Available online @ https://jjem.jnnce.ac.in
https: www.doi.org/10.37314/JJEM.SP0204
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 08 December 2024

Two Level Secured File Storage Using Cloud Computing

Pallavi G R [1], Sampath Kumar S [2]

Student [1], Assistant Professor [2], Department of Master of Computer Applications
JNN College of Engineering, Shimogga

pallavigr907@gmail.com. sampathkumar@jnnce.ac.in

Abstract

As for every business sector starting from military and ending with the higher education needs many kinds of services. As cloud provides almost unlimited storage. Even though many of these clients do not have direct physical interaction with the server computer, it is possible to request to view or to access data in this cloud. How eve'; the most important concern that has been associated with online data storage commonly referred to as cloud storage security. There are number of ways for solving this security issue. The two common solutions that are widely used now are as follows: steganography and cryptography. Nevertheless, there are cases where some single method or Algorithm cannot give very good security Hence, in this paper, we are presenting a newform of security method the is composed of several cryptographic algorithms, namely steganography and symmetric key. The methods used in this recommended system of avoiding data leakage are 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6), and AES (Advanced Encryption Standard). Both Ihe algorithms use 128-bit keys. Thus, the key data is concealed using the ISB steganography method. The key details will he the traits often encrypted pan, the algorithm, and the key to the algorithm. Encryption is performed on the file in three parts. By utilizing multithreading, these various segments of the Jile will then be processed and encrypted through different algorithms at the same time. To embed the important information, LSB method is applied in an image. Enhanced security compliance as well as customer data protection is provided by our approach based on AES for storing encrypted data at one cloud server AES, DES and RC6 algorithm.

Keywords: *Cloud Computing and Storage, AES Algorithm, RSA Algorithm, Blowfish Algorithm.*

l. Introduction

The main intention might be coded in such a way as to escape detection. Perhaps even the real meaning has thus been disguised. It takes away all capacity for translation. Henceforth this memory will have simply to be kept locked up in man's mind. The text-to-data cypher is open source. Symmetric key cryptography uses a number of algorithms, some of which are AES, DES, 3DES, IDEA, BRA, and blowfish. The real trouble lies in giving it out. Even though answers to this kind of inquiry can be given within milliseconds by means of calculations carried out on gigantic computers, nevertheless there remains practically zero chance for genuine safety. The RSA key exchange method can be used in symmetric cryptography just like ECC. Similarly, in asymmetric algorithms such as those based on discrete logarithms or curves on ellipsoids it is possible and indeed desirable to use several variants. While this encryption method offers great security, it requires much longer times for encoding or decoding. The fact is hidden in stenographic wrapping. When one uses it there will be no suspicion that anything has been written on the paper at all. As a result only those who have been given permission know anything. Text steganography technology generates data with extraordinary security. A document envelope holds secret data from this correspondent. Text core files appear to be in good condition and can normally be opened once text has been added to them. The same holds true for obtaining private information, such as when an unauthorized person finds a text file. If the uninvited user attempts to retrieve the actual data, it will take a long time. Using the DES algorithm for this purpose, they

encipher the message in code before converting their result into a string of digits which can be used as access codes. The text will first be encrypted using the DES encryption method, while the original text will remain visible. The greatest need for line abbreviations absolutely outstrips all that can be accomplished with pigtail abridgements. employed the three-bit LSB technique for image steganography. The author, R. T. Patil, has recommended this system. The cover image hides user-identifiable info. And all this includes on-the-fly resource allocation, file retrieval from anywhere in the network, and LSB Steganographic encoding.it might be possible to hide a large quantity into an image. Cryptography is important because the use of cloud storage for storing data is inevitable. Data must be encrypted before being placed in the cloud storage.

