FUTURE_CS_03

Intern Name: Vaibhav Gulati

Domain: Cyber Security

Task Title: Secure File Sharing System

Date: August 2025

💡 Objective

To build a user-friendly and ethically secure web application that allows users to upload files and either encrypt or decrypt them using symmetric cryptography (Fernet). The tool emphasizes simplicity, transparency, and data protection—core values guiding the development.

🔧 Technologies Used

- **Backend Framework**: Flask (Python)

- **Encryption Library**: cryptography.fernet

- **Frontend**: HTML + CSS (inline for simplicity)

- **File Handling**: Local file system storage (uploads/)

🗂 Core Features

- Upload files for **encryption or decryption**

- Symmetric encryption using a **persistent Fernet key**

- Simple and intuitive **index page navigation**

- Success page with **download links and feedback**

📁 Application Structure

| File / Folder	Description
main.py	Flask backend logic for routing and cryptography
templates/	Contains HTML files: index, preview, success
uploads/	Stores encrypted/decrypted files
secret.key	Saves generated encryption key for reuse

🌐 Web Pages Overview

1. index.html

- Minimal design with two clear action buttons: Encrypt and Decrypt
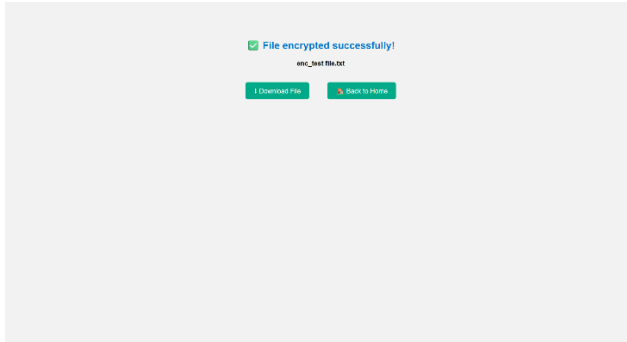- Uses light colors and friendly icons for accessibility
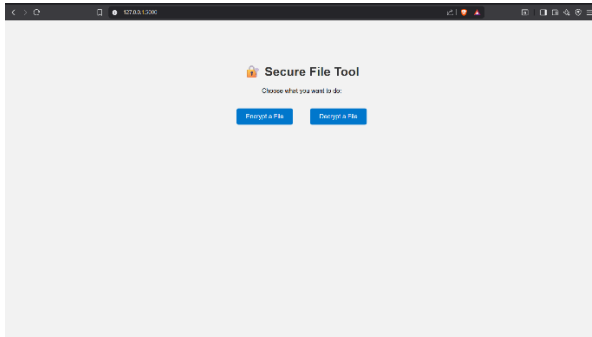
2. preview.html

- Displays a file upload form
- Adjusts text and submit button based on the selected action
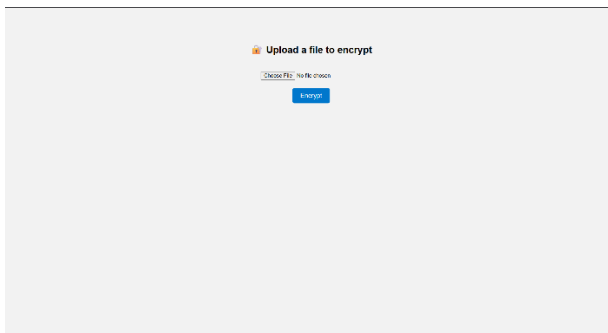
3. **success.html**

- Confirms successful processing of file

- Includes direct download link and navigation back to home

🔐 Cryptographic Approach

- **Fernet** provides encryption using AES in CBC mode with HMAC for integrity

- Key is generated once and stored persistently in secret.key

- Ensures repeatable and secure decryption without key loss

💬 Design Philosophy

- **Trust through transparency**: No hidden logic or data storage

- **User empowerment**: Gives users control over their file security

- **Ethical simplicity**: Easy navigation and visually calm interface