Secure File Storage in Cloud Using Hybrid Cryptography

Meher Sudhakar, Student, Department of Computing Technologies, SRM Institute of Science and Technology, Chennai, India, abbireddimehersudhakar@gmail.com

K.Sai Praneeth, Student, Department of Computing Technologies, SRM Institute of Science and Technology, Chennai, India, praneeth1706@outlook.com

Mrs. M. Revathi, Assistant Professor, Department of Computing Technologies, SRM Institute of Science and Technology, Chennai, India, revathim@srmist.edu.in

Abstract- Cloud computing has roots in earlier distributed computing technology that can be quickly and easily set up and taken down with little involvement from the user or service provider. Unlike traditional computing, where software and files are stored locally on the user's device, cloud computing stores these files on the service provider's servers, leading to potential security concerns. To address this, cloud providers can use encryption techniques like AES, DES, and RSA or steganography techniques like LSB to secure the data and provide a secure environment for users in the cloud.

Keywords: - AES, DES, RSA, LSB steganography, cloud, cryptography, encryption, decryption

I. INTRODUCTION

Technology is advancing rapidly and providing users with numerous convenientservices for managing large amounts of data storage and maintenance. Today, online services such as e-messaging, e-billing, e-transactions, and e-mail require users' data for processing, which may contain sensitive information like healthcare records, bank transactions, or credit card details. To protect this confidential data from malicious activity, there is a high demand for security and protection from unauthorized access. It is essential to develop a secure framework to safeguard confidential data and prevent harm to users. This requires converting personal data into an unreadable form using cryptography, making it indecipherable for attackers and only accessible to authorized users. Cryptography enables us to convert a readable message into an encrypted format that malicious parties cannot understand.

The AES algorithm is a simple implementation that requires less memory and utilizes 128, 192, or 256-bit key sizes. [1]It consists of four steps: Byte sub, shift row, mixed column, and add round key. The byte sub-step is the only non-linear step responsible for creating confusion in the data. In contrast, the rest of the steps are linear, meaning they only involve permutation operations for diffusion. [2]

On the other hand, the RSA algorithm is an asymmetric algorithm that uses both public and private keys for encryption and decryption. [3]

The DES algorithm, on the other hand, is symmetric, using a single key for both encryption and decryption, with a key size of 56 bits. While the DES algorithm has the quickest encryption time, the AES algorithm has a lower memory usage. The encryption time between the AES and DES algorithms varies. [4] [5]

LSB is the Least Significant Bit; as the name suggests, it replaces the least bit with the data bits. Steganography means hiding the data. LSB Steganography uses videos, audio, and images to hide the data [6]. Here we are using an image to hide the keys. Using too many keys may change the image as the bits of the image will be substituted with bits of the data. [7]

Authentication is a crucial aspect in ensuring data confidentiality and integrity security. To address this, the owner should first encrypt their data before transferring it to cloud service providers and only provide the decryption key to authorized users [8]. The use of cryptography helps protect user data by ensuring its confidentiality and security against unauthorized access and malicious attacks. Without the proper key, an unauthorized user cannot view or alter the data. Only authorized users can convert the encrypted data back to its original form. [9] [10]

II. LITERATURE SURVEY

Cloud computing is a widely available, convenient, and on-demand access to a shared pool of configurable resources such as networks, servers, storage, applications, and services that can be quickly provisioned and released with little management effort or interaction with the service provider [11]. This cloud model consists of five

 DOI : 10.35291/2454-9150.2023.0025

essential characteristics, three service models, and four deployment models.

The proposed hybrid encryption/decryption technique combines a new public key and symmetric key algorithm, making it less complex and more secure than a single algorithm. It operates in two stages. [12]Firstly, RSA encryption is performed, and the output is then passed to the knapsack approach in the second stage.

This paper examines the complex security challenges presented by IaaS-based cloud computing and highlights the technological and legal concerns from the perspectives of stakeholders. The author suggests potential areas for future security research and development to improve the security of this technology.

