J. Adv. Res. in Cloud Computing, Virtualization and Web Applications
Volume 3, Issue 1 - 2020, Pg. No. 29-31
Peer Reviewed Journal

Article

Secure Cloud using Cryptography

Shyo Prakash Jakhar[1], Amit Kumar Bhatt[2], Deepali Bhati[3], Deepak Choudhary[4]

[1,2]Assistant Professor, Arya Institute of Engineering Technology & Management, Jaipur.

INFO

Corresponding Author:
Shyo Prakash Jakhar, Arya Institute of Engineering Technology & Management, Jaipur.
E-mail Id:
shyo143@gmail.com
Orcid Id:

How to cite this article:
Jakhar SP, Bhatt AK, Bhati D et al. Secure Cloud using Cryptography. *J Adv Res Cloud Comp Virtu Web Appl* 2020; 3(1): 29-31.

Date of Submission: 2020-05-22
Date of Acceptance: 2020-06-15

ABSTRACT

Cloud Computing is careful as the on-demand obtainability of computer system incomes. The cloud Computing provides data storage and effective computing power, it don't need direct active management by the user. It is blend of number of diverse machineries .this new technology has many advantages including decrease in cost and load. Large volume of structured and unstructured data requires increased processing power and storage. The cloud gives not just promptly accessible framework just as the capacity to scale this foundation rapidly so we can oversee enormous spike in rush hour gridlock or use. As the need of distributed computing for information stockpiling on cloud is expanding, the need of security and classification is additionally turning out to be basic prerequisite, so no unapproved substance can get to the secret data. Encryption is the best answer for the security of information. It is extremely simple to utilize. There are diverse cryptographic calculations are accessible for encryption of information.

The cloud storage likewise defeats the disavowal of an administrations. This paper presents the arrangements which were acquainted with conquer the issues identified with information security and information classification with the assistance of various cryptographic calculations .These calculations are utilized by various association to raise the security in cloud.

Keywords: security, Cryptography, RSA, AES, DES, CIA Encryption and Decryption etc

Introduction

In cloud computing, Cloud is defined as storage server which handles massive amount of big data. There are many factors which entice dissimilar organization to use this cloud storage. These administrations want nothing but security of their data. They only want that the confidentiality of every user remain private. Any storage device works on three objectives which can be identified as CIA[1]. 'C' stand for Confidentiality, 'I' stand for Integrity and 'A' stand for Availability. Confidentiality is a moral responsibility for any organization to keep the user's data and info private. Integrity means to keep the data safe from illegal accessing. Obtainability incomes being talented to use the system as per the supplies.

Cloud computing is based on two type of resources which are hardware and software resources. These resources are managed by different services. The main objective of this service is to deliver authority to access high end network servers and software use. In cloud computing both files and software are not fully contained on the end user's computer. So, this is the server's responsibility to reserve the confidentiality and sensitivity of data. For this we need secure storage server provided by cloud computing. This need of cloud server is fulfilled using cryptography technique. In this the owner encrypts the data with the help of different encryption techniques and after the encryption, data is uploaded to the cloud storage. Whenever the user downloads the data it will be in encrypted form.

These encryption methods will protect data of cloud environment. There can be two convenience modes of data access which are public and private. Public data is shareable data amongst trusted users with no restrictions on usage, on the other hand private data is user's confidential data that must be encrypted to keep it secure and confidential.

Cryptography can be ordered in two forms

- Symmetric
- Asymmetric

In Symmetric cryptography the sender and receiver shares their encryption and decryption keys. These keys are easy to deduce each other. AES (Advanced Encryption Standard) is one of the symmetric cryptography.

In Asymmetric cryptography algorithms are compared on the basis of key size, key cohort time, signature generation time and verification time. RSA (Rivest-shamir-Adleman) is an asymmetric cryptography encryption algorithm.

System Architecture

Cloud security plays an important role in the security of files. It is very significant to have a right security system which could protect the information. The components of cloud infrastructure include APIs, load balancers, management consoles. To avail the best security servers cloud security architecture should be designed withstand various interruption. It should also follow organization's principles and the latest technology architecture. CCM(Cloud Controls Matrix) and CSA(Cloud Security Alliance) are two major aspects to be followed. Cloud audit or continuous security monitoring have become an integral part of cloud security.

During the time spent distributed storage security two distinctive security calculations are consolidated and the picked calculations are DES and RSA. DES utilizes same key for encryption and unscrambling while RSA utilizes two unique keys adversary encryption and decoding. DES and RSA encode the transferred information of client for encryption. The three encryption calculations AES, DES and RC6 make the record totally secure. The key is likewise made sure about by installing it in a picture. Subsequent to applying these calculations no unapproved client would have the option to get to the cloud, it will keep the information secure. The RSA calculation was created by Ron Rivest, Adi Shamir and Leonard Adleman.[1] RSA utilizes both open key and private key for encryption and unscrambling. For decoding private key is utilized and for encryption open key is utilized. Figure 2, is speaking to encryption and decoding calculations. Figure 1, shows the sharing of information in cloud computing.

In the above figure, e and d are public and private keys respectively. M is the Plain text and C is the cipher text.

