**🔒 Security Overview – AES File Upload/Download Portal**

**Project:** Secure file upload/download portal using **Flask + AES encryption**  
**Purpose:** Protect files at rest and in transit, demonstrate secure web file handling

**🛡 Security Objectives**

* **Confidentiality:** Encrypt files before storage
* **Integrity:** Detect tampering via decryption checks
* **Access Control:** Secure upload/download endpoints
* **Minimal Exposure:** Separate directories for encrypted vs decrypted files

**🔑 Encryption Details**

| **Feature** | **Implementation** |
| --- | --- |
| Algorithm | AES (Advanced Encryption Standard) |
| Mode | CBC (Cipher Block Chaining) |
| Key Size | 256-bit (session-generated) |
| IV | Random per file |

**⚠️ Threats & Mitigations**

| **Threat** | **Mitigation** |
| --- | --- |
| Unauthorized access | AES encryption; isolate storage directories |
| Interception during transfer | Use HTTPS (production) |
| Malicious file uploads | File validation; separate encrypted storage |
| Key leakage | Use environment variables or key vaults (production) |

**🔧 Security Controls**

* Files stored as .enc → decrypted only for download
* Upload/download routes validate file names & paths
* Temporary decrypted files stored in separate folder
* Future enhancements: Authentication, rate-limiting, HTTPS

**📊 Risk Analysis**

| **Risk** | **Likelihood** | **Recommendation** |
| --- | --- | --- |
| Key leakage | Medium | Secure storage (env vars / vaults) |
| Malicious uploads | Medium | Validate file type & sanitize input |
| Transfer interception | High if HTTP | Use TLS/HTTPS |
| Decryption errors | Low | Detect integrity issues on decrypt |

**✅ Recommendations for Production**

1. Enable **HTTPS/TLS** for all web traffic
2. Implement **authentication & authorization** for endpoints
3. Use **secure key management** instead of session-only keys
4. Sanitize and validate uploaded files
5. Conduct **periodic security audits**

**Outcome:**

* Demonstrates secure file handling in web applications
* Strong foundation for production deployment with recommended enhancements