IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

# Cloud Storage for Secure Data Sharing Across Platforms

**Ishika P. Wadichar[1], Prof. Vanshika H. Khapekar[2], Prof. Rohan B. Kokate[3]**
Student, Department of Master's of Computer Application[1]
Guide, Department of Master's of Computer Application[2]
Head of Department, Department of Master's of Computer Application[3]
JD College of Engineering & Management, Khandala, Kalmeshwar Road, Nagpur, Maharashtra, India
wadicharishika@gmail.com[1], vanshikakhapekar.sfdc@gmail.com[2], rbk7557@gmail.com[3]

**Abstract:** *In today's digital age, secure and efficient file sharing across multiple platforms has become essential. This project aims to develop a cloud-based secure file sharing system that ensures data privacy, integrity, and accessibility.*
*Users can upload, download, and manage files securely, with advanced features like automated file deletion, password protection, and administrative control. This research paper explores the system architecture, security mechanisms, implementation details, and potential applications, highlighting how cloud technology can optimize data management while maintaining confidentiality...*

**Keywords:** Cloud storage, Secure file sharing, Data privacy, Multi-platform access, Automated file management

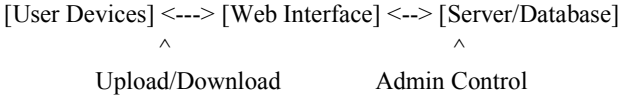
## I. INTRODUCTION

With the rapid growth of digital data, organizations and individuals need a secure and reliable method to store and share files. Traditional file-sharing methods face challenges such as unauthorized access, data loss, and compatibility issues across devices. Cloud storage provides a centralized solution where data can be accessed anytime, anywhere, with proper security mechanisms in place.

**Motivation:**
• Increasing demand for remote access to files across devices.
• Need for data privacy and confidentiality.
• Efficient storage management and file lifecycle handling.

**Objectives:**
1. Develop a secure multi-platform file sharing system.
2. Integrate automated file deletion for privacy.
3.Provide admin control panel for centralized management.
4.Implement encryption and secure authentication.

Diagram 1: System Overview




## II. LITERATURE REVIEW

1. Cloud Storage Systems: Google Drive, Dropbox, OneDrive – secure storage, but privacy challenges exist.
2. Secure File Sharing: Encryption (AES, RSA) and access control mechanisms prevent unauthorized access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

3. Automated File Management: Automatic file deletion ensures sensitive data isn't retained longer than necessary.
4. Security Challenges: Multitenant environments require robust isolation and monitoring.

Diagram 2: File Sharing Process

[User Uploads File] → [Server Encryption] → [Database Storage]
↓
[File Access Control]
↓
[Authorized Download]
[Authorized Download]

## III. SYSTEM ARCHITECTURE

• Client-Server Model: Users access via web interface, files stored securely on cloud server.
• Admin Panel: Monitor uploads/downloads, manage users, enforce security policies.
• Database: Stores user credentials, file metadata, access logs, encryption keys.
• Security Mechanisms:
Password hashing (SHA-256), SSL/TLS encryption, optional 2FA.

Diagram 3: Architecture Flowchart

[User Login] → [Authentication] → [File Upload/Download]
↓
[Encryption Module]
↓
[Database Storage]
↓
[Admin Panel]

## IV. FEATURES OF THE SYSTEM

1. User Authentication: Secure login and registration with email verification.
2. File Upload/Download: Supports large files, multiple formats, encryption.
3. File Management: Search, download, delete, organize files efficiently.
4. Admin Control: Central monitoring, manage users, view logs.
5. Automated File Deletion: Users can schedule automatic deletion after a set period (e.g., 10 days).
6. Activity Logging: All file activities logged for security audit.
7. Notifications: Email alerts for uploads, downloads, deletion events.

