*Secure File Storage on Cloud using Hybrid Cryptography*

Dr. S P Chokkalingam  
Department of Computer Science Engineering  
Amrita School of Computing  
Chennai, India  
[sp\_chokkalingam@ch.amrita.edu](mailto:sp_chokkalingam@ch.amrita.edu)

Venkata Krishna Reddy  
Department of Computer Science Engineering  
Amrita School of Computing  
Chennai, India  
[ch.en.u4cse19113@ch.students.amrita.edu](mailto:ch.en.u4cse19119@ch.students.amrita.edu)

Ravi Venkat Jayanth  
Department of Computer Science Engineering  
Amrita School of Computing  
Chennai, India  
[ch.en.u4cse19136@ch.students.amrita.edu](mailto:ch.en.u4cse19131@ch.students.amrita.edu)

**Abstract**

**Many sectors, including the military, education, and business, use the cloud to offer a wide range of services and store enormous amounts of data. Users can request access to or retrieval of data kept in this cloud without having direct access to the server computer. Because to the rapidly growing use of cloud computing by IT industries and organizations, new software is made accessible at a low cost. The benefits of cloud computing include accessibility to knowledge at minimal cost. Cloud computing has a number of advantages, including low costs and simple Internet access to knowledge. Keeping data from an unstable cloud and safely transmitting it is still a challenge. Our approach stores the data over a single cloud using AES, DES, and RSA algorithms, assuring the security and privacy of sensitive client data.**

**Keywords: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), Hybrid Cryptography.**

**Introduction**  
Cloud file storage security is a major concern for both individuals and businesses. Availability and portability are only a couple of the advantages that cloud storage offers, but it also creates security issues. In order to safeguard data both in transit and at rest, hybrid cryptography is a system that combines the advantages of symmetric and asymmetric encryption. In this method, an asymmetric key is used to encrypt the data after it has been encrypted with a symmetric key. By using this procedure, even when the symmetric key is compromised, the data will still be protected. By adopting hybrid cryptography, cloud storage providers may assure that their customers' data is protected from unwanted access, theft, and other security threats. We shall examine the advantages and disadvantages of hybrid cryptography for secure file transmission in this post.

The system proposed outlines a method for securely storing files in the cloud through the utilization of a hybrid cryptography algorithm. This technology enables users to safely save data in online cloud storage since the files are stored in the cloud in encrypted form and only authorized users can access them. Before being uploaded to the cloud, the user's uploaded data will be encrypted and securely stored using a user-specific key.

User can upload a text file using the upload option. Then user's file will then be split into N separate portions. All of these file sections will be encrypted with cryptographic techniques. Several types of encryption will be utilized by each component.The encryption methods that will be utilised to safeguard these entire file components include AES, DES, and RSA. After being recreated and placed in the user's unique folder, the file was first decrypted.

The same encryption techniques employed to secure these file segments will be employed again for their decryption. Once the components are reassembled, the decrypted file will be made available for the user to download.

**Related Work**

"AHybrid Cryptography-based Secure File Storage System for Cloud Computing" by K. V. Ramachandran, Naveen Kumar, and R. Sriramakavacham. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To guarantee the secrecy, integrity, and validity of the stored files, the authors use symmetric and asymmetric encryption.

Ankit Gupta and Dheerendra Singh's "Hybrid Cryptography based Secure File Storage on Cloud." This research presents a safe file storage system for the cloud utilizing hybrid cryptography. The authors use a combination of RSA and AES encryption to secure data confidentiality and integrity. To ensure safe access to the stored files, the system also has key management and access control components.

"A Hybrid Cryptography-based Approach for Secure File Storage in Cloud Computing" by S. Senthil Kumaran and S. Santhosh K. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To guarantee the confidentiality and integrity of the saved files, the authors combine AES and RSA encryption. The system also contains a key management mechanism for safe access control.

Hybrid Cryptography for Secure File Storage on the Cloud by K. In addition to P. N. Shriram. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To protect the privacy and integrity of the saved files, the authors combine RSA and Blowfish encryption. The system also contains a key management mechanism for safe access control.

"Secure File Storage on Cloud using Hybrid Cryptography and Attribute-based Encryption" by R. M. and Anitha. Hemalatha. This research presents a secure data storage system for the clouds using hybrid encryption and attribute-based encryption. For data security and integrity, the authors combine AES and RSA encryption. For access control, they use attribute-based encryption. In order to distribute keys securely, the system also features a key management mechanism.

Manpreet Kaur and Hardeep Singh examine various methods for protecting information storage on the cloud using hybrid cryptography in their article, "Secure file storage on cloud using hybrid cryptography: a review." They explain the merits and disadvantages of alternative approaches, such as RSA with AES, ElGamal with AES, and RSA with Camellia, and present a comparison of their security properties.

In a study conducted by Both S. Sivasankari and S. Sathish, the authors provide a comprehensive survey on the utilization of hybrid cryptography for secure file storage in the cloud. The research examines recent advancements in this field, shedding light on the current state of the art in cloud-based file security. They examine different encryption schemes, such as symmetric and asymmetric encryption, and hybrid approaches that combine the two. They also talk about potential future research directions and difficulties in putting such systems into practice.

According to J. In "Hybrid Cryptography for Secure File Storage on Cloud: A Survey," The authors, R. Santhi and V. N. Sumathy, evaluate a number of hybrid cryptography systems that have been suggested for safe cloud file storage. They assess these systems' effectiveness and security as well as their applicability for various kinds of data and applications. They also talk about possible directions for this research's advancement.

Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by R. Ramya and R. Kavitha. This study presents a comprehensive evaluation of several hybrid cryptography algorithms used for safe information storage on the cloud. It examines the advantages and limits of each technique and also discusses the problems and future research prospects in this subject.

S. Srinivasan and K. Sathish Kumar's "Hybrid Cryptography based Secure File Storage in Cloud: A Review." The secure file storage in the cloud using hybrid cryptography is the main topic of this survey report. It compares various existing methods and assesses the advantages and disadvantages of different hybrid cryptography techniques.

By M. V. Bhatkar and S. K. Gupta, "A Survey on Secure File Storage on Cloud Using Hybrid Cryptography." This study gives a survey on hybrid cryptography-enabled safe file storage in the cloud. It addresses the benefits and drawbacks of different hybrid cryptography-based techniques, including AES-RSA, AES-ECIES, and RSA-ECIES. The report also identifies current research gaps and suggested future lines of inquiry.

"A Review of Secure File Storage on Cloud using Hybrid Cryptography" by N. G. Patel and J. M. Patel. This survey study presents an overview of safe file storage on the cloud using hybrid cryptography. It examines the currently used methods—including AES-RSA, AES-ECIES, and RSA-ECIES—and assesses how well they perform in terms of security, effectiveness, and scalability. The report also discusses the challenges and potential research directions in this field.

P. S. Verma and P. R. Dubey's "Hybrid Cryptography based Secure File Storage on Cloud: A Systematic Review." This paper presents a systematic review of hybrid cryptography-based secure file storage on the cloud. It investigates the existing approaches, such as AES-RSA, AES-ECIES, and RSA-ECIES, and their applicability for cloud-based file storage. The limitations and future research directions in this area are also mentioned in the paper.

"Hybrid Cryptography Based File Storage Security in Cloud Computing" by Shangquan Wang, Xuelian Lin, and Shengyu He (2020): This study examines various hybrid cryptography techniques that can be applied to cloud-based secure file storage. The authors explain the elements that should be taken into account when choosing an appropriate scheme for a particular application, comparing the advantages and disadvantages of these schemes.

Bhupendra Singh, Ravi Tomar, and Manoj Misra's 2018 paper, "A Survey of Hybrid Cryptography Techniques for Cloud Computing," outlines the following: This paper offers a thorough analysis of hybrid cryptography methods that can be applied to cloud-based secure file storage. The authors go over the benefits and drawbacks of various hybrid cryptography systems and offer suggestions for choosing the best one based on particular needs.

"Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by Gaurav Kumar, Kuldip Singh, and R. K. Jha (2017): In this study, cutting-edge hybrid cryptography methods for safe file storage in the cloud are reviewed. The authors assess the various schemes based on aspects such as security, efficiency, and usability, and make advice for picking an acceptable scheme depending on individual requirements.

Ajay Kumar and S. S. Tyagi's "Hybrid Cryptography for Secure Data Storage in Cloud Computing: A Survey" from 2016: This study examines the various hybrid cryptography methods that can be applied to cloud data storage security. The authors assess the various schemes based on aspects such as security, efficiency, and scalability, and make recommendations for picking an acceptable scheme depending on individual requirements.

**Objectives**  
To establish a file storage system that ensures encryption and security, facilitating secure file transfer among users located remotely.

To improve the security of file stored on cloud storage using AES, DES, RSA algorithms.

To optimize the speed and efficiency of system by splitting the data in different chunks and storing those parts in different servers on cloud.

To implement a robust data storage and retrieval system in the cloud, even in cases where the data owner lacks control, to ensure stringent security measures are in place.

**Algorithm**

1. Depending on the file's length, divide the uploaded file into n pieces.

2 Create a unique symmetric key K at random for each file that will be stored.

3. Use the key K to symmetrically encrypt the file.

4. Produce a public key and a private key pair of asymmetric keys.

5. Use asymmetric encryption to encrypt the symmetric key K using the recipient's public key.

6. Securely keep the encrypted symmetric key and the encrypted file.

7. Get the encrypted symmetric key and the encrypted file.

8. Using the recipient's private key, decrypt the encrypted symmetric key.

9. To decrypt the file, use the decrypted symmetric key.

10. After decrypting, join all of the files.

**Methodology**  
  
**A. Advanced Encryption Standard (AES)**

The AES algorithm, also known as the Rijndael algorithm. The AES algorithm operates on distinct blocks of data, typically 128 bits in size, and utilizes encryption keys of varying lengths, including 128, 192, and 256 bits. Each block is encrypted independently, and the resulting ciphertext is obtained by combining the encrypted blocks. The AES algorithm is based on a substitution-permutation network (SPN) architecture. This design incorporates substitution and permutation operations to achieve secure encryption of data blocks. The AES (Advanced Encryption Standard) algorithm is comprised of multiple interconnected processes, which include bit shuffling and substitution operations. These processes are designed to transform inputs into specific outputs as part of the encryption process, ensuring the confidentiality and integrity of the data being encrypted.

Key Expansion: In the AES (Advanced Encryption Standard) algorithm, a single key is initially used for encryption. However, in subsequent rounds, multiple keys are employed, each applied independently in separate rounds of the encryption process.

**B. Data Encryption Standard (DES)**

It stands for Data Encryption Standard. The key size used by the DES algorithm is 56 bits. This key is used to convert plaintext into ciphertext and vice versa throughout the encryption and decryption procedures. Using a unique key, the DES algorithm converts a 64-bit block of plaintext into a corresponding 64-bit block of ciphertext.

DES is a legacy encryption algorithm that is gradually being replaced by more secure algorithms with larger key sizes, such as AES (Advanced Encryption Standard).

## DES was widely used as a standard encryption algorithm for many years due to its efficiency and widespread adoption, but its key size is now considered inadequate for modern security requirements. If the algorithm utilized an asymmetric encryption approach, the encryption key and the decryption key would not be the same.

**C. RSA Algorithm**

The public key and the private key are the two keys that are utilized in RSA for encryption and decryption, respectively. The private key is kept hidden by the owner and is used to decrypt the encrypted data, while the public key is shared with others and used to encrypt data.

Numerous applications, including secure internet communication, digital signatures, and the encryption of sensitive data, make extensive use of RSA.

**Asymmetric cryptography example:**   
While requesting data from the server, a client (for instance, a browser) transmits the server its public key. The data is encrypted by the server using the client's public key, and then transmitted to the client. The client then decrypts the data using their corresponding privatekey.  
  
As this is asymmetric, nobody else save the browser can decode the data even if a third party obtains the public key of the browser.

To accomplish the previous objective, the following approach must be used:

1. File loading on the computer.
2. The submitted file is divided into N pieces.
3. Encrypting every component of the file with a chosen algorithm
4. A different algorithm is then used to secure the cryptography algorithm keys, and the user is given the public key for this algorithm.

After completing the previously mentioned four procedures, you will have N encrypted files stored on the server, along with a key that can be obtained as a public key and used to unlock the files and download them.

Follow these steps to restore the file:

1. Set the key onto the server.
2. Decrypt the algorithmic keys.
3. Utilizing the same algorithms that were used to encrypt them, decrypt each of the N parts of the file.
4. The N pieces are combined to reconstruct the original file, which is then made available for download to the user.

