International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

A SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUD

KAYALA SHILPA[1], G. RAMESH KUMAR [2]

1.Student, Dept. of computer applications, B. V. Raju College, Bhimavaram. Garagaparru Road, Kovvada, Andhra Pradesh

2.Assistant professor, Dept. of computer applications, B. V. Raju College, Bhimavaram. Garagaparru Road, Kovvada, Andhra Pradesh.

ABSTRACT

With the rapid advancement of cloud computing technologies, a large volume of scholarly big data such as research papers, experimental datasets, academic records, and researcher information is increasingly stored in cloud environments. Although cloud storage offers scalability and flexibility, it also introduces serious concerns regarding data security, privacy, and integrity. Unauthorized access, data leakage, and the absence of reliable verification mechanisms pose significant challenges for protecting sensitive scholarly information. Existing cloud storage solutions mainly emphasize storage efficiency but often lack secure data sharing and integrity verification capabilities. Furthermore, performing efficient searches over encrypted data remains a difficult task using traditional encryption methods. To address these challenges, this paper proposes a secure and verifiable access control scheme for scholarly big data stored in cloud environments. The system adopts a user-differentiated model consisting of authors, editors, and readers, each with specific access privileges. A trusted third party is employed for user authentication and secure communication. Additionally, a cube-based data storage structure is implemented to organize data efficiently and support secure keyword-based search. An integrity verification mechanism is also incorporated to ensure that stored data remains unaltered. Experimental results demonstrate that the proposed system improves data security, access efficiency, and reliability for scholarly big data management in cloud environments.

Keywords

Cloud Computing, Big Data Security, Access Control, Data Integrity Verification, Encrypted Data Search, Trusted Third Party, Cloud Storage Security, Cube Data Storage Structure.

I. INTRODUCTION

The rapid growth of cloud computing and big data technologies has significantly transformed the way data is stored, processed, and shared. Academic institutions, research organizations, and publishers increasingly rely on cloud storage to manage large volumes of scholarly data such as research papers, datasets, academic records, and personal researcher information. Cloud computing offers scalable infrastructure, flexible storage, and cost-effective solutions for handling massive data collections. Despite these advantages, storing sensitive scholarly data in cloud environments introduces serious security challenges. Issues such as unauthorized access, data leakage, and lack of data integrity verification can compromise the confidentiality and reliability of stored information. Traditional access control mechanisms are often insufficient to handle complex user roles and permissions in academic environments. Another challenge is searching encrypted data efficiently. When data is encrypted to protect confidentiality,

conventional keyword search techniques cannot be applied directly. This limitation affects the usability and accessibility of cloud-based scholarly repositories. To address these challenges, this paper proposes a **secure and verifiable access control scheme** for big data storage in cloud environments. The system incorporates role-based access control for authors, editors, and readers, a trusted third party for authentication, and a cube-based storage structure to organize data efficiently. In addition, secure keyword search and integrity verification mechanisms ensure both privacy and reliability of stored scholarly data.

II. LITERATURE REVIEW

Several researchers have explored different techniques to improve security and efficiency in cloud-based big data storage systems.

Smith et al. (2019) proposed an encrypted cloud storage system that protects data confidentiality through advanced cryptographic algorithms. However, their approach lacks efficient search capabilities over encrypted data.

Chen and Liu (2020) introduced a role-based access control model for cloud environments. While the system effectively restricts unauthorized access, it does not provide mechanisms for verifying data integrity.

Wang et al. (2018) developed a privacy-preserving keyword search method that allows users to retrieve encrypted files from cloud servers. Although the method improves search efficiency, it does not address large-scale big data organization.

Zhang et al. (2021) presented a blockchain-based verification mechanism for ensuring data integrity in cloud storage. The system improves trust and transparency but increases computational overhead.

Patel and Sharma (2022) proposed a secure big data management framework with hierarchical access control policies. However, the approach does not support efficient data retrieval structures.

From the existing literature, it is evident that most systems focus on either security, access control, or search efficiency. Very few solutions integrate all these features together. Therefore, this research proposes a comprehensive scheme that combines secure access control, encrypted search capability, structured storage, and data integrity verification.

