CLOUD-BASED HYBRID CRYPTOGRAPHY FOR SAFE DATA STORAGE

[#1]ADICHERLA RAMESH, Associate Professor,

Department of Computer Science and Engineering

[#2]BURLA SRINIVAS, Associate Professor,

Department of Computer Science and Engineering,

MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.

ABSTRACT: Various entities, such as the military, schools, and enterprises, utilize cloud technology to store and execute a range of services. Users can retrieve data from the cloud even in the absence of a computer connection. Security is the paramount factor in cloud storage. Cryptography and steganography are the two most fundamental techniques for safeguarding information. Occasionally, a solitary technique or algorithm lacks enough security measures. We present a novel security mechanism that integrates symmetric key and steganographic cryptography to achieve this objective. Data in this system is safeguarded using the 3DES, RC6, and AES encryption methods. 128-bit keys are used in all algorithms. LSB steganography is employed to safeguard confidential data. The encrypted data, the key of the file, and the procedure are all crucial pieces of information. File encryption involves the division of a file into three distinct portions. In order to simultaneously encrypt these sections of the file, a combination of several techniques and parallel processing will be employed. The LSB method integrates essential visual data. The user data is encrypted and stored on a single cloud server utilizing the RC6, DES, and AES encryption algorithms.

Keywords: Cloud Computing and Storage, AES Algorithm, RSA Algorithm, Blow fishAlgorithm

1. INTRODUCTION

The fundamental idea behind cloud computing was to allocate jobs across a vast scale. As per the National Institute of Standards and Technology (NIST), cloud computing offers convenient and immediate access to a flexible set of computing resources, including network, storage, applications, and services. These resources can be easily provisioned and deprovisioned by administrators or service providers with minimal effort.

In cloud computing, the service provider assumes responsibility for the management of files and tools, relieving the user of this task. To address this problem, the cloud service provider can employ file encryption. This study investigates the security of cloud computing by employing a practical file security framework. This paradigm employs file segmentation and RSA encryption to ensure secure communication between users and servers.

Data security issues

Conventional security methods are not applicable to cloud applications and data due to their open and sharing nature. Here are the issues: The dynamic scalability, location transparency, and service transparency of cloud computing remove the necessity for infrastructure and security obstacles for any data or application. Determining the compromised resource in security events is challenging.

Cloud resources and services might be owned by several companies as a result of the way cloud computing services are provided. One security measure cannot be implemented due to a conflict of interest.

Unauthorized individuals can gain access to user data because to the widespread availability of cloud computing, which enables multiple tenants to share digital resources.

2. HYBRID CRYPTO SYSTEM SCHEME

Cloud storage systems employ hybrid cryptography for protection. There are two approaches that can be used to differentiate between systems that are safe and those that are not. During the initial stage, the text and data undergo encryption using the Advanced Encryption Standard (AES), while the key is encrypted using the RSA algorithm. The second approach utilizes Blowfish and AES algorithms to provide security. This technique is more secure as it employs double encryption for both the key and the data.

The suggested system is comprised of three distinct components. The initial application involves a key switch utilizing the Diffie Hellman cryptographic protocol. Digital signatures are employed only following verification. Upon encryption, the data is thereafter transmitted to the designated cloud server. Unlocking pertains to data that is not subjected to encryption.

RSA and MD5 are cryptographic methods used to ensure data confidentiality, integrity, and non-repudiation. RSA key generation involves the creation of cryptographic keys that can be utilized for both the encryption and decryption of data.The MD5 digest employs 128-bit inputs during the encryption and decryption process, and it adds padding to the outputs.

The collaboration of an NTFS disk, an encrypted file system (EFS), and a cache manager ensures a secure approach to file storage. EFS utilizes cryptography to expeditiously encrypt data. The application saves objects to the NTFS file system prior to caching and then delivering them. The NTFS file system governs the storage and protection of files by providing instructions to EFS.

