ANUSANDHAN- AISECT University Journal
Vol. 06, Issue No. 13, March-2018, P-ISSN 2278-4187, E-ISSN 2457-0656

Cloud Computing Environment through Encryption Algorithms- A Review Paper

Jahangeer Qadiree[1]* Dr. Pratima Gautam[2]

[1]Dept. of IT, RNTU, Bhopal (M.P.) India

[2]Dept. of IT, RNTU, Bhopal (M.P.) India

Abstract – No doubt that the Cloud computing technologies are gaining the ubiquitous adaptation due to the countless features they provide. Security is the main concern of cloud that hinders its wide adaptation as well as the development. The main obstacle or hindrance of the cloud adaptation among the small or big enterprises is the privacy as well as the security of their data. In this paper we have mainly focused at the service provider's side by suggested the various cipher encryption algorithms. So as to make the cloud trusty and offer the desired security features to the cloud user's.

Keywords – Security, Encryption Algorithms, RSA, AES, DSA, Blowfish.

----------♦----------

1. INTRODUCTION

Cloud computing proposes a new way of computing. It provides the development of environment and the allocation as well as the reallocation of computer resources as per the demand. Virtually it satisfies the on demand needs of the user and facilitates the resources "as a service model". The cloud technology offers are we can say it another words that it provides the ability for both small as well as the big organizations to move/shift their data globally. It is a using the remote services through a network. Cloud computing allows its users to use maximum number of resources through minimum resources available at the user's end. The cloud computing environment facilitates the way to use the computing resources through a device that is capable of connect the user to the server at any location across the world and also the users are not bounded to store the data at their end because the data is stored on the server.

Cloud concept reduces the cost of hardware at the user end. Users are not bounded to store their data at the user's end because the data is stored on the cloud. Through the Cloud users can access their data through any location.

(a) Types of Clouds

The environment of cloud computing is divided into three different categories as per their usage and requirement include, private cloud, public cloud and hybrid cloud.

(i) **Private cloud**: Private clouds are owned by the single organization. The private cloud provides better control and more flexibility. They are very expensive and secure when we compare them to other clouds. The providers and the users have a very good control of the cloud infrastructure. One of the best examples of a private cloud is Eucalyptus Systems.

(ii) **Public Cloud**: They are totally hosted and maintained and are shared on a larger scale. Consumers pay for the resources that they use. Users have a little control over the cloud infrastructure. Microsoft Azure, Google App Engine is the examples of public clouds.

(iii) **Hybrid Cloud**: Hybrid clouds is the composition of two or more cloud models, linked each other in a way so that the data transfer takes place between them without affecting each other. These types of clouds are created by the large enterprise. In this model, the company outlines the main goals and requirements of services. But the major drawback of the hybrid cloud is the difficulty in effectively creating and governing such a solution.

(iv) **Community Cloud:** This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

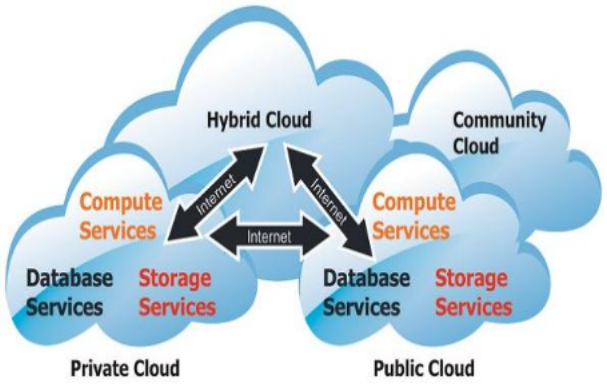


Fig 1: Deployment Models of Cloud Computing

2. MOTIVATION

In cloud computing technology the users work with the applications those are located off-premise. There are numerous organizations those are uncomfortable regarding to store their applications as well as their important data on the system that are not controlled by them personally. Our aim is to suggest a framework that will clarify the cloud computing concept easily. The suggested framework will clarify the confidentially of data, protection of data and the selection of security control needed to the data confidentially.

3. BACKGROUND STUDY

The Cloud computing environment concept is divided into three phases: namely as connectivity, storage, and application. Each part offers different services for the cloud users.. The concept of cloud paradigm allows a new way of computing that allows us to work the applications as per our need and reduces the cost for managing the hardware as well as the software resources. It allows the user's to access the applications that are cloud based through a light weight device that is capable on internet access. The main hindrance of the Cloud Computing is security concern and the Implementation. With the help of different encryption algorithms like- RSA, DSA, DES, Blowfish etc,, Users are able to enhance the security as well protect their sensitive data on the cloud paradigm.

4. ANALYSIS OF VARIOUS ENCRYPTION ALGORITHMS

The Cloud computing technology is used by various communities like, ordinary, enterprise as well as the academia as per their demand. There are various security threats and policy issues. Security is the main concern of cloud that is different from various points of views. Our review focuses mainly on analysis of various encryption algorithms to find the best method as per need.

Our proposed work analysis various available encryption algorithms so as to ensure the data security in cloud computing. The encryption algorithms that are used are analysed below:-

(a) **RSA Algorithm:** It is widely used for securing the data when the data is send to the network. RSA is an asymmetric cryptography technique that consists of two keys public and the second one is private.

Select two prime numbers.

