SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPT OGRAPHY

Project report submitted in partial fulfillment of
the Requirements for the
Award of the Degree of B.Tech in
Computer Science and Engineering

BY

Vaibhav Joshi	(Roll No. 2013566)
Vaibhav Bharti	(Roll No. 2013623)
Mukul Sharma	(Roll No. 2013390)

Under the Guidance
Of

Ms. Saloni Gulati

(Faculty From IBM)

Department of Computer Science and Engineering
Graphic Era Deemed to be University
Dehradun-248002
2022

CERTIFICATE

This is to certify that the project report entitled **Secure File Storage Using Hybrid Cryptography** being submitted by

Vaibhav Joshi	(Roll No. 2013566)
Vaibhav Bharti	(Roll No. 2013623)
Mukul Sharma	(Roll No. 2013390)

in partial fulfillment for the award of the Degree of Bachelor of Technology in Computer Science and Engineering (or Information Technology) to the Graphic Era Deemed to be University is a record of bonafied work carried out under my guidance and supervision.

The results embodied in this project report have not been submitted to any other University or

Institute for the award of any Degree or Diploma.

(**Ms. Saloni Gulati)**

Guide

ABSTRACT

In today’s world 99% people are more interested in sending and receiving data through internet and mobile data storage devices. But among those people don’t encrypt their data though they know that data contains personal information and the chances of data lose or hacking is very high. Information security has always been important in all aspects of life. It can be all the more important as technology continues to control various operations in our day-to-day life.

To store huge amount of data. We can retrieve data from cloud on request of users but the security of files stored on cloud server is very less, to provide the solution to these issues there are multiple ways. Cryptography techniques are more popular nowadays for data security.

Use of single algorithm is not effective for high level of security to data in cloud computing so using multiple layers of algorithm is very problematic as it increases the security but also increases the time for uploading and downloading.

So, in this project we have introduced new security mechanism using symmetric key cryptography algorithm. We have able to use AES, DES and RC6 encryption techniques to encrypt the single file by dividing the file into three separate file and then encrypting them along with that we will also be using LSB technique to enhance the security and file sharing Security breaches are rarely caused by poor cloud data protection. More than 40% of data security breaches occur due to employee error. Improve user security to make storage more secure. Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, user store data on Internet-connected servers. Data Centers manage these servers to keep the data safe and secure to access. Cloud-based solutions are increasingly in demand around the world. These solutions include everything from secure data storage to entire business processes.

ACKNOWLEDGEMENT

We would like to express our sincere thanks to **Ms. Saloni Gulati,** for her valuable guidance and support in completing our project.

We would also like to express our gratitude towards our HOD sir **Dr. Devesh Pratap Sing**h for giving us this great opportunity to do a project on Secure File Storage on Cloud Using Hybrid Cryptography. Without their support and suggestions, this project would not have been completed.

TABLE OF CONTENT

LIST OF FIGURES

1. INTRODUCTION

Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in the cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the security. This security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduced a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and stenography .

In this proposed system 3DES (Triple Data Encryption Standard), RC6 (River Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. All the algorithms uses 128-bit keys. LSB stenography technique is used to securely store the ley information. Key information will contain the information regarding the encrypted part of the file, the algorithms and the key for the algorithm. File during encryption is split into three parts. These individual parts of the e file will be encrypted using different encryption algorithm simultaneously with the help of multithreading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, DES and RC6 algorithm.

1.1 Background

Cloud computing has been around for a while now. It is not a novel technology but rather an innovative model for delivering services and information using current technologies. Fundamentally, cloud computing utilizes existing internet infrastructure to facilitate communication between client nodes and services or applications that reside on a remote server. CSP's (Cloud Service Providers) are responsible for offering cloud services that enable customers to create and utilize web services, much as internet service providers (ISP's) provide access to high-speed broadband to enable internet access. Unlike the internet, cloud platforms act more like an abstracted layer between computing resources and the involved low-level architecture. Rather than own physical computing infrastructure, cloud customers only have to pay subscription fees to a CSP to acquire cloud infrastructure and resources. The key idea with cloud computing is that the subscription model allows customers to save money that they would otherwise have expended on often-expensive resources such as hardware, software, and the attendant licenses. CSPs provide such services. This subscription model has so far proven popular with, observing that disciplined corporate subscribers have achieved cost reductions of up to 18% on information technology (I.T.) budgets and 16% on power costs of data centers.