Zissis highlighted several security issues that must be addressed when adopting cloud computing, such as data integrity, confidentiality, availability, threats, identification, and authentication. A third-party auditor has been introduced to provide auditing services on the user's request, which helps to ensure data integrity. [13] [14]

The paper presents a security model to address the core problem of cloud security. The model implements a hybrid encryption technique that combines blowfish and a document part and employs SRNN for secure communication between clients and servers. However, due to the dynamic nature and multi-tenant qualities of cloud computing, traditional security systems are not suitable [15]. The following challenges are addressed: 1) Due to the dynamic nature of cloud computing and the lack of an established security framework, it is difficult to isolate a specific asset in the case of a security breach and to coordinate a combined security effort; 2) Due to the openness of the cloud and the sharing of virtualized assets among multiple tenants, client data may be accessed by unauthorized users.

III. PROPOSED WORK

A hybrid cryptography method is proposed to enhance security for cloud data compared to traditional techniques that share keys between users. This method uses three types of encryptions: AES, DES, and RSA, along with LSB steganography for secure key sharing. The data is split into three parts, each encrypted with a different technique, and the keys are securely embedded in an image.

This proposed method is expected to meet the security needs of cloud data centers. AES, DES, and RSA provide efficient encryption and decryption with minimum time and maximum throughput compared to other symmetric algorithms. When implemented in a cloud environment, the hybrid approach strengthens server security, increasing trust from users in cloud providers.

Cryptography transforms original data into an unreadable form using keys. Hybrid cryptography is divided into symmetric-key and public-key cryptography, allowing only authorized individuals to access the data from the cloud. While anyone can view the ciphertext data, it remains unreadable without the proper key.

IV. IMPLEMENTATION

In data management, the cloud plays a critical role by offering secure data handling and remote access. Users from anywhere can utilize the cloud to access their data, but as the cloud is a third-party application, security measures must be in place to minimize the risk of data attacks. To achieve this, encryption techniques are employed.

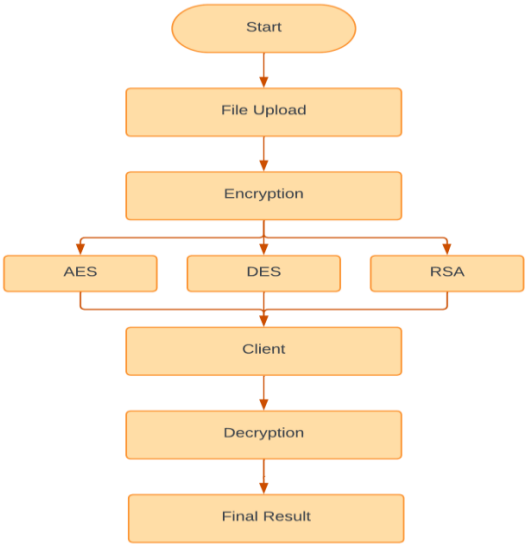

Fig.4.1.System Architecture

Existing methods of providing security for cloud data, such as AES, DES, and RSA, typically only employ a single type of encryption depending on the user's needs. However, the main issue with these methods is using a single key for encryption, which, if exposed, could result in the loss of all data. To address this, a hybrid cryptography approach is proposed, which combines the existing encryption methods in three ways. Upon uploading data to the cloud, the data is divided into three parts and encrypted using different techniques for added security.

1. To register, the owner either logs in if already registered or signs up by providing personal information such as name, email, phone number, and password.
2. The owner then selects a file to transfer by browsing their local storage.
3. The selected file is uploaded, and the owner can view all files they have uploaded or have access to.
4. The owner can divide the file into multiple parts using the split option.
5. The user can log in and request access to the

 DOI : 10.35291/2454-9150.2023.0025

uploaded file in the cloud.

6. The owner accepts the request and sends the necessary keys to the user.
7. The user can then use the keys to decrypt the file.

The owner has the following modules:

1. Registration: It is used to register if the owner does not have an account on the website
2. Login: It is utilized to login into the website
3. File Upload: It is used to upload the files.
4. View Files: It is used to view the uploaded file
5. Split data: It is employed to split the data into keys.
6. View Request: It is used to view user requests.
7. Logout: It is used to log out from the website.

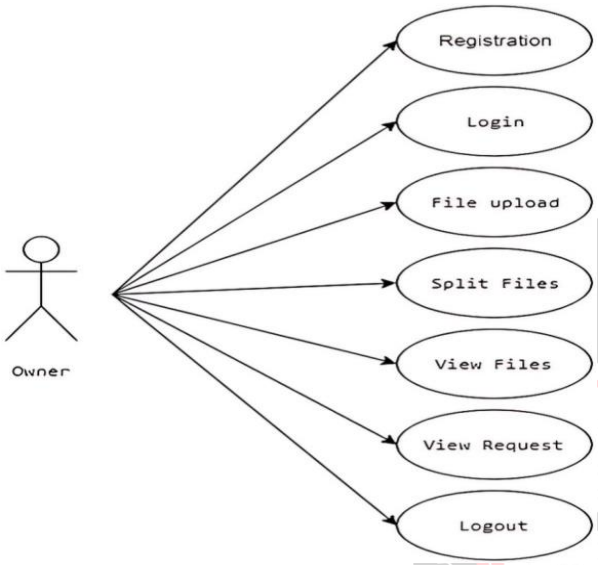

Fig.4.2.Owner

The user has the following modules:

1. Registration: It is used to register if the user is new to the website
2. Login: It is dedicated to login into the website
3. View Files: It is used to view the files in the cloud.
4. Send Request: It is used to send the request to the owner.
5. Download Files: It is used to download the file by providing the necessary keys.
6. Logout: It is used to logout from the website.

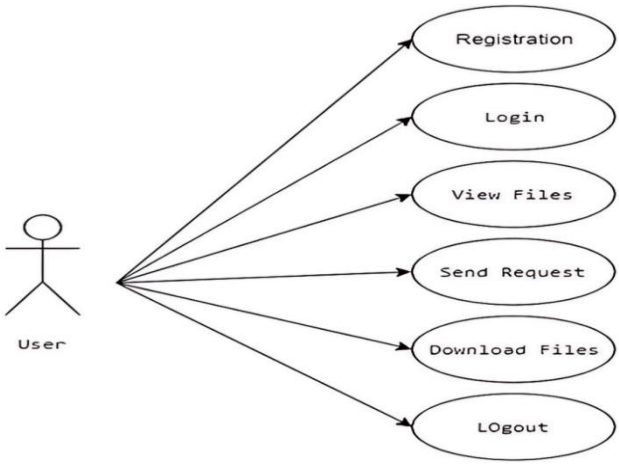

Fig.4.3.User

For the first part, encryption will be performed using the AES algorithm, the second part will be encrypted using the DES algorithm, and the third part will be encrypted using the RSA algorithm. The keys for AES, DES, and RSA are embedded in an image through LSB steganography. To retrieve the data from the cloud, the keys must be extracted from the image and utilized to decrypt the data with AES, DES, and RSA. The decrypted data is combined and saved as a file, offering enhanced security.

V. RESULTS AND DISCUSSION

After examining the performance of single and multiple encryption algorithms, we can conclude that using a hybrid encryption approach with multiple encryption algorithms (such as AES, DES, and RSA) provides significantly better results than using a single algorithm alone.

We have considered three encryption techniques in this project to secure the data. Those three techniques are AES, DES, and RSA. We have also used LSB steganography to store the encrypted keys in the image.

We have designed a website using python and HTML to show the encryption and decryption between sender and receiver. The working is as follows:

First, the sender uploads the file to the cloud and encrypts the file using encryption techniques. Here the encrypted keys are divided into three distinct parts. The first part is encrypted using AES, the second with DES, and the third with RSA. At last, these three different keys will be stored in an image using LSB. If the receiver wants to see the file, the receiver can send the request to the sender. So, the sender now accepts the request and sends the key to the receiver. The receiver can decrypt the file using those keys.

The above working of hybrid cryptography is secure as the keys stored in the image cannot be emanated. By any chance, if cryptography is compromised, steganography helps to hide the keys from the attacker.

