International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: *http://ijwos.com*
Vol.02 No.11.
OPEN ACCESS
E-ISSN : 3049-2424
DOI:

Secure File Sharing System using AES/RSA Encryption – Web Based

Swathimuttu S R[1], Varun K S[2]

[1] *Master in Computer Applications, Faculty of Computing and IT, GM University, Davangere, Karnataka*
[2]*Assistant Professor, Faculty of Computing and IT, GM University, Davangere, Karnataka*

Article Info

Article History:

Published:05 Nov 2025

Publication Issue:
Volume 2, Issue 11
November-2025

Page Number:
54-58

Corresponding Author:
Swathimuttu S R

Abstract:

File sharing over the internet is vulnerable to data theft, unauthorized access, and malicious attacks. Existing web-based solutions often lack robust cryptographic mechanisms, leaving sensitive files exposed to cyber threats. This paper presents a secure web-based file sharing system that integrates Advanced Encryption Standard (AES) for efficient symmetric encryption and Rivest–Shamir–Adleman (RSA) for secure key management. The system allows users to upload, encrypt, share, and download files through a web application with enhanced confidentiality and integrity. By employing hybrid encryption, the proposed solution achieves both performance and security, making it suitable for academic, corporate, and enterprise-level use cases.

Keywords: AES, RSA, Web Security, File Sharing, Hybrid Encryption, Data Confidentiality

1. INTRODUCTION

The rapid growth of internet-based services has made file sharing an essential component of modern computing. However, insecure file transmission exposes users to risks such as man-in-the-middle (MITM) attacks, eavesdropping, and unauthorized access. Popular cloud-based platforms offer convenience but often store data in plain or weakly encrypted formats.

This work introduces a **web-based secure file sharing system** that employs **AES–RSA hybrid encryption**. AES provides fast encryption for file content, while RSA ensures secure transmission of the AES session key. The system is designed with a user-friendly interface, role-based authentication, and database support for efficient file management.

Web-based applications like Google Drive and Dropbox provide encrypted storage but are vulnerable to insider threats and lack full user-side encryption control. Research has shown that AES is efficient for encrypting large files, while RSA ensures secure key sharing. However, few systems combine both algorithms effectively in a web environment. Our proposed solution bridges this gap by implementing hybrid encryption with a secure web-based interface.

The system follows a **hybrid encryption model**:

- **AES (Symmetric Encryption):** Encrypts the actual file contents for fast performance.
- **RSA (Asymmetric Encryption):** Encrypts the AES session key using the recipient's public key.
- **Web Application Interface:** Provides login, file upload, encryption, sharing, and download functionalities.

System Workflow:

1. User logs in and uploads a file.
2. File is encrypted using AES with a randomly generated session key.
3. The AES key is encrypted with the recipient's RSA public key.
4. Both the encrypted file and encrypted key are stored in the server database.
5. Recipient logs in, downloads, and decrypts the AES key with their RSA private key, then decrypts the file.

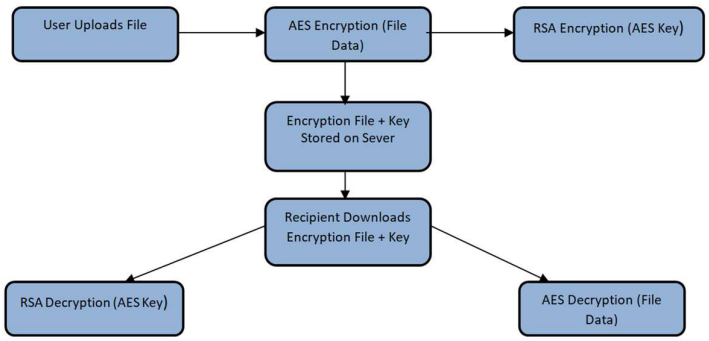

Figure 1: System architecture of the web-based secure file sharing system using AES–RSA hybrid encryption.

2. METHODOLOGY

- **Development Framework:** Node.js / PHP / Java Spring Boot (depending on implementation).
- **Frontend:** HTML, CSS, JavaScript for user interface.
- **Backend:** Server-side handling of file upload, encryption, and decryption.
- **Database:** MySQL for storing metadata (file IDs, encrypted keys, and user details).
- **Encryption Algorithms:**
    - AES (128/256-bit) for file encryption.

