IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

New Generation Cryptographic Security for Cloud Computing

Kislay Kumar

School of Computer Science and Engineering

Galgotias University

Greater Noida, India

V. Arul

School of Computer Science and Engineering

Galgotias University

Greater Noida, India

Abstract— Nowadays, cloud computing usage is rapidly increasing by various IT companies due to its several advantages. It gives lot of benefits with cost savings, high speed, its reliability and also offers advanced online security. By using these three techniques AES, DES and RC2 we are doing encryption and decryption of our data which is already stored into the cloud and in this way, we can preserve our data confidentiality, integrity and data availability. To make sure the security of cloud computing is the major factor. In terms, we have used hybrid encryption with the use of cross breed cryptographic calculations to enhance the security of information present on cloud server. This is what we are going to deal with in this Research Paper.

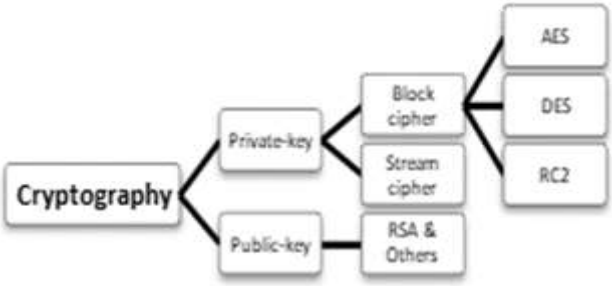
Keywords— Trusted storage, Confidentiality, Integrity, Reliability, AES, DES, RC2.

I. INTRODUCTION

Cryptography is the technique in which we protect the data from unauthorized party by changing that into the unreadable form. The main purpose of cryptography technique is to maintain the privacy of the data from unauthorized party. There are following two types of algorithms which is used for cryptography of data, such as:

(1) Symmetric key algorithm, also called as secret key algorithm

(2) Asymmetric key algorithm, also called as public-key algorithm. In the cloud computing, security is esteemed to be a critical aspect due to the huge amount of data stored in the cloud server. The data can be classified and sensitive. Hence, the management of data should be done very carefully and reliably. It is important that the data in the cloud is secured from hacker or unauthorized party. Security brings concerns in mainly three things Confidentiality, Integrity and availability of the information. Unauthorized access of data results in loss of confidentiality. Data integrity and availability is mainly due to disappointment or failure of cloud administrations. Security services has the following characteristics to be reliable on services. The utility of this cloud and its services are not restricted or bounded to any premises. Everyone such as teachers or students are having permit to use the information whenever and wherever they wanted. This project has cloud that is accessible to all information. The cloud services can be accessed and used with the help of internet from anywhere in the world. The users have to authorized to the cloud server and provide their login details to access the data from cloud server. The cloud service will provide security to the data stored at our server, and stop from the attack of outsider.



II. PROBLEM STATEMENT

Client's stores information at cloud service is unguarded to various danger. Some of the threat model may consider are, our first danger or threat is data integrity. Integrity is a degree confidence that the information in the cloud is what supposed to be present and is guarded against accidentally change in data or intentionally change of data without an authorization. Therefore, a cloud service client cannot entirely depend upon a cloud administration provider to ensure the storage of his information.

Our second danger or threat is the single point failure, which will affect data availability which means that when user require the data but unable to access , that could occur if a server at the cloud administration provider smashed or crashed, which makes it worse for the client to recover his stored information from the server. Availability of data is the most important issue which could be affected, if the cloud administration provider (CAP) failed to provide service. Security is the most important thing for wired network or wireless network transfer to improve what is promised by cloud services. Simply uploading the data on clouds server solves the problem but it is not about data availability, but the problem is about security. The main point of view in this technique is that the secret key has to be combined by reconstructing of the key.

Many of the organizations that have not started using the cloud services just in fear of having their data leaked or shared to an unauthorized party. This accomplishment comes from the fact that the cloud services is a multi-user, where all the information are shared. It is a third-party service, which implies that information is possibly in danger of being seen or mish used by the administration. i.e. attacker, which is the bigger risk when it comes to organization and delicate business information. The best procedure is to rely upon file encryption rather than of the cloud administration provider.

III. PROPOSED MODEL

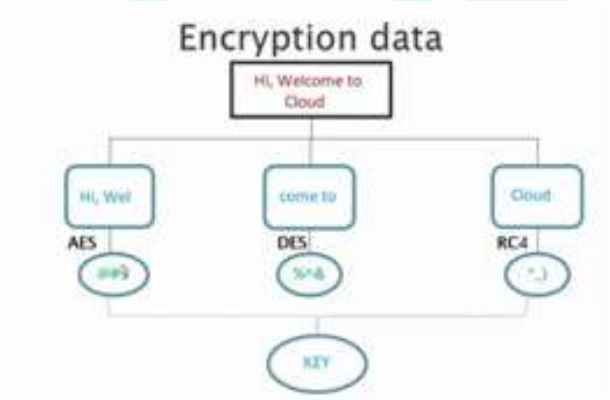


Fig: Encryption Data

Data Encryption Standard (DES)-

Data Encryption standard (DES) could be a symmetric-key block cipher printed by the National Institute Standards and Technology (NIST). DES is an associate degree implementation of a Feistel Cipher. It uses a sixteen spherical Feistel Structure. The block size is 64-bit. though' the key length is 64-bit, DES has an efficient key length of fifty-six bits, since eight of the sixty-four bits of the key don't seem to be employed by the encoding formula (function as check bits only).

