SECURE RECORD CAPACITY ON CLOUD BY UTILIZING ENCRYPTION ALGORITHM

Ch. Divakar
Department of Information Technology,
S R K R Engineering College
Bhimavaram, India
divakar_c@yahoo.com

Abstract

In this paper, we aim to solve this problem by partitioning data into several parts and storing parts on the cloud in a way that preserves data confidentiality, integrity and availability. The rapid adoption of cloud computing by many organizations and IT industries offers new software at low cost. The benefits of cloud computing include low cost and availability of data. However, sharing data in a secure manner while protecting data from untrusted clouds is still a challenge. The security of cloud computing is a key factor in cloud computing environment. While users often use cloud storage providers to store sensitive information, these providers may not be trustworthy. Our approach protects client sensitive information by storing data across a single cloud using encryption algorithms such as AES, DES, and RC2.

Keywords: ***Encryption techniques, Decryption techniques, Cloud***

I. INTRODUCTION

Cryptography is the process of encrypting data from the unauthorized party by converting it into a non-readable form. The primary purpose of cryptography is to protect the data from third parties. There are two main types of algorithms: Symmetric Key Based Algorithm (sometimes called conventional key algorithm), Asymmetric Key Based algorithm (sometimes called public-key algorithm).

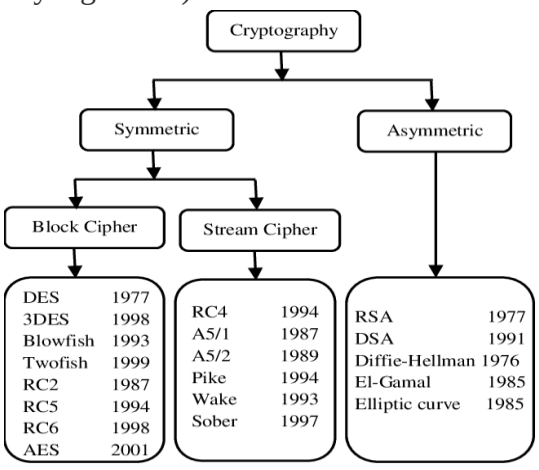


Figure.1. TYPES OF CRYPTOGRAPHY

The importance of security in the cloud computing environment cannot be overstated. Information stored in the cloud can be confidential and extremely sensitive. Therefore, data management should be hundred percentage reliable. It is essential that the information stored in the cloud is protected against malicious attacks. Security raises concerns about confidentiality, integrity and data availability. Unauthorized access to information leads to data confidentiality loss. Data integrity and data availability suffer when cloud services fail. Security has the characteristics of a supplement to reliability

II. PROBLEM STATEMENT:

The data stored by the customer's cloud providers is vulnerable to various threats. In our work, we consider four types of threat models. The first is a single point of failure which affects the availability of data, which can happen when the cloud provider's server fails or crashes, making it difficult for the customer to retrieve stored data from the server. Data availability is also an important issue that could be affected by the termination of service by a cloud service provider (CSP).

Our second risk is data integrity. Integrity is the assurance that data in the cloud should be there and is protected against accidental or deliberate unauthorized modification. Such concerns are no longer matters; therefore the cloud service customer cannot fully trust the cloud service provider to ensure the preservation of their important data. Security is a necessary service to improve the performance of wired networks and wirelessnetwork communications in the cloud. Simply storing datain the cloud solves not the problem of data availability, but the problem of security. The strength of this method is that the secret key must be combined through reconstruction.

Most companies that avoided adopting the cloud did so for fear of their data being leaked.The reason for this achievement is that the cloud is a multi-user environment where all resources are shared. It is also a third-party service, which means that the service provider may represent or manipulate the data incorrectly. It is only human nature to doubt the ability of a third party, which seems to be an even greater risk to businesses and sensitive business data. Also, there are external threats that could cause data leakage, such as malicious hacker from cloud service providers or compromised cloud user accounts. The best strategy is to rely on file encryption and stronger passwords, not the cloud provider itself.

III. FRAME WORK

Symmetric Key Cryptography:

It refers to encryption methods wherein each the sender and receiver percentage the identical key (or, much less commonly, wherein their keys are different, but associated in and without problems computable way). This became the handiest kind of encryption publicly recognized till June 1976. Symmetric key ciphers are applied as both block ciphers or flow ciphers. A block cipher enciphers enter in blocks of plaintext rather than character characters, the enter shape utilized by a flow cipher.

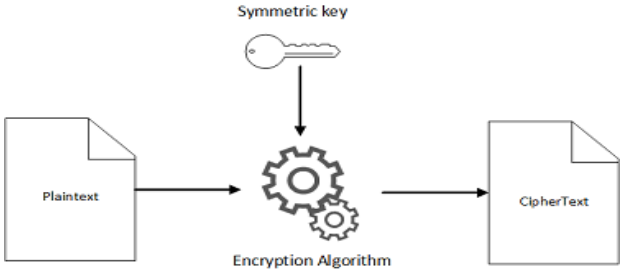


Figure.2. Encryption Algorithm

Asymmetric Key Cryptography:

Public-key algorithms are most customarily primarily based totally on the computational complexity of "hard" issues, often from range theory. For example, the hardness of RSA is associated with the integer factorization problem, at the same time as Diffie– Hellman and DSA are associated with the discrete logarithm problem. More recently, elliptic curve cryptography has developed, a machine wherein protection is primarily based totally on range theoretic issues concerning elliptic curves. Because of the problem of the underlying issues, maximum public-key algorithms contain operations such as modular multiplication and exponentiation, which are tons greater computationally luxurious than the techniques utilized in maximum block ciphers, specifically with ordinary key sizes.

