IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Secure File Storage on Cloud using Hybrid Cryptography

Aditya Poduval[1*], Abhijeet Doke[2], Hitesh Nemade[3], Rohan Nikam[4]

[1] Department of Computer Engineering, M. E. S. College of Engineering, Savitribai Phule Pune University, Pune, India
[2] Department of Computer Engineering, M. E. S. College of Engineering, Savitribai Phule Pune University, Pune, India
[3] Department of Computer Engineering, M. E. S. College of Engineering, Savitribai Phule Pune University, Pune, India
[4] Department of Computer Engineering, M. E. S. College of Engineering, Savitribai Phule Pune University, Pune, India

[*]*Corresponding Author: podu2997@gmail.com, Tel.: +91-96731-72062*

Available online at - www.ijcseonline.org

Accepted: 20/Jan/2019, Published: 31/Jan/2019

***Abstract*—** In this era cloud computing is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduces a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and steganography. In this proposed system 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. All the algorithms use 128-bit keys. LSB steganography technique is used to securely store the key information. Key information will contain the information regarding the encrypted part of the file, the algorithm and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithm simultaneously with the help of multithreading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, 3DES and RC6 algorithm.

***Keywords*—**Cryptography, Encryption, Decryption, Cloud Security, Cloud Storage.

I. INTRODUCTION

Technological advancements are resulting in trends and movements that improve the quality of life. In this fast life where every person uses a smartphone and has access to the internet, the major concern that the people face is regarding the security of their information present online. This security concern is also about the file that is stored online on a cloud. This can be solved with the help of cryptography.

Cryptography techniques convert original data into Cipher text. So only legitimate users with the right key can access data from the cloud storage server. The main aim of cryptography is to keep the security of the data from hackers, online/software crackers, and any third party users. Non-legitimate user access to information results in loss of confidentiality. Security has the characteristics to block or stop this kind of unauthorized access or any other kind of malicious attacks on the data here by securing the users' trust.

In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored on the cloud and the different services provided to the users. This data can be confidential and extremely sensitive. Hence, the data management and security should be completely reliable. It is necessary that the data in the cloud is protected from malicious attacks.

So for the security of the data, we introduced a new mechanism in which we are using a combination of multiple symmetric key cryptography algorithm and steganography. In this proposed system Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6) algorithms are used to provide security to data. LSB algorithm is used for image steganography. Sensitive data of the user is hidden into a cover image for security purposes.

AES, RC6, and 3DES algorithms are combined to form a hybrid algorithm to accomplish better security. The steganography part assists in storing the key information

safely. It makes it difficult for the attacker to recover the secret file of the user.

II. RELATED WORK

Security is an important factor in this digital age. So a huge amount of research is conducted in this domain to protect client's information from any security breach and leaks.

A. K. Shahade and V. S. Mahale [1] in their research introduced a Hybrid encryption algorithm which was a combination of RSA algorithm and AES algorithm. In their system, the user creates and stores the RSA private key with himself and also create an RSA public key while uploading the data. In the cloud, the server calls the RSA and AES algorithm for encryption of the file and then properly store the file on the server.

P. Uddin[2] researched an efficient way for information hiding using Text Steganography along with Cryptography. In this study, steganography of pure text was proposed, including private key cryptography that provides a high level of security. According to the algorithm after embedding the cipher text in the cover text, the text seems like ordinary text.

S. D. Patil[3] suggested a system for the hiding text in cover images using the LSB algorithm and for decoding using the same method. The use of the data of this algorithm can be stored in the Least Significant Bit of the title image. Even then, the human eye cannot notice the hidden text in the image.

S. Hesham[4] in her research proposed an algorithm that increases the efficiency of the Advanced Encryption Algorithm. The proposed method reduces the critical path delay of the original algorithm. Compared to the original AES encryption/decryption algorithm the proposed algorithm provides an efficiency improvement of 61% and 29% respectively.

III. ALGORITHM

Symmetric Key Cryptography:

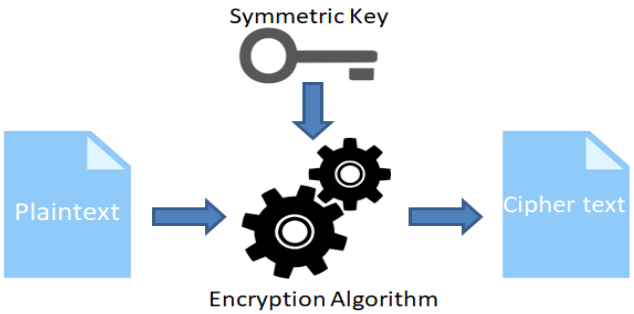
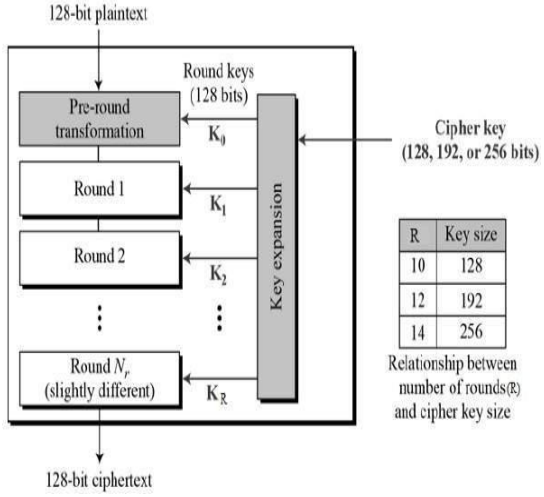


