Name:- Rudrapriy
Malgundkar

AES Secure File Storage System – Project Report

Abstract

This project implements a secure file storage system using AES-256 encryption. It allows users to encrypt, decrypt, and verify files using a password-derived key. The system ensures confidentiality, integrity, and tamper detection through authenticated encryption (AES-GCM) and metadata-based verification.

Introduction

With increasing digital threats, securing sensitive files has become essential. This project provides a lightweight and robust encryption tool that protects files from unauthorized access. By using AES-256 and PBKDF2-based key derivation, the system ensures strong encryption while remaining user-friendly.

Tools Used

- Python 3
- Cryptography library (AESGCM, PBKDF2-HMAC-SHA256)
- ReportLab (for report generation)
- Standard Python modules: hashlib, json, os, argparse

Steps Involved in Building the Project

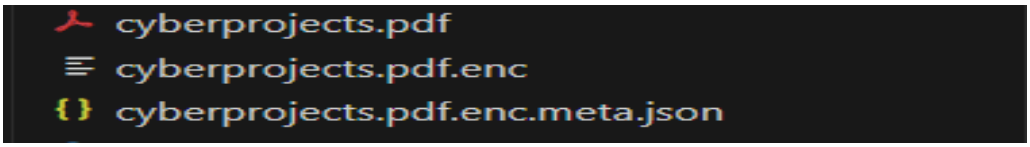
1. Designed the encryption workflow using AES-GCM for confidentiality and integrity.
2. Implemented PBKDF2 key derivation to convert passwords into secure 256-bit keys.
3. Built encryption and decryption functions with automatic metadata creation.
4. Added SHA-256 hashing for tamper detection and verification.
5. Developed a command line interface to perform encrypt, decrypt, and verify operations.
6. Generated a structured metadata file containing salt, nonce, and file integrity values.

Screenshots of the Project

Encryption of the file

```
C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\aes_secure_storage.py:105: DeprecationWarning: datetime.datetime.utcnow() is deprecated and schedul
ed for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  "timestamp_utc": datetime.utcnow().isoformat() + "Z",
Encrypted: C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\cyberprojects.pdf -> C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\cyberprojects
.pdf.enc
```

Creation of encryption and json file



Decryption of the file

```
PS C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project> python aes_secure_storage.py decrypt "C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\cyb
erprojects.pdf.enc"
Password:
Decrypted: C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\cyberprojects.pdf.enc -> cyberprojects.pdf
```

Verification of the file

```
PS C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project> python aes_secure_storage.py verify "C:\Users\Shreepad Malgundkar\OneDrive\Desktop\Project\cybe
rprojects.pdf.enc"
Password:
OK: SHA256 matches metadata.
```

Conclusion

The AES Secure File Storage System successfully provides a safe and reliable method to protect files using modern cryptographic standards. The project demonstrates key concepts in encryption, integrity checking, and secure key derivation, making it suitable for academic, professional, and practical cybersecurity applications.