International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

Joseph Selvanayagam[1], Akash Singh[2], Joans Michael[3], Jaya Jeswani[4]

[1,2,3] Student of Xavier's Institute of Engineering, Mahim. Mumbai.
[4]Assiatant Professor of IT Dept. Of Xavier's Institute Engineering, Mahim, Mumbai.

Abstract – *In this paper we aim to securely store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures availability. The rapidly increased use of cloud computing in the many organization and IT industries provides new software with low cost. Cloud computing is beneficial in terms of low cost and accessibility of data. Cloud computing gives lot of benefits with low cost and of data accessibility through Internet. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may be untrusted. So sharing data in secure manner while preserving data from an untrusted cloud is still a challenging issue. Our approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES, DES and RC2 algorithm.*

Index Terms – Cloud, Encryption/Decryption Techniques.

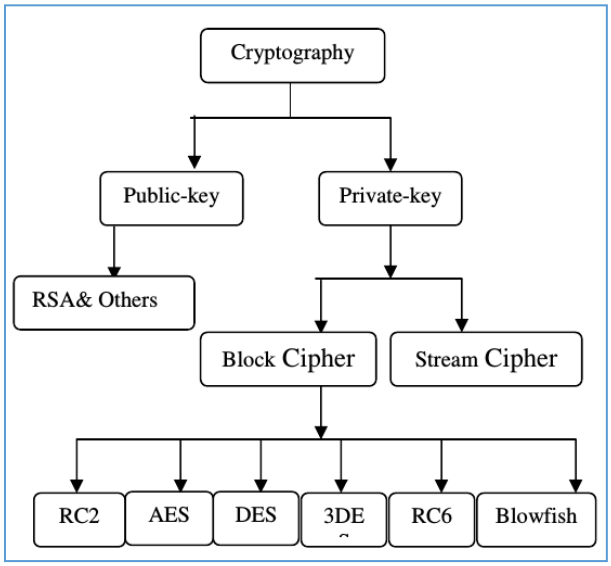
1. INTRODUTION

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party. There are following two types of algorithms such as: (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key algorithm. Symmetric algorithm can be further divided into two types.

In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored in the cloud. The data can be confidential and extremely sensitive. Hence, the data management should be completely reliable. It is necessary that the information in the cloud is protected from malicious attacks. Security brings in concerns for confidentiality, integrity and availability of data. Unauthorized access to information results in loss of data confidentiality. Data integrity and availability suffers due to failure of cloud services. Security has the characteristics of a complement to reliability.

The utility of this cloud and its services are not restricted to a domain or any premises. All the users such as principal, teachers and students are allowed to use this data whenever needed. This project has cloud that is accessible to all, a database to store college related data and all information, website for users to login to the cloud.

The cloud can be accessed through internet from anywhere. The users have to login to the cloud and provide details to access the data from database. The cloud will also provide security to all the data stored at our server.



2. PROBLEM STATEMENT

Customer's stores data at cloud service providers is vulnerable to various threats. In our work, we consider four types of threat models. First is the single point of failure, which will affect the data availability that could occur if a server at the cloud service provider failed or crashed, which makes it harder for the customer to retrieve his stored data from the server. Availability of data is also an important issue which could be affected, if the cloud service provider (CSP) runs out of service.

Our second threat is data integrity. Integrity is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Such worries are no more beneficial issues; therefore, a cloud service customer can not entirely rely upon a cloud service provider to ensure the storage of his vital data.

Security is a necessary service for wired network as well as wireless network communication to improve what was offered in cloud .Simply storing the information on clouds solves the problem is not about data availability, but about security. The strong point of this method is that the secret key has to be combined by reconstructing.

Most of the businesses that have held back from adopting the cloud have done so in the fear of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is only human nature to doubt the capabilities of a third-party, which seems like an even bigger risk when it comes to businesses and sensitive business data. There are also a number of external threats that can lead to data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts. The best strategy is to depend on file encryption and stronger passwords, instead of the cloud service provider themselves.

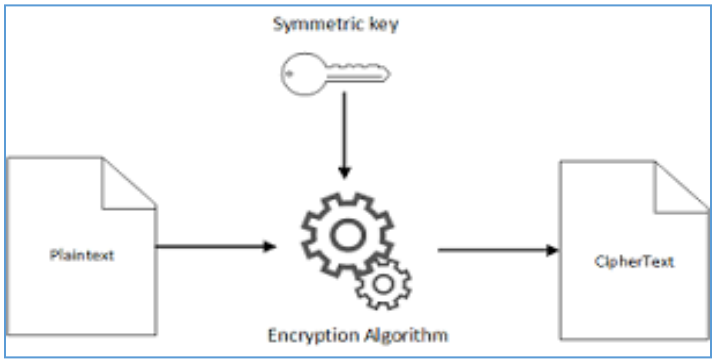
3. FRAMEWORK

Symmetric Key Cyroptography:

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).