Figure 1 : Symmetric key Cryptography

Cryptography with symmetric keys gives an encryption method in which the recipient and sender of the file use the same key to encrypt data and decrypt data.

1) Advanced Encryption Standard (AES)

The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continues serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations).
All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing.



R	Key size
10	128
12	192
14	256

Figure 2 : AES Encryption

AES algorithm is of three types namely AES-128bit, AES-192bit, and AES-256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256-bits, respectively. Rijndael method was enhanced to accept extra block sizes and also extra key lengths, but for AES, those functions were not inherited.

Till the current day, the AES algorithm is used many times and supported on both digital level and physical level. Furthermore, AES comprises of built-in limberness of key length, this allows a certain "future proof" against the process in the ability to perform comprehensive key searches.

2) Triple Data Encryption Standard (3DES)

In cryptography, 3DES is an inherited enhanced version of DES (Data Encryption Standard). In the Triple DES algorithm, DES is used trice to increase the security level. Triple DES is also referred to as TDES or Triple Data Encryption Algorithm (TDEA).
TDES has following keying options :

1. All keys being different

2. Key 1 and key 2 being different & key 1 and key 3 is the same.
3. All three keys being identical.

The third option forms the Three DES. In triple DES the key size is increased to confirm addition security through encryption capabilities.

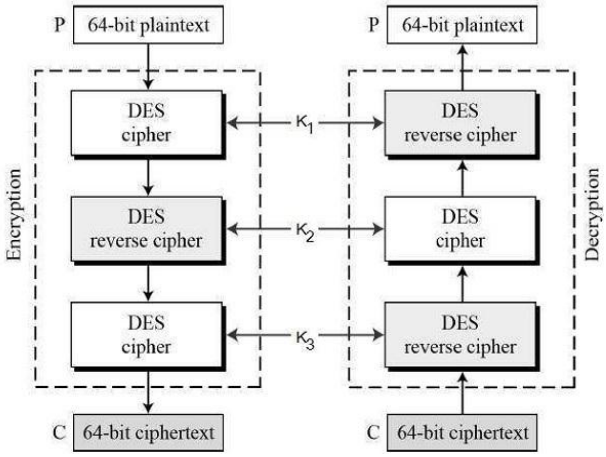


Figure 3 : 3DES Encryption

TDES is slowly invisible from use, it is maximally replaced by the AES (Advanced Encryption Standard). A far-reaching anomaly is in the digital payments industry, which still uses 2TDES and scatters standards on that basis (e.g. EMV, the standard for inter-operation of "Chip cards", and IC capable POS terminals and ATM's). This guarantees that TDES will remain as an agile cryptographic standard in the future.

3) Rivest Cipher 6 (RC6)

RC6 is a symmetric key block cipher. RC6 (Rivest Cipher 6) is an enhanced version of the old RC5 algorithm. RC6 – w/r/b means that four w-bit-word plaintexts are encrypted with r-rounds by b-bytes keys. It is a proprietary algorithm patented by RSA Security.

RC6 operators as a unit of a w-bit word using five basic operations such as an addition, a subtraction, a bit-wise exclusive-or, a multiplication, and a data-dependent shifting. The RC6 algorithm has a block size of 128 bits and also works with key sizes of 128-bit, 192-bit, and 256 bits and up to 2040 bits. The New features of RC6 include the use of four working registers instead of two and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication significantly increases the diffusion per round, which allow more security, fewer laps and greater performance. Furthermore, like RC5, it can also support various word-lengths, key sizes and number of rounds. RC6 algorithm is very similar in structure to the RC5 algorithm. In fact, RC6 could be considered as two parallel RC5 encryption processes, although RC6 uses an additional multiplication operation that is not used in RC5 algorithm to make the rotation of each bit in a word dependent, not just the least significant bits.

