International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES & RSA Algorithms

Mrs. M.Swarnalatha
Computer Science HOD
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
lswarna@sphoorthyengg.ac.in

P. Shivani
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
shivani512.reddy@gmail.com

N. Kiran Kumar
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
kirankumarnelluri11@gmail.com

D. Akshitha Reddy
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
akshitha0205@gmail.com

***Abstract*— The cloud is widely used in various industries, military, and educational institutions to store large amounts of data and provide various services. However, security is a major concern when storing data in the cloud. To address this concern, various techniques like cryptography and steganography are commonly used. But, a combination of cryptographic algorithms of symmetric key and steganography0 is a more secure approach. AES and RSA algorithms are used to encrypt and decrypt data with keys of different sizes. In AES 128, 192, 256 bit keys are used to encrypt and decrypt data where as in RSA algorithm there are 2 keys public and private (typically of size 1024-4096 bits). The methodology involves splitting the file into three parts and encrypting them using different encryption algorithms. This ensures better security and protection of customer data by storing encrypted data on a single cloud server using AES and RSA algorithms.**

The cloud is used in many fields for services and storing data, but security is a major concern. Symmetric key of cryptography provides better security. AES and RSA algorithms with keys of different sizes are used. The file is split into three parts and encrypted using different algorithms. Data is stored on a single server using AES and DES algorithms for better protection.

Keywords*— *cryptography, AES Algorithm, RSA Algorithm, cloud computing and storage, Hybrid cryptography, Encrypt, Decrypt.

I. INTRODUCTION

Nowadays we are using safe file storage over the network due to the expanding use of mobile devices and advancements in networking technology. The most widely used technique for all kinds of data security is cryptography. This suggested plan will also guarantee that mechanisms for confidentiality, integrity, and availability are applied throughout the model. Our project's suggested approach is capable of providing all the necessary security for cloud-based data [4]. AES and RSA are used to secure the files because they have the highest throughput for encryption and decryption compared to other symmetric algorithms. The primary goal is to fulfill the data security principle, which is accomplished through splitting and merging. When the hybrid method is used in a cloud environment, the remote server becomes more secure, allowing the cloud providers to gain the user's increased confidence.[6] Public key cryptography and symmetric key cryptography are two types of Encryption that are used to transform the original data into an unintelligible format. This method employs keys to convert data into an unintelligible format. Therefore, only authorized users are able to view data on cloud servers. Data encrypted with a cipher is accessible to everyone. [6]

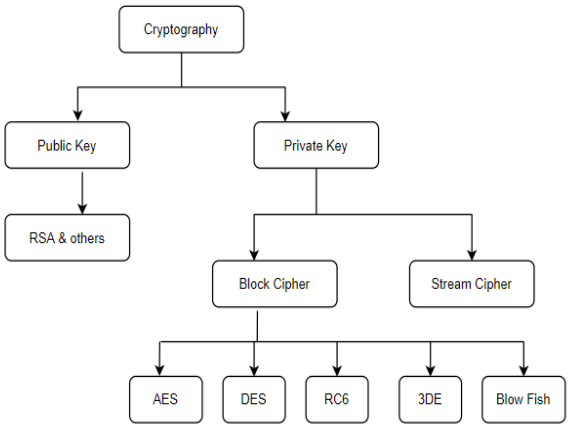

Fig.1. Cryptography

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A. Cloud Computing:

The term "cloud computing" refers to an established idea. A user of a system can store, retrieve, change, and update the contents of that specific system while using it. However, cloud computing refers to such operations that are carried out online.

A model called "cloud computing" makes it possible to quickly provision and release a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) over a network while requiring little management work or service provider interaction. [7].

By reducing operational and capital expenses, cloud computing enables IT teams to concentrate on strategic initiatives rather than maintaining storage security and availability. The following are the features of cloud computing: a large network, on-demand self-service, resource sharing, quick elasticity, and measured service.

B. Cryptography:

Data is shielded from third parties by being converted into an unreadable format using cryptography. The primary goal of cryptography is to keep data secure from outside parties [6]. There are two different kinds of algorithms, namely (i) symmetric key-based algorithms, also referred to as conventional key algorithms, and (ii) asymmetric key-based algorithms, also referred to as public-key algorithms. There are two additional categories for symmetric algorithms.

C. Hybrid Cryptography:

The combination of two encrypted methods, symmetric encryption and asymmetric encryption, is known as "hybrid cryptography". You can combine the speed and strength of the two algorithms if you can use several different kinds of algorithms to strengthen the encryption [5].This technique is employed to guarantee secure cloud-based storage systems. To illustrate the distinction between less secure and more secure systems, two methods are used here. The first technique uses the AES and RSA methods, with AES being used for informational or text encryption and RSA being used for key encryption. The second, safe method employs the AES algorithm. This method offers double encryption over data and keys, which offers higher protection than the first [2].