 DOI : 10.35291/2454-9150.2023.0025

While there were undoubtedly myriad of benefits to the study, there are also several limitations that should be considered, such as:

- The data size limit imposed on system subscribers may hinder users from deploying the desired resources for storage and sharing, among others.
- If a user's access permission is deleted, then it becomes necessary to modify all the keys and public values known to that user, rendering such schemes impractical.
- The initial cost of acquiring space from the cloud service provider could have been more manageable, leading the study to focus on a restricted scope.
- The cloud domain's resource security level may not meet users' needs, highlighting the potential for further research to improve resource security.

VI. CONCLUSION

The proposed approach enhances security by using a hybrid of AES, DES, and RSA encryption, which is stronger than the existing method that only employs DES. This method encrypts messages with AES, DES, and RSA and hides the cipher text keys inside an image using LSB image steganography. Steganography is a robust tool for secret information exchange and is becoming more popular with the growth of digital technology and the internet. The proposed method requires attackers to possess knowledge of both cryptography and steganography to extract data from the image. The encryption time is faster than the existing method, and brute-force cracking is difficult due to the use of AES & RSA with the DES Key. The proposed method provides better security; in the future, it can be combined with other steganography techniques for enhanced security.

Our future plans include implementing additional encryption algorithms and public key encryption techniques into the project. We intend to analyze the hybrid algorithm's performance in real time on the cloud and against various cryptanalytic attacks to assess its strength and reliability. Our ultimate goal is to provide better and enhanced ongoing security solutions that result in more efficient and improved user experiences with cloud services, effectively addressing information security, vulnerability, and non-repudiation. In the future, we aim to achieve high-level security by hybridizing public key cryptography algorithms.

REFERENCES

[1] S. J. H. G. R. V. A. W. a. V. Y. Gajanan Tikhe, "Secure File Storage on Cloud Using Hybrid Cryptography," *International Research Journal of Engineering and Technology,* vol. 8, no. 6, June 2021.

[2] M. a. D. J.Ajay Kanna, "SECURITY IN CLOUD USING HYBRID CRYPTOGRAPHY," *International Journal of Advanced Science and Engineering Research,* vol. 5, no. 1, 2020.

[3] S. Karishma, "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm," *IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES,* vol. 5, no. 3, 2018.

[4] T. M.Naveetha Krishnan, "SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY," *International Journal of Advanced Research in Computer Science Engineering and Information Technology,* vol. 6, no. 3, April 2021.

[5] S. B. a. N. P., "Development of Secure File Storage on Cloud using Hybrid Cryptography," *International Journal of Innovative Research in Science, Engineering and Technology,* vol. 9, no. 4, 2020.

[6] P. T. A. J. Shruti Kannat, "Review of Secure File Storage on Cloud using Hybrid Cryptography," *International Journal of Engineering Research & Technology,* vol. 9, no. 2, February 2020.

[7] P. V. M. a. A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," *International Conference on Wireless Communications, Signal Processing and Networking,* 2016.

[8] A. SadanandGhadi, "Secure File Storage Using Hybrid Cryptography," *International Journal of Innovative Science and Research Technology,* vol. 5, no. 12, December 2020.

[9] U. K. a. J. Prakash, "Secure File Storage on Cloud Using Hybrid Cryptography Algorithm," *International Journal of Creative Research Thoughts,* vol. 8, no. 7, July 2020.

[10] P. A. R. B. a. E. J. S. Gokulraj, "Secure File Storage Using Hybrid Cryptography," *SSRN,* 11 March 2021.

[11] B. a. D. B. R. Singh, "SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM," *International Journal of Advance Research in Science and Engineering,* vol. 6, no. 11, November 2017.

[12] A. K. D. R. K. B. a. R. M. W. Vinay Ponduval, "Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography," *International Journal of Recent Technology and Engineering,* vol. 8, no. 6, March 2020.

[13] A. N. a. S. M. Shinde, "Implementation of Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm," *International Journal of General Science and Engineering Research,* vol. 4, no. 2, 2018.

[14] P.Suganya, "SECURE FILE STORAGE PLATFORM USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY," *International Journal of Applied Engineering and Technology,,* vol. 9, 2020.

[15] P. S. a. R. Malik, "A Hybrid Cloud Security Model for Securing Data on Cloud," *Workshop on Computer Networks & Communications,* vol. 2889, no. 13, 2021.

 DOI : 10.35291/2454-9150.2023.0025