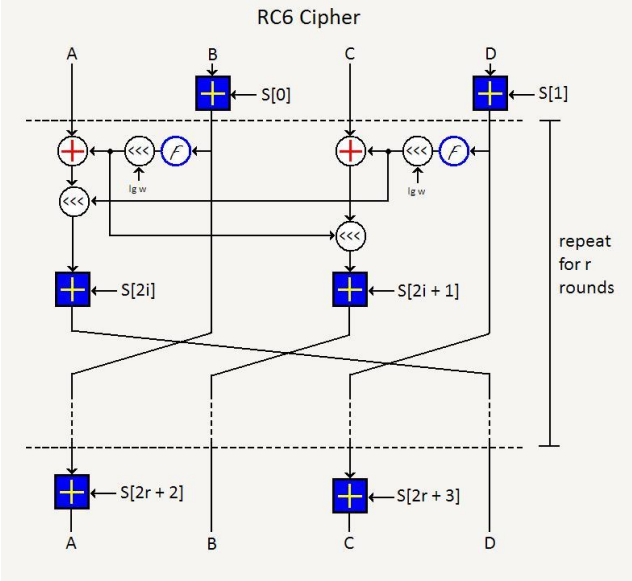


Figure 4 : RC6 Encryption

IV. PROPOSED SYSTEM

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files.

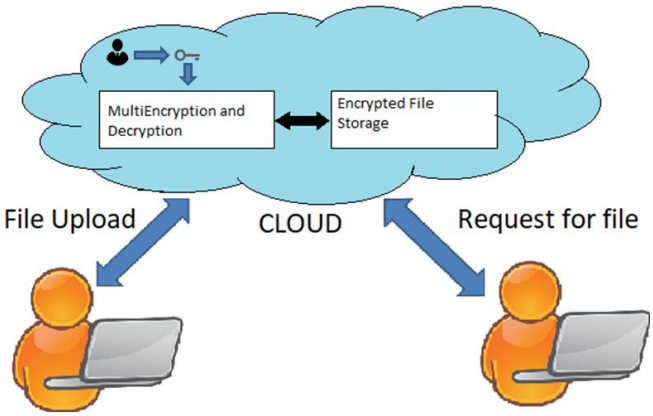


Figure 5 : System Overview

The above figure gives an overview of the system. As in the above figure, the files that the user will upload on the cloud will be encrypted with a user-specific key and store safely on the cloud.

1) Registration of User

For accessing the services the user must first register themselves. During the registration process various data like

the name, username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

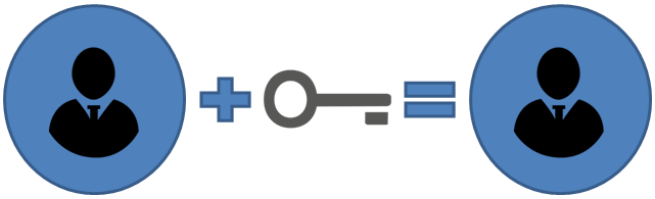


Figure 6 : Image Steganography

2) Uploading a File on Cloud
When the user uploads a file on the cloud first it will be uploaded in a temporary folder.

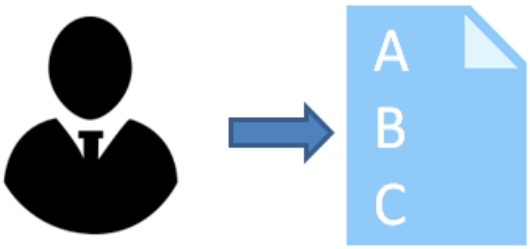


Figure 7 : User's File

Then this file will be split into three parts.

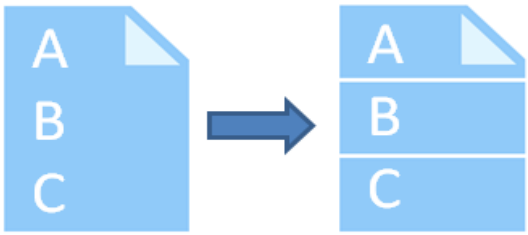


Figure 8 : Split File into Three Parts

These three parts will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.

These three parts will be encrypted using three different algorithms that are AES, 3DES, RC6. The key to these algorithms will be retrieved from the steganographic image created during the registration.

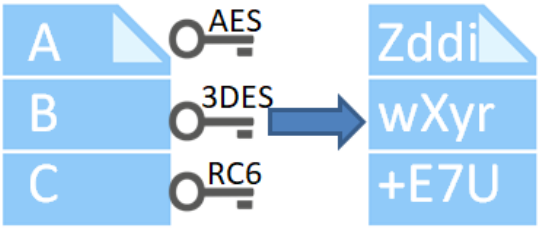


Figure 9 : Encryption of the Three Parts

After the split encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.

