Data Protection on Cloud using Cryptography and Steganography

Anagha Prabhu M[1], Deekshita Mahale[2], Sadhan Shetty[3], Swathi Shetty[4], Pragathi Hegde[5]

[1,4]*Information Science and Engineering, Canara Engineering College (India)*
[5]*Assistant prof., Department of Information Science and Engineering, Canara Engineering College. (India)*

Abstract— *Cloud computing is used in various fields lfor various services and storage of huge amount of data online. Data stored in this cloud can be accessed from anywhere. Also,the data can be retrieved on the users request .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 steganography. In this proposed system 3DES, RC6 and AES algorithms are used to provide security to data... LSB steganography technique is used to securely store the key used in encrypting files. 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 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— Steganography, RivestCipher, Advanced Encryption Standard, Triple Data Encryption Standard

1. INTRODUCTION

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 . To ensure the safety of data stored online we have used Cryptography techinique .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 data secure 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 steganography. In this proposed system 3DES, AES and RC6 algorithms are used to provide security to data. LSB algorithm is used for image steganography. AES, RC6, and 3DES algorithms are combined to form a hybrid algorithm to accomplish better security. The steganography part assists in storing the key 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 with the help of multithreading technique. The key 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.

2. EXISTING SYSTEM

2.1 Hybrid Encryption using RSA and AES

[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 algorithm for encryption of the file and then properly store the file on the server

2.2 Text Steganography along with Cryptography

[2] 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.

2.4 Algorithm for Improving AES Performance

S. Hesham [4] in his research proposed an algorithm that maximizes the efficiency of the Advanced Encryption Algorithm. The proposed method minimizes the delays of the critical algorithm of the original algorithm. Compared with the original AES algorithm / decryption algorithm the proposed algorithm offers an efficient improvement of 61% and 29% respectively.