Calculate $n = p * q$

Calculate $f(n) = (p-1)(q-1)$

Select e such that e is relatively prime to $f(n)$ and less than $f(n)$

Determine d such that de congruent modulo $1(\text{mod}$ $f(n)$ and $d < f(n)$

Public key = $\{e, n\}$ Private Key $= \{d, n\}$

= {d, n}

Cipher text c = message e mod n

Plain text p = cipher text d mod n

(b) **DSA Algorithm:** stands for digital signature and was proposed by NIST in the month of august 1991. DSA algorithm consists of two parts namely key generation, generation of digital signature and verification.

Key Generation:

(i) Choose a prime number q, known as the prime divisor.

(ii) Choose another primer number p, such that $p - 1 \bmod q = 0. p$ is called the prime modulus.

(iii) Choose an integer g, such that $1 < g <, g^{**} q \bmod p = 1 and g = h^{**}((p-1)/q)$ mod p. q is also called g's multiplicative order modulo p.

(iv) Choose an integer, such that $0 < x < q.$

(v) Compute y as $g^{**} x$ mod p.

(vi) Package the public key as $\{p, q, g, y\}$

Jahangeer Qadiree[1]* Dr. Pratima Gautam[2]

(vii) Package the private key as $\{p,q,g,x\}$

Signature Generation: the signer wants to sign the document $x \in \{0,1\}^*$. the signer uses the hash function

$$SHA-1:\{0,1\}^* \rightarrow \{0,1\}^{160} \quad \textbf{(A)}$$

Chooses a random number $k \in \{1,2,.....q-1\}$ computes $r=(g^k \bmod p) \bmod q,$ and sets $s=k^{-1}(SHA-1)(x)+ar) \bmod q$ **(B)**

Here, k^{-1} Is the inverse of k module q, the signature of x is $(r,s).$

Verification: when the document is received by the receiver end, the signature is verified. The receiver obtains the signer's public key $(p,q,g,A).$ and verifies

$$1 \le r \le q-1 and 1 \le s \le q-1. \quad \textbf{(C)}$$

if the above condition is violated, then the signer's signature is rejected, otherwise he verifies

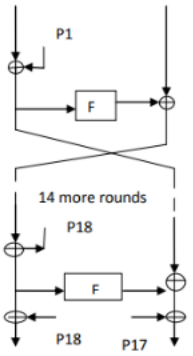
$$r=\left((g^{(s^{-1}h(x)) \bmod q} A^{(rs^{-1}) \bmod q} \bmod p) \bmod q\right)$$

(D)

if the signature is constructed according as (A), (B). Then (D) holds.

The construction implies. $g^{(s^{-1}h(x)) \bmod a} A^{(rs^{-1}) \bmod q} \equiv g^{s-1(h(x)+ra)} \equiv g^k \bmod p,$

(c) Blowfish Algorithm: It was designed by Bruce Schneier in the year of 1993 as an free alternative to the existing encryption standards. It is a symmetric encryption algorithm that encrypts 64 bit block with a variable length 0f 128 to 448 bits. The main important feature of this algorithm is that it is an open source for all the users worldwide. Blowfish is a 16-round feistel cipher and uses various key dependent S-boxes and each S-box accepts the input of 8-bits and then produces the output of 32 bits.



(d) AES Algorithm: Stands for advanced encryption standard. It's a symmetric cipher standard designed and developed by Vincent Rijmen and Joan Daemen. AES consists the following features.

1. Block encryption implementation.
2. Single key for both encryption as well as decryption.
3. Easy implementation.
4. 128-bit group encryption.

Encryption Algorithms Specifications

Algorithm	Key Size	Initial vector size	Key used	Execution time
RSA	1024 bits	1024 bits	Public and Private	Maximum
AES	128,192,256 bits	128 bits	Same key for both encryption as well as decryption	Faster as compared to others
DES	56 bits	64 bits	Same key for both encryption as well as decryption	Same as AES
Blowfish	32-448 bits	64 bits	Same key for both encryption as well as decryption	Less

5. CONCLUSION

The most important part of the cloud is the security concern. This paper proposes various existing encryption algorithms to concern the security issues and make the data secure on cloud. We have also made the comparisons between the various cipher algorithms, so as to use the best cipher standard. As we know that the Encryption algorithms play a vital role in the life cycle of data security on cloud. The demand or adaptation of cloud technology worldwide is increasing. therefore, the proposed cipher's are helpful as per the demand.

REFERENCES

D L. Ponemon (2010), Security of Cloud Computing Users, vol. 34-No. 2, International Journal of Computer Theory and Engineering.

Iankoulova, I.; Daneya, M., (2012). Cloud computing security requirements: A systematic review, Research Challenges in Information Science (RCIS), Sixth International Conference on, On page(s): pp. 1-7.

Sarathy, R, dhar, K. (2006). Secure and useful data sharing Decision Support System, vol.42-No.1, Computer Science press.

Uma Somani, Kanika Lakhani, Manish Mundra, (2010). "Implementing digital signature with RSA Encryption Algorithm to enhance the data security of cloud in Cloud Computing".

Xing Zhou, Xiaofei Tang (2011). Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.

Corresponding Author

Jahangeer Qadiree*

Dept. of IT, RNTU, Bhopal (M.P.) India

E-Mail – Jahangir.ahmad17@gmail.com