International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year
Available at www.ijsred.com

RESEARCHARTICLE OPENACCESS

Cloud Data security using SHA Algorithm & Identity based data sharing on cloud

Attar Misba Jamir*, Alina Mohd Rafique Shaikh**, Rutik Prakash Kalaskar***, Sanchita Suresh Kharat****,
*(Computer Engineering, Kj's Trinity Polytechnic, Pune and Pune, India,
Email: attarmisba21@gmail.com)
**(Computer Engineering, Kj's Trinity Polytechnic, Pune and Pune, India,
Email: alinashaikh1126@gmail.com)
***(Computer Engineering, Kj's Trinity Polytechnic, Pune and Pune, India,
Email: rutikkalaskar11@gmail.com)
****(Computer Engineering, Kj's Trinity Polytechnic, Pune and Pune, India,
Email: sanchitakharat18@gmail.com)

----------**********----------

Abstract:

The system is developed using Java-based technologies and provides a secure cloud data storage and sharing framework through a web-based interface. It integrates key components such as user authentication, file upload, SHA-256 hashing, encryption, and identity-based data sharing to ensure data protection.

The SHA-256 algorithm generates unique hash values for files, enabling data integrity verification and detection of unauthorized modifications. To strengthen security, files are encrypted and fragmented before cloud storage, reducing the risk of data leakage. Identity-based authentication verifies users, while OTP-based verification ensures secure file sharing among authorized users.

Performance evaluation shows that the system provides secure data access with minimal response time and effective access control features such as permission management and revocation.

Experimental results indicate that the system successfully protects cloud data and ensures reliable sharing. The combination of multiple security mechanisms and efficient design makes it a practical solution for secure cloud environments.

Keywords — Cloud Computing, Data Security, SHA-256, Encryption, Identity-Based Authentication, OTP Verification, Secure Data Sharing.

----------**********----------

I. INTRODUCTION

- In recent years, cloud computing has become widely used for storing and sharing data, but security has emerged as a major concern due to risks such as unauthorized access, data leakage, and tampering. Users often lack reliable mechanisms to ensure data confidentiality and secure sharing in cloud environments.
- To address this issue, the proposed system introduced the secured cloud data storage and sharing framework using **SHA-256** hashing, encryption, and identity-based authentication techniques. The system ensures data integrity, protects sensitive information, and enables controlled access through OTP-based verification.
- The application is designed with a simple and user-friendly interface, allowing users to upload, store, and share files securely with minimal complexity. This system enhances overall data protection and provides a reliable solution for secure cloud environments.

II. SCOPE OF THE PROJECT

The scope of this project includes the development of a secure cloud-based system capable of storing, protecting, and sharing data using advanced security techniques such as SHA-256 hashing, encryption, and identity-based authentication.

1) Current Scope

• Secure storage of files in cloud environments
• Data integrity verification using SHA-256 hashing
• Encryption and fragmentation of files for enhanced security
• Identity-based authentication and OTP-based access control

2) Future Scope

• Integration with advanced security technologies like blockchain
• Multi-cloud storage for improved scalability and reliability
•AI-based monitoring systems for detecting suspicious activities
• Implementation of intrusion detection systems
• Development of mobile application for easy access

The system can be further extended to support enterprise-level cloud security solutions and large-scale data protection systems.

III. SYSTEM ARCHITECTURE

The proposed system follows a modular architecture consisting of the following components:

1. User Interface Layer

- Developed using JSP, HTML, CSS, and JavaScript
- Allows users to register, login, upload, and access files

2. Authentication Module

- Handles user registration and login verification
- Ensures only authorized users can access the system

3. SHA-256 Hash Generation Module

- Generates unique hash values for uploaded files
- Acts as a digital fingerprint of the data
- Helps detect any unauthorized modifications

4. Encryption and Fragmentation Module

- Encrypts files before storing them in the cloud
- Divides files into multiple fragments for added security
- Prevents unauthorized reconstruction of data

5. Cloud Storage Layer

- Stores encrypted and fragmented data in the database
- Manages secure file storage and retrieval

6. Identity-Based Authentication Module

- Verifies user identity using registered credentials
- Controls secure access to shared files

