Security Overview Document

Project:

Secure File Share System (AES-128 Encryption)
Future Interns – Cyber Security Internship | Task 3

1. Overview

This document provides a security overview of the Secure File Share System, focusing on encryption methods and key handling practices implemented in the project. The system is designed to securely upload, store, and download files while ensuring confidentiality and integrity.

2. Encryption Methods

The project uses AES-128 encryption in CBC (Cipher Block Chaining) mode. Key points include:

- • AES-128 ensures strong symmetric encryption using a 16-byte key.
- • CBC mode adds an initialization vector (IV) for each file to prevent pattern detection.
- • Files are encrypted before being saved on the server and decrypted only during download.
- • The IV is stored alongside the ciphertext to allow proper decryption.

3. Key Handling

Proper key management is critical for security. The system implements the following practices:

- • The AES key is stored securely in a `.env` file and never hard-coded in the source code.
- • Access to the `.env` file is restricted and should not be committed to version control.
- • Keys are 16 bytes long (128-bit) and randomly generated for strong security.

4. Security Practices

Additional security measures in the project include:

- • Using secure file names and sanitization to prevent path traversal.
- • Flash messages for feedback without exposing sensitive information.
- • Separation of encryption logic into a dedicated module (`crypto.py`) for maintainability.

5. Threats and Recommendations

Potential threats and best practice recommendations:

- • Unauthorized access to the server – recommend implementing authentication.
- • Key leakage – ensure `.env` is secure and use access controls.
- • Use HTTPS in production to protect files during transit.

6. Conclusion

The Secure File Share System uses AES-128 encryption with proper key handling practices to ensure file confidentiality and integrity. While suitable for internship demonstration, additional measures are required for production deployment.