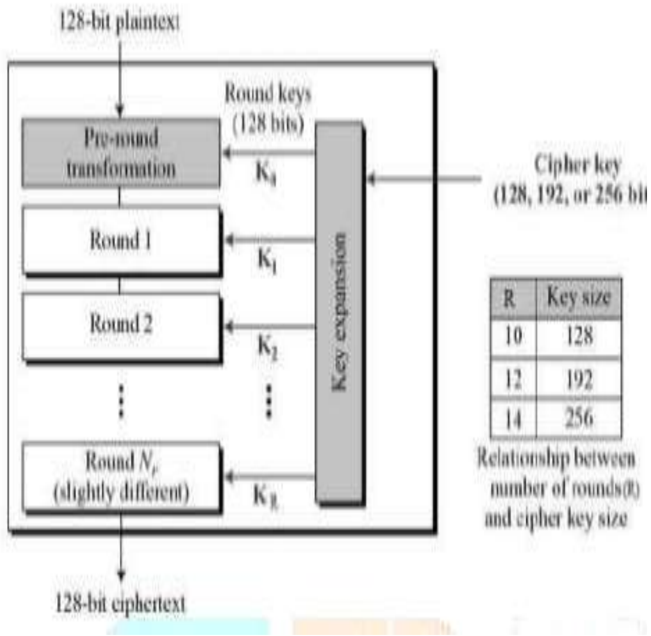
The Cloud Storage Security Service necessitates the presence of computer servers. Output of data, input by the user, and retention of data. If one of the servers has a failure, the data is stored on the remaining two servers. The User Input server employs robust security measures to protect user files and input data from unauthorized access, ensuring the prevention of data theft. However, it still enables users to undergo the necessary validation process. The user input is encrypted using the Advanced Encryption Standard (AES) and then transmitted from the data store server to the user output server. The user output server transmits the deciphered file.

Algorithm Used

Advanced Encryption Standard(AES)

The Rijndael and AES algorithms exhibit a high degree of similarity. Rijndael encryption techniques utilize a range of different key and block sizes.

The system comprises a succession of operations, where certain operations are responsible for altering the bit sequence, while others are responsible for modifying the output.



The AES code is implemented using bytes as the fundamental unit of data instead of bits. The Advanced Encryption Standard (AES) partitions 128 bits of unprocessed data into a 4x4 matrix consisting of 16 bytes, thereby facilitating its manipulation.

The AES code is offered in three different lengths: 128 bits, 192 bits, and 256 bits. During each cycle, data segments undergo encryption and decryption using keys that are either 128 bits, 192 bits, or 256 bits in length. Rijndael, in contrast to AES, permitted the use of longer key lengths and larger block sizes.

Triple Data Encryption Standard (3DES)

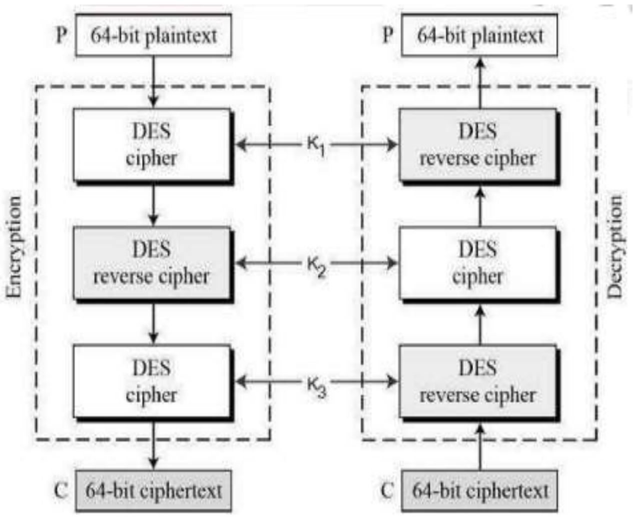
The Data Encryption Standard (DES) was enhanced to 3DES by a process of transfer. Triple DES enhances security by utilizing the DES algorithm three times. TDEA and TDES are synonymous representations of Triple DES.

The TDES key consists of the following symbols: The characters possessed distinct and individual qualities.

Key 1 and Key 3 are indistinguishable, whereas

Key 1 and Key 2 are distinct.

Each key is identical.



The use of TDES will be gradually discontinued upon the release of AES. Digital payments are characterized by the utilization of 2TDES encryption and the widespread adoption of standards like EMV (often referred to as "Chip card") and IC-enabled point-of-sale devices and automated teller machines (ATMs). The adoption of TDES remains advantageous as a cryptographic standard in this particular method.

Rivest Cipher 6(RC6)

The RC6 keys are symmetric. The new RC6 algorithm will supersede the outdated RC5 code. The encryption process of RC6 involves encrypting four lines, each consisting of w bits, using keys that are b bytes long. The encryption is performed in r cycles. RSA Security has obtained a patent for a confidential algorithm.

RC6 operators employ bit-wise exclusive-or, multiplication, data-dependent shifting, addition, and subtraction to construct words consisting of w bits. RC6 has the capability to process keys of various lengths, including 128, 192, and 256 bits, as well as up to 2040 bits, due to its 128-bit block size. RC6 incorporates the inclusion of integer multiplication and the addition of four registers, which is an improvement from the previous two registers. When you increase the per-round dispersion, security, circuit count, and total performance all increase. It is compatible with various word lengths, key sizes, and round counts, similar to RC5. The RC5 and RC6 algorithms exhibit significant structural similarities. By incorporating a multiplication operation, RC6 achieves the same level of encryption as two concurrent RC5 algorithms. Nevertheless, it performs a rotation operation on every bit within a word, rather than exclusively on the least significant bits.

Blow fish

Blowfish employs a Fiestal network and undergoes 16 recurrent encryption cycles for the purpose of decoding. Additionally, it possesses a practical and efficient design. The blowfish cipher utilizes four 32-bit Substitution boxes, eighteen 32-bit P-boxes with 256 characters each, and a block size of 64 bits. The possible range for the length of the key is between 0 and 448 characters.

The diagram illustrates the program's design. Key expansion occurs after the process of data encryption. Key expansion is the division of a single key into multiple smaller keys. Data security is ensured through the utilization of 16-round networks. Each round involves permutations and replacements that depend on the keys and data.

Hybrid Crypto system Phases-

A two-step hybrid cryptosystem is employed for file protection:

process 2 has an additional distinct process for encryption.

Encryption Phase

Related to the process of encoding information

Only the selected components will be included in the encrypted file. The user's provided Blowfish key is used to encrypt each portion of the file.

RSA public key encryption ensures the secure storage of keys.

Upon completion, we possess encrypted keys and fragments of files.

Decryption Phase

In order to decrypt, one must possess n RSA private keys, where n corresponds to the number of segments generated during the encryption process. The server utilizes the RSA private key on the slice to decipher the Blowfish key.

Decrypted Blowfish keys are utilized to access file sections stored on the server.

A new file is created by reassembling the decrypted components.

Design and Implementation

An advantage of cloud storage is the elimination of the need to physically transport storage devices. There exist numerous methods for storing information on the cloud.

Conventional ways of preserving data are susceptible to data loss in the event of device loss, virus infection, or a natural calamity. Conversely, cloud backup is secure.

Cloud storage is more cost-effective as it eliminates the requirement for purchasing any physical infrastructure.

Cloud storage accelerates file sharing and facilitates collaboration among developers.

Utilizing computer storage can enhance security. The proposed technique employs encryption to secure data that is kept in the cloud. The proposed technique employs encryption to enhance the security of data stored in the cloud.

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

To sign in or register, the user enters their name, The user inputs their name, email address, phone number, account password, and additional information to register or authenticate.

Subsequently, the user selects the file from their local storage for the purpose of sharing.

Subsequently, the user selects an encryption technique. The approach is compatible with both AES and RSA encryption algorithms, as well as AES and Blowfish.

Once the file has been encrypted using appropriate techniques, it is transmitted.

Users have the ability to access files, see their contents, and upload them.

The decryption key is transmitted to the email address provided by users during the registration or login process when they download files.

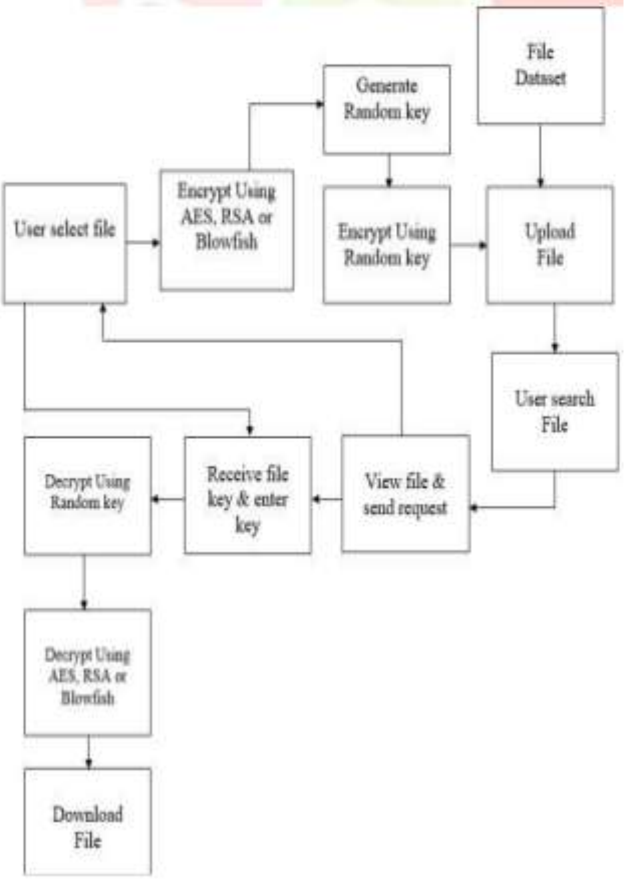
This key enables users to receive both encrypted and unencrypted files.

