International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Secure File Upload, Storage and Access Control using Hybrid Approaches

Vedansh Mevada[1], Hitarth Raval[2]

Abstract

Secure file upload and cloud storage mechanisms have become a critical component in modern digital services, especially for sensitive documents uploaded through web applications. Traditional cloud solutions ensure stored data security through encryption, while the modern attack vectors lie in the vulnerabilities that occur during the initial upload stage, misconfigured cloud storage permissions, or weak mechanisms for file access. This paper reviews sixteen recent publications related to secure file storage, cloud encryption, attribute-based access control, hybrid cryptography, web upload vulnerabilities, blockchain storage, and machine learning-based exploit detection. The analysis of these highlights the strengths and limitations of each approach, identifies major research gaps, and suggests a unified security framework that integrates secure upload validation, encrypted storage, attribute-based policy enforcement, and cloud misuse prevention for future applications.

Keywords: Secure cloud storage; file upload security; access control; cloud vulnerabilities; exploit detection.

1. Introduction

The features of file upload and cloud storage have been widely applied to web applications, such as e-government service systems, digital education portals, healthcare systems, and enterprise documentation platforms. Large amounts of sensitive files, including identity proofs, certificates, and confidential records, are uploaded and stored on cloud platforms. This makes them a critical target in the sight of security threats. The attack scenarios include malicious file upload, misconfiguration of cloud access, bypassing validation, unauthorized data access, manipulation of data, and leakage of privacy.

While modern security mechanisms focus on the encryption of the file and storage confidentiality, recent research illustrates attackers use not only weaknesses of storage mechanisms but also weaknesses in the upload procedure itself. Consequently, confidentiality, integrity, privacy, malware detection, and secure architecture of uploading should be taken into consideration while managing files securely.

The aim of this review is to analyze state-of-the-art mechanisms including hybrid cryptography, attribute-based access models, decentralized cloud file systems, privacy-preserving storage, and security validation against malicious uploads.

Literature Review

1.1. Hybrid Cryptography

Various works are suggesting the use of hybrid encryption models combining symmetric and asymmetric algorithms for better confidentiality and key protection. AES provides performance efficiency in encryption, while RSA or ECC does this securely for the exchange of encryption keys [1][2][4][12][13][15][16].

1.2. Attribute-Based Access Control

Attribute-Based Encryption methods like ABE, CP-ABE, MA-ABE, and vFAC achieve the desired functionality of privacy-preserving sharing by policy-based encryption instead of by static user identities. These methods support fine-grained access permissions, dynamic policy control, and partial attribute hiding [1][5][6][14].

1.3. Privacy-Preserving and Healthcare Systems

The secure storage and restricted access in the healthcare cloud system using hybrid encryption, role-based permissions and audit mechanisms, are stressed by many studies [3][8][14].

1.4. Blockchain and IPFS Storage

Blockchain and IPFS enable decentralized, tamper-resistant data storage, while smart contracts control user access to ensure transparency and verifiable document integrity [10].

1.5. Machine Learning for Exploit Detection

Some recent research works propose the use of ML-based exploit detection, such as opcode classification and API call modeling, which are able to detect obfuscated malware, webshell uploads, and runtime exploits [6][7][9].

1.6. File Upload Security Vulnerabilities

Detailed research brings out multiple attack patterns based on uploads, which include MIME spoofing, null-byte insertion, extension bypassing, embedded malware, and dangerous cloud upload token misconfigurations [11][15][16].

2. Problem Statement

Most of the existing solutions primarily focus on data encryption or secure access models but fail to address upload-level security threats, cloud credential weaknesses, and real-time malicious content detection. There is no unified architecture capable of integrating upload validation, secure key exchange, cryptographic storage, fine-grained access control, and cloud misconfiguration prevention simultaneously.

3. Aim and Objectives

This review aims to evaluate the mechanisms for secure file upload, encrypted cloud storage, and fine-grained access control, while finding a unified approach.

Objectives:

- Evaluate encryption and hybrid cryptographic mechanisms.
- Compare various access control approaches, including CP-ABE and multi-authority ABE.
- Review exploit detection and upload security challenges.
- Identify gaps related to cloud storage misconfiguration.
- Propose a combined model for future systems.

4. Research Questions & Identified Gaps

- Can encryption alone secure files against upload-based attacks ?
    - No, because encryption protects only stored data, not uploaded files.
- Can RBAC or ABE protect sensitive files independently?
    - No, access control mechanisms lack upload validation and exploit detection.
- Can cloud storage be trusted without configuration monitoring?
    - No, misconfigured upload credentials can allow file theft, overwrite or billing attacks.
- Does a complete secure upload-to-storage framework exist?
- No current solution integrates file validation, encryption, access control, and cloud-security controls.

