**Data Protection On Cloud Using Hybrid Cryptography And Image Steganography**

**Anagha Prabhu M1, Deekshita Mahale 2, Sadhan Shetty3, Swathi Shetty4, Pragathi Hegde5**

*1Information Science and Engineering, Canara Engineering College (India)*

*2Information Science and Engineering, Canara Engineering College (India)*

*3Information Science and Engineering, Canara Engineering College (India)*

*4Information Science and Engineering, Canara Engineering College (India)*

*5Assistant prof., Department of Information Science and Engineering, Canara Engineering College. (India)*

***Abstract— Cloud computing is often used in various fields like industry, medicine, 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. We have introduced in our proposed project a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and image 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 hidden in an image by 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— Advanced Encryption Standard, Cloud Security RivestCipher, Steganography, Triple Data Encryption Standard.***

# **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 and Cryptography technique is used here. 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. Nonlegitimate user access to information results in loss of confidentiality. 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. This system focuses on providing complete security to the data on cloud. We have introduced a new mechanism in which we are using a .combination of multiple symmetric key cryptography algorithm and image steganography. In this proposed system Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Rivest Cipher 6 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. File that the user wants to store on cloud is split into three part for encryption. These three parts of the file will be encrypted using different encryption algorithm mentioned above. 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.

# **Existing System**

## **Hybrid Encryption using RSA and AES**

K. Shahade and V. S. Mahale [1] in the research a Hybrid encryption algorithm was introduced 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 algorm for encryption of the file and then properly store the file on the server.

**2.2 Text Steganography along with Cryptography**

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.

**2.3 System for Hiding Text in Cover Images using LSB**

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.

***2.*4Algorithm to Improve the efficiency of the AES**

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.

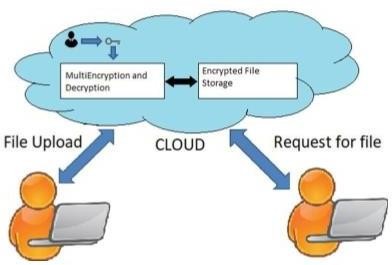
**2.5 New Cryptography algorithm with High**

**Throughput**

D. Nilesh , M Nagle[5] in their study, new Cryptography algorithm has been generated and new Cryptography algorithm has been compared by using some components like throughput of key generation,to generate Encryption text and to generate Decryption text. In this algorithm some logical mathematical operations are performed.

# **Proposed System**

The architecture for whole process is shown in Figure 1. 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. syntactic arrangement. In this system, dictionary looks up with the morphological analysis.



**Figure 1 System Overview**

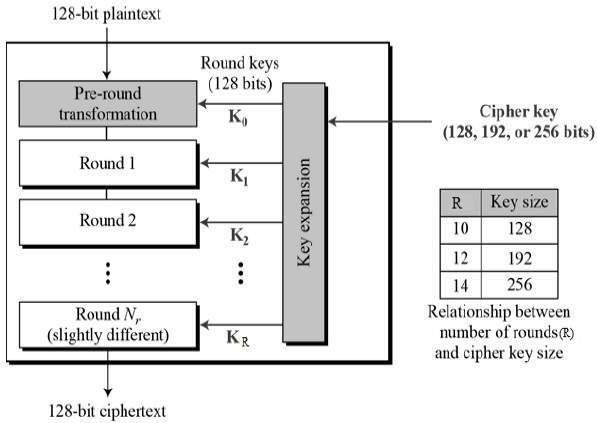
The above figure gives an overview of the system. As in the above figure, the files that the user will upload on the cloud will be encrypted with a user-specific key and store safely on the cloud. The file uploaded is then split into three which is then encrypted by using the three algorithms as mentioned above. Them the key generated is stored in the form of the image using the Steganography technique and is stored in the users profile. If the user wants the file the file is then decrypted by using the same algorithms that are being used for encryption. Then the decrypted files are merged together and file is sent to the user for further use.

1. **IMPLEMENTATION**

In this section we will discuss about the different algorithms that make the project a whole

4.1 **Advanced Encryption Standard (AES)**

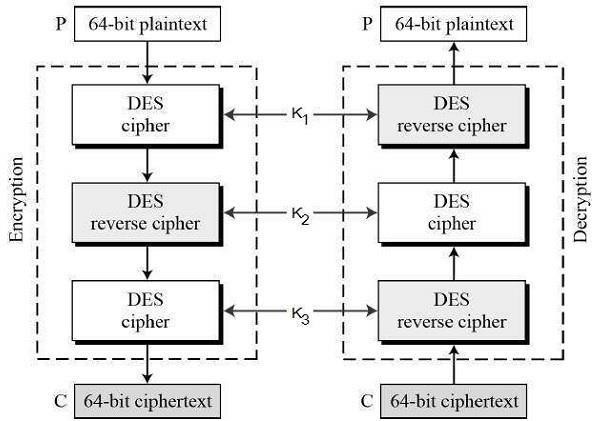
The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continues serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of the mixing of bits (permutations). 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. AES algorithm is of three types namely AES-128bit, AES192bit, and AES256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256-bits, respectively.



