Secure File Storage On Cloud Using Cryptography

Arun Pratap Singh, Himanshu Pundir

B.tech-4th year student, Galgotias University,U.P,India,
Associated Professor, Galgotias University, U.P,India

Abstract

In this paper we expect to safely store data into the cloud, by parting information into a few lumps and putting away pieces of it on cloud in a way that jelly information confidentiality, uprightness and guarantees accessibility. The quickly expanded utilization of distributed computing in the numerous association and IT businesses gives new programming minimal effort. Distributed computing is useful as far as ease and openness of information. Distributed computing gives parcel of advantages with ease and of information availability through Internet. Guaranteeing the security of distributed computing is a main consideration in the distributed computing condition, as clients regularly store delicate data with distributed storage suppliers, yet these suppliers might be untrusted. So sharing information in secure way while safeguarding information from an untrusted cloud is as yet a difficult issue. Our methodology guarantees the security and protection of customer touchy data by putting away information across single cloud, utilizing AES, DES and RC2 calculation.

INTRODUCTION

Cryptography is the shielding method of information from the unapproved party by changing over into the non-comprehensible structure. The principle reason for cryptography is keeping up the security of the information from outsider. There are following two kinds of calculations, for example, (I) symmetric key based calculation, here and there known as traditional key calculation and (ii) topsy-turvy key based calculation, otherwise called open key calculation. Symmetric calculation can be additionally isolated into two kinds.

In the distributed computing condition, security is considered to be a urgent perspective because of the centrality of data put away in the cloud. The information can be private and incredibly touchy. Subsequently, the information the executives ought to be totally dependable. It is essential that the data in the cloud is shielded from malignant assaults. Security acquires worries for secrecy, uprightness and accessibility of information. Unapproved access to data brings about loss of information privacy. Information honesty and accessibility endures because of disappointment of cloud administrations. Security has the qualities of a supplement to unwavering quality.

The utility of this cloud and its administrations are not confined to an area or any premises. All the clients, for example, head, instructors and understudies are permitted to utilize this information at whatever point required The cloud can be gotten to through web from anyplace. The clients need to login to the cloud and give subtleties to get to the information from database. The cloud will likewise give security to all the information put away at our server.

PROBLEM STATEMENT

Client's stores information at cloud specialist organizations is powerless against different dangers. In our work, we consider four kinds of risk models. First is the single purpose of disappointment, which will influence the information accessibility that could happen if a server at the cloud specialist organization fizzled or smashed, which makes it harder for the client to recover his put away information from the server. Accessibility of information is likewise a significant issue which could be influenced, if the cloud specialist organization (CSP) comes up short on administration.

Our subsequent danger is information trustworthiness. Uprightness is a degree certainty that the information in the cloud is what should be there, and is ensured against coincidental or purposeful adjustment without approval. Such concerns are not any more gainful issues; thusly, a cloud administration client can not so much depend upon a cloud specialist organization to guarantee the capacity of his essential information. Security is a vital help for wired system just as remote system correspondence to improve what was offered in cloud .Simply putting away the data on mists tackles the issue isn't about information accessibility, however about security. The solid purpose of this technique is that the mystery key must be consolidated by remaking.
The majority of the organizations that have kept away from receiving the cloud have done as such in the dread

of having their information spilled. This accomplishment comes from the way that the cloud is a multi-client condition, wherein all the assets are shared. It is likewise an outsider help, which implies that information is possibly in danger of being seen or misused by the supplier. It is just human instinct to question the abilities of an outsider, which appears to be a much greater hazard with regards to organizations and delicate business information. There are additionally various outer dangers that can prompt information spillage, including malevolent hacks of cloud suppliers or bargains of cloud client accounts. The best procedure is to rely upon record encryption and more grounded passwords, rather than the cloud specialist co-op themselves.

FRAMEWORK

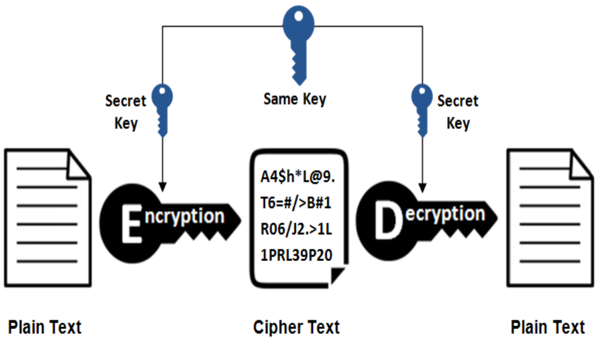
Symmetric-key cryptography:

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).

Symmetric Encryption

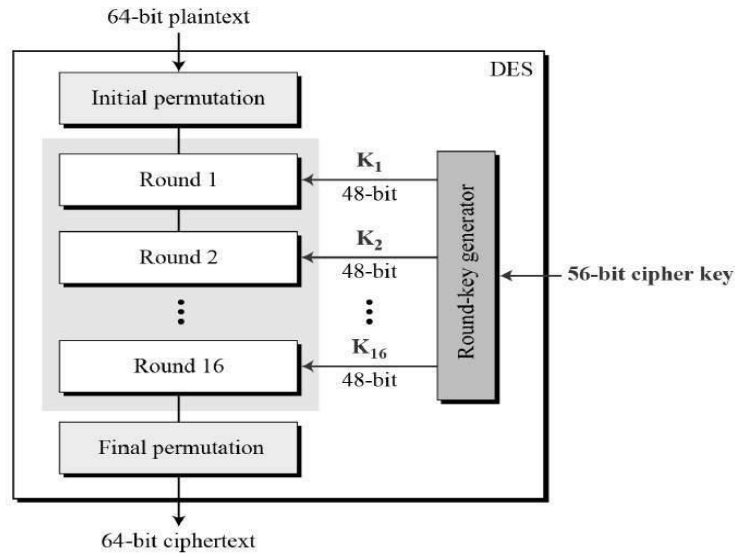


Asymmetric Key Cyroptography:

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, Vincent Rijmen 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

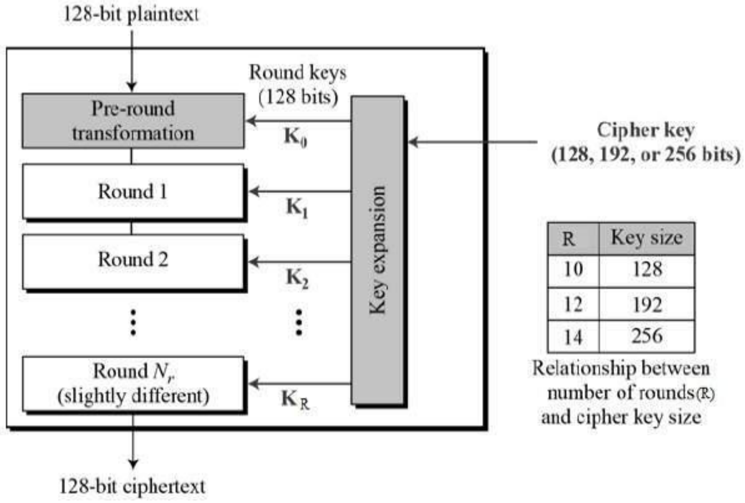
The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

□ Add round key

□ Mix columns

□ Shift rows

□ Byte substitution



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

RC-2 Encryption Algorithm:

In cryptography, RC2 (also known as ARC2) is a symmetrickey 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 Rivestincorporated. After further negotiations, the cipher was approved for export in 1989.

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.

REFERENCE

[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, SantoshkumarBiradar, “*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. 52155223, 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