Secure File Storage System with Encryption and Access Control Using File Handling

Submitted by:

Labor, Kim C.

Eng, Marc Russel R.

Fernandez, Arzay D.

Submitted to:

Dela Peña, Jerome

February 21, 2025

TABLE OF CONTENT

1. Introduction

This document provides an overview of the user authentication and file encryption system. The system allows users to register, log in, and manage text files securely using encryption and decryption features.

2. Features

- **User Authentication:** Secure login system with password hashing.
- **User Registration:** New users can register with a unique username and password.
- **Role-Based Access:** Admins have additional privileges over regular users.
- **File Management:** Users can create, encrypt, and decrypt text files.
- **Security Measures:** File integrity verification, bcrypt password hashing, and AES encryption.

3. User Roles

Admin:

- Can create and delete users.
- Can encrypt and decrypt any file.
- Can view all files and users.
- Can create admin-only files.

Regular User:

- Can only manage their own files.
- Can create, encrypt, and decrypt their own files.
- Cannot view other users' files.

4. System Flow

1. The program starts and displays the Login Screen.
2. The user enters a username and password:
    - If valid, the user is redirected to their respective menu (Admin/User).
    - If invalid, an error message is displayed.
3. In the Admin Menu, the admin can manage users and files.
4. In the User Menu, the user can manage their own files.
5. Users can encrypt and decrypt their files.
6. The system ensures file integrity before decryption.
7. Users/Admins can log out and return to the login screen.

5. File Management

- Creating Files: Users can create new text files and add content.
- Encrypting Files: Files are encrypted using AES encryption (Fernet).
- Decrypting Files: Users can decrypt their own files if they have permission.
- File Integrity Check: The system verifies if an encrypted file has been tampered with.

6. Security Measures

- **Password Hashing:** User passwords are hashed using bcrypt.
- **File Encryption:** Files are encrypted with a secure AES key.
- **Integrity Check:** The system calculates a file's hash before and after decryption.
- **Restricted Access:** Admins cannot modify user-owned files directly.

7. Graphical User Interface (GUI)

- The system is built using **Tkinter**.
- The **Login Screen** has input fields for username and password.
- The **Admin Menu** has buttons for user and file management.
- The **User Menu** has buttons for file management.

- Message boxes are used to display notifications and errors.

8. Conclusion

This system provides a secure method for managing user authentication and file encryption. With role-based access control, password security, and integrity checks, it ensures a reliable environment for file storage and protection.