■Security Overview Document

Author: RishavRaj

1. Introduction

This document outlines the security framework of the Secure File Sharing System. The platform enables users to upload files, which are then encrypted before being stored, ensuring protection during both storage and transfer. Authorized users can later decrypt these files, preserving confidentiality and safeguarding sensitive data from exposure.

2. Encryption Methodology

The system implements AES (Advanced Encryption Standard) to perform both encryption and decryption. AES is a trusted symmetric encryption technique recognized for its strong security and performance. Every uploaded file is encrypted with a unique key, guaranteeing data integrity and confidentiality.

3. Key Management

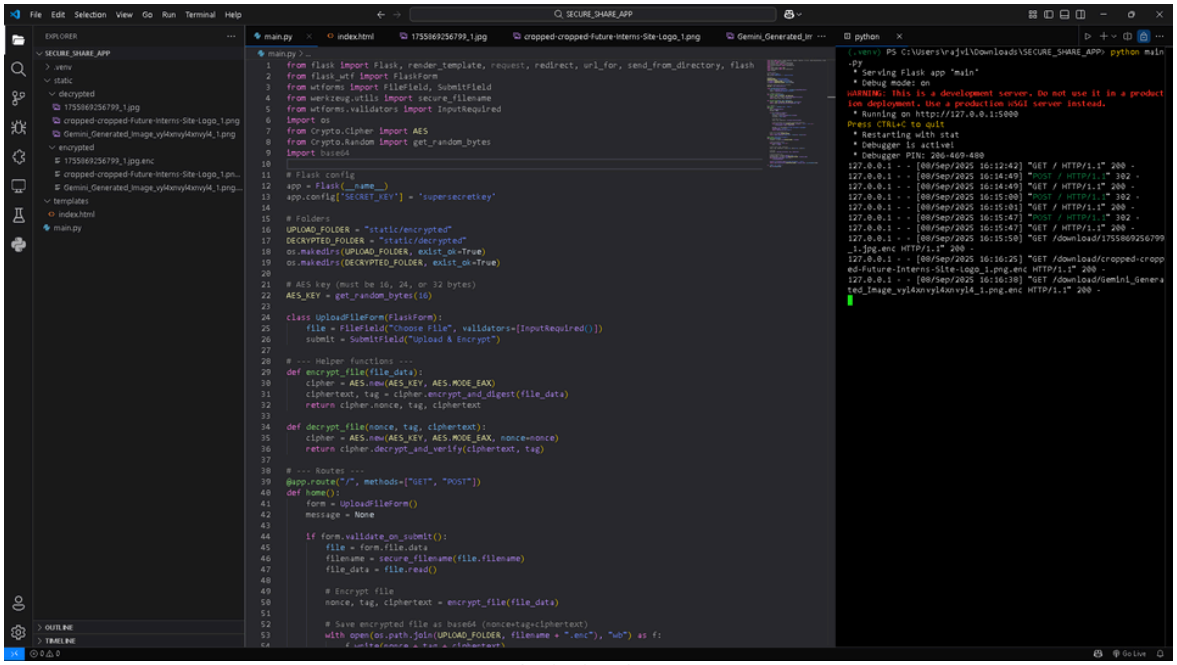
All encryption keys are generated internally by the system and kept away from unauthorized access. To strengthen security, periodic key rotation is recommended, and keys should be stored in a secure vault or key management system instead of plain storage.