Data Encryption Standard:

DES is the archetypal block cipher—a set of rules that takes a fixed-period string of plaintext bits and transforms it thru a sequence of complex operations into every other cipher text bit string of the identical period.

In the case of DES, the block length 64 bits. DES additionally makes use of a key to personalize the transformation, in order that decryption can supposedly handiest be done through folks who recognize the unique key used to encrypt. The key ostensibly is composed of 64 bits; however, only 56 of those are surely utilized by the set of rules. Eight bits are used completely for checking parity, and are thereafter discarded. Hence the powerful key period is 56 bits. The key's nominally saved or transmitted as eight bytes, every with atypical parity. Before the principle rounds, the block is divided into 32-bit halves and processed alternately; this criss-crossing is referred to as the Feistel scheme. The Feistel shape guarantees that decryption and encryption are very comparable processes—the handiest distinction is that the sub keys are carried out with inside the opposite order whilst decrypting.

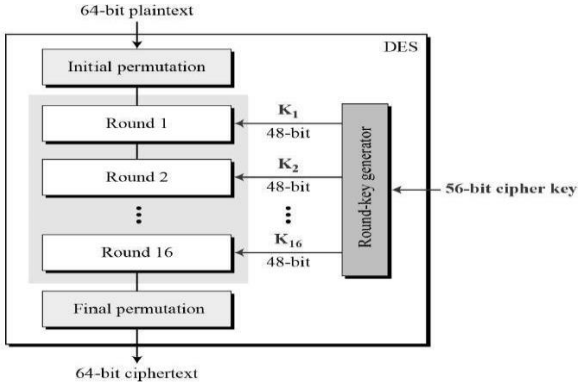


Figure.3. Operation of DES

Advanced Encryption Standard (AES):

It also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a variant of the Rijndael block cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, 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.

Encryption process:

1. ***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.

2. ***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 −

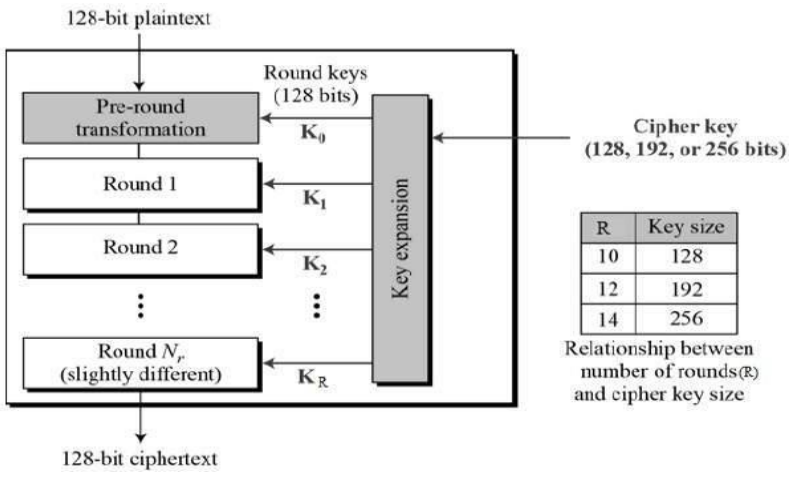
- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.

3. ***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.

4. ***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 cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.



R	Key size
10	128
12	192
14	256

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

Figure.4. Operation of AES

Decryption Process:

The process of decryption of an AES cipher text 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 need to be separately implemented, although they are very closely related.

RC-2 Encryption Algorithm:

In cryptography, RC2 (additionally called ARC2) is a symmetric key block cipher designed through Ron Rivest in 1987. "RC" stands for "Ron`s Code" or "Rivest Cipher"; different ciphers designed through Rivest encompass RC4, RC5, and RC6.

The development of RC2 turned into subsidized through Lotus, who was looking for a custom cipher that, after assessment through the NSA, may be exported as a part of their Lotus Notes software. The NSA counseled multiple changes, which Rivest incorporated. After similarly negotiations, the cipher turned into authorized for export in 1989.

IV. CONCLUSION

The main purpose is to safe storage and use of data in the cloud, which is not under the control of the owner of the data. We use elliptic curve encryption technology to protect data files in the cloud. The two components of the cloud server have improved the performance of data storage and access. The ECC encryption algorithm used for encryption is an advantage that improves the performance of the encryption and decryption process. We expect this way of storing and accessing data to be much more secure and efficient. We are trying to solve the group sharing problem in the data section of the shared data, because in this system, only the group member has access to the data stored in the shared data. One-to-many, many-to-many, many-to-many communication is not possible.

REFERENCES

[1] A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security risks and their management in cloud computing,” 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.

[2] Ahmed Albugmi Madini, O. Alassafi Robert Walters,” Data Security in Cloud Computing”, 2016.

[3] 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.

[4] Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly Algorithms June 2020International Journal of Advanced Science and Technology 29(5):12315-12331, Advin Manhar.

[5] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[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] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).

[8] M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.

[9] 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

[10] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.

[11] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[12] Swapnila S Mirajkar, Santoshkumar Biradar, “Enhance Security in Cloud Computing, ”International Journal of Advanced Research in Computer Science and Software Engineering,2014

[13] www.google.com

[14] VijayaPinjarkar, Neeraj Raja, KrunalJha, AnkeetDalvi, “Single Cloud Security Enhancement using key Sharing Algorithm, ”Recent and Innovation Trends in Computing and Communication, 2016.

[15] 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.

[16] 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.