The system also evaluates the security level of the two hybrid encryption algorithm combinations.

AES, RSA, and Blowfish are all encryption algorithms.

The proposed plan incorporates hybrid cryptography as a means of safeguarding cloud files. This technology enhances the security of online cloud storage by employing encryption to ensure that only authorized users are able to access and view the content.

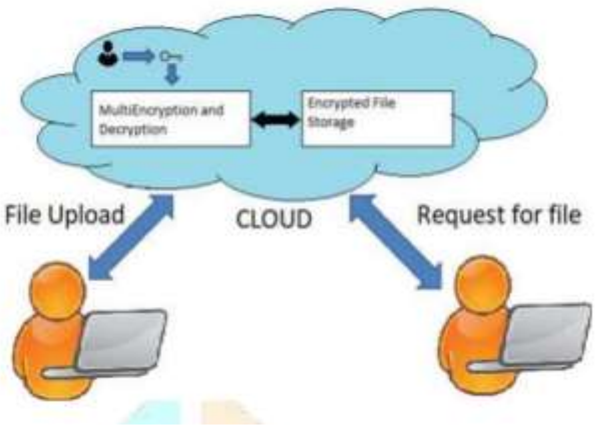
The image depicted above illustrates the process of encrypting shared data in the cloud, ensuring their security by utilizing a distinct key for each user.



3. PROPOSEDSYSTEM

Prior to utilizing the services, users are required to register. Upon registration, it is necessary to provide your name, username, password, email address, and phone number. The server has the capability to generate encryption and decryption keys for individual users using this information. The key will not be stored in the database but will be concealed within the user's profile picture.

Upon sending a file to the cloud, a transient directory is created.



The file will consist of N sections.

User Registration

The file sections will be encrypted using AES, Each component of the file will be safeguarded using a cryptographic key. Distinct encryption algorithms will be employed for various components.

Uploading a File on Cloud

The file sections will be encrypted using AES, 3DES, RC6, and other cryptographic algorithms. The registration steganographic picture contains the crucial key for the algorithm.

Following the process of splitting the encryption, the file was subsequently reassembled and stored within the designated folder of the user. The initial file has been relocated from the temporary location.

Assembling encrypted fragments of a file.

Download a File from the Cloud

Upon initial retrieval, the file is divided into N segments.

These portions of the file will be decoded using the same techniques.

The registration steganographic image is utilized to obtain the cryptographic decryption key.

These fragments will be reassembled to create an encrypted file.

Subsequently, the individual can obtain the file.

4. CONCLUSION

Its primary function is to securely store and access confidential data in a cloud environment. Cryptography and steganography are employed to ensure the security of data stored in the cloud. The data is safeguarded using AES, 3DES, and RC6 encryption algorithms. Steganography, specifically utilizing the Least Significant Bit (LSB) approach, ensures the security of confidential data. Employing many threads enhances the efficiency of both encryption and decoding processes. The proposed security system enhances data security, privacy, authentication, and reliability. To mitigate potential client-server data transfer concerns in the future, we can employ the use of public key cryptography.

REFERENCES

1. Kumar, A., Lee, B. G., Lee, H., &Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 InternationalConferenceonICTConvergence(ICTC).
2. Rewagad, P., &Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
3. Ping,Z.L.,Liang,S.Q.,&Liang,L.X.(2011).RSA EncryptionandDigitalSignature.2011InternationalConferenceonComputationalandInformationSciences.
4. Sunita Sharma, Amit Chugh:’Suvey Paper on Cloud Storage Security’.
5. Rawal, B. S., &Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud(Smart Cloud).