3. ALGORITHM

3.1 Advanced Encryption Standard (AES)

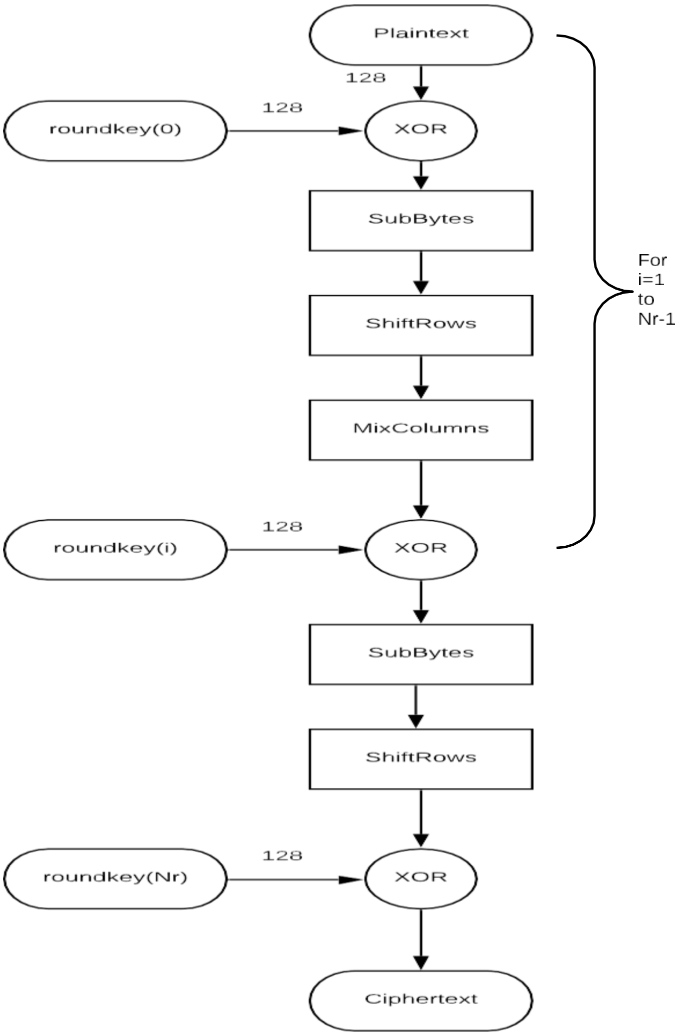


Figure 1 AES Logical Implementation

The AES algorithm is related to Rijndael's encryption. Rijndael is a family of encryption algorithms of various keys and block sizes. It contains continuous serial operation, some of which include output (output) and other bits of mixing bits (permissions). All AES algorithm calculations are done in bits instead of traps. Therefore, in the Advanced Encryption Standard, 128 bits of blank data are treated as a block of 16 bytes These 16 bytes are arranged in a 4x4 processing matrix. The algorithm is of three types namely AES-128bit, AES192bit, and AES-256bit. Each of the encrypts encrypts and decrypts data into blocks using 128-bits or 192-bits keys or 256-bits, respectively.

3.2 Triple Data Encryption standard (3DES)

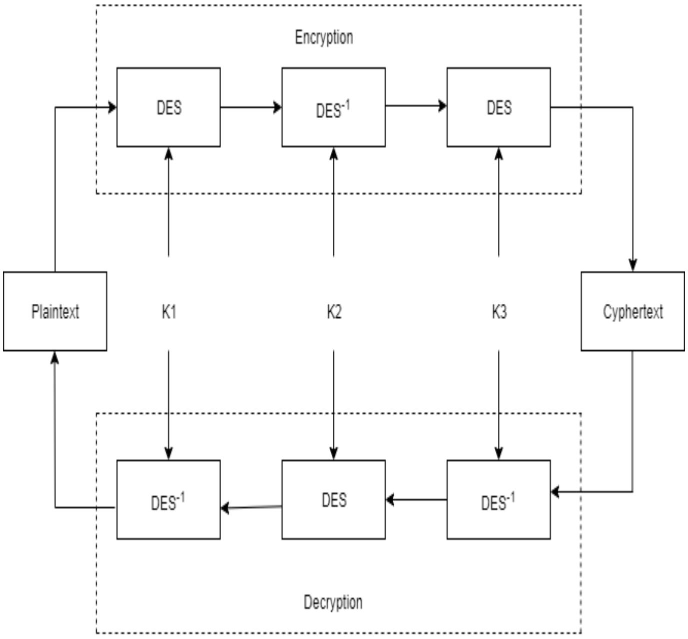


Figure 2 3DES Logical Implementation

In cryptography, 3DES is a version that has been made as a value of DES (Data Encryption). In the Triple DES algorithm, DES is used a strategy to increase the security level. Triple DES is also called TDES or Triple Data Encryption Algorithm (TDEA). TDES has the following options to follow: 1. All keys are unique.2. Key 1 & Key 2 are different & Key 1 & Key 3 are the same. 3. All three keys are the same. The DES triple the key size is expanded to ensure additional security by using encryption capabilities. The far-reaching anomaly is the digital payment industry, which uses 2TDES and distributes rates on that basis (e.g. EMV, interactive "Chip Cards" standard, and IC and ATM's interactive storage spaces). The TDES will remain as the cryptographic standard for the future.