4. Security Best Practices

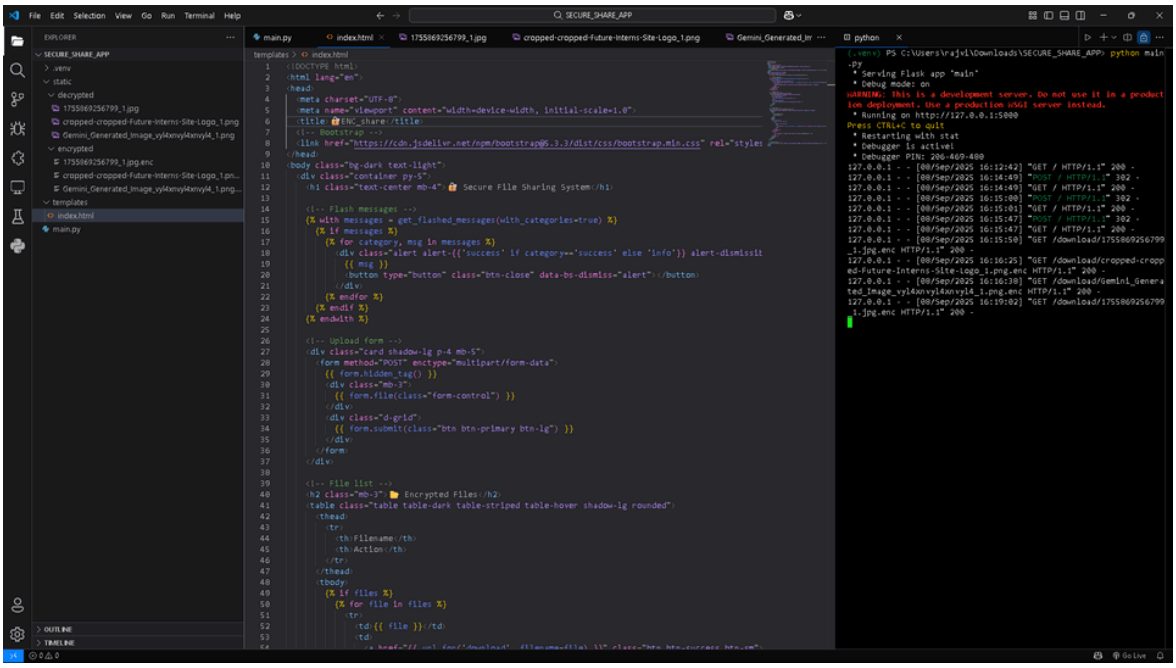
- Adopt robust key management procedures. - Enforce HTTPS for secure communication and file transfer. - Limit access to encrypted and decrypted files to authorized users only. - Conduct regular monitoring and audits of the encryption mechanisms. - Follow the principle of least privilege when assigning access permissions.

5. Visual Demonstrations

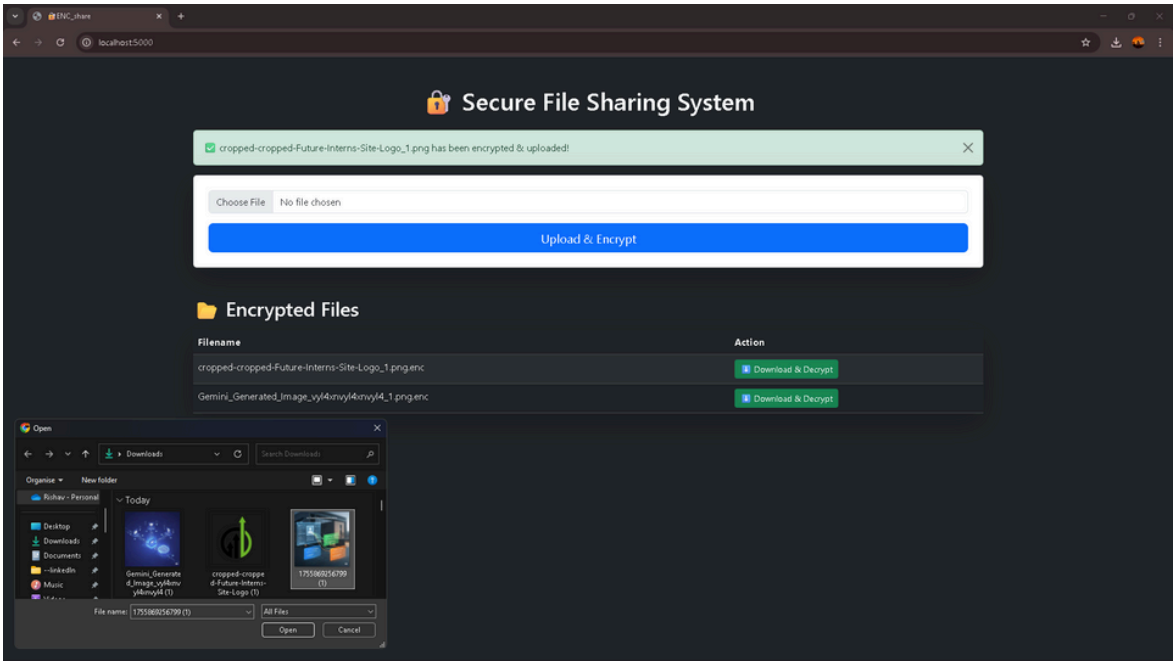
Screenshots provided in this report illustrate the functionality and workflow of the Secure File Sharing System, highlighting file upload, encryption, and decryption processes.



