International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 4, April 2021
https://www.ijramt.com | ISSN (Online): 2582-7839


# Secure File Transfer on Cloud with Encryption

Niteen Kale[1], Abraar Khan[2*], Swapnil Sawant[3], Atharva Shrotre[4], S. M. Bhadkumbhe[5]
[1,2,3,4,5]*Department of Computer Engineering, PDEA's College of Engineering, Pune, India*

***Abstract*: In this paper, we aim to securely transfer files on the cloud in a manner that preserves data confidentiality, integrity and ensures availability. The rapidly increased use of cloud computing in many organizations and IT industries provides new software at a coffee cost. Cloud computing is useful in terms of low cost and accessibility of knowledge. Cloud computing gives tons of advantages with low cost and data accessibility through the web. Ensuring the safety of cloud computing may be a major thing about the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers could also be untrusted. So, sharing data in secure form while preserving the info from a source that's not trusted remains a challenging issue. Our approach ensures the safety and privacy of client-sensitive information by transferring data across one cloud, using the AES algorithm, etc.**

***Keywords*: Cloud computing, Cloud security, Cryptography, Encryption/Decryption techniques, AES algorithm, Amazon S3 Bucket.**

## 1. Introduction

This project has an AWS cloud that's accessible to all or any, a system that has the means to transfer data and every one information, an internet site for users to access the landing page to transfer the files through the cloud. The cloud is often accessed through the web from anywhere. The users need to visit the system page where the user can transfer files. The cloud also will provide security to all or any files transferred.

### *A. Statement of the problem*

Customer transfers or shares data at cloud service providers are susceptible to various threats. In our work, we consider four sorts of threat models. First is that the single point of failure, which can affect the info available that would occur if a server at the cloud service provider failed or crashed, which makes it harder for the customer to retrieve his stored data from the server. Availability of knowledge is additionally a crucial issue that would be affected if the cloud service provider (CSP) runs out of service. Our second threat is data integrity. Integrity is that the degree of confidence that the info within the cloud is what's alleged to be there, and is protected against accidental or intentional alteration without authorization. Security may be a necessary service for the wired network also as wireless network communication to enhance what was offered within the cloud. Simply storing the knowledge on clouds solves the matter isn't about data availability, but about security. Most of the companies that have held back from adopting the cloud have done so within the fear of getting their data leaked. It's also a third-party service, which suggests that data is potentially in danger of being viewed or mishandled by the provider. It's only attributed to doubt the capabilities of a 3rd party, which looks like a good bigger risk when it involves businesses and sensitive business data. Several external threats can cause data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts.

## 2. Literature Review

[1] *Secure File Storage on Cloud Using Hybrid Cryptography Algorithm - Uttam Kumar, Mr. Jay Prakash*

Cloud is employed in various fields like industry, military, college, etc. for various services and storage of giant amounts of knowledge. Data stored during this cloud are often accessed or retrieved at the user's request without direct access to the server computer. But the main concern regarding the storage of knowledge online that's on the cloud is Security.

Disadvantage: The System may get slower encryption and decryption thanks to multiple algorithms.

[2] *Secure File Storage in Cloud Computing - Hrithik Dhakrey*

We aim to supply cloud security for securely store information into the cloud, by splitting all the info into sub-data or chunks, we offer data confidentiality, integrity and ensures availability. In present days cloud computing is increasing uses by almost every organization and IT industry. Cloud computing may be a benefit in terms of low cost and availability of knowledge through the web.

Disadvantage: The speed of encryption and decryption may vary counting on file size.

[3] *Review of Secure File Storage on Cloud using Hybrid Cryptography - Shruti Kanatt, Amey Jadhav, Prachi Talwar*

In this system, the user uploads a file to the portal, it gets encrypted then uploaded onto the cloud. The user can then download their files from the cloud through the portal, which ends up within the decrypted (or original) file getting downloaded to their local computer. The system also uses AES and RSA algorithms.

Disadvantage: The process is sort of time-consuming as there are multiple algorithms involved.

[4] *Development of Secure File Storage on Cloud using Hybrid Cryptography - Sahana Bisalapur, Ninad Patil, Rahul R., Rushikesh Tarale, Sanket Honashetti, S.G. Balekundri*

*Corresponding author: iamabraarkhan@gmail.com

We have taken the strongest features of all the techniques and designed a hybrid cryptographic system involving one of the three strongest algorithms known to man. The algorithms utilized in this technique are AES-256, SHA-256, and MD5. The utilization of 256-bit algorithms makes it impossible to crack. We are employing a random generator to get a key which adds to the advantage of encrypting the files. For decryption reverse process of encryption is applied using an equivalent key.

