Security Overview Document

Intern :

ABAKTA Haana Camille

Organization :

Future Interns

Assignment

Task 3 - Secure file sharing system

Date :

January 17, 2026

SUMMARY

1. Introduction

This document provides a security overview of the Secure File Sharing System, developed as part of Task 3 during my online cybersecurity internship at Future Interns.

The main objective of this system is to ensure the confidentiality of shared files by applying strong encryption mechanisms and secure key handling practices.

2. Encryption Algorithm Used

2.1. Advanced Encryption Standard (AES)

The system uses AES (Advanced Encryption Standard), a widely adopted symmetric encryption algorithm recognized for its security and efficiency.

Key characteristics:

- Symmetric encryption (single secret key)
- High security level
- Well-suited for encrypting large files

AES is a standard used in many real-world secure systems and applications.

3. File Encryption (Data at Rest)

Before being stored on the server:

- Files are encrypted using the AES algorithm
- Only encrypted files are saved on the storage system
- Plain (unencrypted) files are never stored

This approach ensures that even in the event of unauthorized access to the server storage, the data remains protected and unreadable.

4. Data Security in Transit

During file upload and download operations:

- Data is transmitted through secured HTTP requests
- Server-side encryption ensures that sensitive file content is never exposed in plain text

In a production environment, the use of HTTPS (TLS) is strongly recommended to further secure data transmission.

5. Key Management

Key management is a critical aspect of the system's security design:

- A secret AES key is used for both encryption and decryption
- Encryption keys are not directly exposed to end users
- Access to encryption keys is restricted to the server side

Potential improvements for a real-world deployment include:

- Storing keys using environment variables
- Using a secure secret management service
- Implementing regular key rotation policies

6. Limitations and Future Improvements

Identified limitations:

- Basic key management implementation
- No advanced user authentication mechanism
- No role-based access control
- Possible future enhancements:
- Strong user authentication and authorization
- Hybrid encryption model (RSA for key exchange + AES for file encryption)
- Logging and auditing of file access
- Permission-based access control system

7. Conclusion

This project demonstrates a practical implementation of fundamental cryptographic principles applied to a secure file sharing system.

It provides a solid foundation for further improvements and deployment in a real-world production environment.