The extensive adoption of cloud services has yet introduced various challenges for subscribers and CSPs. Various studies agree that establishing and maintaining the security of services and information stored on cloud infrastructures remains the most significant challenge. For example, contend that cloud-computing concerns, particularly the security of data and privacy protection, are the main factors inhibiting cloud storage’s further adoption. The study observes that the security concerns in this area of cloud computing arise from the fact that it is third parties who are usually unknown to clients that are responsible for data and infrastructure management on cloud platforms. The researchers note critically that any signs of security severance may precipitate the loss of customers and hence the cloud services business despite the efforts by CSPs to ensure the provision of highly secured password-protected accounts. agree that data security is the main issue with cloud storage and attribute the challenge to the fact that cloud storage involves multiple users sharing the same storage facilities. For the researchers, the security of data and information stored on cloud facilities may be compromised due to weak data access control and identity management mechanisms. The challenges above have so far necessitated the implementation of various technological measures to enhance the security of data and information stored on cloud platforms. While there is a wide range of security measures for cloud storage, this review will examine current perceptions regarding cloud storage security and hence analyze the role of hybrid cryptographic techniques and their future in cloud storage.

1.2Aims & Objective

II. To investigate current perceptions regarding the security of cloud storage.

III. To analyze the implementation of hybrid cryptography as it pertains to securing file storage on cloud infrastructure.

IV. investigate the future direction of hybrid cryptographic techniques on securing data, information, and services residing on cloud infrastructure.

1.2.1 Sub-Objective:

I. Development of UI/UX

Here we will develop the design of a user interface and create basic user interactive interface where the users will be prompted to for storing any file in our secure storage system. We will develop it according to the need of this project.

We may use technologies like HTML, CSS, Bootstrap, etc.

II. **Testing Algorithms**

Here we will parallelly test and configure our algorithms techniques defined for encryption and decryption of file.

We will test it locally on our pc’s datasets and check for any error or anomaly In the encryption or decryption method algorithms.

III. **Combining of Algorithms**

Here we will merge our already tested different encryption and decryption techniques into one.

We will again test it locally on our datasets should combining of these algorithms/methods give rise to any kind of error.

IV. **Connecting with Cloud**

Here firstly, we will connect our webpage to cloud where the user will store his/her file in a secure system.