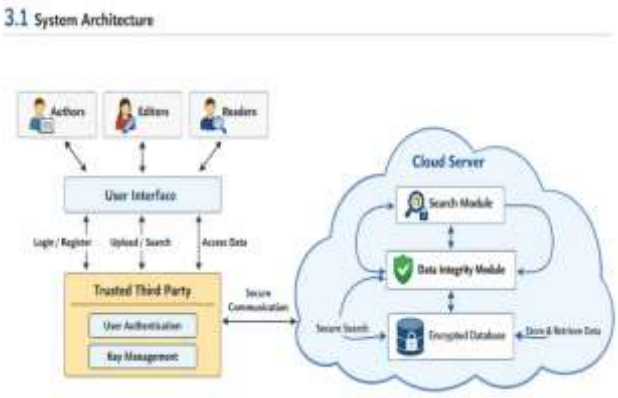
III. Proposed Methodology

The proposed system introduces a secure cloud-based architecture designed to protect scholarly big data while enabling efficient data access.

The methodology consists of the following components:

1. **User Role Classification**
   The system classifies users into three categories:
   - Authors – upload research papers and datasets.
   - Editors – manage and verify academic publications.
   - Readers – search and access available scholarly data.
2. **Trusted Third Party (TTP)**
   A trusted authority is responsible for authenticating users, generating cryptographic keys, and managing access privileges.
3. **Data Encryption**
   Before uploading data to the cloud, authors encrypt the data using secure cryptographic techniques to ensure confidentiality.
4. **Cube-Based Data Storage**
   Data is stored using a cube structure that organizes information into multi-dimensional blocks. This structure improves indexing and retrieval efficiency.
5. **Secure Keyword Search**
   Encrypted keyword indexes allow users to search for data without decrypting the stored files.
6. **Data Integrity Verification**
   Hash-based verification mechanisms ensure that the data stored in the cloud has not been modified or tampered with.

IV. SYSTEM ARCHITECTURE



The proposed system architecture consists of four main entities:

1. **Data Owners (Authors)**
   Authors upload research papers and related data after encrypting the files.
2. **Cloud Server**
   The cloud server stores encrypted scholarly data and manages storage resources.
3. **Trusted Third Party (TTP)**
   The TTP verifies user identities, manages encryption keys, and monitors system security.
4. **Data Users (Editors and Readers)**
   Editors review and manage research content, while readers search and access available data.

The architecture supports secure communication between all entities using encrypted channels and authentication protocols.

System Workflow:

1. User registration and authentication
2. Key generation by TTP
3. Data encryption and upload by authors
4. Secure storage in cube data structure
5. Keyword search by users
6. Integrity verification before data access

V. ALGORITHMS USED

1. AES Encryption Algorithm

AES (Advanced Encryption Standard) is used to encrypt data before uploading to the cloud.

1. SubBytes (Byte Substitution)

Each byte in the state is replaced using an **S-Box substitution table.**

Formula concept:

$$S'(i,j) = SBox(S(i,j))$$

Where:

- $S(i,j)$ = original byte
- $SBox()$ = nonlinear substitution table
- $S'(i,j)$ = substituted byte

2. ShiftRows

Rows of the state matrix are shifted cyclically.

$$S'(r,c) = S(r,(c+r)\ mod\ 4)$$

Where:

- r = row index
- c = column index

Shift pattern:

- Row 0 → no shift
- Row 1 → shift left by 1
- Row 2 → shift left by 2
- Row 3 → shift left by 3

Steps:

1. Convert data into blocks.
2. Apply key expansion.
3. Perform substitution and permutation rounds.
4. Generate encrypted ciphertext.

2. Secure Hash Algorithm (SHA-256)

SHA-256 generates hash values to verify data integrity.

International Journal of Engineering Research and Science & Technology

1. Message Padding

The original message is padded so its length becomes **a multiple of 512 bits**.

$$L + 1 + k + 64 \equiv 0 \pmod{512}$$

Where

- L = original message length
- k = number of zero bits added

Steps:

1. Input data message.
2. Apply compression functions.
3. Generate 256-bit hash value.
4. Compare stored and computed hash values for verification.

Choice Function

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

Majority Function

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

3. Role-Based Access Control (RBAC)

RBAC ensures only authorized users can access specific data.