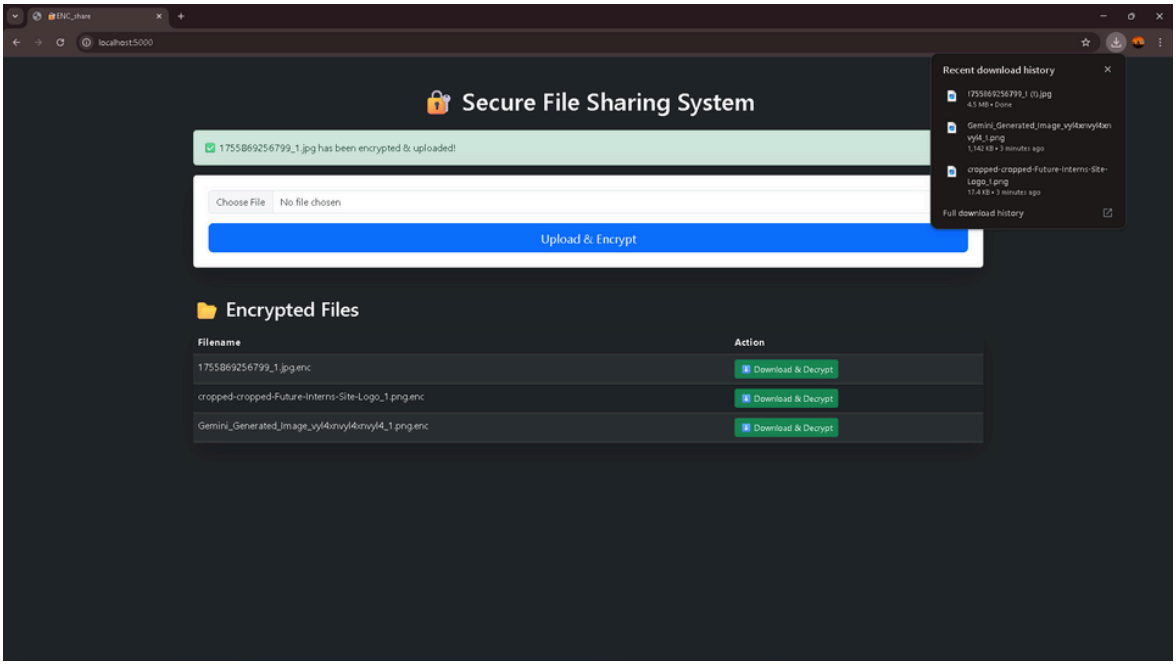
app.py



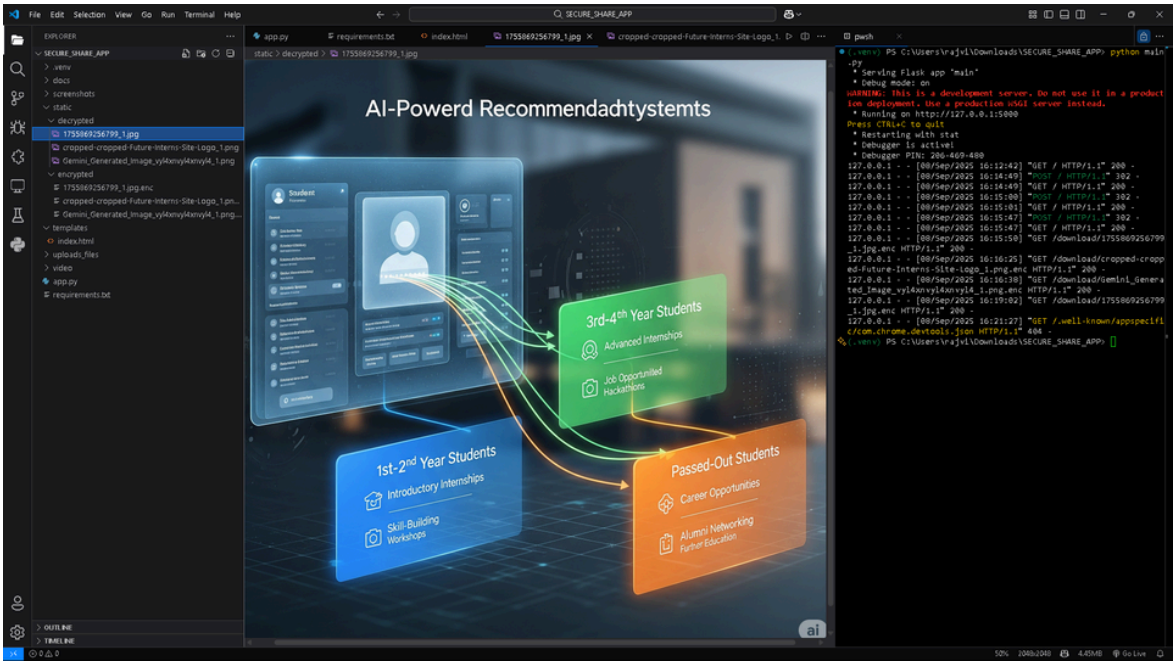
index.html



