Indian Institute of Information Technology Pune
Department of Computer Science Engineering 2022-2023

SECURE CLOUD USING HYBRID CRYPTOGRAPHY

BY :-
G.MANOJ REDDY (112015054)
R.SURAJ RAO (112015108)
U.VINOD KUMAR (112015158)
V.BHARADWAJ (112015160)

Mentor : Dr. Mahendra Pratap Yadav

OUTLINE

- Introduction
- Motivation
- Objective
- Literature survey
- Methodology
    - Algorithms used
        - RSA
        - AES
- Future scope
- References

INTRODUCTION

Nowadays, security in cloud is a rising issue. Since the majority of companies changing their old ways of storing data from traditional to Cloud storage, data security is a main hitch in adopting cloud computing for many organizations.

With the advancements in modern technology and easy access to the internet, traditional methods such as the Caesar Cipher were not a huge bottleneck in front of cryptanalysts or adversaries who like to break into a system or message just for the sake of pride, enjoyment or fame.

The aim of this project is to develop a secure cloud storage application for Google Drive, box, Dropbox etc. We are designing a suitable key management system for our application to share files securely.

MOTIVATION

- Need of data security is an essential issue in the domain of computing traditionally.
- There has been a tremendous increase in the usage of cloud storage for storing files and these files are prone to leakage.
- There has to be a solution, and encryption of files is the only way. Our motive is to develop a system which encrypts the files in our cloud and decrypts when it is downloaded to the local system.

OBJECTIVE

- The main objective of this project is to make files more secure using hybrid encryption.
- To develop an application which takes a file to encrypt and upload it on the cloud storage so even if there is a data breach the file is seen in encrypted form only and original data is unknown
- To also extend the feature of downloading the uploaded file from the cloud and decrypt the file without altering the original contents of the uploaded file.

LITERATURE SURVEY

Author	Title	Techniques	Year
Uttam Kumar, Jay Prakash	Secure file storage using Hybrid Cryptography	Asymmetric key cryptography	2020
Sanjeev Kumar, Garima Karnani.Madhu Sharma Gaur, Anju Mishra	Cloud Security using Hybrid Cryptography Algorithms	DES, RSA models	2021
Alibi Orobosade, Thompson Aderonke, Alese Boniface, Arome J. Gabriel	Cloud application security using hybrid encryption	AES,ECC Algorithms	2020
Shruti Kanatt,Amey Jadhav,Prachi Talwar	Review of Secure File Storage on Cloud using Hybrid Cryptography	AES,RSA,BLOWFISH	2020

Aditya SadanandGhadi	Secure File Storage Using Hybrid Cryptography	Digital Signatures,AES,Steganography,Dynamic Hashing	2020
B.Swathi, Sri .Dr. Bhaludra Raveendranadh Singh	Secure file storage in cloud computing Using hybrid Cryptography Algorithm	Blowfish,RSA	2017
Moulika Bollinadi, Vijay Kumar Damera	Cloud Computing: Security Issues and Research Challenges	APIs,Iaas,AWS	2017

MAIN SECURITY CHALLENGES IN CLOUD

- Data Loss
- Interference of Hackers and insecure API's
- User Account Hijacking
- Changing Service Provider
- Lack of skill
- Denial of service attack

HYBRID CRYPTOGRAPHY

- The hybrid encryption algorithm combines the advantages of fast encryption speed of AES algorithm, easy management of RSA algorithm key, and digital signature to ensure the secure transmission of confidential documents.

Hybrid encryption includes:

- RSA Encryption Algorithm
- AES Encryption Algorithm

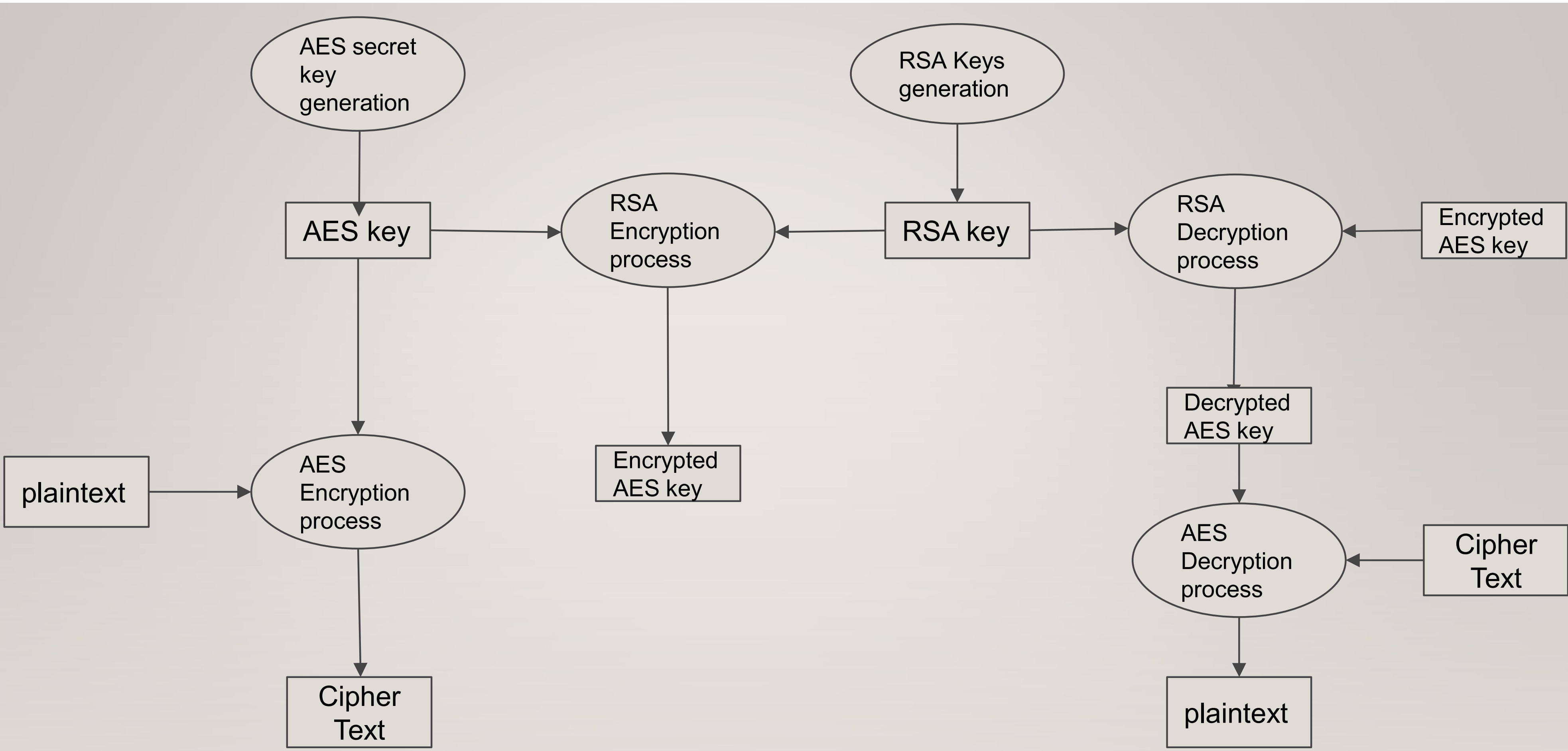
Working:

- Creates directories and files for generated RSA and AES keys and store it.
- For encryption takes the AES key file reads it and decrypt it using RSA private key and then encrypt the selected file using AES key and store at local system.
- For decryption takes the AES key file reads it and decrypt it using RSA private key and then decrypt the selected file using AES key and store at local system.

METHODOLOGY

We have a thought of doing hybrid model which is a mixture of AES and RSA key algorithm,which can be achieved by following methodology:

1. Select the file from local system which user want to encrypt or decrypt.
2. If the user wishes to encrypt the file to ensure security, he would hit the encryption tab.
3. And if he wishes to decrypt the file,then he would hit the decryption tab.
4. AES algorithm is used which allows the user to store and access their data securely in the local system by encrypting the data and decrypting the data after downloading.
5. The keys for this AES algorithm is then secured using a different algorithm called RSA and then the key for this algorithm is provided to the user as private key