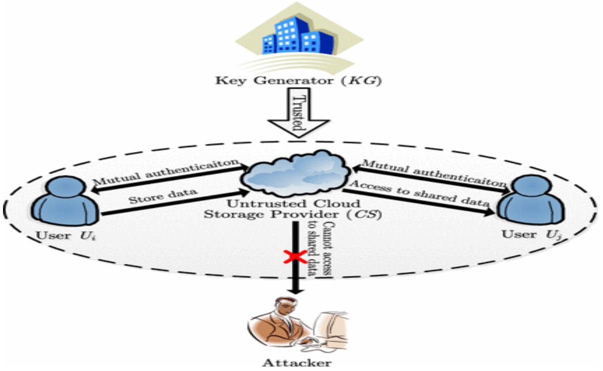
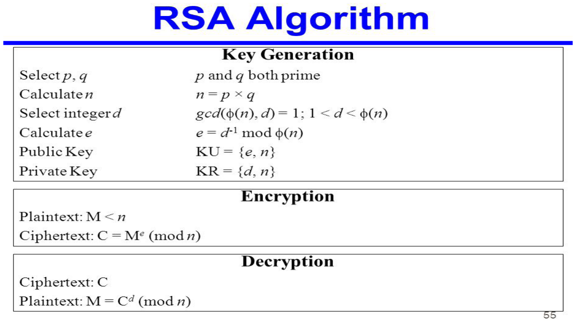


Figure 1.Secure Data Sharing in Cloud Computing


RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$gcd(\phi(n), d) = 1;\ 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	$KU = \{e, n\}$
Private Key	$KR = \{d, n\}$

Encryption

Plaintext: $M < n$
Ciphertext: $C = M^e \pmod n$

Decryption

Ciphertext: C
Plaintext: $M = C^d \pmod n$

55

Figure 2.Encryption and Decryption using RSA algorithm

A DFD is used to characterize system components and the flow of data in a system. DFD is a data flow diagram, it represents input, output and also the procedure of data. This system represents the flow of information at different level of abstraction. The different levels of DFD also depict the functional details. Four symbols are used to represent data sources, data flow, data transformations and data storage in a flow diagram. Nodes are represented by stages and transformations are represented by circles. Input data is transformed to output data using a series of functions and this will also modify the input data. Figure 3, shows the DFD of various instances.

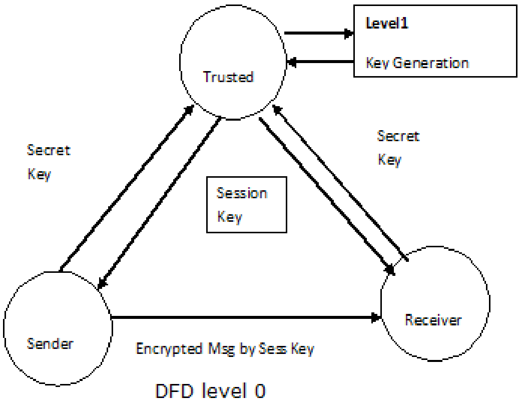


Figure 3.Data Flow Diagram of level 0

The cloud verification process is the first process which is run in cloud server system. It validates the user by verifying his/her username and password. The verification details are sent to the masquerading router. The verification server also updates the client's list which reduces the authentication time.

The secure data modification module deals with the modification to the secure data. The user operates on the block level if he wants to insert or delete his files. The verification becomes important here.

An activity diagram is a graphical illustration step-by-step workflow of components in a system. There is an execution phase in activity diagram. It contains four dissimilar modules which are client module, storage of data module, cloud authentication process and secure data modification. In client server, an authenticated client sends a request query to the server. For security purpose client's username and password is verified. If the verification details are correct then the process is accessed further otherwise request is denied. In the further process the server searches the requested file and provides it to the user. If the server finds an intruder then an alternate path 1 set for the intruder.

In storage data module, it deals with storage part of the cloud. The storage data of user is stored in a cloud server in cloud computing. The stored data on different server which are maintained by the cloud service providers. The enormous amount of data is stored on cloud server which is not favorable for smooth performance of system. The stored data should also be secured. The third party auditors are used to maintain security and feasibility of the system.

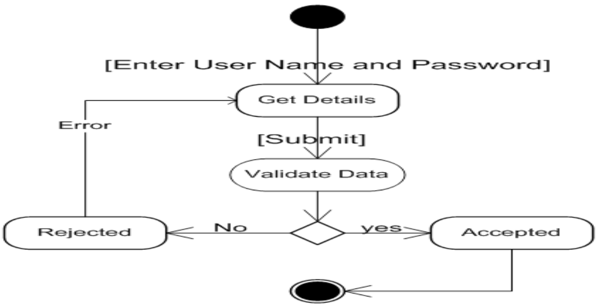


Figure 4.Activity diagram of User Login

Figure 4 shows the activity diagram of the system.

Conclusions

Cloud computing is the concept in which the programs run and produces required output. Cloud computing is new technology developed that has the potential to have a great impact on the world. Cloud computing is a collection of resources and services. Since in this new technological world each and every association is generating huge amount of data every day, to store this huge amount of data the reliable storage services is on condition that by cloud service benefactors. There is also a need of security against the unofficial modification, access and denial of services.

References

1. Saharsh, Srivastava S, Lavanya MC. Security on cloud computing Using Cryptography.
2. Deshmukh A, Janda HK, Bhusari S. Security On Cloud Using Cloud Computing. 2015 *In International Journal of Advanced Research in Computer Science and Software Engineering.*
3. Maitri PV, Verma A. Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm". 2016 IEEE WiSPNET 2016 conference.
4. Jaspher G, Katherine W. A secure framework for enhancing user authentication in cloud environment using Biometrics. 2017 International conference on Signal Processing and Communication (ICSPC'17).
5. Jitendra Singh Adam et al. A Changed cryptographic plan improving information. *journal of Advanced Research in Computer Science and Software Engineering,* 2012; 2.
6. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. in proceedings of the IEEE Symposium on Security and Privacy (SP' 07) 2007; 321-334.
7. Sahai A, Waters B. Fuzzy Identify-Based Encryption. Proceedings of the EUROCRYPT, 2005: 457473.
8. Fan CI, Huang SM, Raun HM. Arbitrary state Attribute-based encryption with dynamic membership. *IEEE Transactions on computers* 63(8):1951-1961.