3.3 Rivest Cipher 6 (RC6)

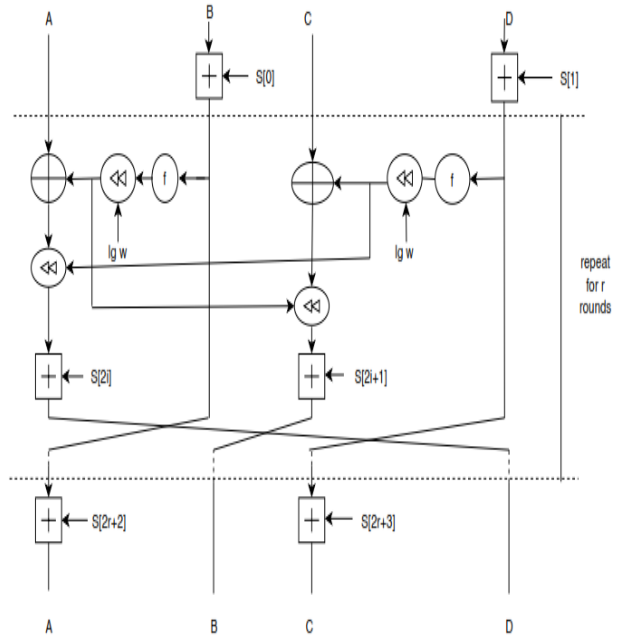


Figure 3 RC6 Logical Implementation

RC6 is a cipher block cipher key. RC6 (Rivest Cipher 6) is an upgraded version of the old RC algorithm. RC6 - w / r / b means that four poles of w-bit-encrypetched names per round are b-bytes key. It is a copyrighted content algorithm developed by RSA Security. RC6 operators as a w-bit word unit using five basic functions such as addition, subtraction, special-precision-or, multiplication, and data-dependent variables. The RC6 algorithm has a block size of 128 bits and operates at significant 128-bit, 192-bit, and 256 bits size up to 2040 bits. The new features of the RC6 include the use of four double-duty registers and the addition of a number multiplier as an additional starting function. The use of duplicates greatly increases the coverage in each cycle, allowing for more security, fewer thighs and greater efficiency.

4. PROPOSED SYSTEM

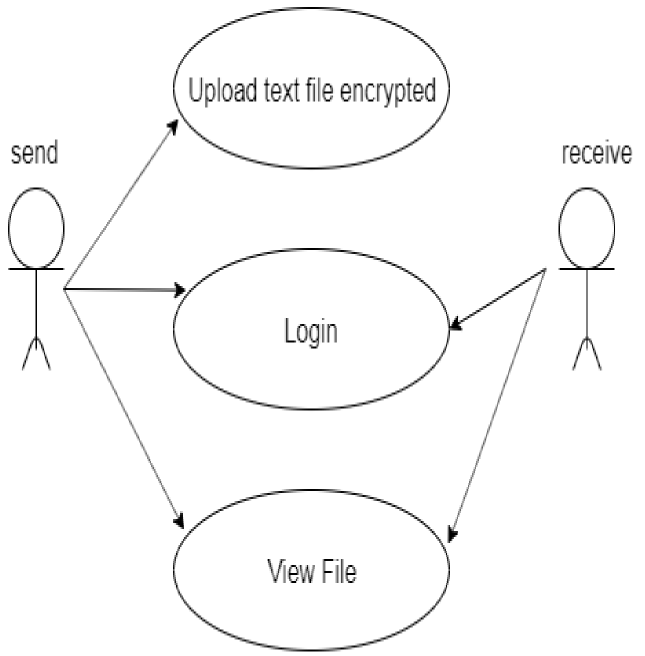


Figure 4 System Overview

The architecture for whole process is shown in Figure .4
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. 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.

5. IMPLEMENTATION

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

5.1 Sender Architectural design

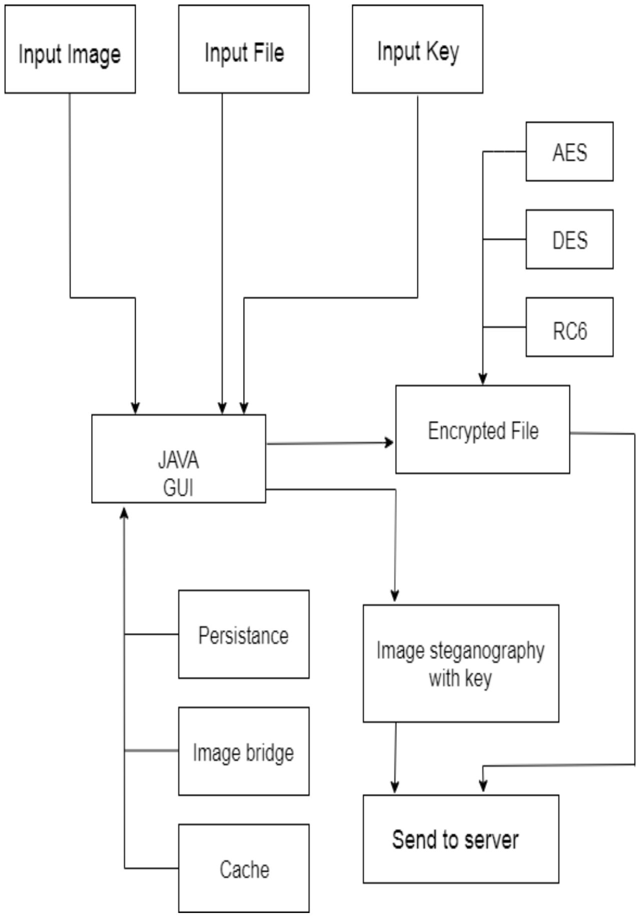


Figure 5 Represents the Sender Architectural Design

Figure 5 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. The file is then subjected to three algorithms AES, 3DES and RC6. The encrypted file with the stegno image is sent to the server.