Advanced Encryption Standard (AES)-

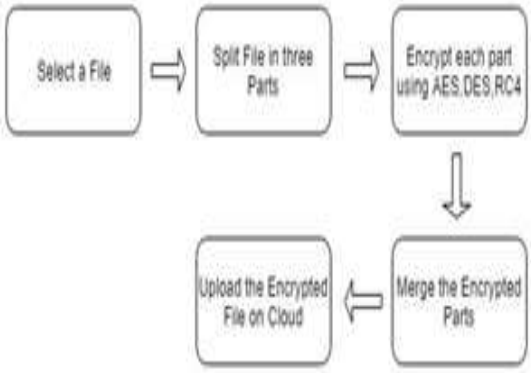
AES is associate degree unvarying instead of a Feistel cipher. supports the 'substitution–permutation network'. It contains a series of connected operations, a number of which involve exchange inputs by specific outputs (substitutions) et al. involve shuffling bits around (permutations). Apparently, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES treats the 128 bits of a plaintext block as sixteen bytes. These sixteen bytes are organized in four columns, four rows for process as a matrix - in contrast to DES, the number of rounds in AES is variable and depends on the length of the key. AES uses ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys. every of those spherical uses a special 128-bit round key, that is calculated from the first AES key.

IV. FLOW DIAGRAM

The given file for encryption is encrypted using the hybrid encryption as shown in figure above. The file is selected and diving into three equal parts using the file system module. Then, each part is encrypted using the AES, DES and RC4 encryption techniques. The encrypted parts are then merged and saved into a single file which, then, can be uploaded on the cloud servers.

Encryption of the file is carried out as shown:



For, decryption the encrypted file is download from the cloud servers and then split into three parts using a certain special character into three parts whereupon each part is then decrypted using the same techniques which were used for encryption, i.e. AES, DES and RC4. The decrypted parts are merged into one and the retrieved file can then be used.

Decryption of the file is carried out as shown:

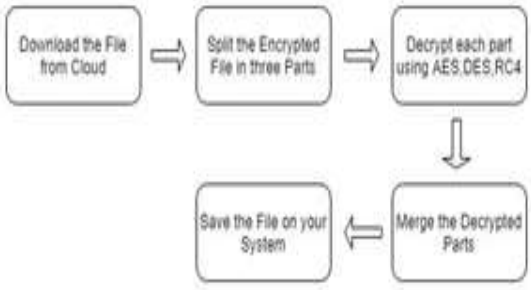


Fig: Decryption Flow Diagram

V. RESULT

An example of generating a RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are terribly high).

Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.

Choose e = 5, that could be a valid alternative since there's no variety that's a standard issue of 5 and (p - 1) (q - 1) = 6 × 12 = 72, aside from one.

The combine of numbers (n, e) = (91, 5) forms the general public key and might be created available to anyone whom we have a tendency to wish to be ready to send us encrypted messages.

Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output is going to be d = 29.

The d calculated is correct by computing - de = 29 × 5 = 145 = 1 mod 72

Thus, public key is (91, 5) and private keys is (91, 29).

RSA Encryption

- Suppose the sender needs to send some text message to somebody whose public key is (n, e). The sender then represents the plaintext as a series of numbers but less than n
- To code the primary plaintext P, that could be a number modulo n. The encryption method is an easy mathematical step as −

C = Pe mod n

- In different words, the ciphertext C is capable of the plaintext P increased by itself e times then reduced modulo n. This suggests that C is additionally a number less than n
- Returning to our Key Generation example with plaintext P = 10, we have a tendency to get ciphertext C

C = 105 mod 91

RSA Decryption

- The decoding method for RSA is additionally very simple. Suppose that the receiver of public-key combine (n, e) has received a ciphertext C
- Receiver raises C to the power of his private key d. The result modulo n are going to be the plaintext P

Plaintext = Cd mod n

- Returning once more to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 −

Plaintext = 8229 mod 91 = 10

VI. REFERENCES

[1] Vijaya Pinjarkar, Neeraj Raja, Kruna Jha, Ankeet Dalvi, “Single Cloud Security Enhancement using key Sharing Algorithm”2016.

[2] V.Vankireddy, N.Sudheer, R.Lakshmi Tulasi, “Enhancing security and Privacy in Multi Cloud Computing Environment” International Journal of Computer Science and Information Technologies,2015.

[3] G.L. Prakash, M. Prateek and I. Singh, “Data Encryption and Decryption algorithms using key rotation for data security in cloud computing”, International Journal of Engineering and Computer Science vol.3, issue 4. pp.5215.5223, April 2014.

[4] N. Sarvanam, A. Mahendiran, N.V. Subramanian and N. Sairam, “An Implementation of RSA Algorithm in Google Cloud”, Research Journal of applied Science, Engineering and Technology, Oct 1, 2012.