Cryptography project

Secure File Storage Using Cryptography

Under the guidance:
Dr.Garima Singh

Abstract

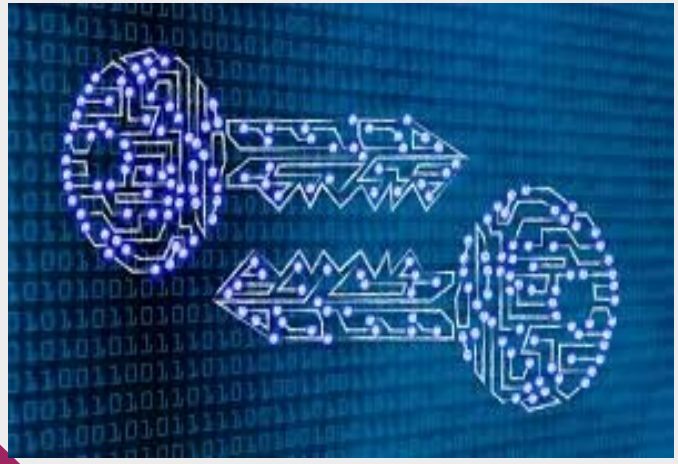
- This Project is about giving security to the files uploaded in cloud it uses some algorithms to encrypt the file uploaded in the cloud and gives key to the user.Whenever the user wants to download the file again he/she should give the key given while uploading.So by this only the user can download his files

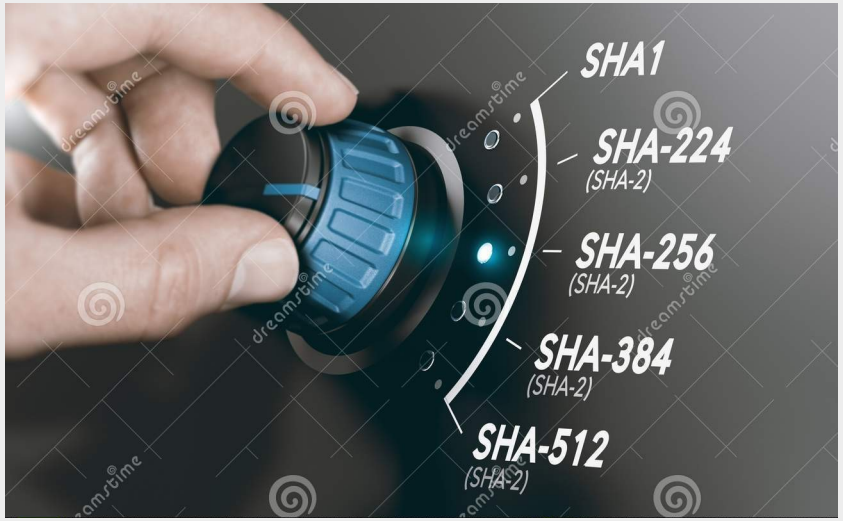
Objective

- To Achieve a secure plateform for storing of files on Cloud using Cryptography

Introduction

- Cryptography techniques convert original data into Cipher text. So only legitimate users with the right key can access data from the cloud storage server. The main aim of cryptography is to keep the security of the data from hackers, online/software crackers,and any third party users. Non-legitimate user access to information results in loss of confidentiality. Security has the characteristics to block or stop this kind of unauthorized access or any other kind of malicious attacks on the data here by securing the user's trust. In this project the uploaded file will be divided into some parts and it will be encrypted using some random algorithms(in Round Robin Fashion) like Fernet,ChaCha20,AES-GCM,AES-CCM and stored securely in cloud. To restore the file user needs to upload the key then the file can be downloaded.





Problem Statement

- Now a days cloud computing is used in many areas like industry, military colleges etc to storing huge amount of data. We can retrieve data from cloud on request of user. But there is a high chance for security threats.To provide the solution to security issues there are n number of ways. Use of a single algorithm is not effective for high level security to data in cloud computing but combining different cryptography techniques will give some security upto some extent.So this project can be used to store files securely in cloud.

Literature Survey

- Mumbai, Public Cloud security incidents hit India the hardest in the last year with 93 per cent of the country's organisations experiencing such an issue, said a survey of 26 nations by cybersecurity company Sophos.
- "Ransomware, not surprisingly, is one of the most widely reported cybercrimes in the public Cloud," Chester Wisniewski, Principal Research Scientist at Sophos said in a statement.
- The cybersecurity incidents that Indian organisations suffered most included ransomware (53 per cent) and other malware (49 per cent), exposed data (49 per cent), compromised accounts (48 per cent), and cryptojacking (36 per cent), said the report titled "The State of Cloud Security 2020"
- In 2019 -Cybercriminals attacked a Mumbai cloud server honeypot with more than 678,000 attempts over a 30-day period, second to a US-based honeypot at Ohio that recorded more than 950,000 login attempts during the same period.
- The cloud servers were subjected to 13 attempted attacks per minute per honeypot on average. The most used password by cybercriminals for login attempts globally was 123456.