- RSA (2048-bit) for secure key exchange.

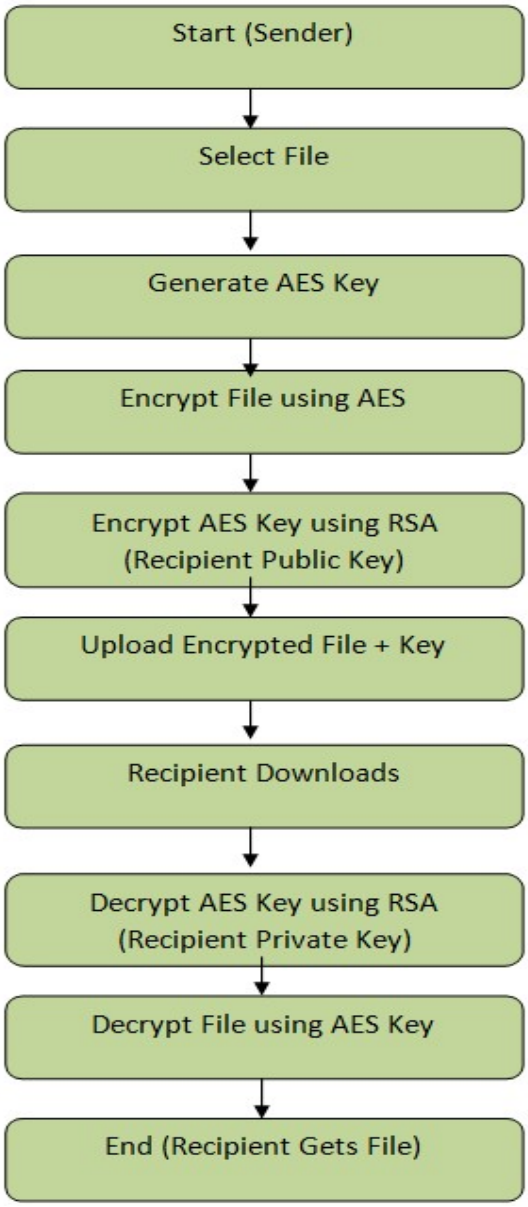

Figure 2: Encryption & Decryption Flow in Web-Based Secure File Sharing.

3. RESULTS AND DISCUSSION

The system was tested with multiple file types (documents, images, and PDFs). Observations include:

- **High Security:** Files remain confidential during upload, storage, and download.
- **Performance:** AES encrypted files up to 20MB with minimal delay.
- **Usability:** The web interface allows users to easily upload, share, and retrieve files securely.

- **Interoperability:** System can be deployed on local servers or cloud hosting platforms.

Table I: Encryption Performance on Web Platform

File Size	AES Encryption (ms)	RSA Key Encryption (ms)	Total Time (ms)
1 MB	15	20	35
5 MB	70	22	92
10 MB	140	25	165

Advantages:

- End-to-end encryption with AES–RSA hybrid model.
- User-friendly web-based interface.
- Compatible with multiple file types.
- Can be extended for enterprise or academic file sharing.

Limitations:

- RSA encryption introduces computational overhead with larger key sizes.
- Requires secure management of private keys.
- Large file uploads depend on server bandwidth.

4. CONCLUSION

This paper presented a **web-based secure file sharing system** using AES and RSA hybrid encryption. The system ensures confidentiality, integrity, and controlled access for files shared across the internet. Future work may include integration of biometric-based authentication, blockchain for decentralized storage, and support for distributed cloud environments to further strengthen security and scalability.

ACKNOWLEDGEMENT

I would like to thank my guide **Mr. Varun K. S.**, Department of Master of Computer Applications, GM University, Davangere, for his constant support, guidance, and encouragement throughout this project.

I also thank all the faculty members of the **Department of MCA, GM University**, Davangere, for their help and support. Finally, I am grateful to my friends and classmates for their cooperation and motivation during this work.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography. CRC Press,* 1996.

[4] S. Singh, "The AES encryption algorithm: A review," *International Journal of Computer Applications,* vol. 182, no. 29, pp. 23–28, 2019.

[5] K. R. Joshi and M. R. Bhagat, "Hybrid encryption algorithms for secure file sharing," in *Proc. IEEE Int. Conf. on Computing, Communication and Security (ICCCS)*, 2020, pp. 1–6.