Disadvantage: The block size of the implemented algorithm is low leading to less security.

[5] *Literature Survey on Cloud Cryptography for Data Security - Jyoti Gangesh Tiwari, Gayatri Sanjay Chavan*

It includes completely different encoding and secret writing techniques that area units want to stay our data safe and secure on the cloud. In Cloud Cryptography we tend to use public and private keys for Encrypting and Decrypting Data to stay up the integrity of data. The new idea is getting used today i.e., CaaS (Crypto as a Service) this has brought the thought of cloud computing.

Disadvantage: The execution alongside the time constraints is way more as there are too many algorithms implemented. Points.

## 3. Methodology

### A. *Existing system*

In the existing system single algorithm is employed for data encode and decoding purposes. But the utilization of one algorithm isn't accomplished high-level security. If we use a public key cryptography algorithm then we've to face security problems for storing public keys. Key transmission problem occurs while sharing key into the multiuser environment. Public key cryptography algorithms accomplish high security but the utmost delay is required for data encrypt and decrypt. To unravel the above issues, we've introduced a replacement security mechanism.

#### 1) *Disadvantages*

1. Block size of blowfish is low i.e., 64 bits.
2. It must get the key to the person out of the band, not through the unsecured channel.
3. RC6 isn't universally practiced.
4. Inter multiplications on rotation.

### B. *Proposed system*

In this system, the user can store the file safely in online cloud storage as these files are going to be stored in encrypted form within the cloud and only the authorized user has access to their files. We will store all kinds of files like text, audio, video, images, pdf, doc, and all other files format. Other combination of algorithms might not encrypt all types of files like audio and video which has continuous bits of knowledge which can end in loss of knowledge after encryption, but the proposed system is strong enough to encrypt all kinds of files with none loss of knowledge which makes it useful for real-time purposes. AES-256 is that the most robust security protocol, it uses a better length key size that's 256 bits. It's useful in encrypting audio and video files. As data security is vital, we during this project are providing security to the confidential files during the transfer on the cloud file transfer system, by encrypting the file using AES 128-bit encryption employing a predefined key securely stored on an AWS S3 bucket not known by the other person. In the proposed system, a way for securely storing files within the cloud employing a hybrid cryptography algorithm is presented. During this system, the user can store the file safely in online cloud storage as these files are going to be stored in encrypted form within the cloud and only the authorized user has access to their files.

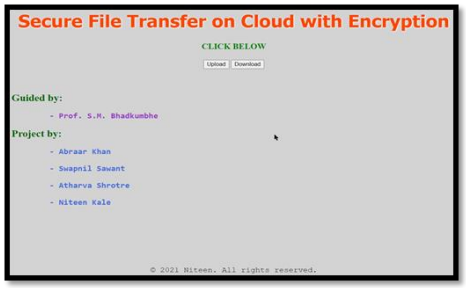


Fig. 1. System overview

## 4. Design and Implementation

There are 2 main phases within the system:

#### 1) *Uploading Phase*

In the Uploading Phase, steps are as follows:

1. Load the file on the server.
2. Dividing the uploaded file into N parts.
3. Encrypting all the parts of a file using any one selected algorithm.
4. The keys for cryptography algorithms are secured employing a different algorithm and therefore the key of this algorithm is provided to the user because of the public key.
5. After the above 4 steps you'll have N files in encrypted form which are stored on the server and therefore the keys downloaded as a public key for decrypting/downloading it.

#### 2) *Downloading Phase*

In the downloading phase, the steps are as follows:

1. Load the key on the server.
2. Decrypt the keys of the algorithms.
3. Decrypt all the N parts of the file using an equivalent algorithm that was used to encrypt them.
4. Combine all the N parts to make the first file and supply it to the user for download.