Hybrid cryptosystem phases:

Phases of a Hybrid Cryptosystem Two stages make up the hybrid cryptosystem, which is used to secure files:

Encryption Phase:

The encryption stage as depicted in Figure 2, the encryption procedure was carried out in a number of steps. Start by using the file system module to segment the downloaded file into three sections after encryption. Using two distinct cryptographic methods, RSA, AES and MD5 each part is encrypted. The file that contains the merged regions is then reloaded to the cloud. [1]

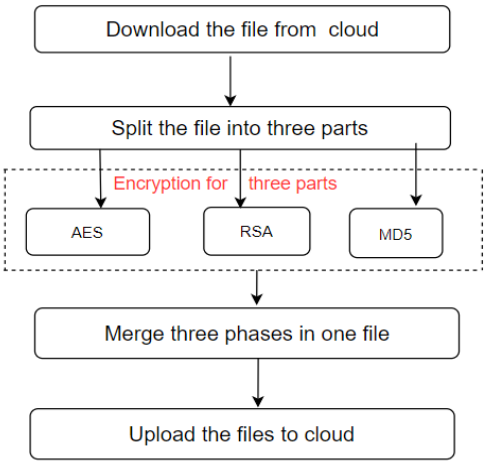

Fig.2. Encryption Phase

Decryption Phase:

The decryption phase, in comparison, proceeds in the exact manner as the encryption phase [1]. Download the protected file first, after which it will be divided into three parts that will be used for decoding in accordance with the RSA, AES and MD5 encryption algorithms. The proposed technique's decryption process is depicted in Figure 3.

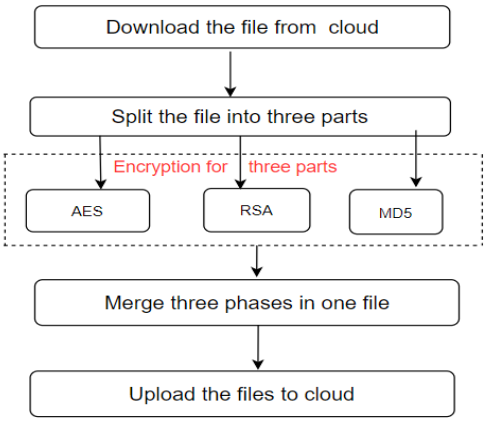

Fig.3. Decryption Phase

II. Problem Statement

Customers' information stored by cloud service providers is susceptible to numerous dangers. In our job, we take into account four different threat models. The first is a single point of failure, which will have an impact on data availability and make it more difficult for the customer to recover his stored data from the server in the event that a cloud service provider's server fails or crashes. Data

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

accessibility is another crucial concern that might be impacted if the cloud service provider (CSP) goes out of business.[6]

The data integrity danger is the second one. Integrity refers to the degree of trust that the data in the cloud is accurate and secure against unauthorized, unintentional or malicious alterations. Such concerns are no longer helpful, so a customer of a cloud service cannot fully depend on the cloud service provider to ensure the storage of his important data.

The majority of companies that have been hesitant to embrace cloud computing have done so out of concern that their data may have been compromised.[4] Because the cloud is a multi-user setting where all the resources are shared, this accomplishment is possible. Additionally, because it is a third-party tool, the provider may view or improperly handle the data. Humans are prone to having doubts about another person's abilities, which makes companies and confidential business data seem like an even bigger risk. In addition, there are a number of outside dangers that can cause data leakage, such as malicious attacks on cloud service providers or unauthorized access to user profiles. [4]

III. LEARNING METHODOLOGY

A. Advanced Encryption Standard

The Advanced Encryption Standard (AES), which is also recognized as 'Rijndael,' represents a symmetric-key block cipher algorithm. This algorithm possesses three stable 128-bit block ciphers that have cryptographic key sizes of 128, 192, and 256 bits, respectively.

Regarding its specifications, the AES algorithm has a maximum block size of 256 bits, whereas its key size is boundless. The AES design relies on a substitution-permutation network (SPN) and not on the Data Encryption Standard (DES) Feistel network. This distinction makes AES more potent and rapid than Triple-DES, which utilizes the Feistel network.

Step-wise description of the algorithm:[9]

Key Expansions:

Round keys are derived from the cipher key by the usage of AES key schedule, it also requires a separate 128-bit round key block for each round plus one more.

Initial round:

Upload round Key - the use of bitwise XOR each byte of the state is blended with a block of the round key.

Rounds:

(a) Sub Bytes - consistent with a lookup table each byte is changed with every other in a non-linear substitution step.

(b) Shift Rows - A transposition step in which the final three rows of the nation are shifted cyclically a sure quantity of steps.

(c) Mix Columns - A blending operation which operates on the columns of the state, combining the four bytes in each column.

(d) Add round Key

Final Round (no blend Columns).