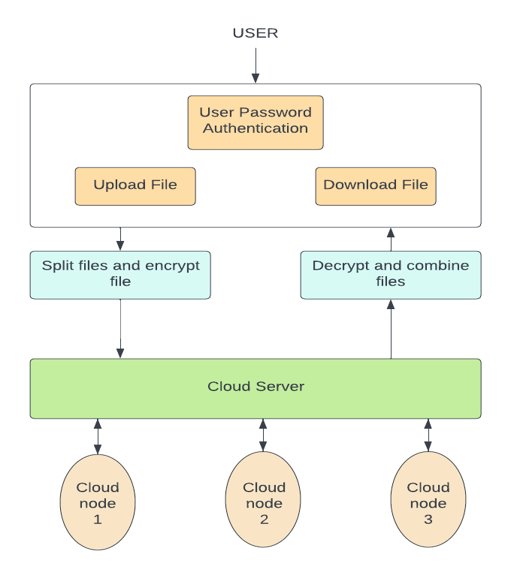
**Control Flow Diagram**  
  


Fig 1: Control Flow Diagram

**Splitting and Encrypting files**

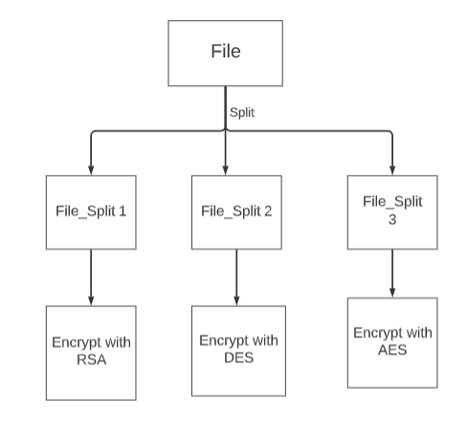


Fig 2: Splitting and Decrypting Files

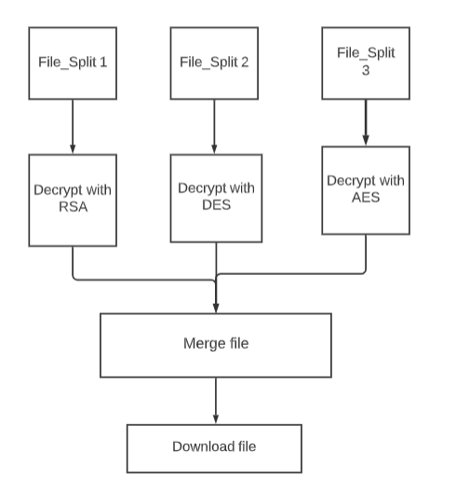
**Decrypt and Merging Files**  


Fig 3: Decrypt and Merge Files

**Existing Work**

Cloud servers are being utilised to store, manage, and compute a variety of data. Applications are moving to cloud computing platforms in large numbers, which must be managed. Under the current system, just one algorithm is employed to encrypt and decrypt data. Yet, high level security cannot be achieved with the use of a single algorithm. If we employ the public key cryptography algorithm, then the security of storing the public key becomes a concern.Key sharing in a multiuser scenario can cause transmission problems. High security is achieved with public key cryptography algorithms, but data encryption and decryption take the longest time possible.  
  
**Proposed Work:**

The owner of the cloud server uploads the data via our technology. To strengthen file security in cloud computing, the source file is separated into numerous portions. Each encryption algorithm is employed to encrypt every component of the file. Cloud storage is used to store encrypted files. Each component of the file is stored on a different cloud database server.

Even in the event of an attack, no critical data is compromised, as only a single fragment of each uploaded file, in any format, is stored on the cloud server.