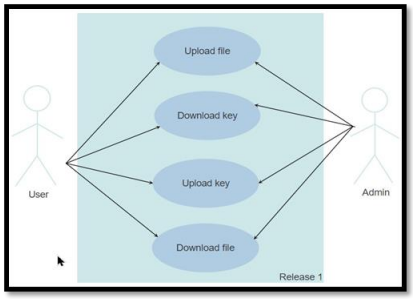


Fig. 2. Use-case diagram

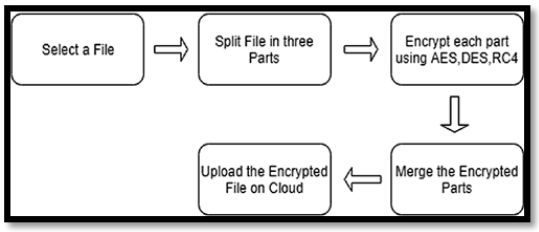


Fig. 3. Flow diagram

### *B. Advanced Encryption Standard (AES)*

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is that the Advanced Encryption Standard (AES). It's found a minimum of six fold faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it had been considered vulnerable against exhaustive key search attacks. Triple DES was designed to beat this drawback but it had been found slow. AES is that the block chain symmetric algorithm. AES comprises three block ciphers like AES-128, AES-192, and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively.

#### *1) Advantages*

1. The stored image file is secured, because the file is being encrypted not by just using one but three encryption algorithms which are AES, DES, and RC6.
2. The key's also safe because it embeds the key in a picture using LSB.
3. The system is extremely secure and robust.
4. Data is kept secure on a cloud server which avoids unauthorized access.

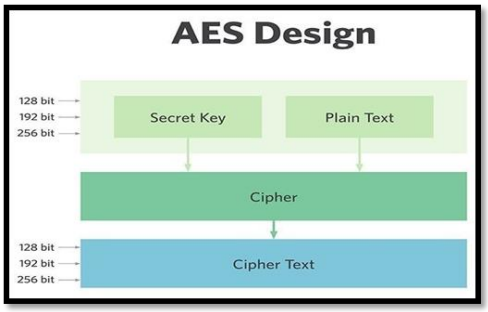


Fig. 4. AES design

### *C. Amazon S3 Bucket (Simple Storage Service)*

Amazon S3 or Amazon Simple Storage Service may be a service offered by Amazon Web Services (AWS) that gives object storage through an internet service interface. Amazon S3 uses an equivalent scalable storage infrastructure that Amazon.com uses to run its global e-commerce network. Amazon S3 is often employed to store any sort of object which allows for uses like storage for Internet applications, backup and recovery, disaster recovery, data archives, data lakes for analytics, and hybrid cloud storage. In its service-level agreement, Amazon S3 guarantees 99.9% uptime, which works bent but 43 minutes of downtime per month. Although Amazon Web Services (AWS) doesn't publicly provide the small print of S3's technical design, Amazon S3 manages data with an object storage architecture that aims to supply scalability, high availability, and low latency with 99.999999999% durability and between 99.95% to 99.99% availability (though there's no service-level agreement for durability).

### *D. Flask*

Flask may be a Python web framework built with a little core and easy-to-extend philosophy. Flask is an implementation of the concept of the online framework. Flask was originally designed and developed by Armin as an April fool's Day joke in 2010. Despite the origin as a joke, the Flask framework became wildly popular as an alternate to Django projects with their monolithic structure and dependencies.

## 5. Conclusion

The main aim of this technique is to securely store and retrieve data on the cloud that's only controlled by the owner of the info. This project implements a double-stage encryption algorithm that gives high security, scalability, confidentiality, and therefore the easy accessibility of multimedia content within the cloud. The proposed algorithm is crucial within the second stage, the randomly generated key provides more security than the traditional encryption system. The cipher text is stored within the cloud rather than original multimedia content. The cipher text is undoubtedly hard to recover the first content for a random asymmetric key. Wide application of the proposed algorithm protects the knowledge from the side channel attacker to grab the multimedia data from the cloud. Thus, the multimedia content is safe within the cloud.

## References

[1] Jasleen K., S.Garg "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, vol. 3, no. 5, pp. 300-305, 2015.

[2] Joseph Selvanayagam, Akash Singh, Joans Michael, Jaya Jeswani, Secure File Storage on the cloud using cryptography: (IRJET), 2018.

[3] Aditya, P., Abhijeet, D., Hitesh, N and Rohan, N. Secure File Storage on Cloud using Hybrid Cryptography. *International Journal of Computer Sciences and Engineering*, vol. 7, no. 1, pp. 587-591, 2019.

[4] B. Bindu, K. Lovejeet and L. Pawan, "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm", International *Journal of Advanced Research in Computer Science*, vol. 9, no. 2, 2017.

[5] Mahalakshmi, B. and G., Suseendran. (2019). 'A Hybrid Cryptographic Algorithm for Securing Data in Cloud Storage'. *Journal of Advanced Research in Dynamical and Control Systems*. vol. 11, no. 6, 2019.

[6] https://en.wikipedia.org/wiki/Cryptography.