Secure File Storage System with AES

Introduction

This project is a secure file storage system that enables users to encrypt and decrypt files using AES-256 encryption. It ensures that stored files are protected from unauthorized access, while providing a user-friendly interface for interaction.

Abstract

The objective of this project is to develop a local file storage system that encrypts files using AES (Advanced Encryption Standard) before saving. The project uses the 'cryptography' library in Python for AES encryption and decryption, and PyQt5 for creating a graphical user interface. The system also includes features for verifying file integrity using SHA-256 hashing and maintains metadata securely.

Tools Used

1. Python 3.x
2. cryptography (AES)
3. PyQt5 (GUI)
4. hashlib (SHA-256)
5. json (metadata storage)

Steps Involved in Building the Project

1. User uploads the file via the GUI.
2. File is encrypted using AES (Fernet).
3. Encrypted file is saved with a '.enc' extension.
4. Metadata (filename, timestamp, hash) is saved securely.
5. Decryption retrieves and verifies the original file using metadata.

Conclusion

Secure File Storage System with AES

This secure file storage system ensures confidentiality and integrity of sensitive files using industry-standard encryption.

It is simple to use, lightweight, and ideal for personal and professional data protection scenarios.