Flow Chart of the hybrid cryptographic model

ALGORITHMS USED

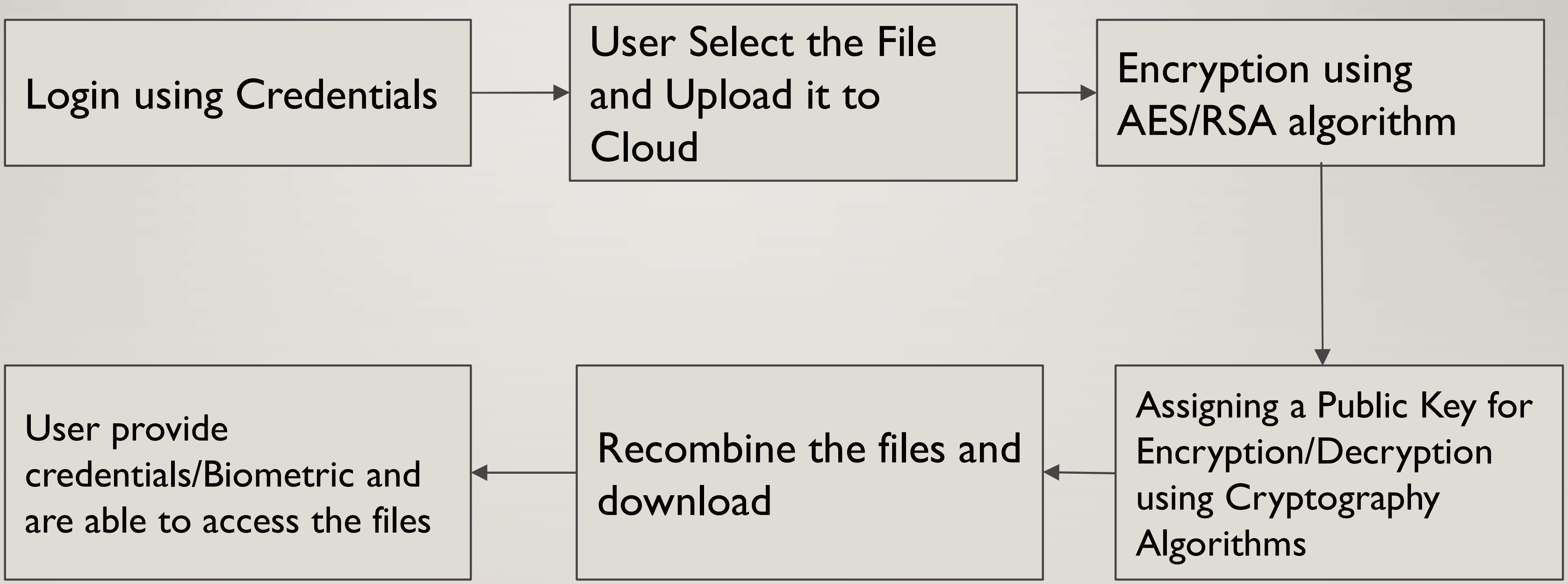
AES:-

- The Advanced Encryption Standard (AES) also known as 'Rijndael' is a symmetric-key block cipher algorithm.
- It takes plaintext in blocks of sizes 128, 192 and 256 bits, respectively.
- The AES algorithm has maximum block size of 256 bits whereas Key size is unlimited.The AES design is based on a substitution- permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network, thus making it stronger and faster than Triple-DES.

RSA

- RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key.
- As the name describes that the Public Key is given to everyone, and the Private key is kept private.
- The idea of RSA is based on the fact that it is difficult to factorize a large integer.
- The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers.
- Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long.