(a) Sub Bytes

(b) Shift Rows

(c) Upload round Key

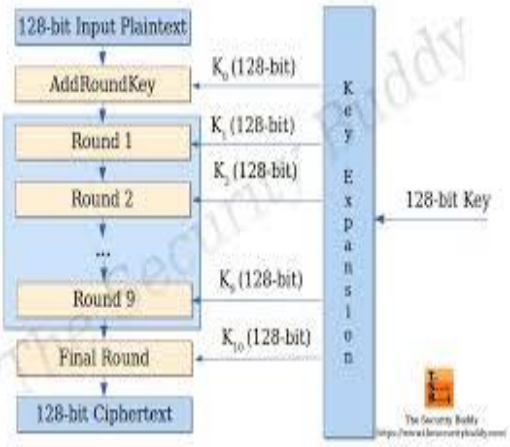

Fig.4. Working of AES algorithm

B. Rivest -Shamir-Adleman (RSA)

The algorithm known as Rivest-Shamir-Adleman (RSA) is widely recognized as a highly secure method for public-key (asymmetric) cryptography. This is due in large part to the inability to efficiently factor numbers that are very large, typically in the range of 100-200 digits, which the algorithm takes advantage of.

The algorithm for using an encryption key (e, n) is as follows: [9]

- Represent the message as an integer between 0 and (n-1). If the message is huge, break it up into several blocks and represent each block using an integer within the same range.
- Encrypt the message by computing its eth power modulo n, resulting in a cipher text message C.
- To decrypt the message, compute its dth power modulo n.
- The encryption key (e, n) is made public, while the decryption key (d, n) is kept private by the user.
- The optimal values for e, d, and n can be determined as follows:

  1. Select two large prime numbers represented as p and q.

  2. Set n equal to p * q.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

3. Choose a large integer d such that its greatest common divisor (d, ((p-1) times (q-1))) = 1.

4 Find e such that e *d = 1 (mod (p-1) * (q-1)).

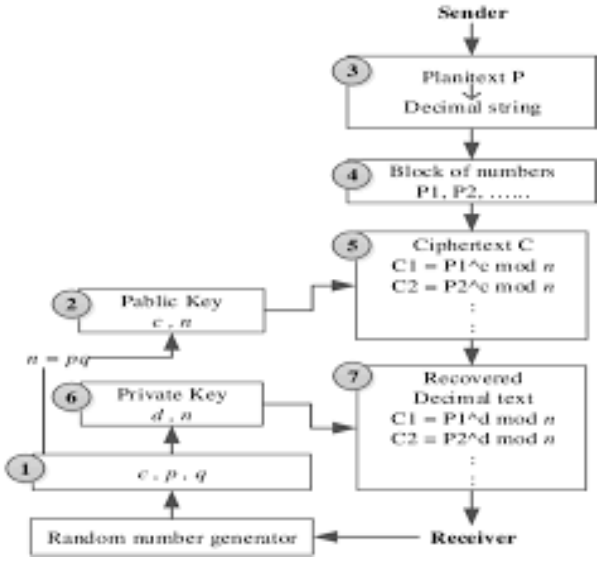

Fig.5. Working of RSA Algorithm

IV. CONCLUSION

The security of data saved on the cloud is one of the most important user concerns because cloud storage is one of the most commonly used services in almost every field. One of the most important security measures to maintain confidentiality is encryption, which is routinely carried out before transferring data from the device to the cloud over networks. For the cloud storage environment, combining two encryption methods—one of each kind—creates a better cryptosystem enhancement.[8] A high degree of security is offered by hybrid cryptosystems in addition to maintaining confidentiality, usability, and scalability. Instead of storing the data in its original form, the cloud stores it as cipher text. By storing the data as ciphertext in the cloud, even if the cloud provider experiences a data breach or unauthorized access, the encrypted data remains protected. The original content is difficult to recover without the specific symmetric key that was used to encrypt it, which is securely encrypted with the recipient's public key. Overall, the use of a hybrid cryptosystem in cloud storage environments enhances security, while maintaining usability and scalability. It ensures that sensitive data remains confidential and protected from unauthorized disclosure or tampering.

REFERENCES

[1] A. Bermani, T. Murshedi and Z. Abod, "A hybrid cryptography technique for data storage on cloud computing", Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 6, pp. 1613-1624, 2021.

[2] U. Kumar and M. Prakash, "A Hybrid Encryption Algorithm for Secure Data Storage on Cloud", International Journal of Creative Research Thoughts (IJCRT), vol. 8, no. 2320-2882, 2020.

[3] U. Kumar and M. Prakash, "A Hybrid Encryption Algorithm for Secure Data Storage on Cloud", International Journal of Creative Research Thoughts (IJCRT), vol. 8, no. 2320-2882, 2020. Available: IJCRT2007048.pdf

[4]] T. Gaur and N. Kharb, "Security of Data Storage in Cloud Computing", Nanomedicine & Nanotechnology Open Access, vol. 5, no. 2, 2015. Available: Security of Data Storage in Cloud Computing (ijcaonline.org)

[5] https://www.researchgate.net/publication/361262267_Secure_File_Storage_On_Cloud_Using_Hybrid_Cryptography

[6] International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

[7] Security of Data Storage in Cloud Computing Tania Gaur M. Tech (CSE) Student ITM University Nisha Kharb Assistant Professor ITM Universit International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 10, January 2015.

[8] e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, Open Access, Fully Refereed International Journal) Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

[9] rnational Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV9IS020014 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : www.ijert.org Vol. 9 Issue 02, February-2020