**Implementation**

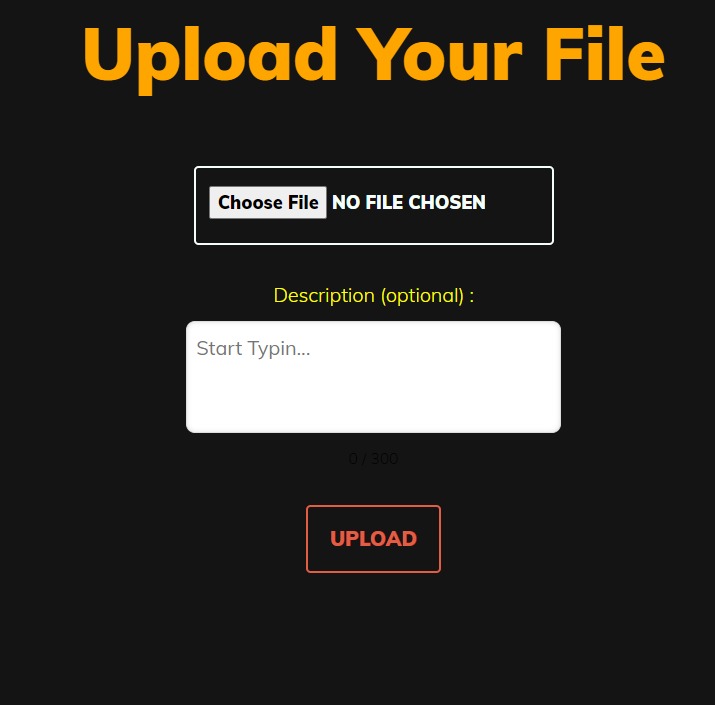


Fig 4: Upload File

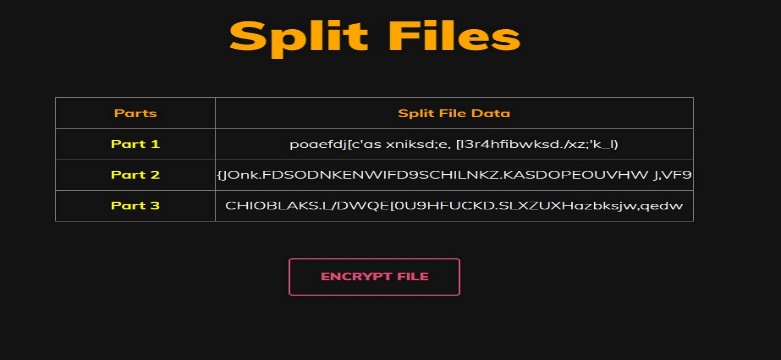


Fig 5: Split Files



Fig 6: Enter Secret keys



Fig 7: Encrypted Files

**Future Enhancements**

In this project we have considered only text files as of now. In future we can add more file types for securely storing. Implement better ways to share the key file to user like embedding the key in images etc. Hybrid cryptography is a useful method for protecting cloud-based data storage. Using hybrid cryptography, the following potential future improvements could be implemented to further increase the privacy of file storage in the cloud:

Quantum-resistant algorithms: With the introduction of quantum computing, standard encryption methods may become vulnerable to assaults. Quantum-resistant algorithms, like lattice-based or code-based cryptography, could be added to hybrid cryptography to strengthen it against upcoming threats from quantum computers.

Multi-factor authentication: Hybrid cryptography could be paired with multi-factor authentication (MFA) to add an additional layer of protection. Before granting access to the encrypted data, MFA includes employing several authentication factors, such as a password and a biometric.

Zero-knowledge proofs: Zero-knowledge proofs (ZKP) allow one party to convince another that they are aware of specific details without actually disclosing those details. ZKP could be used to hybrid cryptography to improve secure data flow between many parties without disclosing the encryption key.

**Conclusion**

The implementation of the suggested approach, including the encryption and decryption of files, is thoroughly described in the paper. The suggested solution provides a reliable and secure technique for storing files on the cloud, guaranteeing that information is shielded from unauthorized access or change. To guarantee that the system continues to be effective, potential vulnerabilities must be constantly addressed and updated, just like with any security solution. The suggested approach calls for symmetric AES and DES encryption of the data, followed by asymmetric RSA encryption of the AES and DES keys. The paper provides a detailed explanation of how the suggested approach is put into practice, including how files are encrypted and decrypted. The suggested solution offers a trustworthy and secure method for uploading files to the cloud, ensuring that data is protected from illegal access or modification. To ensure that the system remains to be successful, potential vulnerability must be regularly identified and revised, just as with any secure solution. According to the suggested method, the data would first be encrypted using symmetric AES and DES before the AES and DES keys would be encrypted using asymmetric RSA.

**References**

1. "A Hybrid Cryptography-based Secure File Storage System for Cloud Computing" by K. V. Ramachandran, Naveen Kumar, and R. Sriramakavacham.
2. Ankit Gupta and Dheerendra Singh's "Hybrid Cryptography based Secure File Storage on Cloud."
3. "A Hybrid Cryptography-based Approach for Secure File Storage in Cloud Computing" by S. Senthil Kumaran and S. Santhosh K.
4. Hybrid Cryptography for Secure File Storage on the Cloud by P. N. Shriram.
5. "Secure File Storage on Cloud using Hybrid Cryptography and Attribute-based Encryption" by R. M. and Anitha. Hemalatha.
6. A survey of secure cloud file storage using hybrid cryptography is presented by S. Both Sivasankari and S. Sathish.
7. "Hybrid Cryptography for Secure File Storage on Cloud: A Survey," by R. Santhi and V. N. Sumathy.
8. S. Srinivasan and K. Sathish Kumar's "Hybrid Cryptography based Secure File Storage in Cloud: A Review."
9. "A Review of Secure File Storage on Cloud using Hybrid Cryptography" by N. G. Patel and J. M. Patel.
10. P. S. Verma and P. R. Dubey's "Hybrid Cryptography based Secure File Storage on Cloud: A Systematic Review."
11. "Hybrid Cryptography Based File Storage Security in Cloud Computing" by Shangquan Wang, Xuelian Lin, and Shengyu He
12. "Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by Gaurav Kumar, Kuldip Singh, and R. K. Jha
13. Ajay Kumar and S. S. Tyagi's "Hybrid Cryptography for Secure Data Storage in Cloud Computing: A Survey"