Graphic Era (Deemed To Be) University, Dehradun

A

Major Project Synopsis

Submitted in

Complete Fulfillment of The Requirements
For The Degree Of

Bachelor of Technology

In

Computer Science & Engineering
With Specialization in Cloud Computing

By

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

:Venue:

Department of Computer Science & Engineering
Graphic Era (Deemed) University Dehradun, India

Objective: To Achieve a secure platform for storing of files on Cloud using Hybrid Cryptography.

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.

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.

PROPOSED METHODOLOGY

The project base on how the system secure file storage on cloud using hybrid cryptography. The project is only for educational pupose.

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 (Algorithm 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 downloading 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 encrypt them.
4. Combine all the N parts to form the original file and provide it to the user for downloading.

HARDWARE AND SOFTWARE REQUIREMENTS

- **Hardware**
    - Desktop/laptop
    - RAM 256MB (Minimum)
- **Software**

- Web browser
- Python

REFERENCE

- https://ibmcloud.com/
- https://awscloud.com/
- https://en.wikipedia.org/wiki/Cryptography
- Thakor, Vishal A.; Razzaque, Mohammad Abdur; Khandaker, Muhammad R. A. (2021). "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities"