Volume: 10 Issue: IV Month of publication: April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41332

Secure the File Storage on Cloud Computing Using Hybrid Cryptography Algorithm

Chetan Vijaykumar Dalave[1], Anushka Alok Lodh[2], Tushar Vijaykumar Dalave[3]

[1, 2]*Dept.Of Computer Engineering Savitribai Phule Pune University, RMD Sinhgad College of Engineering Pune, Maharashtra, India*

[3]*Dept.Of Information Technology Engineering Savitribai Phule Pune University, of Engineering Pune, Maharashtra, India*

Abstract: The proposed of this paper is for the security needs of the cloud data center. Blowfish is used to convert encrypt file cuts, takes the minimum amount of time, and has the extreme throughput for encryption and decryption from other compatible algorithms. The idea of spreading and mixing meets the principle of information security. The hybrid approach makes the remote servers more secure when deployed in a cloud environment and, thus helps cloud providers gain more trust from their users. Used for data safety and privacy issues, the basic challenge of separating sensitive data and access control has been met. Cryptography techniques translate original data into an unreadable format. The encryption technique is divided into private key encryption and public-key encryption. Here we will use AES 128-algorithm, DES, RC, and LSB encryption techniques. This technique uses keys to translate data into an unreadable format. Therefore only authorized persons can access data from the cloud server. Ciphertext data is visible to all.

Keywords: Cloud, AES, RSA, Blowfish algorithms, Encryption/Decryption Techniques.

I. INTRODUCTION

Cloud computing is used in various areas like industry, military, colleges, etc. To store a huge amount of data. We can retrieve data from the cloud and requests of users. But the security of files stored on cloud servers is very less to provide a solution to these issues. There are multiple ways of cryptography and steganography techniques are the most popular nowadays for data to security. The use of single and problem is not effective for a high level of security to data in cloud computing. So using multiple layers of the algorithm is very problematic as it increases the security but also increases the time for uploading and downloading. So in this, we are using an asymmetric key cryptography algorithm and steganography. Here we will be using AES, DES, and RC6 encryption techniques to encapsulate by dividing the file into three separate files and then encryption along with it we also are using the LSB technique to enhance security and file sharing.

II. LITERATURE SURVEY

Sr. No	Paper Title/Publication Details.	Procedure	Accuracy	Limitations	Advantages/Disadvantages
1.	Secure File Storage Using Hybrid Cryptography. Aditya SadanandGhadi, International Journal of Innovative Science and Research Technology ISSN No:-2456-2165, Volume 5, Issue 12, December – 2020.	The ECC algorithm performs authentication, key, generation, encryption and decryption.	86%	Only one key is use for encryption and decryption so it less secure.	ECC algorithm is very difficult and more difficult to implement
2.	Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption. Y. Yusfrizal, A. Meizar, H. Kurniawan and F. Agustin, *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674278.	Use of Diffie Hellman for key exchange. Digital Signature gives Authentication.	63%	It take three different steps by using different techniques are execute.	Digital signature requires a lot of time to authenticate.
3.	Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. F. J. Aufa, Endroyono and A. Affandi, *2018 4th International Conference on Science and Technology (ICST)*, 2018, pp. 1-5, doi: 10.1109/ICSTC.2018.8528584.	RSA algorithm in mixture with MD5 ensures data security on cloud database.	76%	MD5 gives single text encryption and multiple text encryptions. And RSA algorithm gives only key encryption.	RSA algorithm can be very slow in case there large amount data needs to encrypted.
4.	Review paper on cloud storage security. GULSHAN, ABHISHEK KAJA, VOLUME :05 Issue 02 Paper id-IJIERM-V- II-1130 , April 2018.	Using inbuilt EFS to secure data file by cryptography system.	82%	EFS inbuilt providing better modification for security measures is very hard to implement.	No Windows instances.

5.	Secure Cloud Storage and File Sharing. B. S. Rawal and S. S. Vivek, *2017 IEEE International Conference on Smart Cloud (SmartCloud)*, 2017, pp. 78-83, doi: 10.1109/SmartCloud.2017.19.	Two servers are uses for output function and input storage.	76%	There can be synchronization problem as well as connection issues by using three different servers.	Limited ability to synchronization documents offline.
6.	Cloud Security using Hybrid Cryptography Algorithms. S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377	AES algorithm takes some steps of encryption and decryonpti.	96%	AES allow you to choose a 128-bit, 192-bit, 256-bit key.	256-bit cannot be uses for encryption.
7.	A Study on Secure File Storage in Cloud Computing using Cryptography. Thilina Dinendra Dharmakeerthi, ReseacherGate, MAY 2020.	3DES, DES algorithm is uses only standard arithmetic and logical operation on number of 64 bits.	88%	DES is a symmetric encryption which generates a pair of key one public, one private key.	3DES which requires three time as many calculation as DES, is correspondingly slower.
8.	Review on Secure File Storage on cloud using Hybrid Cryptography. Shruti Kanatt, Amey Jadhav, Prachi Talwar, International Journal of Engineering Research & Technology (IJERT), 02 February- 2020.	Blowfish uses a single encryption key to both side of encrypt and decrypt data.	60%	Blowfish algorithm can't offer authentication as well as non-repudiation as two people have the same key.	The process is quite time consuming as there weakness in decryption process over the other algorithm.
9.	Development of Secure File storage on cloud using Hybrid Cryptography. Sahana Bisalapur, Ninad Pati, Rahul R, Rushikesh Tarale, Sanket Honashetti, ", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) | e-ISSN: 2319-8753, p-ISSN: 2320-6710| |Volume 9, Issue 4, April 2020	RC6(Rivest cipher 6) is a symmetric key block cipher derived form RC5	91%	RC6 has block size of 128 bit and key sizes of 128, 192, 256 bit up to 2040-bits.	.RC6 is secure , and has no effective limit on input size.
10.	Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography. Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020.	Three algorithms are uses for encryption and for key generation LSB technique is use.	60%	LSB Steganography is use for hide message inside an image by replace least significant bit of image with the bits of message to be hidden.	There is large overhead to hide very tiny amount of information.

A. *Problem and Formation Design*

Many of the benefits of using cloud storage include:

1) It removes the need for physical storage Tools.
2) Data can be saved in any format using cloud storage.
3) Cloud storage provides secure backup, as opposed to. Physical storage devices, data loss computer virus corruption, and natural disasters, among other reasons, can lead to data loss.
4) Cloud storage is more cost-effective because it eliminates. Need to invest in hardware.
5) Cloud storage also helps developers work together and share their work more efficiently and fast.

Another benefit of cloud storage can be added. The future security system's main aim is to make cloud storage. Secure the system using data encryption. Thus, the purpose of to enhance the security of the data uploaded to the proposed system. Cloud uses encryption algorithms to create systems more secure**.**

III. ALGORITHM USED

A. *Advanced Encryption Standard (AES):*

The AES algorithm is related to Rijndael's encryption. Rijndael is a family of encryption algorithms with different keys and blocks size it consists of ongoing serial operations, some of which include the input of certain output (substitutions) and others Bits mix (permutations).

Altogether AES calculation algorithms are executed in bytes instead of bits. Therefore, for the advanced encryption standard, 128 bits is simple data is treated as a block of 16 bytes. These 16 bytes are organized in 4x4 matrixes for processing.

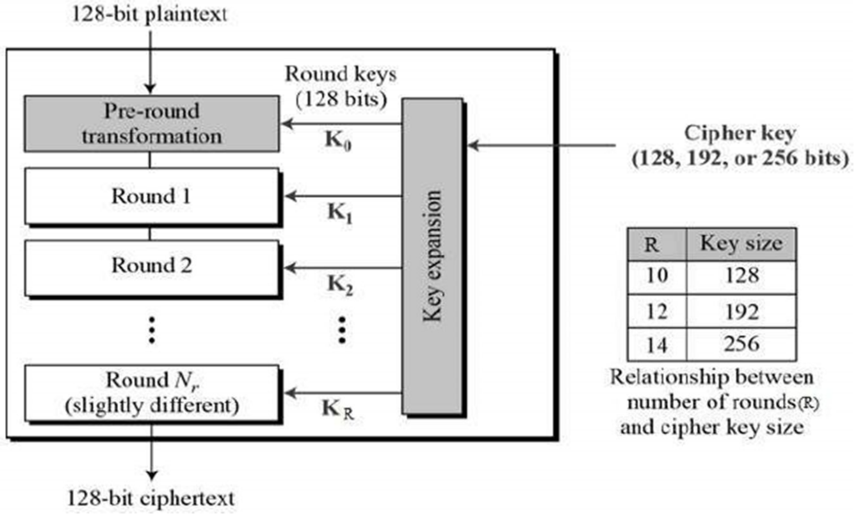

Fig.1. AES Diagram showing working of system

There are the three types of AES algorithms: AES-128bit, AES-192bit, and AES-256bit each iteration encrypt and decrypts the data blocks using 128 bits or 192 bits or 256 bits keys, respectively. The Rijndael method was extended to accept extras. Block size and more key length, but for AES, those functions were not inherited.

B. Triple Data Encryption Standard (3DES):

In encryption, 3DES is an inherited better-quality version of DES (Data Encryption Standard). In the triple DES algorithm, DES is used twice to increase the security level. Triple DES is also known as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has the following key:-

1) All the keys are different.
2) Key 1 and key 2 are different and key 1 and key 3 are identical.
3) All keys are the same.

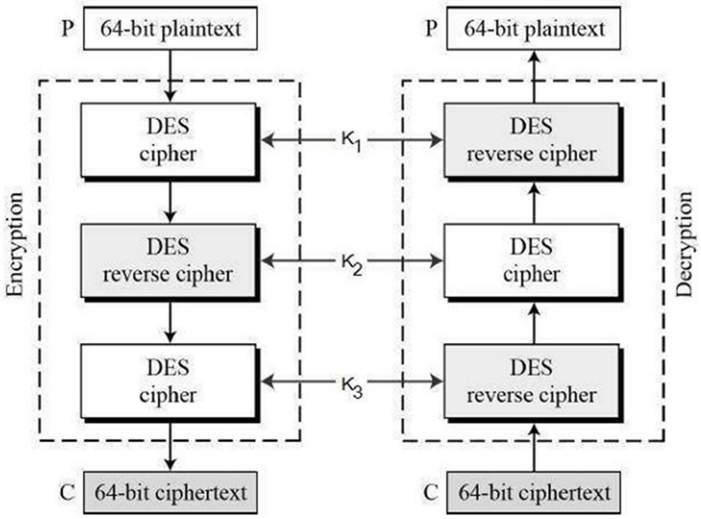

Fig.2. TDES Diagram showing working of system

TDES is slowly disappearing from use; it is increasingly being replaced by AES (Advanced Encryption Standard). There is a far-reaching anomaly in the digital payments industry, which still uses 2TDES and scatter standards on this basis (eg:- EMV, "chip cards" and IC compatible POS terminals, and ATM collaboration standards). This security that TDES will continue to act as the standard of future cryptography.

C. Rivest Cipher 6 (RC6)

RC6 is a compatible key block cipher. RC6 (Rivest Cipher 6) is an enhanced better quality version of the old RC5 algorithm. RC6 - means w / r / b that four w-bit-word plaintexts are encrypted with r-rounds via b-bytes keys. This is a proprietary algorithm unproved by RSA security. RC6 operators use five basic operations as a unit of W-bit words such as increment, subtraction, slightly specific-or, a Multiplying, and shifting depending on the data. The block size of the RC6 algorithm is 128 bits and it also works with key sizes 128 bits, 192 bits, and up to 256 bits and 2040 bits dissimilar features of the RC6 include the use of four working registers instead of adding numerical multiplication as two and one additional initial processes. Significant use of multiplication increases spread per round, allowing more security, fewer laps, and more efficiency. Furthermore, like the RC5, it can also support different word lengths, key sizes, and a number of rounds. The RC6 algorithm is very similar in structure to the RC5 algorithm In fact, RC6 can be thought of as two parallel RC5 encryption processes, although RC6 uses additional multiple operations that are not used in the RC5 algorithm to make the rotation of each bit in a word dependent, not just the least important bits.

D. Blowfish

Blowfish is a powerful cipher that uses 16 rounds of Fiesta network, difficult encryption, and decryption functional design the size of the design used is 64 bits and the key size can be up to 448 of any length. Blowfish Cipher uses 18 subs each of the 32 bits is commonly known as a P-Box and four alternatives to each of the 32 bits, 25 entries in each algorithm design is merged into the shape. It consists of two phases: a key extension phase and data encryption in step key extensions, the key is converted to multiple levels of keys, and in data encryption, through encryption. 16 round networks each round has a key council and an alternate selection on a key and data.

IV. CONCLUSIONS

The main purpose of this system is to securely store and retrieve data in the cloud which is only under the control of the data owner. Data security cloud storage issues are solved by using encryption and steganography techniques. Data security is achieved by RC6, 3DES and AES algorithms. Key information is securely stored using LSB technique (steganography). It takes less time for the process of encryption and decryption using multi-threading techniques. And so help of the proposed security mechanism, we improved data integrity, high security, low latency, authentication and confidentiality. We may add in the future public key encryption to avoid any attack during data transfer from client to server.

REFERENCES

[1] Aditya SadanandGhadi,” Secure File Storage Using Hybrid Cryptography”, International Journal of Innovative Science and Research Technology ISSN No:-2456-2165, Volume 5, Issue 12, December – 2020.

[2] Y. Yusfrizal, A. Meizar, H. Kurniawan and F. Agustin, "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674278.

[3] 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), 2018, pp. 1-5, doi: 10.1109/ICSTC.2018.8528584

[4] 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-IJIERM-V- II-1130 , April 2018.

[5] B. S. Rawal and S. S. Vivek, "Secure Cloud Storage and File Sharing," 2017 IEEE International Conference on Smart Cloud (SmartCloud), 2017, pp. 78-83, doi: 10.1109/SmartCloud.2017.19.

[6] S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377.

[7] Thilina Dinendra Dharmakeerthi, “A Study on Secure File Storage in Cloud Computing using Cryptography”, ReseacherGate, May 2020

[8] Shruti Kanatt, Amey Jadhav, Prachi Talwar,Review of Secure File Storage on Cloud using Hybrid Cryptography, International Journal of Engineering Research & Technology (IJERT), 02 February- 2020

[9] 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-ISSN: 2320-6710||Volume 9, Issue 4, April 2020

[10] 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, March 2020.

[11] Swami C, Marrynal S.Eastaff, “Secure the file storage in Cloud Computing Using Hybrid Alogrithm”, Infokara Research, 2019.

[12] Dr. Sumagna Patnaik, A.Sunil, Rakesh Reddy, Hybrid Cryptography algorithm for secure file storage in cloud, JAC : A Journal Of Composition Theory, October 2021.

[13] M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 123-127, doi: 10.1109/CSASE48920.2020.9142072. https://ieeexplore.ieee.org/document/9142072

[14] Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam, Secure the file on Cloud using hybrid algorithm, International Journal of Computer Sciences and Engineering, Jan 2019.

[15] Ronak Karani, Tejas Choudhari, Anindita Bhajan, Madhu Nashipudimath, Secure File Storage Using Hybrid Cryptography, IJIRT Journal , 9 February 2020.

[16] 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, 04 April-2021

[17] Parth Tandel, Abhinav Shubhrant, Mayank Sohani, A Review of Encryption Techniques Used in Cloud Computing, IJSRCSEIT, April 2021

[18] 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

[19] 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: 04 | Apr -2017

[20] Imran 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, August 2019