cryptography: -

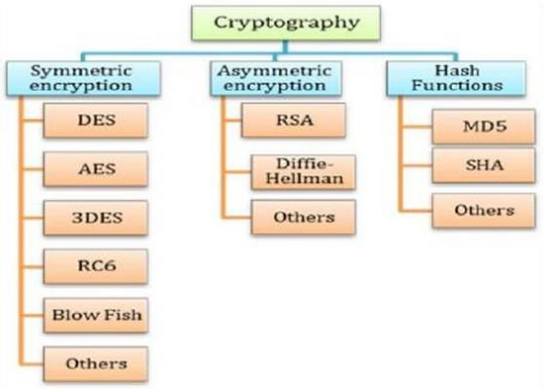

Figure 1: The three main categories of standard cryptography algorithms.

In this paper such cloud computing infrastructure as a service(IAAS)present and implement a high throughput design into use From paper1 like cloud computing. IAAS utilizes the internet to provide users with Cloud Storage a basic utility. This service has the following advantages: Internet and extra time to find the user process in case of problems.

2.Related work

Imran A. Khan and Rosheen Qazi et al. [1], Several encryption algorithms, including DES (Data Encryption Standard), RC6, and AES (Advanced Encryption Standard), are frequently used by the system. By using distinct methods to encrypt each section of a file, algorithmic diversity can be used to improve security. For instance, dividing a file into multiple sections and encrypting each with a distinct algorithm in a round-robin manner makes it more difficult for attackers to crack the entire file without being aware of all the encryption techniques utilized.

According to Wid A. Awadh, Ali S. Hashim et al. [2], They employ steganography, which embeds sensitive data using the Least Significant Bit (LSB) approach, to conceal data within photographs, This technique makes sure that even in the event that data is captured, it stays hidden among seemingly innocent pictures. By using many levels of encryption, their system uses the Multi-Level Encryption Algorithm (MLEA) and the Two Level Encryption Algorithm (TLEA), which provide strong security. Unauthorized access is considerably more difficult to achieve with this method.

According to Afrah Alba law, Nermin Hamza et al. [3], Their approach involves the integration of symmetric and asymmetric encryption algorithms, typically combining AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman). This dual-layer encryption ensures robust protection by leveraging the strengths of both encryption methods. The use of these hybrid techniques addresses common vulnerabilities and enhances the confidentiality and integrity of data stored in the cloud.

Parth Tandel, Abhinav Shubhrant, Mayank Sohani et al. [4], The use of hybrid cryptography, which combines symmetric and asymmetric encryption methods, is highlighted. Techniques like RSA and AES

are commonly combined to leverage the strengths of both methods. RSA provides secure key exchange while AES ensures fast and efficient data encryption.

Fully homomorphic encryption allows computations to be performed on encrypted data without decrypting it first, ensuring data privacy even during processing. This method is seen as highly secure but computationally intensive, making it suitable for highly sensitive data.

Raj Parab, Anwit Paul, Urjit Mojumdar, Rahul Patil et al. [5] One prevalent approach involves the combination of encryption and steganography techniques. For instance, the use of algorithms like RC6, 3DES, and AES ensures data security during storage and transfer. In particular, RC6 offers enhanced security with fewer rounds and higher efficiency due to its advanced operations, whereas 3DES, despite being phased out, still sees usage in certain applications due to its robustness. Blowfish, another powerful cipher, uses a Feistel network structure for effective encryption and decryption processes.

Dr. Sumagna Patnaik, A. Sunil, Rakesh Reddy et al. [6], To encrypt and safeguard data, the researchers suggest combining several cryptographic algorithms, including RC6 (Rivest Cypher 6) and AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard). Using a hybrid approach instead of a single encryption method allows for a more robust security architecture by utilising the strengths of each algorithm. The system uses steganography methods, especially the Least Significant Bit (LSB) approach, in addition to encryption to conceal important data inside files. Because of this dual-layer strategy, the keys are safe and unavailable to unauthorised users even in the event that encrypted data is intercepted.

Swami C, Marrynal S. Eastaffet al. [7], This this paper presented the Their approach combines multiple encryption techniques like AES, Blowfish, and RSA to enhance data security. By integrating steganography methods such as the Least Significant Bit (LSB) technique, they ensure that encryption keys are hidden within the data, adding an extra layer of security. This dual-layer security framework addresses data confidentiality, integrity, and performance efficiency, making it harder for unauthorized users to access sensitive information

Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul et al. [8], discusses the implementation of hybrid cryptography combined with image steganography for enhancing data security. Their study, published in the International Journal of Recent Technology and Engineering (IJRTE), focuses on leveraging both symmetric (AES and 3DES) and asymmetric (RSA) encryption algorithms to create a robust security framework. Additionally, they incorporate the Least Significant Bit (LSB) technique in image steganography to conceal encryption keys within images, providing an extra layer of security to the stored data. This dual-layered approach aims to protect sensitive information from unauthorized access while ensuring data integrity and confidentiality in cloud environments.

Swami C, Marrynal S.Eastaff et al. [9], This system uses a variety of cryptographic approaches in an attempt to overcome the security issues related to cloud storage. The authors suggest a hybrid strategy to improve the security of cloud file storage by combining symmetric and asymmetric encryption techniques. The Blowfish algorithm, which uses symmetric encryption, is efficient in encrypting data blocks rapidly and at a high throughput. By doing this, the data is safeguarded both during transmission and storage.

M. S. Abbas, S. S. Mahdi and S. A. Hussien et al. [10], Cryptographic keys and sensitive data are stored in the private cloud, while less sensitive data is preserved in the public cloud. This department ensures that critical information remains secure even in the case of a public cloud hack. This method preserves data privacy during processing by permitting computations on encrypted data without first decrypting it. It is particularly useful for processing sensitive data via third-party cloud services without revealing the real.

3.Proposed system

A way of preserving the documents in the cloud by applying combination cryptography methods is explained in the suggested system. This system also enables users to securely share their data with other users as well as storing their files. The files that are saved under the cloud are in an encrypted form and therefore only those who are authorized can gain access to them.

3. 1 User Registration:

This means that, before a user gets a chance to access the services offered by our system, they must register themselves with several details like username, email, password, and company password. After registration, the user is taken directly to the login page.

3.2 Login:

The user is required to submit the registration information so that they can log in and use the services of our system and download and upload files.

3.3 Upload File:

Among the things that the user can do after log-in IS file upload. They provide their data security by making the files available for uploading. Encryption, on the other hand, occurs after the file has been uploaded.

For Encryption:

3.3.1 The server has loaded the file.

3.3.2 The file consists of four equally splits.

3.3.3 To that end, we encrypt every section using one of the four distinct approaches. The Chacha20 Poly1305 technique is used to encrypt the second part; AES-GCM is utilised to encrypt the third part; and AES-CCM is employed to encrypt the fourth component. The Fernet approach is then used to secure the keys created during the encryption process.

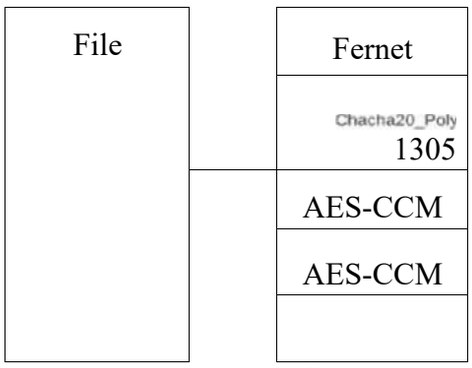

Figure 3.3: Splitting the file into 4 parts

3.4 Download File

Some of the actions available to the user after they signed in are as follows: downloading various files from the cloud. This is as follows: The user has been confirmed for this. To ensure that only a correct user can request a download, the user is prompted to type in his/her email address and name. The owner gets the user's name and email address and then can decide whether they want to open their files to this user or not. These facts go to the owner through email. An owner is allowed to download their file and a key is emailed to the user in the process.

For Decryption:

3.4.2 Request the server to load the key.

3.4.2 The user inputs the key to unlock the files and it is divided into four parts.

4.Results and Discussion

We understand that data protection in cloud environment has limitations of one sort or another, hence we propose a solution that eliminates as far as possible those restrictions. Key control, subordinate control, permission withdrawal, efficiency enhancement, and adaptability are the components of this solution. Firstly, each user in our scheme has a pair of private and public keys of identity-based encryption (IBE) type. In fact, some of the users might still have a second set of keys that are of the Public Key Encryption (PKE) type. Each of these is made by a reliable outside party, and each user has their own unique share of the private key. It is important to note that the sharing of the private key with other users is never a requirement. For instance, in a case where a user needs to update a given data set in the cloud, they can use the IBEtype encryption method to encrypt the data. That implies that our scheme is compatible and easily transportable, and it can be easily applied at any preexisting system. This optimization will be explained in next section. Thirdly, we determine and explain how to change and withdraw the permissions given. Users can also revoke permissions whenever they wish to restrict others from accessing the data they had shared. Then we incorporate all these features into one plan. The first intended design goal can be stated as helping users achieve precise control over file sharing and storage in the clouds. Our specific objective is to ensure that data owners hold the sovereignty of their data and not the cloud service providers. Moreover, we should like to design a scheme that is perfect and contains all the ingredients, which potentially can be used for a practical system, such as searches for data, type conversions, permission withdrawal, etc. In order to facilitate both ciphertext heterogeneous transformation and fine-grained control, this study suggests improving the PRE algorithm. An AES symmetric encryption system, along with additional algorithms, is used in the construction of a multi-security level cloud storage system. A cryptographic algorithm based upon the properties of elliptic curves has been introduced into the working mechanism.

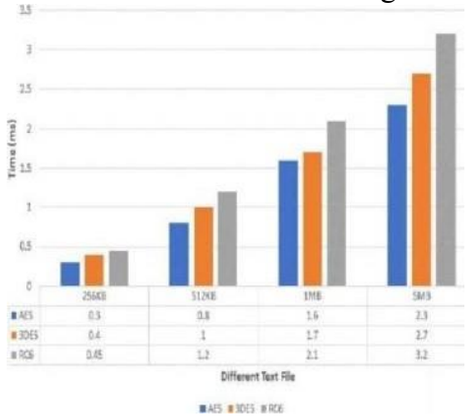

Figure 4.1: Performance comparison results of AES, 3DES, and RC6

In the relation figure 2 it describes noted that diagram isn't provide an interpretation for the results achieved through experimentation regarding storage capacity for purposes such as these chosen four text samples all consisting of five digits.

Table 1: Comparison of proposed algorithm evaluation

Symmetric Key Algorithm	Key Size (bits)	Number of Rounds	Block Size bits	Security	Speed
3DES	112, 1681	48	64	Very Good	Slow
AES	128, 192, 256	10, 12, 14	128	Excellent	Fast
RC6	128, 256	20, 26	32	Good	Fast

4.1.1 AES-GCM: -

It can also be combined with streaming cipher methods such as CTR-AES GCM. It can thus be applied not only in conventional messaging services but also those using carrier pigeons.