**Figure 2 Adavanced Encryption Standard**

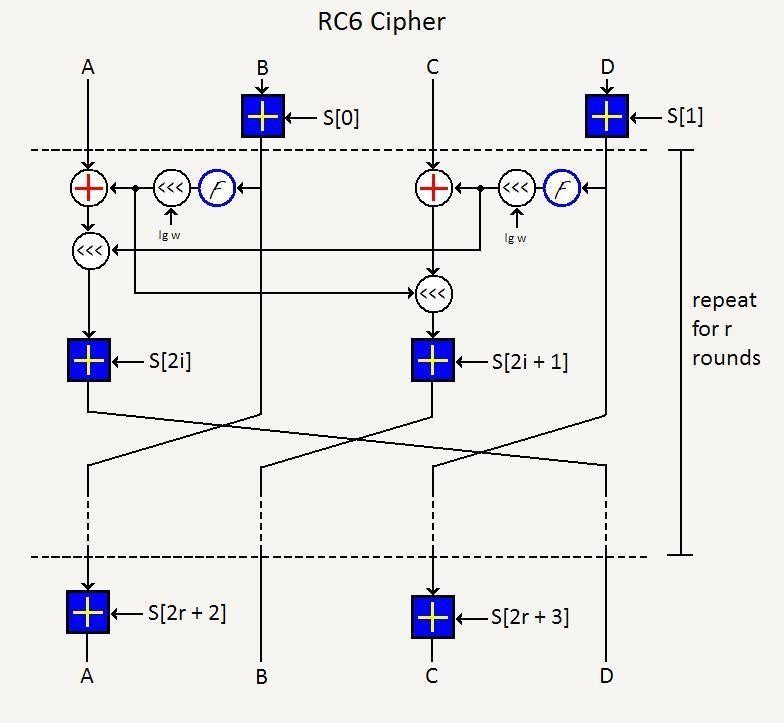
4.2 **Triple Data Encryption Standard (3DES)**

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. In 3DES the key size is increased to confirm addition security through encryption capabilities. 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.



**Figure 3 Triple Data Encryption Standard**

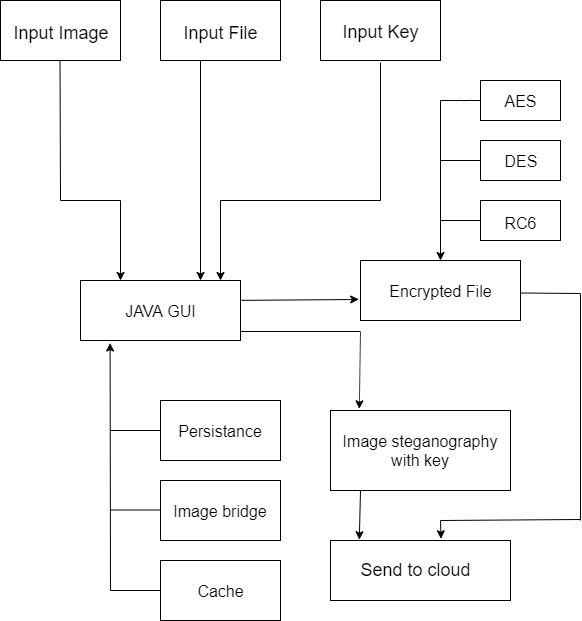
4.3 **Rivest Cipher 6 (RC6)**

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.

**Figure 4 Rivest Cipher 6 (RC6)**

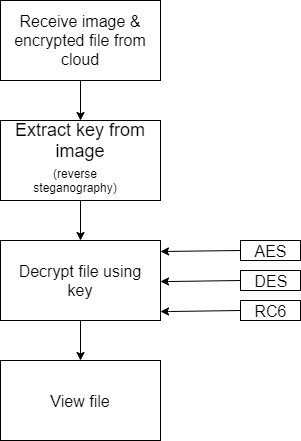
**4.4 Architectural design**

An architecture description is a formal description and representation of a system, organized in a way that supports reasoning and behavior of the system.



**Figure 5 System Sender Architecture**

Figure 5 represents the sender architectural design of the system where the interface asks the user to input the file he wants to store on cloud , image he chooses to hide the key and the key.The file then subjected to three algorithms AES,3DES and RC6. The encrypted file with the stegno image is sent to the server.



**Figure 6 System Reciever Architecture**

Figure 6 represents the reciever architectural design of the system.The image and the encrypted file is received from the server . The key from the image is extracted using reverse steganography . The file is decrypted using AES,3DES and RC6 . The user then receives the file in the original form.

**5 . CONCLUSION**

The main aim of this system is to securely store and retrieve data on the cloud. Cloud storage issues of data security are solved using the combination of 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] *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 K 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” Communication and Signal Processing, pages 953-956, April 2014.*

[5] *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,*