**SECURE FILE SHARING ON CLOUD USING HYBRID CRYPTOGRAPHY**

**Guide Name :** Dr. L. Sai Ramesh

**Reg No. :** 2019272022

**Name :** ManjulaR.

**Course Name :** MCA(SS)

**ABSTRACT**

Cloud computing is an emerging paradigm that aims to provide computing resources, massive data storage capacity and flexible data sharing services. The explosive growth of data produced persuade business and users, driven by the cloud-top features, to outsource their data to the cloud storage systems.

However, the confidentiality and integrity of sensitive data in remote cloud servers are becoming a major concern. Data must be encrypted prior to storing it in the potentially untrustworthy cloud.

Existing traditional encryption systems impose a heavy burden of managing files and encryption operations on data owners. They suffer from serious security, efficiency, and usability issues, and some schemes are inappropriate for protecting cloud data. Here, a user-side encrypted file system, focused on providing a transparent encryption for stored and shared data. We utilize a hybrid encryption scheme structure based on symmetric and asymmetric methods.

**INTRODUCTION**

Secure File Sharing motive is to reduce the physical documents and empower sharing of e-documents over intervention.

The objective of this application is that individual’s documents and images can be secured in the cloud platform. It will help the user to protect their documents or files from an intruder and also prevent from losing manually.

**PROBLEM STATEMENT**

Cloud computing provides a flexible and convenient way for data sharing, offering broad social advantages as well as individuals.

However, there is a natural reluctance for consumers, since data often provide valuable information, to outsource the shared data directly to the cloud server.

Cryptographically improved control of access on the shared data should also be enforced.

**OBJECTIVE**

* To store the personal files and confidential documents on cloud platform.
* To share the shared files on cloud platform in the secured (encrypted) manner.
* To view or download the shared files from secured folder of cloud storage.

**ARCHITECTURE DIAGRAM**

Encrypt using AES and RSA

View File & Send Request

Receive and Enter file key

Decrypt using Random key

Download File

Secure Folder – shared files

Upload on Cloud

Encrypt using Random Key

Generate Random Key

Select File

Upload File

File Dataset

**ARCHITECTURE EXPLANATION**

The system is designed such that it works in the following way:

1. The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id, phone number, password for account etc.

2. The user then selects the file that is to be uploaded by browsing from local storage.

3. The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RSA.

4. The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.

5. The user also has the option of viewing the files that they have uploaded or have access to and downloading them.

6. On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration or sign-up.

7. Using this key, the user can download the decrypted or original file.

8. The system also provides a comparison with respect to security between the two hybrid encryption algorithm combinations i.e. AES and RSA hybrid combination.

**MODULES**

* User Registration
* Upload File on Cloud
* Download File from Cloud

**1.User Registration**

For accessing the service the user must first register yourselves. During the registration process various data like name, username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user’s profile picture.

**2. Uploading a File on Cloud**

• When the user uploads a file on the cloud first it will be uploaded in a temporary folder.

• Then user’s file will be split into N parts.

• These all parts of file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.

• These all parts of file will be encrypted using different algorithms that are AES, RSA. The key to these algorithms will be retrieved from the steganographic image created during the registration.

• After the split encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.

• Then Combining all Encrypted Parts of file.

**3. Download a File from the Cloud**

• When the user requests a file to be downloaded first the file is split into N parts.

• Then these parts of file will be decrypted using the same algorithms with which they were encrypted. The key to the algorithms for the decryption process will be retrieved from the steganographic image created during the registration.

• Then these parts will be re-combined to form a fully decrypted file.

• Then file will be sent to the user for download.

**TECHNOLOGY**

Development Platform : VS Code

Python – Backend

Flutter – Frontend

AWS – Cloud Storage

**REFERENCES**

* File Storage on cloud - <https://ijcrt.org/papers/IJCRT2007048.pdf>
* Secure data sharing for mobile cloud computing using RSA - <https://iopscience.iop.org/article/10.1088/1757-899X/1055/1/012108/pdf>
* Secry – Secure file storage on cloud - <https://www.slideshare.net/alinbabu2010/secry-secure-file-storage-on-cloud-using-hybrid-cryptography-236803722>