Secure File Sharing System

(Internship Task 4 – Internee.pk)

1. Introduction

Secure file sharing is a key requirement for organizations that exchange. sensitive information with third parties. Conventional file sharing techniques, such as email attachments or public links, which often leave data vulnerable to security threats including unauthorized access and data leakage. This task is about designing a secure file sharing system that ensures confidentiality, integrity, and controlled access to files. The system utilizes encryption, private cloud storage, and signed URLs to securely exchange files. This assignment was done as a part of the Cybersecurity Internship at Internee.pk.

2. Objective of the Task

The primary objective of this task is to ensure secure file exchange between Internee.pk and external users. The specific goals include:

- Encrypting files before uploading them to cloud storage.
- Storing files securely in a private cloud environment
- Sharing files using temporary and controlled access links
- Preventing unauthorized or public access to sensitive data

This approach ensures that files remain protected during upload, storage, and download.

3. Overview of Secure File Sharing

Secure file sharing involves multiple security layers to protect data. In this task, the system follows a structured security approach:

- Files are encrypted before being uploaded.
- Encrypted files are stored in private cloud storage.
- Access is provided through signed URLs with expiration times.
- Files are decrypted only by authorized users.

This layered approach reflects real-world security practices used by organizations.

4. File Encryption Using AES-256

Before uploading files to the cloud, all files are encrypted using. AES-256 encryption. AES-256 is a robust symmetric encryption algorithm commonly used to secure confidential information. Encryption is the process of making data unreadable. Even if an If the unauthorized user can access the file, the data is still protected without the proper decryption key. This ensures confidentiality of files both during storage and transfer.

5. Cloud Storage Implementation

The encrypted files are maintained in a secure cloud storage setup using Amazon S3. The S3 bucket has public access blocked to prevent unauthorized access. Only the bucket owner has permission to upload, read, or manage files. This ensures that files are stored in a secure manner and are not accessible to the public on the internet.

6. Signed URLs for Secure File Access

For securely transferring files, pre-signed URLs are used for encrypted files stored in the cloud. A signed URL gives temporary access to a private file without making it public. Each signed URL has an expiration time. After the time limit is reached, Consequently, the link will automatically become invalid, and further access will not be this ensures that file sharing is done in a secure manner while still adhering to a strict access control.

7. Secure Download and Decryption

Files are downloaded using signed URLs and remain encrypted during transfer.
After download, the file can only be accessed by decrypting it using the
correct AES-256 secret key.

This ensures that:

- Files remain protected during transmission.
- Only authorized users can access the original content.
- Unauthorized users cannot read the file even if they download it.

8. Data Sources Used

The following data sources were used for testing purposes:

- Sample reports provided by Internee.pk.
- Test datasets obtained from Kaggle.

All datasets used in this task are non-sensitive and intended only for testing and demonstration.

9. Tools and Technologies

The following tools and technologies were used in this task:

- AES-256 Encryption
- Amazon S3 (Cloud Storage)
- AWS Pre-Signed URLs
- Kaggle (Test Data)

10. Security Benefits of the System

The implemented secure file sharing system provides several benefits:

- Protection of files through strong encryption
- Secure cloud storage with restricted access
- Controlled file sharing using time-limited URLs.
- Reduced risk of data leakage or unauthorized access

This approach ensures that sensitive information is shared securely.

11. Conclusion

This task demonstrates how secure file sharing can be implemented using encryption, cloud storage, and controlled access mechanisms. By combining AES-256 encryption, private Amazon S3 storage, and signed URLs, files can be exchanged securely without exposing sensitive data.Overall, this task provided hands-on experience with real-world file security concepts and strengthened understanding of secure data sharing practices used in professional environments.