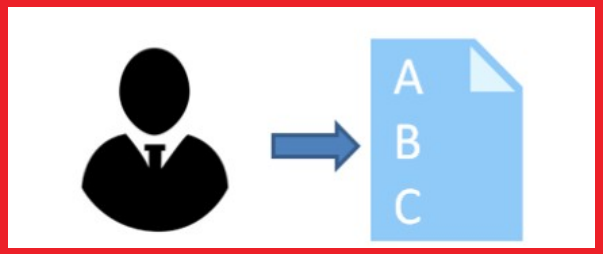
Methodology

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

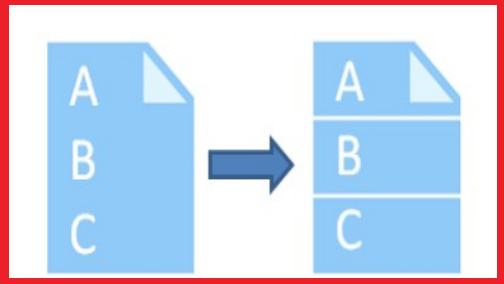
- 1. Load the file on the server.
- 2. Dividing the uploaded file into N parts.
- 3. Encrypting all the parts of the file using any one of the selected algorithms (Algorithm is changed with every part in round robin fashion).
- 4. The keys for cryptography algorithms is then secured using a different 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:

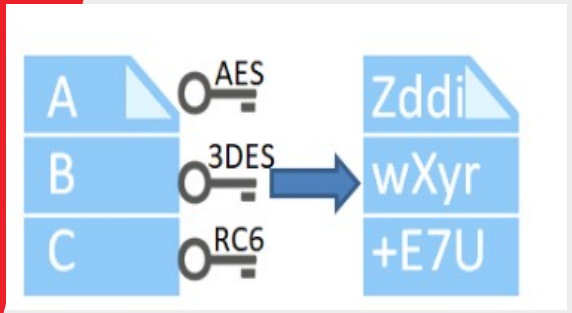
- 1. Load the key on the server.
- 2. Decrypt the keys of the algorithms.
- 3. Decrypt all the N parts of the file using the same algorithms which were used to encrypt them.
- 4. Combine all the N parts to form the original file and provide it to the user for downloading.



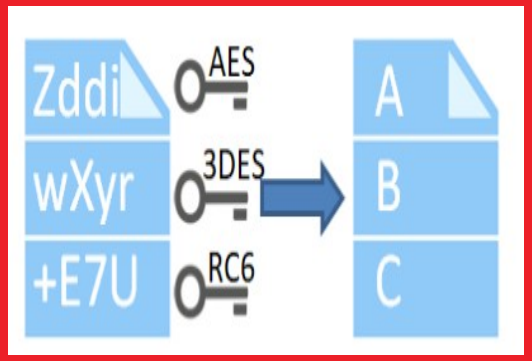
- User uploads files



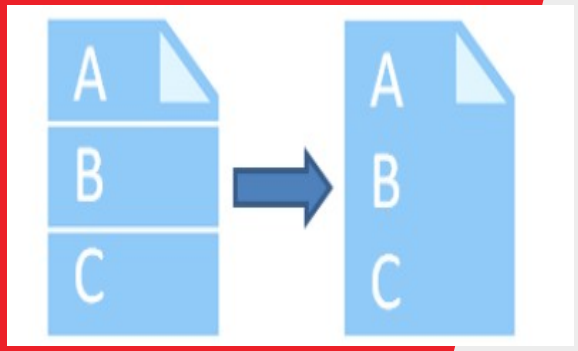
- Split into parts



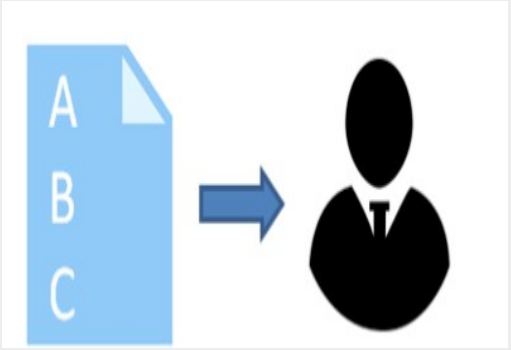
- Encrypts the parts



- Decrypts the parts



- Combines decrypted parts



- User gets file

Algorithm

- This project totally uses symmetric key cryptography(mainly AES)
  - *Fernat
  - *ChaCha20
  - *AESGCM
  - *AESCCM

THANK YOU

- Neeraj kumar - 19BCN7259