Key Gaps:

- Upload validation not integrated with encryption.
- Limited multi-authority management for access revocation.
- Missing cloud-level credential security.
- Lack of unified end-to-end security design.

5. Proposed Solution (Scope for future work)

Future secure systems should integrate :

- Client-side hybrid encryption
- Secure upload filters and content validation
- Multi-authority attribute-based access
- Cloud least-privilege upload credentials
- ML-based malicious detection
- Blockchain integrity proof

This integrated approach can ensure confidentiality, privacy-preserving access, secure sharing, exploitation resistance, and cloud safety

6. Conclusion

Secure cloud storage requires multiple complimentary protections beyond encryption. Fine-grained access policies, hybrid cryptography, decentralized verification, upload security mechanisms, and malicious detection are essential components of secure cloud ecosystems. However, existing solutions address these areas separately. A unified framework integrating secure upload procedures, cryptographic storage, multi-level access control, and cloud configuration security is necessary for modern web applications.

References

1. Patel, J., & Trivedi, A. (2022). Cloud based secure file sharing using access control. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(4), 337–348.
2. Chandana, D. K., & Supriya, M. (2025). Cloud-based secure file storage using hybrid cryptography. International Journal of Scientific Research in Engineering and Management, 9(8), 1–10.
3. Reddy, S. M., Sana, M., Sushma, M., & Divya Sri, M. (2024). Enhanced data privacy and security in cloud storage: A robust authentication scheme for cyber-physical-social systems. Journal for Educators, Teachers and Trainers, 15(5), 383–392.
4. Chincholkar, A., Londhe, A., Joshi, M., Gole, P., & Mirgale, S. (2025). Ensuring confidentiality and integrity in cloud storage using AES encryption and SHA-256 hashing. International Journal of Engineering Research & Technology, 14(10), 1–7.
5. Liu, J., Tang, H., Li, C., Sun, R., Du, X., & Guizani, M. (2018). vFAC: Fine-grained access control with versatility for cloud storage. arXiv.
6. Kokol, D., Faristi, F., & Sutrisno, A. (2023). Machine learning framework for efficient exploit detection (ML-FEED). Proceedings of the International Conference on Sustainable Engineering and Technology (ICSET), 1–8.
7. Guo, Y., Marco-Gisbert, H., & Keir, P. (2020). Mitigating webshell attacks through machine learning techniques. Future Internet, 12(1), 12.
8. Dhanalakshmi, G., & George, G. V. S. (2023). Secure and privacy-preserving storage of E-Healthcare data in the cloud: Advanced data integrity measures and privacy assurance. International Journal of Engineering Trends and Technology, 71(10), 238–253.
9. Chitti Babu, E., & Vamsi Krishna Yadav, S. (2024). Secure cloud storage with file access and file sharing control. International Journal of Creative Research Thoughts, 12(3), Article IJCRT24A3289.
10. Venkataradha krishnamurty, V., & Naveen, C. (2024). Secure data transfer and file storage access control using IPFS and blockchain technique. Journal of Engineering Sciences, 15(8), 1490–1495.
11. Shimpikar, S., Shedge, S., Sonawane, H., & Nair, B. (2025). Secure file sharing system using access control. Journal of Emerging Technologies and Innovative Research, 12(4), 676–682.
12. Gandhodi, H. V., Maddali, S. T., Morthala, K. R. R., Sadda, S. M., & Vijay Kumar, S. (2023). Secure file storage & sharing on cloud using cryptography. International Journal of Current Science (IJCSPUB), 13(2).

13. Kurian, K., Nair, L. S., Joby, P. P., Jose, R. M., & John, R. M. (2023). Secure file storage in cloud using hybrid encryption. International Journal of Engineering Research & Technology, 11(4), NCASCD-2023, 147–151.
14. Gupta, R., Kanungo, P., Dagdee, N., Madhu, G., Sahoo, K. S., Jhanjhi, N. Z., Masud, M., Almalki, N. S., & AlZain, M. A. (2023). Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing. Sensors, 23(5), 2617.
15. Pooj, K., & Patil, S. (2016). Understanding file upload security for web applications. International Journal of Engineering Trends and Technology, 42(7), 342–347.
16. Understanding the security risks of websites using cloud storage for direct user file uploads. (2017). Unpublished manuscript.