Table 1: Feature Summary

| Feature | Description | Security Benefit |
|---|---|---|
| File Encryption | AES/RSA | Prevent unauthorized access |
| Auto-delete | 10 days | Privacy & storage optimization |
| Admin Panel | Central monitoring | Policy enforcement |
| Notifications | Email alerts | Transparency |

## V. IMPLEMENTATION DETAILS

• Frontend: HTML, CSS, JavaScript for responsive UI.
• Backend: PHP for server-side scripting.
• Database: MySQL to store users, files, metadata securely.


DOI: 10.48175/IJARSCT-33941

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

• Security:
o Password hashing with SHA-256.
o File encryption with AES before storage.
o HTTPS/SSL for secure communication.

Diagram 4: File Upload Process

[User Select File] → [Client-side Validation] → [Server-side Encryption] → [Database Storage]

## VI. CHALLENGES AND SOLUTIONS

| Challenges | Solutions |
|---|---|
| Data Security | Encryption, authentication, access control |
| Cross Platform Access | Web-based interface compatible with all devices |
| Large Handling File | Chunked uploads, compression |
| Automated Deletion | Server-side CRON jobs for scheduled deletion |

## VII. APPLICATIONS

• Educational institutions for sharing assignments and lecture notes securely.
• Organizations for internal document management and secure collaboration.
• Personal use for storing sensitive data with privacy guarantees.

## VIII. CONCLUSION

The Cloud Storage for Secure Data Sharing Across Platforms project demonstrates how cloud technology can be leveraged to provide secure, e icient, and user-friendly file sharing. The system not only ensures data privacy and security but also optimizes storage through automated file management. Future enhancements can include AIdriven file categorization, real-time collaboration tools, and enhanced security features like biometric authentication.

## REFERENCES

[1]. https://www.ieee.org/conferences/publishing/templates
[2]. https://csrc.nist.gov/publications/det ail/sp/800-145/final
[3]. https://azure.microsoft.com/enus/overview/storage/ https://aws.amazon.com/s3/
[4]. https://cloud.google.com/storage/doc
[5]. https://www.ibm.com/cloud/storage
[6]. https://www.oracle.com/cloud/storage/
[7]. https://www.techtarget.com/searchst orage/definition/cloud-storage
[8]. https://www.cisco.com/c/en/us/solut ions/cloud/cloud-security.html
[9]. https://www.cloudwards.net/bestcloud-storage/
[10]. https://standards.ieee.org/initiatives/ cloud/ https://owasp.org/www-projectcloud-security/
[11]. https://www.techrepublic.com/article /cloud-storage-securityissuesandsolutions/
[12]. https://cloudsecurityalliance.org/rese arch/securhttps://cai.ieee.org/2025/pa per-submission-and-guidelines/ity guidance/
[13]. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.
[14]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.
[15]. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

[16]. Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24–31.
[17]. Popa, R. A., et al. (2011). Enabling security in cloud storage SLAs. ACM Cloud Computing Security Workshop.
[18]. Wang, C., Wang, Q., Ren, K., Lou, W., & Li, J. (2010). Public verifiability and data dynamics for storage security in cloud computing. IEEE Trans. on Parallel and Distributed Systems, 22(5), 847–859.
[19]. Ristenpart, T., et al. (2009). Information leakage in third-party compute clouds. CCS 2009.
[20]. Li, H., et al. (2013). Cloud storage: Architecture, security, and challenges. J. of Computer and System Sciences, 79(5), 696–717.
[21]. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69–73.
[22]. Modha, K., & Dave, M. (2017). Secure cloud storage: Data confidentiality and integrity. Int. J. of Adv. Res. in CS, 8(4), 102–107.
[23]. Zhang, R., & Liu, L. (2010). Security models and requirements for cloud computing. IEEE Int. Symp. on Dependable, Autonomic and Secure Computing.
[24]. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50– 57.
[25]. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. IEEE Conf. on Computer Science & Electronics Eng.
[26]. Badger, L., et al. (2012). Cloud computing synopsis and recommendations. NIST Special Publication 800-146.
[27]. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357–383.
[28]. Subramanian, A., et al. (2018). Cloud-based file sharing security techniques and models: A review. J. of Cloud Computing, 7(1), 1–16.