Web based application for secure data storage using hybrid cryptography

Team Details
1. P Shivani (20eg105237)
2. Juhi Mohta (20eg105221)
3. K Hemasri (20eg105240)

Project Supervisor
Name : DR.V.Subrahmanyam
Designation : Asso.professor

Introduction

The protection of sensitive data and information is of utmost importance in the modern digital age. As cyberattacks and data breaches become more frequent, it is essential to provide safe file storage on a local host. By using hybrid cryptography techniques to safeguard files kept on a local host, this project tries to address this problem.

This project offers a reliable and effective solution for securing local file storage by combining these two techniques.

Problem Statement

In an era of increasing digitalization, the need for secure file storage solutions is crucial, particularly when it comes to sensitive or confidential data stored on local machines. Traditional encryption methods have their limitations, often posing challenges in terms of both security and user-friendliness.

In the realm of data security, traditional file storage systems are vulnerable to a multitude of threats, including unauthorized access, data breaches, and malicious attacks. To safeguard the confidentiality and integrity of stored files, an advanced security mechanism becomes imperative.

Traditional symmetric encryption algorithms, such as AES, are efficient in terms of speed and resource usage but have challenges related to key management. Asymmetric encryption algorithms, like RSA, address these key management issues but tend to be slower and resource-intensive for bulk data encryption.

Proposed Method

The project aims to address the critical need for secure file storage on a local host by implementing a robust solution based on hybrid cryptography techniques.

This project seeks to develop a hybrid cryptography method that combines the strengths of both symmetric and asymmetric encryption techniques, for secure file storage on a local host.

The project involves encryption and decryption processes, key management, and authentication mechanisms to protect files from unauthorized access and tampering.

In this approach, a random symmetric key is generated for each file, and the file is encrypted with this key. The symmetric key is then encrypted using an asymmetric key pair (public-private key) and stored alongside the encrypted file. This combination of symmetric and asymmetric encryption offers a secure and efficient solution for local file storage.

Proposed Method

Scenario: Bob wants to securely store a sensitive spreadsheet on his server, ensuring confidentiality and integrity.
Local Host: Bob's server
Encryption Algorithms: AES (Symmetric Encryption), RSA (Asymmetric Encryption)
Keys:
Symmetric Key (AES_Key)
Public and Private Key Pair (RSA_Public_Key, RSA_Private_Key)
Key Generation:
Symmetric Key (AES_Key) for AES encryption.A pair of Public and Private Keys (RSA_Public_Key, RSA_Private_Key) for RSA encryption.
File Encryption:
Encrypt the sensitive spreadsheet using the Symmetric Key (AES_Key) with AES encryption.
Key Distribution:
Use the recipient's public key (RSA_Public_Key) to securely share the Symmetric Key (AES_Key) for decryption.

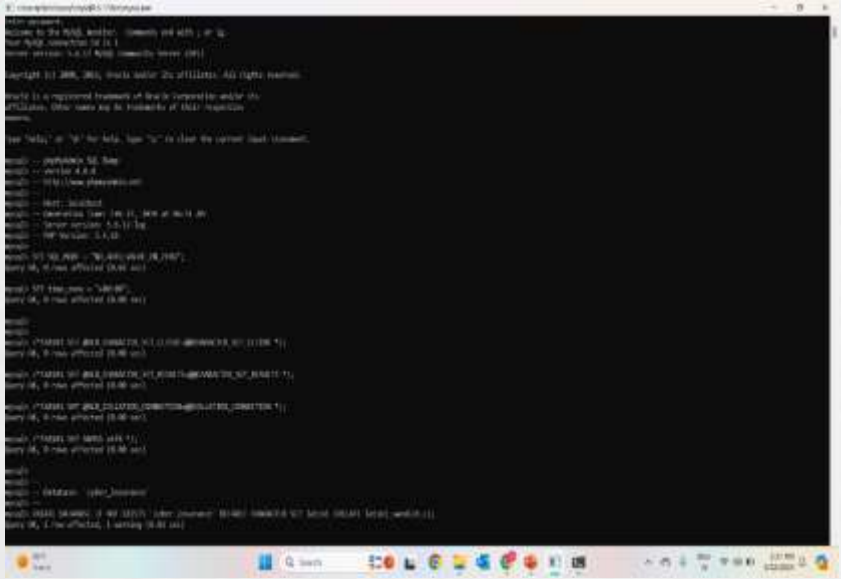
File Decryption:
When an authorized user requests access to the spreadsheet, use their private key (RSA_Private_Key) to decrypt the Symmetric Key (AES_Key).Use the decrypted Symmetric Key (AES_Key) to decrypt the sensitive spreadsheet. In our project we ensure the security with the help of one time password generation. An OTP is generated which requested for download and sent to the mail.

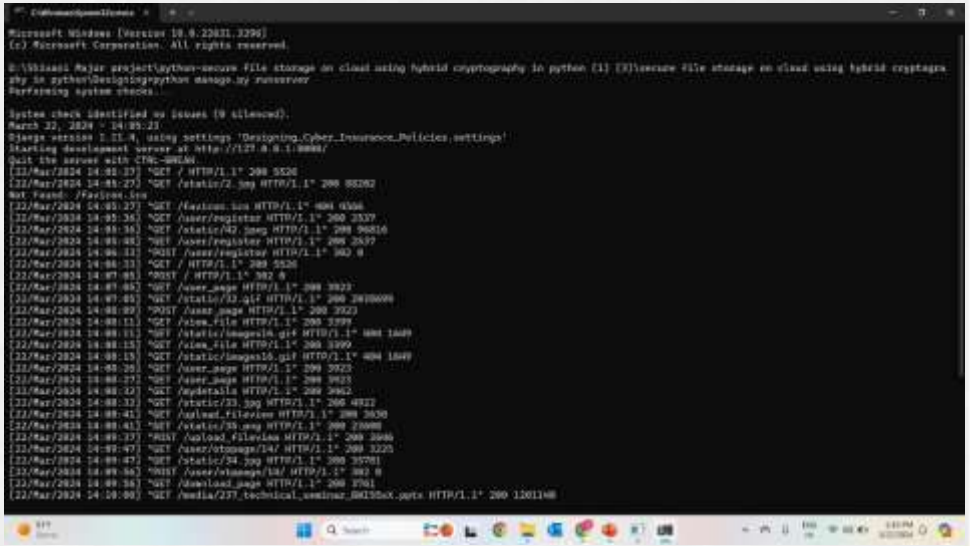
Experiment Environment

Software Requirements

- Operating system: Windows Family.
- Coding Language: J2EE (JSP,Servlet,Java Bean)
- Data Base: mySQL.
- Web Server: Wamp server
- Tools: Django and python

Experiment Screen shorts





Experiment Results


Web based application for secure data storage using hybrid symmetric algorithm
REGISTRATION


MY DETAILS
UPLOAD PAGE
VIEW UPLOAD DOCUMENT
DOWNLOAD REQUEST PAGE
FEEDBACK
LOGOUT

Experiment Results

Experiment Results

Finding

Justification

1.What are parameters improved by your method

2.Mathametic formulas for calculating parameter values

3 why your parameter values improved?