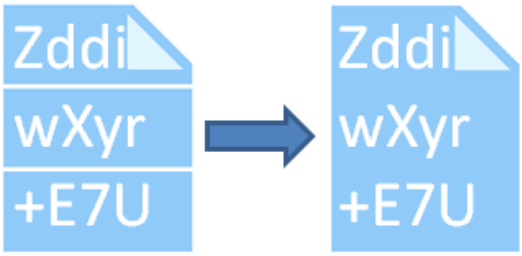


Figure 10 : Combining Encrypted Parts

3) Downloading a File from the Cloud
When the user requests a file to be downloaded first the file is split into three parts.

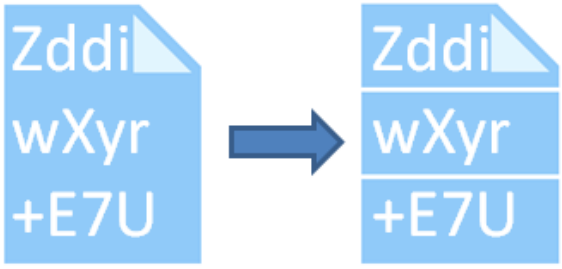


Figure 11 : Splitting up the Encrypted Parts

Then these three parts will be decrypted using the same algorithms with which they were encrypted. The key to the algorithms for the decryption process will be retrieved from the steganographic image created during the registration.

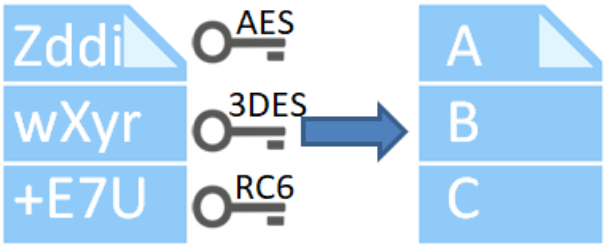


Figure 12 : Decryption of the Encrypted Parts

Then these parts will be re-combined to form a fully decrypted file.

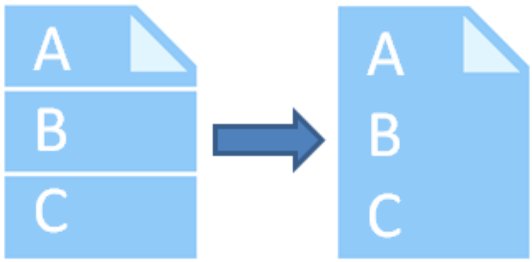


Figure 13 : Combining the Decrypted Parts

Then this file will be sent to the user for download.

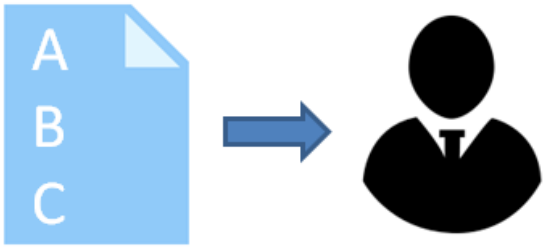


Figure 14 : Sending the Decrypted File to the User

V. CONCLUSION AND FUTURE SCOPE

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using RC6, 3DES and AES algorithm. Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server.

REFERENCES

[1] A. K. Shahade, V.S. Mahalle, "*Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm*", IEEE, INPAC, pp 146-149, Oct .2014.

[2] Palash Uddin, Abu Marjan, "*Developing Efficient Solution to Information Hiding through text steganography along with cryptography*", IEEE, IFOST, pages 14-17, October 2014.

[3] R. T. Patil and P. S. Bhendwade , "*Steganographic Secure Data Communication*",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.

[4] Klaus Hofmann and S. Hesham, "*High Throughput Architecture for the Advanced Encryption Standard Algorithm*" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.

[5] D. Nilesh, M. Nagle, "*The New Cryptography Algorithm with High Throughput*", IEEE, ICCCI, pages 1-5, January 2014.

[6] LI Yongzhen, Zhou Yingbing, "*The Design and Implementation of a Symmetric Encryption Algorithm Based on DES*", IEEE, ICSESS, pages 517-520, June 2014.

[7] A. Hasan, N. Sharma, "*A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)*", IEEE, International Conference.

[8] S.Rajendirakumar, Dr.A.Marimuthu, "Cryptographic Algorithms used in Cloud Computing – An Analysis and Comparison", International Journal for Research in Applied Science & Engineering Technology, Vol 6, Iss. 1, 2018.

[9] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology, Network, Vol. 13, Iss. 15, 2013.

Authors Profile

Aditya Poduval is pursuing Bachelor of Engineering in M. E. S. College of Engineering, Pune. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security, and Privacy.

Abhijeet Doke is pursuing Bachelor of Engineering in M. E. S. College of Engineering, Pune. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security, and Privacy.

Hitesh Nemade is pursuing Bachelor of Engineering in M. E. S. College of Engineering, Pune. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security, and Privacy.

Rohan Nikam is pursuing Bachelor of Engineering in M. E. S. College of Engineering, Pune. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security, and Privacy.