5.2 Reciever Architectural design

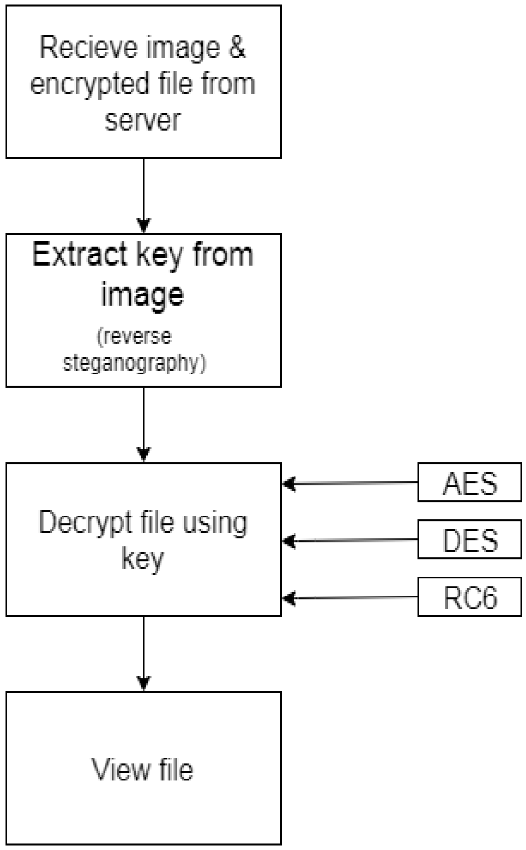


Figure 6 Represents the Reciever Architectural Design

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.

6. EVALUATION PARAMETRS

This section focuses on performance of different algorithms.

A. Quantitative measures – Block Size (Bits)

The block size plays an important role in encryption and execution, which is the basic data unit (Figure 7). The larger block size provides higher security where some features were considered to be equivalent to specific algorithms. AES uses a block size of 128 bits which is twice as many as other symmetric algorithms such as RSA, DES, BLOWFISH.

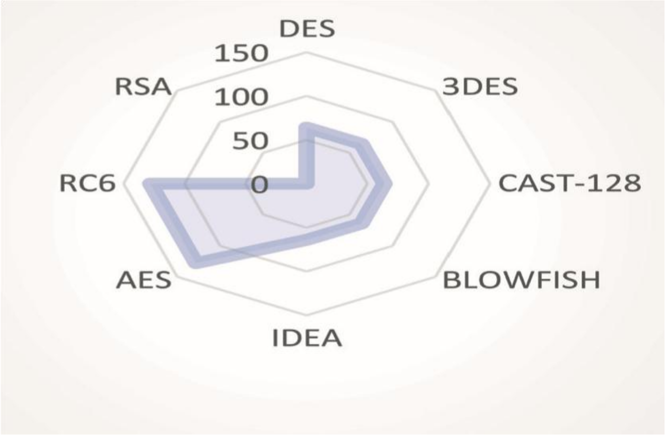


Figure 7 Quantitative Measure- Block Size (Bits).

B. Quantitative measures – Key Size (Bits)

Increasing performance in rounds, strengthens security as the Feistel round one provides insufficient security. DES and BlOWFISH have 16 operating standards. 3DES has 3 DES sessions (48 cycles). AES has a different number of cycles depending on the key size. RC6 is the best candidate for a 20-cycle process with regard to the process involved. The main problem with symmetric key algorithms is the brute force attack, where all possible keys are tried until the exact output key is obtained. The maximum length decreases the magnitude of the attack, since the number of integrations is increased (Figure 8).