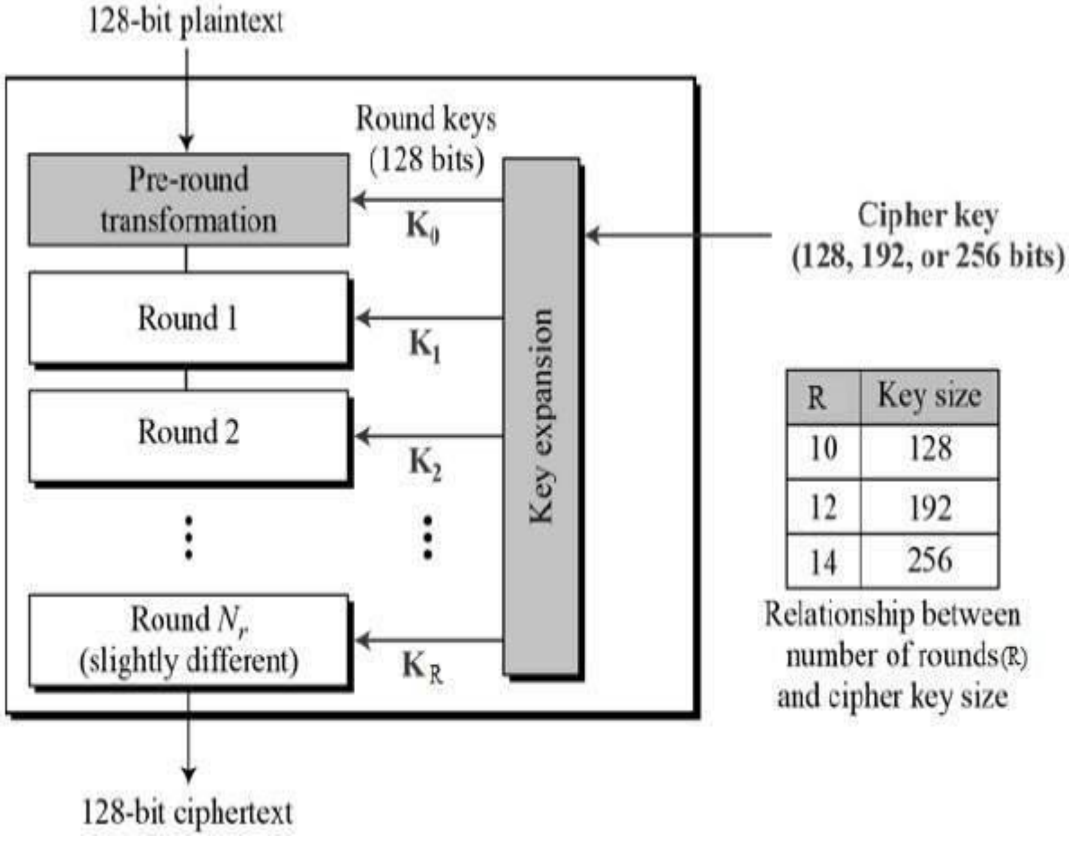
We will try to do some modifications to our website and if possible, add some additional features to make it easy to use.

2. LITERATURE REVIEW

2.1 Algorithm Used

1) Advanced Encryption Standard (AES)

The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continues serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations). All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 2.1 AES Algorithm Structure

AES algorithm is of three types namely AES-128bit, AES192bit, and AES-256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256-

bits, respectively. Rijndael method was enhanced to accept extra block sizes and also extra key lengths, but for AES, those functions were not inherited.

Till the current day, the AES algorithm is used many times and supported on both digital level and physical level. Furthermore, AES comprises of built-in limberness of key length, this allows a certain “future proof” against the process in the ability to perform comprehensive key searches.

2) Triple Data Encryption Standard (3DES)

In cryptography, 3DES is an inherited enhanced version of DES (Data Encryption Standard). In the Triple DES algorithm, DES is used trice to increase the security level. Triple DES is also referred to as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has following keying options:

1. All keys being different
2. Key 1 and key 2 being different & key 1 and key 3 is the same.
3. All three keys being identical.

The third option forms the Three DES. In triple DES the key size is increased to confirm addition security through encryption capabilities.

