

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



```
per to the MAS, and but Tomaco, and add to an in-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       invesselt Mindows [Version 18.6.22631.3296]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     c) Astroport Corporation. All rights recorved
   tall to been been made by a stillers. All right market
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          Wilsest Major project/sythen-secure FILe storage on cloud using hybrid cryptography to python [1] [3] became FILe storage on cloud using hybrid cryptography to python [1] [3] became FILe storage on cloud using hybrid cryptography
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               sty in sythen Gerigningraythan damago sy sumerver
Perferming eyetse checks
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   outes theck identified on issues (9 sitesced)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   arch 32, 2824 - 14/85:25
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Djaga strika I II.4, using settings "Designing Opher Insursoce Policies settings"
tarting deselagant verser in 1919/7127 & S.1.9868/
julk the karsen with CTM-SMIAN
                     to be I have always and the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     II/Aur/1824 14.82.27] "GCT / HTTM/L.1" 368 5526
II/Aur/1824 14.81.27] "GCT /statle/2_3ep HTTM/L.1" 268 85262
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   or Found: /Factions.fem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   22/Aur/2020 (4.00.27) "NET / Heptons ton MTT0/1.1" see 4566
22/Aur/2020 (4.00.27) "NET / Heptons ton MTT0/1.1" see 4566
22/Aur/2020 (4.00.20) "NET / Auro/register HTT0/1.1" 200 2007
22/Aur/2020 (4.00.20) "NET / Auro/register HTT0/1.1" 200 2007
22/Aur/2020 (4.00.20) "NET / Auro/register HT0/1.1" 200 2007
22/Aur/2020 (4.00.10) "NET / Auro/register HT0/1.1" 200 2007
22/Aur/2020 (4.00.10) "NET / Auro/register HT0/1.1" 200 2007
   list, of Joseph Affining Chief and I
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   22/Mar/2004 (4:00:01) 7001 (1000/0000000 1107/L1* 100.0 0 22/56ar/2004 (4:00:01) 7007/ (1107/L1* 200.520) 22/56ar/2004 (4:00:01) 7002 (7:00:00) 7007/ (1107/L1* 200.52) 7005/ (22/56ar/2004 (4:00:01) 7007/ (1107/L1* 200.52) 7005/ (22/56ar/2004 (4:00:01) 7007/ (100:00:00) 7007/ (1107/L1* 200.50) 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              23/4ar/2004 14:08:29] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:29] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:11] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:11] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:10] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:10] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:29] 2027 Austr page NIDVL 1: 200-2022

23/4ar/2004 14:08:19] 2027 Austr page NIDVL 1: 200-2022

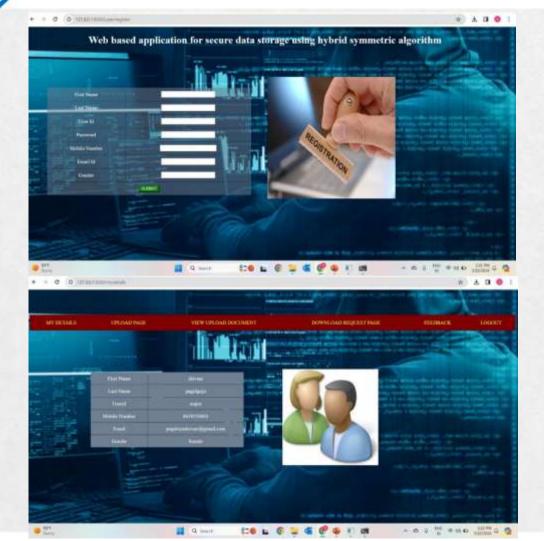
23/4ar/2004 14:08:19] 2027 Austr page NIDVL 1: 200-2020

23/4ar/2004 14:08:19] 2027 Austr page NIDVL 1: 200-2020
              PROBLEM STATE CONTRACTOR, NOT CO. THE ARROWANCE OF THE STATE OF
            PORTE OF BUILDING OF STREET, BOARDS OF BUILDING
     CHARLEST AND DELOTED COMMITTEE BUILDING CONTINUES.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   22(4a)/234 A 87 37 983 (a) a) a (1797) 1 268 3966
22(4a)/234 A 87 37 937 (a) a) a) a (1797) 1 268 3966
22(4a)/234 A 87 37 937 (a) a) a (1797) 1 39 322
22(4a)/234 A 87 37 937 (a) a) a (1797) 1 39 327
22(4a)/234 A 87 38 93 (a) a) a (1797) 2 32 32 32
22(4a)/234 A 87 38 93 (a) a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a (1797) 2 32 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) a (1797) 2 32
22(4a)/234 A 87 38 (a) 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   22/Mar/2029 14:10:00) "GET /mmdia/237 technical_meminar_SECSDaX.parts HTTP/1.1" 200 1201108
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ----
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         - - - T TOO STORY OF
```

Experiment Results



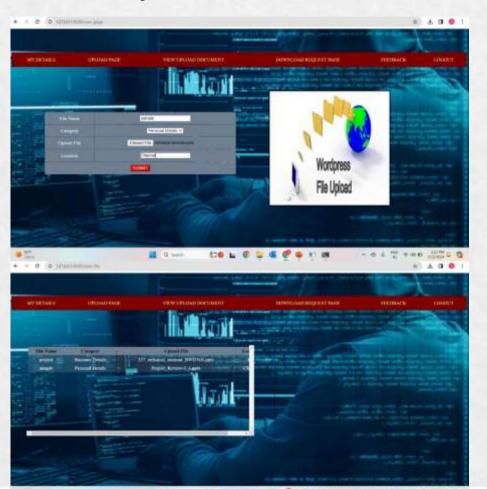






Experiment Results





Experiment Results





ANURAG

Finding



Justification



1. What are parameters improved by your method

2. Mathametic formulas for calculating parameter values

3 why your parameter values improved?