Secure file sharing system

Cybersecurity internship Task _03

Future interns

Title : secure file sharing system

Intern name : ODAI WAHIB

Date : 28-08-2025

Secure File Portal - Project Report

Introduction

The Secure File Portal is a Flask-based web application that provides a secure way to upload and download files. The project ensures data confidentiality by using AES-GCM encryption with an envelope encryption model. Each file is encrypted with a Data Encryption Key (DEK), which is further wrapped with a Key Encryption Key (KEK).

Features

- Upload files securely through the web interface or using curl commands.

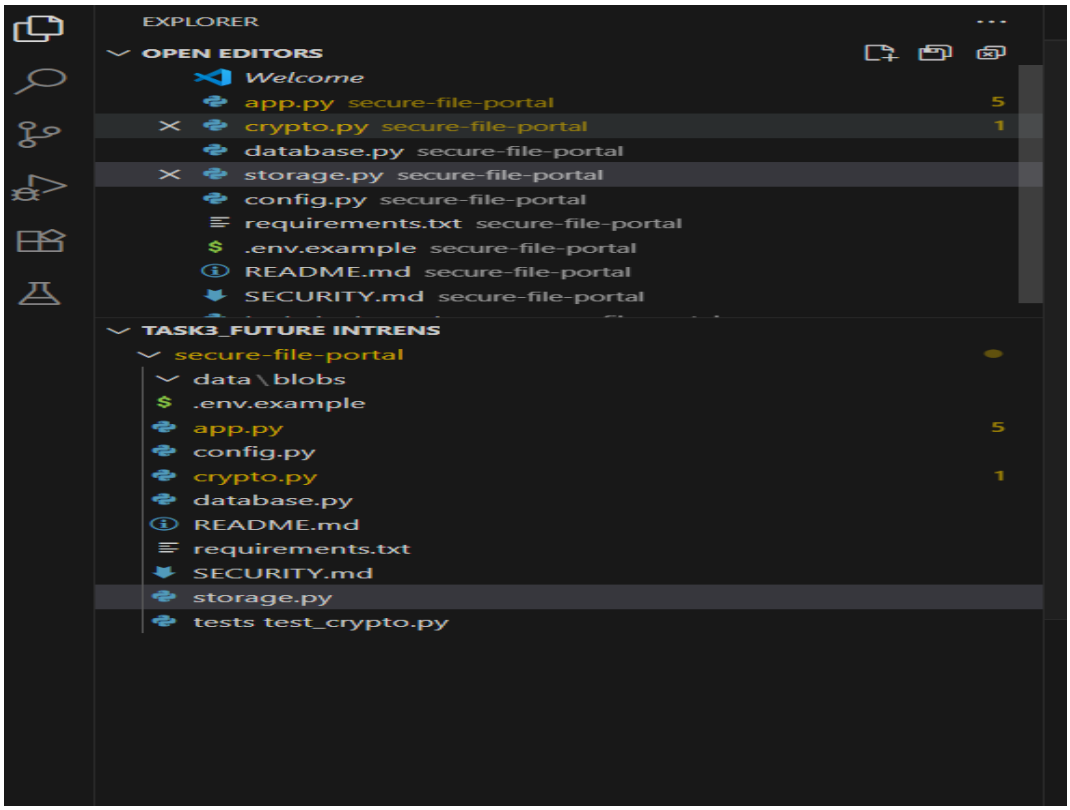
- Files are encrypted with AES-GCM before storage.

- Encrypted file metadata (nonce, tag, wrapped DEK) stored in database.

- Files can be downloaded and automatically decrypted.

- Uses Flask framework with SQLAlchemy for database handling.

- Simple and secure design for confidentiality.



