Information Security Project

Secure File Sharing System

Group Members

Mujtaba Haider (21L-5613)

Kamran Ishtiaq (21L-6253)

Khurram Imran (21L-6256)

Project Overview

This project aims to create a secure, web-based file-sharing platform that prioritizes data privacy. Files uploaded to the system are encrypted on the client side before they reach the server, ensuring the server never has access to the unencrypted content. When a recipient downloads a file, they will decrypt it on their own system. This client-side encryption/decryption approach prevents any unauthorized access and keeps data secure throughout its journey.

Objectives

The main objectives of this project are:

- To provide a secure platform for file sharing using AES encryption.
- To enable end-to-end data protection by encrypting files on the client side before upload and decrypting on the client side after download.
- To implement a straightforward and intuitive interface for file sharing while maintaining a high standard of data security.

Technologies Used

- Python: Core backend logic and integration with encryption mechanisms.
- Flask: Web framework for backend routing, API endpoints, and server configuration.
- Cryptography Library: To implement AES encryption and decryption.
- HTML/CSS: Frontend interface for file upload, download, and user interactions.
- SQLite: Lightweight database for storing user information and file metadata.

Project Scope and Features

User Authentication and Secure Session Management

- Users can securely register, log in, and manage their sessions.
- Authentication will be managed with hashed passwords, stored in the database, ensuring user information remains secure.
- Each session will be protected with secure tokens to prevent unauthorized access.

File Encryption and Decryption

- AES encryption is applied to files on the client side before upload, ensuring the server only stores encrypted files.
- Upon download, the client will decrypt the file locally to access the original content.
- File encryption and decryption are managed by a robust, well-tested encryption library to ensure data security.

Web Interface for File Handling

- User-friendly web interface to facilitate file uploads and downloads.
- Clear navigation for users to upload, access, and download encrypted files.
- Encrypted file handling will ensure only authorized users can download and decrypt files.

Division of Work Among Team Members

The project is divided into three main sections, each handled by a dedicated team member:

1. User Authentication, Database Setup, and Secure Session Management
    - Implement user registration and login with secure password hashing and storage.
    - Set up an SQLite database to store user data and file metadata.
    - Manage secure sessions to maintain user authentication and prevent unauthorized access.
2. File Encryption and Decryption Logic, and Integration
    - Develop client-side AES encryption for files before upload.
    - Implement client-side decryption for downloaded files.
    - Integrate encryption and decryption into the file upload and download flows.
3. Web Interface for File Upload/Download and Encrypted File Handling
    - Design and build a responsive and user-friendly interface for file sharing.
    - Ensure intuitive controls for file upload and download with clear indications of file status.
    - Manage frontend/backend communication to support encrypted file handling.

Expected Outcomes

- A secure, end-to-end encrypted file-sharing platform accessible via a web interface.
- A reliable user authentication and session management system.
- Complete file encryption and decryption workflows ensuring client-side privacy.
- An easy-to-navigate interface that simplifies encrypted file sharing for users.

Conclusion

This project will deliver a highly secure web-based file-sharing platform with end-to-end encryption. By encrypting files client-side, it provides data privacy even when files are stored on a server. The team members will collaborate to

build a well-integrated, secure, and user-friendly system that meets modern data protection standards.