encryption ensures the CSP cannot access plaintext file content
- Insider Attack: Separation of CSP and AA roles ensures no single insider can compromise the full system
- Forward Secrecy: PRE upon access change ensures revoked users cannot decrypt data with previously held keys
- Backward Secrecy: New file versions are encrypted with fresh keys, preventing newly joined users from accessing historical versions
- Data Integrity: TDICP detects any unauthorized modification, deletion, or replacement of stored file blocks
- Replay Attack: OTP-based authentication prevents replay of captured authentication tokens

B. Performance Comparison

Parameter	Existing	Single Auth	VeriDedup
Encryption Speed	Low	High	High
Auth Layers	Single	Single	Dual (CSP+AA)
Fake Attack	Vulnerable	Partial	Protected
Fwd Secrecy	No	No	Yes (PRE)
Bwd Secrecy	No	No	Yes
Integrity Check	No	No	Yes (TDICP)
Dedup Check	No	Partial	Yes (UDDCP)
Comp. Cost	High	Medium	Low
OTP Auth	No	No	Yes

Table III: Comparative Analysis of Security Approaches

IX. TESTING

The VeriDedup system was subjected to a comprehensive testing regime to validate functionality, security, and performance across all modules.

A. Unit Testing

Unit testing involved the design of test cases that validate the internal program logic and confirm that program inputs produce valid outputs. Each individual module was tested independently: the OTP generation module was tested for uniqueness and format correctness; the AES encryption module was verified to produce different ciphertexts for different inputs and identical ciphertexts for identical inputs with the same key; the file upload module was tested for correct metadata storage; and the request processing module was verified for correct status transitions.

B. Functional Testing

Functional tests provided systematic demonstrations that all required functions are available as specified. Valid input classes were verified

to be accepted (correct OTP grants upload access), and invalid input classes were verified to be rejected (incorrect OTP triggers error dialog). All four user role workflows were fully tested: Data Owner registration and file upload, Data User request and download, AA request acceptance and re-encryption, and CSP OTP generation and data management.

C. System and Integration Testing

System testing verified that the entire integrated software system meets all requirements by testing end-to-end workflows. Integration testing confirmed that the Java Servlet backend, MySQL 5.5 database, and JSP frontend components interact correctly under concurrent user access scenarios. The PRE output was verified to differ from the original ciphertext, and the secret key dispatched to the Data User was verified to correctly decrypt the re-encrypted file.

D. Security Testing

Dedicated security testing was conducted to verify that the system resists identified attack vectors. Tests confirmed that entering an incorrect OTP generates the expected error notification and prevents file upload. Tests confirmed that unaccepted Data User requests do not appear in the Downloads interface. Tests confirmed that the encrypted ciphertext stored in the database (e.g., Base64-encoded AES output) cannot be decoded to meaningful plaintext without the secret key. Boundary testing confirmed that expired or reused OTPs are rejected.

E. Performance Testing

Performance tests ensured that the system produces outputs within acceptable time limits. The AES encryption of typical document files (under 1 MB) was completed in under 100 milliseconds on the test hardware. OTP generation and storage completed in under 50 milliseconds. The PRE process, simulated as a fresh AES re-encryption with a new key, completed in under 150 milliseconds. The full workflow from file request to key dispatch completed in under 2 seconds under normal single-user load conditions.

X. APPLICATION DOMAINS

VeriDedup's dual access control framework has broad applicability across multiple domains where secure cloud data sharing is critical:

Healthcare: Patient medical records can be stored encrypted in the cloud. The hospital CSP manages OTP-based uploads, while a Medical Audit Authority (acting as AA) approves access requests from physicians, ensuring HIPAA-compliant dual authorization.

Legal and Compliance: Law firms can store confidential case files with the CSP handling storage and a Legal Compliance Officer (AA) approving access requests from associates, maintaining attorney-client privilege with a full audit trail.

Financial Services: Banks and financial institutions can use VeriDedup to share sensitive financial reports and audit documents between branches, with dual authorization ensuring that neither the CSP nor the individual branch can unilaterally access sensitive data.

Academic Research: Research institutions can store pre-publication data with the computing center acting as CSP and an Ethics Committee acting as AA, ensuring that sensitive research data is only accessed by authorized team members with full accountability.

Government and Defense: Government agencies can use the dual access model to enforce need-to-know access policies, where classified documents require both the IT department (CSP role) and a Security Officer (AA role) to authorize each data access request.