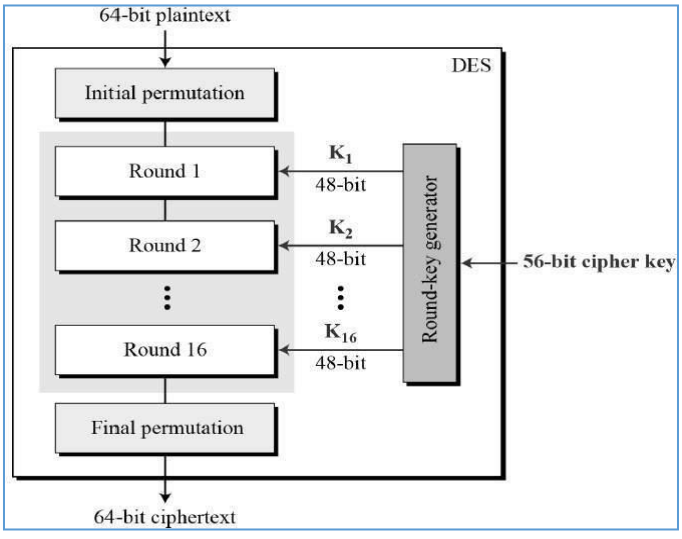


Asymmetric Key Cyroptography:

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. More recently, elliptic curve cryptography has developed, a system in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes.

Data Encryption Standard:

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.The key is nominally stored or transmitted as 8 bytes, each with odd parity. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes—the only difference is that the subkeys are applied in the reverse order when decrypting.



Advanced Encryption Standard:

AES is a subset of the Rijndael cipher developed by Belgian cryptographers, VincentRijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

A. Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

B. Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

C. MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

D. Addroundkey

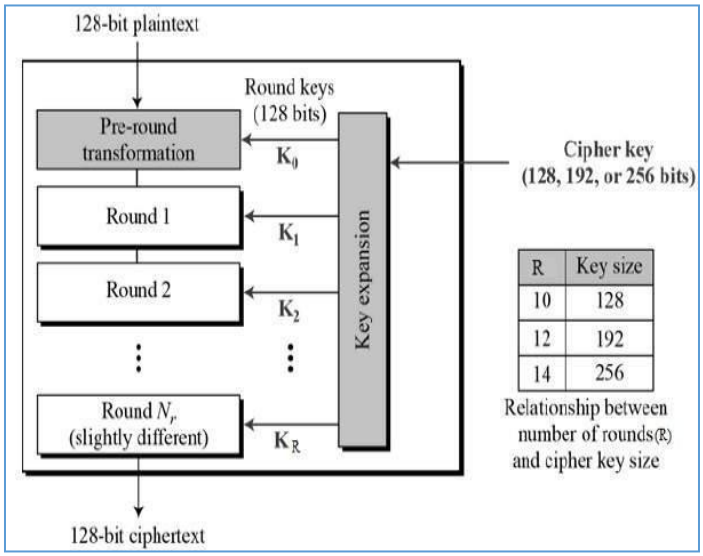
The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

E. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related



RC-2 Encrypion Algorithm:

In cryptography, **RC2** (also known as **ARC2**) is a symmetric-key block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5, and RC6.

The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989.

4. CONCLUSION

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of elliptic curve cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. The ECC Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way

of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of group sharing of data in the shared data section as in this scheme only member of group can access the data stored over shared data section. One to many, many to one, many to many communication is not possible.

5. REFERENCES

[1]VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, "Single Cloud Security Enhancement using key Sharing Algorithm, "Recent and Innovation Trends in Computing and Communication, 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] Swapnila S Mirajkar, Santoshkumar Biradar, "Enhance Security in Cloud Computing, "International Journal of Advanced Research in Computer Science and Software Engineering,2014.

[4] Ashalatha R, "A survey on security as a challenge in cloud computing,"International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology,2012.

[5]www.google.com

[6] G. L. Prakash, M. Prateek and I. Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal Of Engineering And Computer Science vol. 3, issue 4, pp. 5215-5223, April 2014

[7] N. Saravanan, A. Mahendiran, N. V. Subramanian and N. Sairam, 'An Implementation of RSA Algorithm in Google Cloud using Cloud SQL', Research Journal of Applied Sciences, Engineering and Technology, Oct. 1 2012