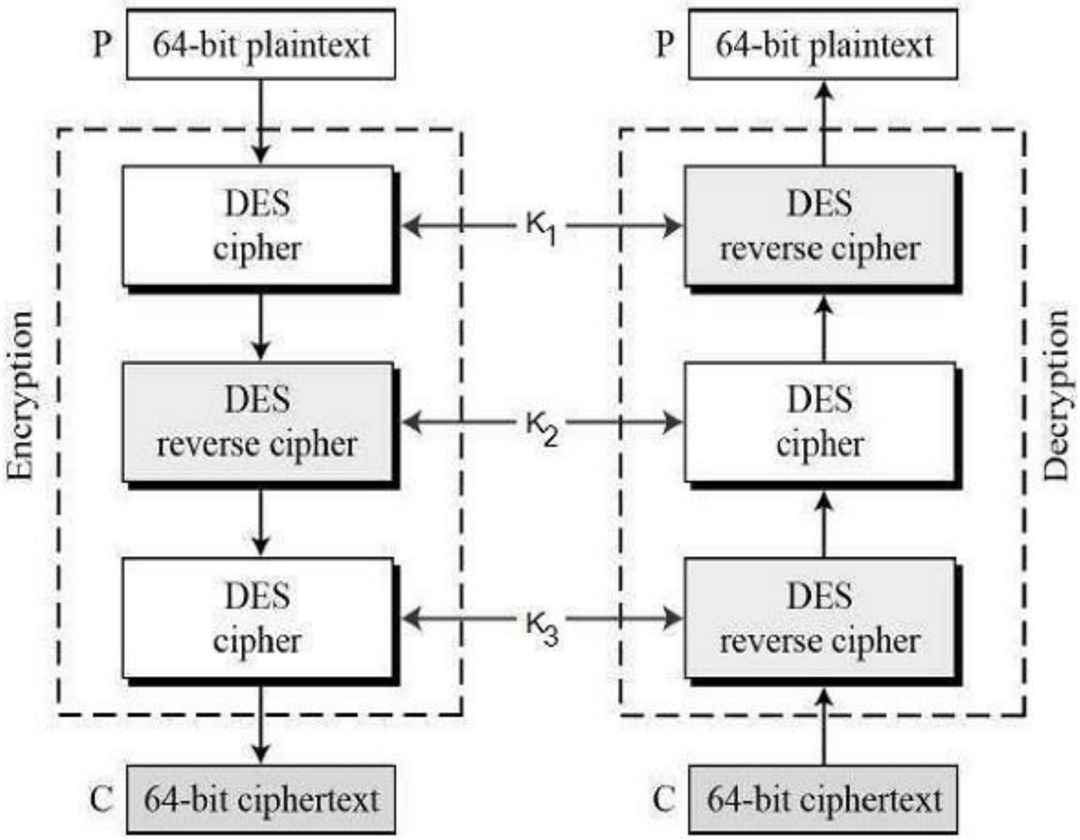


Figure 2.2 3DES Algorithm Structure

TDES is slowly invisible from use, it is maximally replaced by the AES (Advanced Encryption Standard). A far-reaching anomaly is in the digital payments industry, which still uses 2TDES and scatters standards on that basis (e.g. EMV, the standard for inter-operation of "Chip cards", and IC capable POS terminals and ATM's). This guarantees that TDES will remain as an agile cryptographic standard in the future.

3) Rivest Cipher (RC 6)

RC6 is a symmetric key block cipher. RC6 (Rivest Cipher 6) is an enhanced version of the old RC5 algorithm. RC6 –w/r/b means that four w-bit-word plaintexts are encrypted with r-rounds by b-bytes keys. It is a proprietary algorithm patented by RSA Security.

RC6 operators as a unit of a w-bit word using five basic operations such as an addition, a subtraction, a bit-wise exclusive-or, a multiplication, and a data-dependent shifting.

The RC6 algorithm has a block size of 128 bits and also works with key sizes of 128 -bit, 192-bit, and 256 bits and up to 2040 bits. The New features of RC6 include the use of four working registers instead of two and the inclusion of integer multiplication as an additional primitive operation.

