Project Title: Secure File Storage System with AES

Introduction

Storing files securely is critical in cybersecurity. This project encrypts files using AES-256 and verifies integrity using hashing, ensuring both confidentiality and data consistency.

Abstract

This project uses the `cryptography` module (Fernet) for AES encryption and `hashlib` for SHA-256 file verification. It demonstrates how to securely encrypt, store, and retrieve files with integrity checks in a CLI environment.

Tools Used

- Python

- Cryptography (AES via Fernet)

- Hashlib (SHA-256)

Steps Involved

1. Generate AES-256 key and store securely.

2. Encrypt a text file and save as `.enc`.

3. Generate a SHA-256 hash of the original file.

4. Decrypt the file and compare hash values.

5. Print a message verifying integrity after decryption.

Conclusion

The project successfully secured files using strong encryption and verified their integrity, offering a basic model of secure file storage that is practical, portable, and easy to deploy.