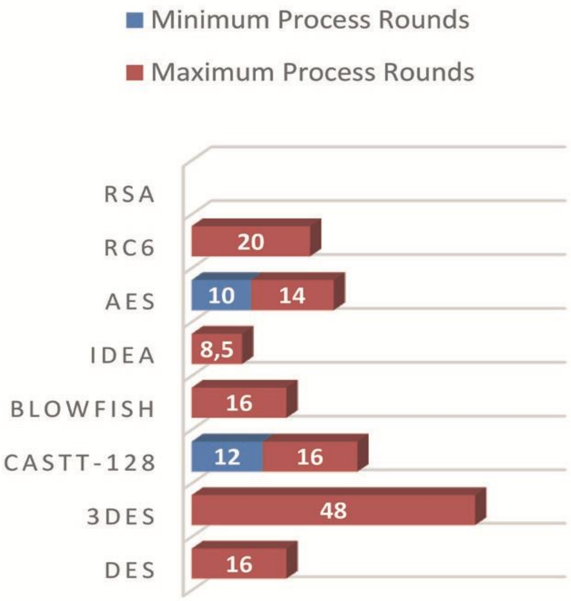


Figure 8 Quantitative Measure- Block Size (Bits)

7. RESULTS

7.1 Login page

The figure below displays options for login into user account who are already registered with the application and only registered users can use the application .For successful logging in the user has to enter valid username and password that are already registered with the application.

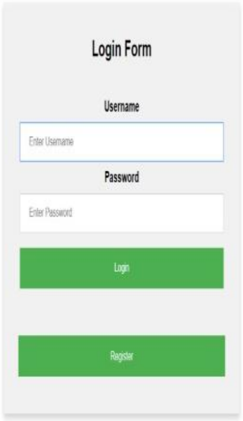


Figure 9. Login Page

7.2 User page

Upon successful logging in by the user ,the home page containing two options encryption and decryption will be displayed as shown in the below figure. The user has two select either encryption or decryption.

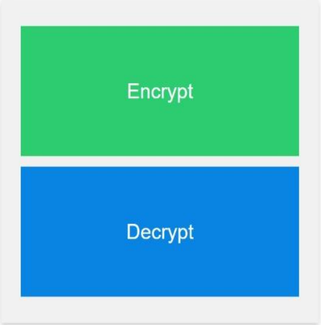
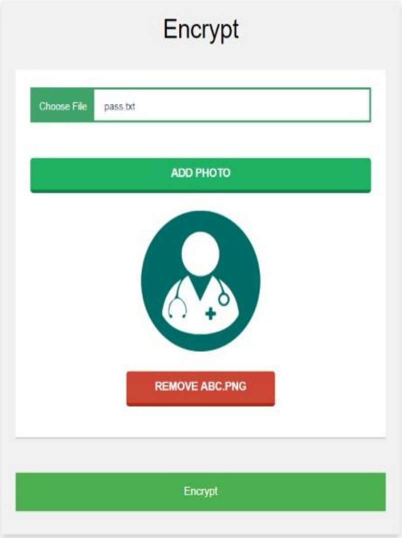


Figure 10 . User Page

7.3 Encryption Panel

In case if the user selects encryption, then he has to choose the file which is to be encrypted and a image from his device to hide key as shown in the below figure.


Encrypt

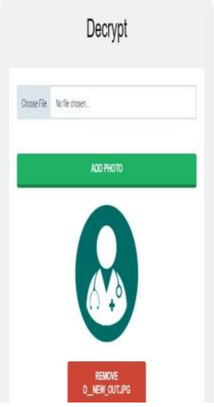
Choose File pass.txt

Figure 11 . Encryption Panel

On clicking the encrypt button in the above figure the user will be able to download the encrypted file and stego image which he can send it to the receiver via mail or any other medium.

7.4 Dencryption Panel

In case if the user selects decryption, then he has to choose the file which is to be decrypted and stego image received as shown in the below figure.


Decrypt

Choose File No file chosen.

Figure 12 User Page

Once the user chooses the file which is to be decrypted and clicks on "decrypt", the decryption process takes place within the application. The user then will be able to download the decrypted file.

8. 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*" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167-170, April 2014.

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

[6.] 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.

[7.] 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