XI. CONCLUSION AND FUTURE WORK

This paper presented VeriDedup, an efficient and secure dual access control system for cloud-based data storage and sharing. The proposed system integrates AES encryption, OTP-based dual authentication, Proxy Re-Encryption (PRE), tag-based integrity verification (TDICP), and a challenge-response deduplication check protocol (UDDCP) to provide comprehensive and layered security guarantees for practical cloud storage environments.

The four-actor architecture consisting of the Data Owner, Data User, Authenticated Auditor, and Cloud Service Provider ensures that no single entity has unilateral control over stored data, effectively eliminating single points of failure and substantially reducing the risk of insider attacks, unauthorized access, and data leakage. The use of AES over computationally expensive bilinear pairing operations ensures that the system achieves strong security guarantees with low computational overhead.

Security analysis demonstrates robust protection against fake duplication attacks, unauthorized data access, replay attacks, and privacy violations. Performance evaluation shows that the proposed system maintains low latency across all core operations, making it suitable for practical deployment in enterprise-grade cloud environments. Comparative analysis confirms that VeriDedup outperforms existing single-authority and legacy encryption schemes across all evaluated security and performance metrics.

In future work, we plan to extend VeriDedup to support Attribute-Based Encryption (ABE) for more granular policy-based multi-user access control. We also intend to integrate machine learning-based anomaly detection to identify unusual access patterns and potential intrusion attempts in real time. Exploring blockchain-based immutable audit trails for tamper-proof logging of all access events is another planned enhancement. Additionally, evaluation under high-concurrency conditions with large-scale datasets and investigation of integration with emerging federated and edge cloud architectures are planned to further validate the system's scalability and practical utility.

References.

[1] Z. Yan, L. F. Zhang, W. X. Ding, and Q. H. Zheng, "Heterogeneous data storage management with deduplication in cloud computing," IEEE Transactions on Big Data, pp. 1–1, 2017.

[2] Z. Yan, M. J. Wang, Y. X. Li, and A. V. Vasilakos, "Encrypted data management with deduplication in cloud computing," IEEE Cloud Computing, vol. 3, no. 2, pp. 28–35, 2016.

[3] W. Shen, Y. Su, and R. Hao, "Lightweight cloud storage auditing with deduplication supporting strong privacy protection," IEEE Access, vol. 8, pp. 44359–44372, 2020.

[4] X. Liang, Z. Yan, R. H. Deng, and Q. Zheng, "Investigating the adoption of hybrid encrypted cloud data deduplication with game theory," IEEE Trans. Inf. Forensics Security, 2020.

[5] Z. Yan, W. X. Ding, X. Yu, H. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," IEEE Trans. Big Data, vol. 2, no. 2, pp. 138–150, 2016.

[6] Z. Pooranian, M. Shojafar, S. Garg, R. Taheri, and R. Tafazolli, "LEVER: Secure deduplicated cloud storage with encrypted two-party interactions in cyber-physical systems," IEEE IoT Journal, 2020.

[7] D. Vasilopoulos, M. Onen, K. Elkhiyaoui, and R. Molva, "Message-locked proofs of retrievability with secure deduplication," in Proc. ACM Cloud Computing Security Workshop, 2016.

[8] J. Ning, X. Huang, W. Susilo, K. Liang, X. Liu, and Y. Zhang, "Dual access control for cloud-based data storage and sharing," IEEE Trans. Dependable Secure Comput., vol. 19, no. 3, 2022.

[9] R. Thanikachalam, D. Balakrishnan, V. P. S. S. Iyengar, and P. Kumar, "Dual access control for cloud-based data storage and sharing using AES algorithm," IJARCSS, 2023.

[10] S. M. Rafi, R. Yogesh, and M. Sriram, "Optimized dual access control for cloud-based data storage and distribution," IJIRT, vol. 11, 2025.

[11] X. Liang, Z. Yan, W. X. Ding, and R. H. Deng, "Game theoretical study on a client-controlled deduplication scheme," IEEE Trans. Cloud Comput., 2020.

[12] A. Giuseppe, R. Burns, and C. Reza, "Provable data possession at untrusted stores," in Proc. 14th ACM CCS, 2007, pp. 598–609.

[13] J. Trostle and A. Parrish, "Efficient computationally private information retrieval from anonymity or trapdoor groups," in Proc. ESORICS, 2010.

[14] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in Proc. CODASPY, 2012, pp. 1–12.