4.1.2 AES-CCM: -

The actual goal of cryptography used for security purposes (such as SSL) is precisely encryption encrypting data before sending it. One key component of "CCM" is its ability to shield private information, like encryption keys or email contents, from prying eyes

while still allowing unprotected lines to carry them through without damage. The main advantage of CCMP compared to TKIP lies in protecting ephemeral states such as encryption keys, secret data, counters used for synchronization between communicating devices etc., all those which must be processed before being transferred across wireless channels,

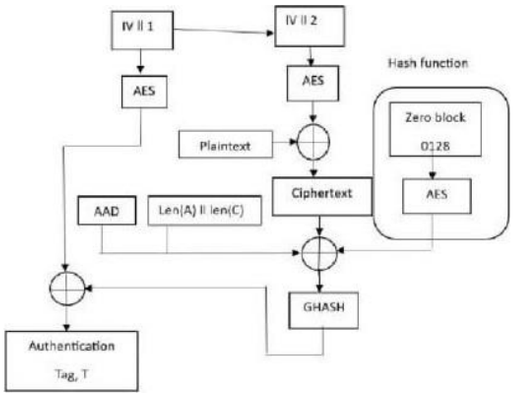

Figure 4.2: AES-GCM Encryption/Decryption.

Conclusion:

This project showcases a two-level encryption method with cloud computing to create a strong and safe file storage system. We have developed a highly secure architecture that guards sensitive data from unauthorized access by integrating the advantages of the AES, DES, and RC6 algorithms. Fast and effective data encryption is ensured by the first level of encryption, which uses AES. An extra layer of protection is added by the second level of encryption, which uses DES and RC6. The data is protected by this approach, even in the event that one encryption layer is breached. Scalability, dependability, and ondemand access to saved files are all made possible by using cloud computing. The potential of cloud computing with multi-layered encryption to guarantee the availability, secrecy, and integrity of sensitive data is demonstrated by this project.

Reference:

1. lmran A. Khan and Rosheen Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptography", International Journal of Computer & Communication Network (IJCCN), ISSN: 2664-9519 (Online); vol. 1, Issue 1, 2019.
2. Wid A. Awadh, Ali S. Hashim, "Using Steganography for Secure Data Storage in Cloud Computing", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 2017.
3. Afrah Albalaw, Nermin Hamza, "A Survey on Cloud Data Security using Image Steganography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 1, 2020.
4. Parth Tandel, Abhinav Shubhrant, Mayank Sohani, A Review of Encryption Techniques Used in Cloud Computing, IJSRCSFIT, 2021.
5. Raj Parab, Anwit Paul, Urjit Mojumdar, Rahul Patil, "Secured Cloud Storage Using Hybrid Cryptography", e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science, 2021.
6. Dr. Sumagna Patnaik, A. "Sunil, Rakesh Reddy, Hybrid Cryptography algorithm for secure file storage in cloud", JAC : A Journal Of Composition Theory, 2021.
7. Swami C,Marrynal S. Eastaff, "Secure the file storage in Cloud Computing Using Hybrid Alogrithm", Infokara Research, 2019.
8. Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul, "Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, 2020..
9. Swami C, Marrynal S. Eastaff, "Secure the file storage in Cloud Computing Using Hybrid Alogrithm", Infokara Research, 2019.

10. M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography, "lnternational Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 123-127, 2020.
ll. Sahana Bisalapur, Ninad Pati, Rahul R, Rushikesh Tarale, Sanket Honashetti, "Development Of Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) e-ISSN: 2319-8753, p-1SSN: 2320-6710 Volume 9, Issue 4, 2020.
12. Shruti Kanatt, Amey Jadhav, Prachi Talwar,"Review of Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Engineering Research & Technology (IJERT), 2020.
13. B. S. Rawal and S. S. Vivek, "Secure Cloud Storage and File Sharing", 2017 IEEE International Conference on Smart Cloud (SmartCloud), pp. 78-83, doi: 10.1109 SmartC10ud, 2017.
14. Gulshan, Abhishek Kaja, " A review on cloud storage security", International journal of innovation in engineering research & management Issn: 2348-4918, volume: 05 issue 02 paper id-1JIERM-v- ii-1130 ,2018.
15. F. J. Aufa, Endroyono and A. Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm," 2018 4th International Conference on Science and Technology (ICST), pp. 1-5, doi: 10.1109/1CSTC. 2018.