Steps:

1. Identify user role.
2. Assign access privileges.
3. Verify permissions before data access.
4. Grant or deny access.

4. Keyword Search Algorithm

Allows secure searching over encrypted data.

Steps:

1. Generate encrypted keyword index.
2. User submits search keyword.
3. System matches encrypted indexes.
4. Retrieve corresponding data blocks.

VI. EXPERIMENTAL RESULTS

The proposed system was implemented using a simulated cloud environment to evaluate performance in terms of security, search efficiency, and storage management.

Performance Metrics:

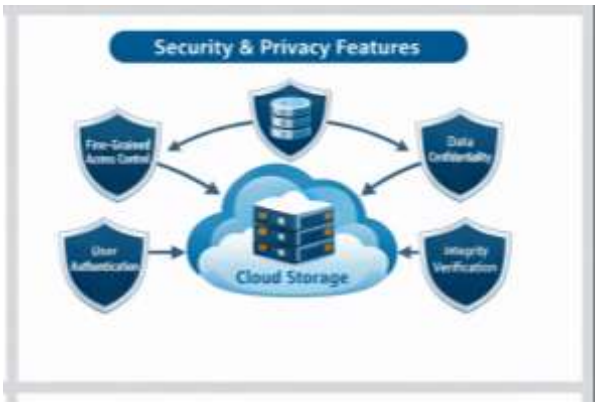
1. Data encryption time
2. Keyword search response time
3. Data retrieval efficiency
4. Integrity verification accuracy

Results Summary

Parameter	**Existing System**	**Proposed System**
Data Security	Medium	High
Search Efficiency	Low	High
Integrity Verification	Not Available	Available
Access Control	Basic	Role-Based

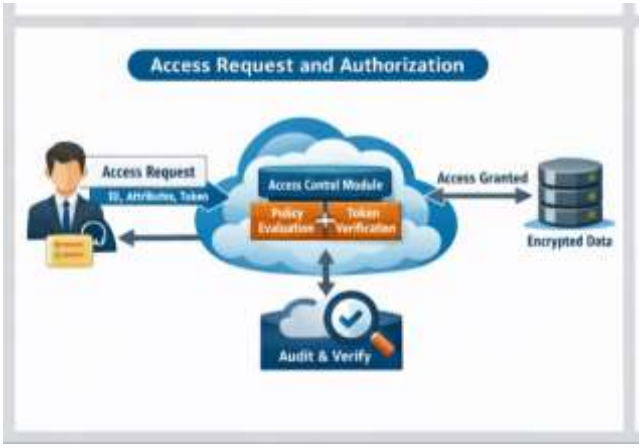
The results indicate that the proposed system significantly improves data security and search efficiency compared to traditional cloud storage approaches.





A. Home Page





G. User Registration



If data owner updates the access policy using old access policy and file id. And finally they use new access policy. When they change policy type in cloud side the updated file is re- encrypted.



A. User Login



Before user login the user registers the details. The cloud verify the user then cloud provide they private key to the user. Using this key, the user can do the work.

The user searching the file. The user requests the file. Requested details are send the cloud. Then data owner distributes the key to user mail id. Using the key user download the file.

VII. Conclusion & Future Work

This paper presented a secure and verifiable access control scheme for storing scholarly big data in cloud environments. The proposed system integrates role-based access control, encrypted keyword search, cube-

based data storage, and integrity verification mechanisms to enhance both security and efficiency.

The system successfully protects sensitive academic data from unauthorized access while enabling efficient retrieval through secure search techniques. Experimental evaluation shows improved performance in terms of data security, access control, and search efficiency.

Future work will focus on integrating blockchain technology to further strengthen trust and transparency in cloud-based scholarly data management. Additionally, machine learning techniques may be applied to optimize data indexing and search operations.

REFERENCES

1. M. Armbrust et al., "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
2. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
3. C. Wang et al., "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.
4. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Financial Cryptography*, 2010.
5. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE Symposium on Security and Privacy*, 2007.
6. Q. Wang et al., "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, 2011.
7. S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," *IEEE INFOCOM*, 2010.
8. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Eurocrypt*, 2005.
9. R. Buyya et al., "Cloud Computing and Emerging IT Platforms," *Future Generation Computer Systems*, 2009.
10. H. Takabi, J. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing," *IEEE Security & Privacy*, 2010.