7. OTP Verification Module

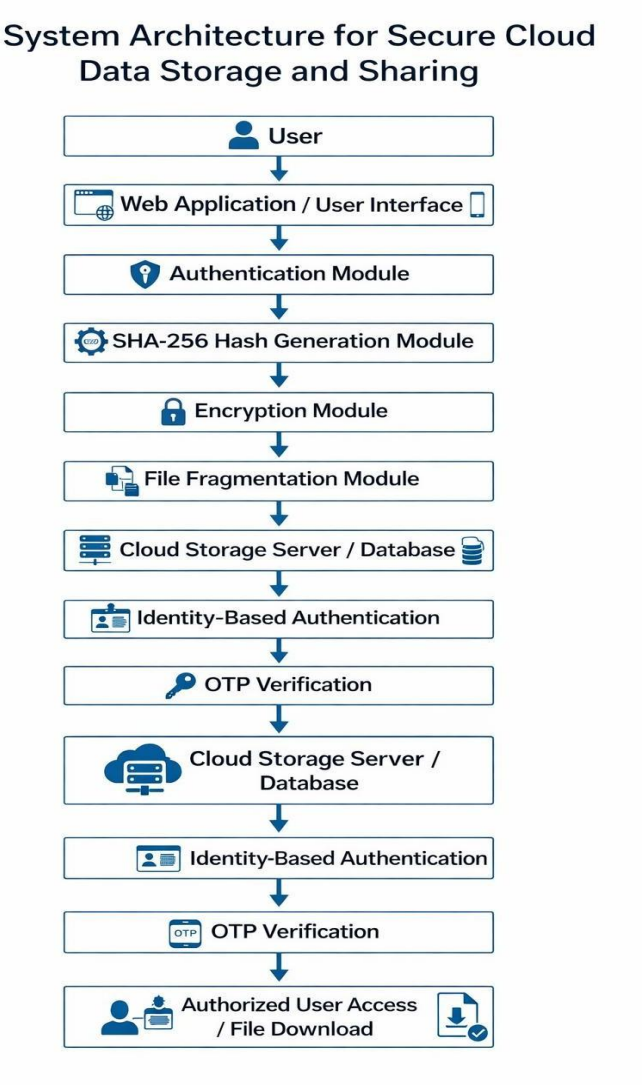
- Generates and sends one-time passwords to users
- Ensures secure and controlled file sharing

8. Secure Access Module

- Allows authorized users to access and download files
- Reconstructs and decrypts files securely

Working Flow

User Input → Authentication → File Upload → SHA-256 Hash Generation → Encryption & Fragmentation → Cloud Storage → Identity Verification → OTP Verification → Secure File Access / Download.



IV. METHODOLOGY

The proposed system is developed using the following methodology:

1. User Authentication

Users register and log in using secure credentials. Identity-based authentication ensures that only authorized users can access the system.

2. File Upload

Authenticated users upload files through the web interface. The system prepares the file for secure processing.

3. SHA-256 Hash Generation

A unique hash value is generated for each uploaded file. This helps in verifying data integrity and detecting any unauthorized changes.

4. Data Encryption and Fragmentation

The file is encrypted and divided into multiple fragments before storage. This enhances confidentiality and prevents data reconstruction.

5. Cloud Storage

Encrypted file fragments are securely stored in the cloud database, ensuring safe and scalable storage.

6. Secure Data Sharing

Identity-based authentication and OTP verification are used to control file sharing and access between users.

7. File Access and Download

Authorized users can access and download files after verification. The system reconstructs and decrypts the file securely.

8. Testing and Evaluation

The system is tested to ensure data security,performance, and reliability.

V. CONCLUSION

The proposed system provides an effective solution for enhancing cloud data security by integrating multiple security techniques such as SHA-256 hashing, encryption, identity-based authentication, and OTP verification. It enables users to store and share data securely while ensuring confidentiality, integrity, and controlled access.

The system is simple, user-friendly, and capable of providing secure file operations with minimal delay. It ensures that any unauthorized modification in data can be detected easily, and only authorized users can access shared files. Although the system currently operates on a structured framework, it can be further improved by integrating advanced technologies such as real-time monitoring and AI-based security

mechanisms.

Overall, the proposed system has strong potential as a reliable cloud security solution and can contribute significantly to secure data management in modern cloud environments.

REFERENCES

[1] W. Shen et al., "Enabling Identity-Based Integrity Auditing and Data Sharing for Secure Cloud Storage," IEEE Trans., 2019.

[2] J. Sivakumar et al., "Integrity Auditing for Secure Cloud Storage," ICMNWC, 2022.

[3] Y. Xu et al., "Privacy-Preserving Cloud Storage Auditing Scheme," IEEE Systems Journal, 2021.

[4] B. Deepthi et al., "Hybrid Secure Cloud Storage using Encryption Scheme," ESCI, 2021.

[5] J. Shen et al., "Privacy-Preserving Group Data Sharing in Cloud Computing," IEEE, 2022.

[6] I. Gupta et al., "Secure Data Storage and Sharing Techniques in Cloud," IEEE Access, 2022.

[7] A. S. P. et al., "Identity-Based Integrity Auditing for Cloud Storage," ICICICT, 2022.

[8] Oracle Corporation, "Java Documentation," 2025.

[9] MySQL Documentation, "Database Reference Manual," 2025.

[10] Apache Software Foundation, "Tomcat Server Documentation," 2025.