System Requirements

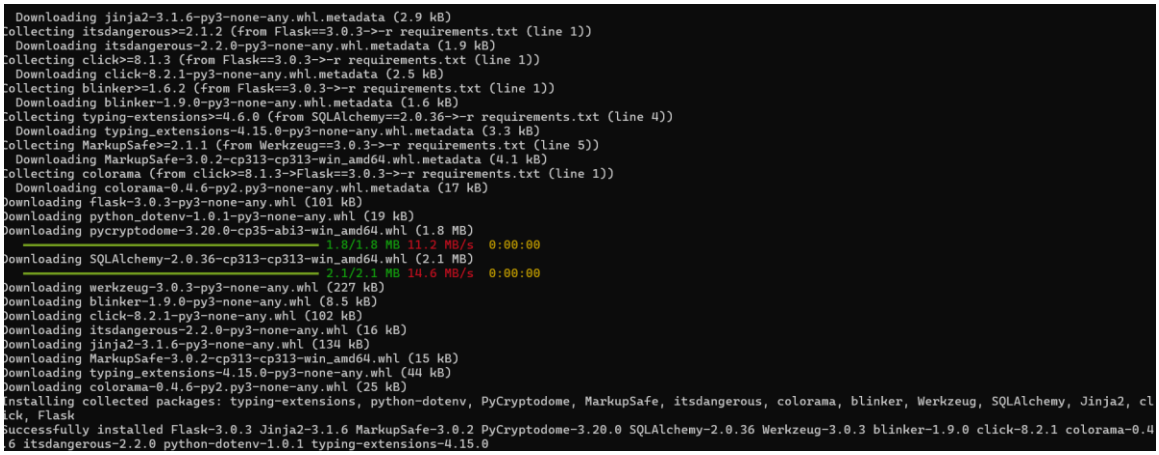
- Python 3.9 or above

- Flask

- SQLAlchemy

- cryptography library

- curl (for testing uploads/downloads)



Project Structure

The project consists of the following main files:

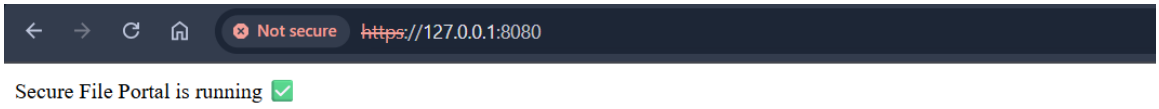
- app.py : Flask application entry point.

- crypto.py : Encryption and decryption logic.

- storage.py : File storage and retrieval logic using database.

- database.py : Database models and migration setup.

- config.py : Configuration file (database URL, KEK, etc.).



Workflow

1. Start the Flask server by running: python app.py

2. Upload a file using curl:

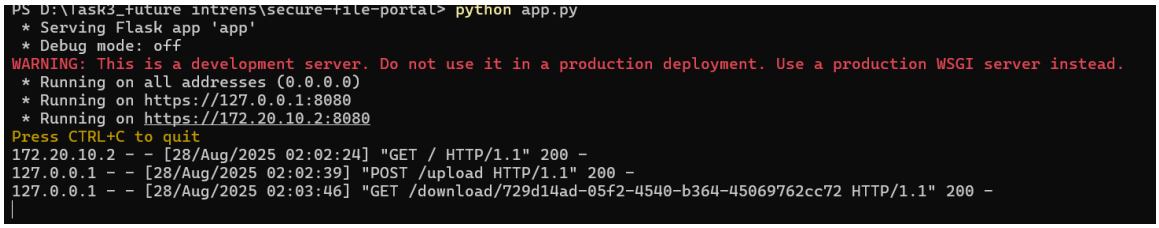
   curl.exe -k -F "file=@test.txt" https://127.0.0.1:8080/upload

   Response will return a unique file_id.

3. Download the file using:

   curl.exe -k -o downloaded.txt https://127.0.0.1:8080/download/<file_id>

4. The file is decrypted automatically upon download.



Conclusion

The Secure File Portal successfully demonstrates a secure system for handling files using Flask and cryptographic best practices. With AES-GCM encryption and KEK/DEK envelope encryption, it ensures that uploaded files remain confidential and protected.