DESIGN AND IMPLEMENTATION PLAN



Login using Credentials

User Select the File and Upload it to Cloud

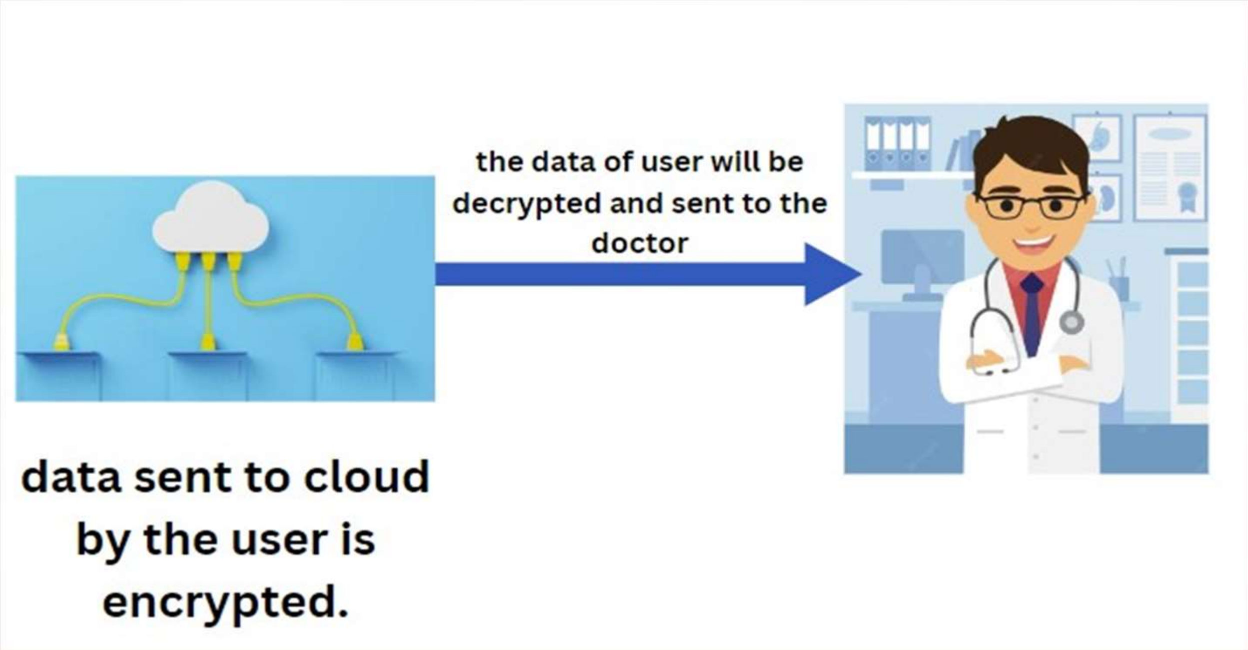
Encryption using AES/RSA algorithm

Assigning a Public Key for Encryption/Decryption using Cryptography Algorithms

Recombine the files and download

User provide credentials/Biometric and are able to access the files

- In medical field, the patient information must be confidential and should not be accessible to everyone.
- Whenever the patient’s personal health records need to be reviewed or updated, a private key is generated which allows primary healthcare providers to access the patient’s medical records.



the data of user will be decrypted and sent to the doctor

data sent to cloud by the user is encrypted.

FUTURE SCOPE

- The end result of the proposed system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography techniques.
- With the help of the proposed security mechanism, we are trying to accomplish better data integrity, high security, low delay, authentication, and confidentiality.
- The first step is to develop the encryption and decryption part of the file.
- In the next step we will focus on developing an user friendly interface which includes login and authentication where the owner can have various options that can be prompted on the file.

REFERENCES

[1]Uttam Kumar,Jay Prakash., 2020, July. Secure File Storage on Cloud Using Hybrid Cryptography. In *2020 International journal of creative research and thoughts(IJCRT)(ISSN 2320-2882)*

[2]Kumar, S., Karnani, G., Gaur, M.S. and Mishra, A., 2021, April. Cloud security using hybrid cryptography algorithms. In *2021 2nd International conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE.

[3]Orobosade, A., Aderonke, T., Boniface, A. and Gabriel, A.J., 2020. Cloud application security using hybrid encryption.

[4]Kanatt, S., Jadhav, A. and Talwar, P., 2020. Review of Secure File Storage on Cloud using Hybrid Cryptography. *International Journal of Engineering Research & Technology (IJERT)*.

[5]Aditya SadanandGhadi., 2020. Secure File Storage Using Hybrid Cryptography *International Journal of Innovation Science & Research Technology (IJERT)*.

[6]B.Swathi, 2 Sri .Dr. Bhaludra Raveendranadh Singh., 2017. Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm *International Journal of Advance Research in Science & Engineering (IJARSE)*.

THANK YOU!