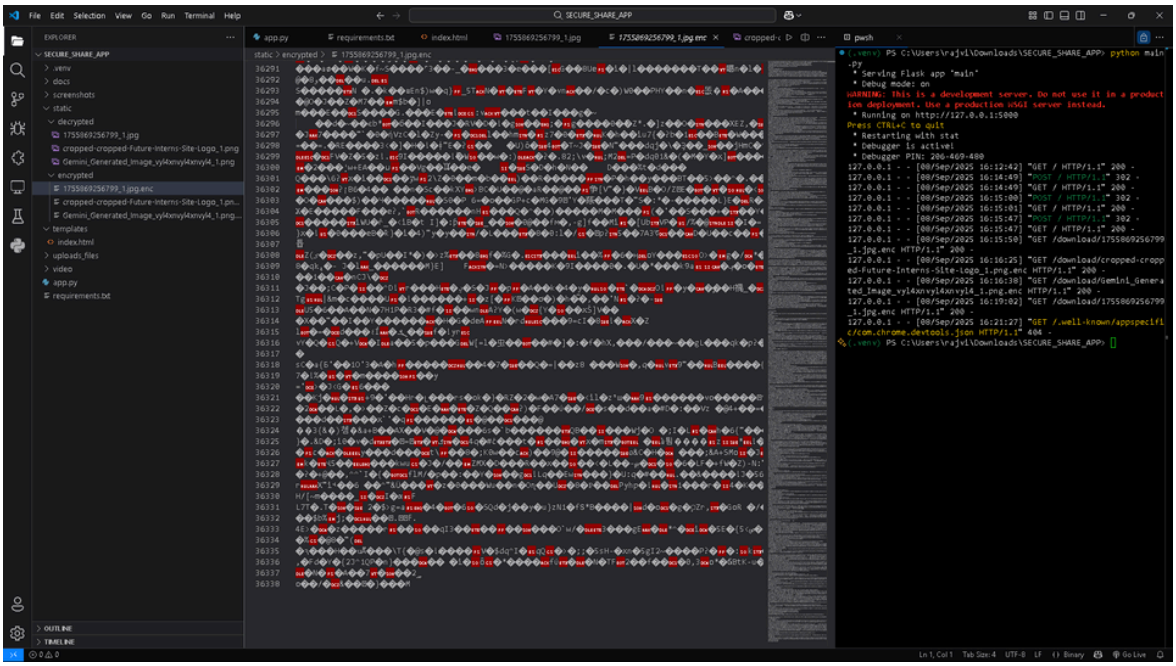
uploading & encrypting



downloading & decrypting



decrypted file



encrypted file