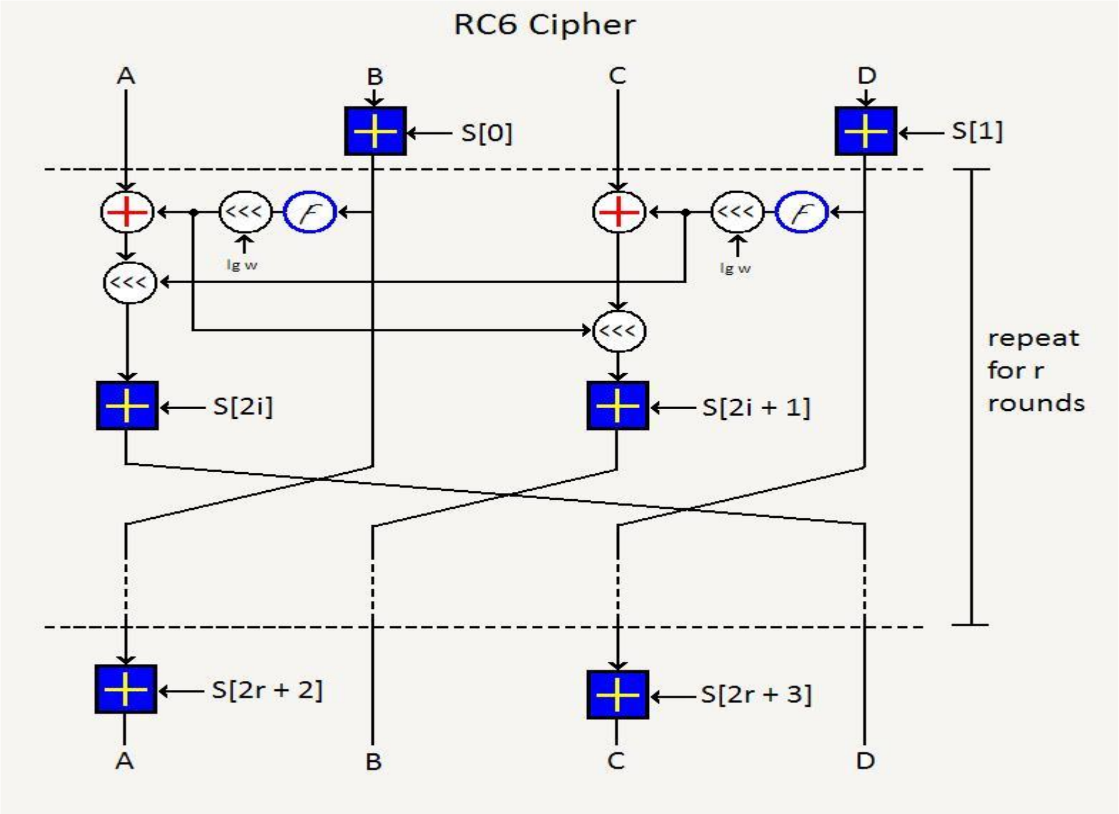


Figure 2.3 RC6 Algorithm

The use of multiplication significantly increases the diffusion per round, which allow more security, fewer laps and greater performance. Furthermore, like RC5, it can also support various word-lengths, key sizes and number of rounds. RC6 algorithm is very similar in structure to the RC5 algorithm.

In fact, RC6 could be considered as two parallel RC5 encryption processes, although RC6 uses an additional multiplication operation that is not used in RC5 algorithm to make the rotation of each bit in a word dependent, not just the least significant bits.

2.2 Problem Formulation and Design

The many advantages of using cloud storage include:

1. It eliminates the need for carrying physical storage devices.
2. Data in any format can be stored using cloud storage.
3. Cloud storage provides safe backup, as opposed to physical storage devices where loss of device, data corruption by a computer virus, natural disasters, amongst other causes, can lead to loss of data.
4. Cloud storage is more cost-effective as it eliminates the need to invest in hardware,
5. Cloud storage also helps developers collaborate and share their work in a more efficient and speedy manner.

Another advantage of cloud storage could be additional security. The proposed system aims to make the cloud storage system secure using data encryption. Thus, the aim of the proposed system is to increase security of data uploaded onto the cloud by using encryption algorithms to make the system more secure.

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 et cetera.
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 or AES and Blowfish.
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 and AES and Blowfish combination.

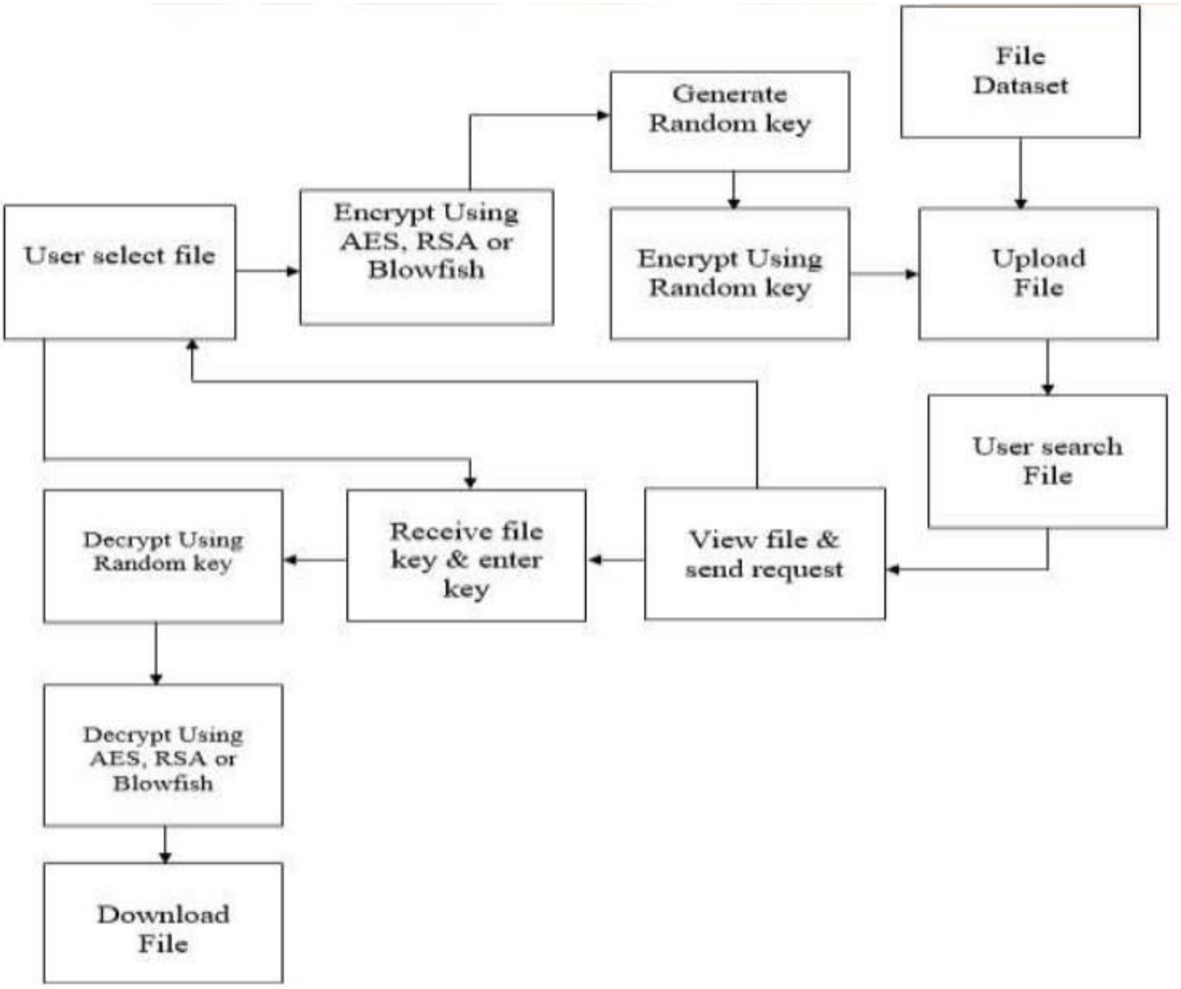


Figure 2.4 Flow chart

The system is thus secure, as it provides a double layer of security. Confidential user logi n credentials are the first layer of security. The second layer is the encrypted file. Since th e file is encrypted and then stored on the cloud, even if an attacker gains access to the clo ud, they would only have access to the encrypted files. The file can be decrypted using on ly the
decryption key, which is only sent to the user's email id which was entered during registr ation/sign-up time.

Therefore, the proposed system is designed to provide cloud storage features to users of t he portal such as uploading and downloading files to the cloud, wherein the selected files are
first encrypted and then uploaded to the file, and can be downloaded using only secret de cryption key.

An additional feature is the comparative study between the two hybrid algorithm approac hes, namely AES and RSA combination and AES and Blowfish combination.

2.3 Proposed System

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files.

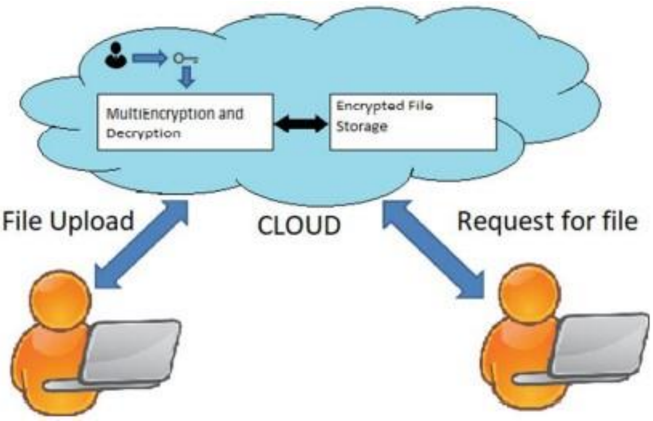


Figure 2.5 Proposed System

The above figure gives an overview of the system. As in the above figure, the files that the user will upload on the cloud will be encrypted with a user-specific key and store safely on the cloud.

1) Registration of User

   For accessing the services the user must first register themselves. During the registration process various data like the 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. These three parts will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.

These three parts will be encrypted using three different algorithms that are AES, 3DES, RC6. 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.

3) Downloading a File from the Cloud

When the user requests a file to be downloaded first the file is split into three parts. Then these three parts 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 this file will be sent to the user for download.

3. PROPSED METHODOLOGY

To achieve the above goal, the following methodology needs to be followed:

1. Load the file on the server.
2. Dividing the uploaded file into N parts.
3. Encrypting all the parts of the file using any one of the selected algorithms (Algorith m is changed with every part in round robin fashion).
4. The keys for cryptography algorithms is then secured using a different algorithm and the key for this algorithm is provided to the user as public key.

After the above 4 steps you will have a N files which are in encrypted form which are stored on the server and a key which is downloaded as public key for decrypting the file and down loading it.

To restore the file, follow the following steps:

1. Load the key on the server.
2. Decrypt the keys of the algorithms.
3. Decrypt all the N parts of the file using the same algorithms which were used to encr ypt them.
4. Combine all the N parts to form the original file and provide it to the user for downlo ading.

4. SYSTEM REQUIREMENT SPECIFICATION

Specification Requirement Specification is a complete specification of the behaviour of the system to be developed. It includes a set of use cases that describes all the interactions user will have with the software. Use cases are also known as functional requirements. In addition to use cases, the document also contains non-functional requirements, Non-functional requirements are requirements which impose constraints on design on implementation.

4.1 Software Requirements

- Operating System (Linux, macOS, Windows)
- Internet Browser (Google Chrome, Microsoft Edge, Safari, etc)
- Python version 3.9.0
- Cryptography version 3.3.2

4.2 Hardware Requirements

- Desktop/Laptop
- RAM 256 MB (Minimum)
- ROM 1 GB Free Space

CONCLUSION

This project implements a double stage encryption algorithm that provides high security, scalability, confidentiality and the easy accessibility of multimedia content in the cloud. The proposed algorithm is crucial in the second stage, the randomly generated key provides more security than the conventional encryption system. The ciphertext is stored in the cloud instead of original multimedia content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protects the information from the side channel attacker to grab the multimedia data from the cloud. Thus, the multimedia content is safe in the cloud.

5. REFERENCE

- *A. K. Shahade, V.S. Mahalle,* “Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm”, IEEE, INPAC, pp 146-149, Oct .2014.

- *Palash Uddin, Abu Marjan,* “Developing Efficient Solution to Information Hiding through text steganography along with cryptography”, IEEE, IFOST, pages 14-17, October 2014.

- *R. T. Patil and P. S. Bhendwade ,* “Steganographic Secure Data Communication”,IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.

- *Klaus Hofmann and S. Hesham,* “High Throughput Architecture for the Advanced Encryption Standard Algorithm” IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.

- *Sunita Sharma,Amit Chugh*:’Suvey Paper on Cloud Storage Security’.

- *Rawal, B. S., & Vivek, S. S.* (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).

- *Razzaque, Mohammad Abdur; Khandaker, Muhammad R. A.* (2021). "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities”.