RESEARCH ARTICLE OPEN ACCESS

Security Algorithms in Cloud Computing

T.Ramaporkalai
Assistant Professor
Department of Computer Science
Madurai Sivakasi Nadars Pioneer Meenakshi Women's college, Poovanthi
Tamil Nadu - India

ABSTRACT
Network and Internet applications are growing very fast, since the need to secure these applications are very fast. For this purpose cryptography algorithms (symmetric & Asymmetric) are proposed. The use of relevant algorithm deals with the level of data safety in cloud because data security in cloud computing is a serious issue as the data centers are located worldwide. Authentication is the most essential procedure to ensure the cloud data in a secured manner. However, strong user authentication is the main requirement for cloud computing that reduces the unauthorized user access of data on cloud. Data security is a more important issue of cloud computing. Thus, the need to ensure the safety of information that being exchanged between the users and the cloud became more significant. Many security and authentication techniques have been proposed to secure the exchanged data. These techniques aim to keep the authentication, privacy and reliability levels of data. Here in this survey paper, I have presented security algorithms in cloud computing.

Keywords:- Cloud computing, Cryptography, Encryption, Decryption, Cipher Text, DES, TDES, AES, RSA, Homomorphic, IDEA, Blowfish.

I. INTRODUCTION

Cloud is nothing but the group of servers and datacenters that are placed at different places and these severs and datacenters are responsible for providing on demand service to its users with help of internet. The service provided by cloud is not present on user's computer. User has to access these services with help of internet connection through subscribing them. The main advantage of Cloud computing is that it eliminates the need for user to be in same location where hardware software and storage space is physically present. Cloud makes it possible to store and access your data from anywhere anytime without worrying about maintenance of hardware software and storage space. All these services are provided to user at low cost. User has to pay according to storage space he is using. Due to this flexibility everyone is transferring his data on cloud.

Security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away [1]. While sending of data and during storage data is under threat because any unauthorised user can access it, modify it, so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorised disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorised user. Availability refers to assurance that user has access to information anytime and to any network. In the cloud confidentiality is obtained by cryptography.

II. SECURITY ISSUES OF CLOUD COMPUTING

Cloud computing is a huge collection of inter connected network. . There are so many risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be changed by third party while transferring [4]. The major issues related to data security include data integrity, data availability, data confidentiality, privacy, transparency of data [2] and control over data where data resides. There are various aspects for providing data security such as by providing access controls and encryption methods. The service provider must be ensuring that their infrastructure that providing is secure and client's data remain protected [3].On the side of client, they should look into the security measures related to data that what are the security techniques are provided by cloud provider.

III. PROBLEM STATEMENT

There are various policies issues and threats in cloud computing technology which include privacy, segregation, storage, reliability, security, capacity and more. But most important among these to concern is security and how service provider assures it to maintain. Generally cloud computing has several customers such as ordinary users, academia and enterprises who have different motivations to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises most important problem is also security but with different vision.

So, we mainly concentrate on data security of cloud computing.

IV. EXISTING ALGORITHMS

Many organisations and people store their important data on cloud and data is also accessed by many persons, so it is very important to secure the data from intruders. To provide security to cloud many algorithms are designed. Some popular algorithms are:-

A. Data Encryption Standard (DES)

This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher. [5]

Algorithm:

function DES_Encrypt (M, K)
where M = (L, R)
M←IP (M)
For round←1 to 16 do
K←SK (K, round)
L←L xor F(R,K_i)
swap(L, R)
end
swap (L, R)
M←IP^{-1}(M)
return M
End

B. Advance Encryption Algorithm (AES)

(Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES Encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications. [6][7]

C. Triple- DES (TDES)

This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. [6][8].

Algorithm:

For j = 1 to 3
{
$C_{j,0}$= IV_j
For i = 1 to n_j
{
$C_{ji} = E_{KEY3}(D_{KEY2} (E_{KEY1} (P_j, iC_{j, i-1})))$
Output $C_{j, i}$
}
}

D. Blowfish Algorithm

This was developed in 1993. It is one of the most common public algorithms provided by Bruce
Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [8].

Algorithm:

Divide x into two 32-bit halves: x_L , x_R
For i = 1to 16:
$x_L = x_L$ XOR Pi
$x_R = F(x_L)$ XOR x_R
Swap x_L and x_R
Next i
Swap x_L and x_R (Undo the last swap.)
$x_R = x_R$ XOR P17
$x_L = x_L$ XOR P18
Recombine x_R and x_L

E. IDEA

International Data Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used. What is the sequence of operations performed in each round? Let I1, I2 …I6 be the inputs to [5] round 1, functions in round 1 are:-

(i) Multiply I1 and K1.
(ii) Add I2 and K2.
(iii) Add I3 and K3.
(iv) Multiply I4 and K4.
(v) Now, step 1 is EXOR with step 3.
(vi) Step 2 EXOR with step 4.
(vii) Multiply step 5 with K5.

Similar operations are performed in other rounds.

F. Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key [10]. In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

G. RSA

This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [9].

Algorithm

Key Generation: KeyGen(p, q)

Input: Two large primes –p, q

Compute n = p. q

$\varphi(n) = (p-1)(q-1)$

Choose e such that $\gcd(e, \varphi(n)) = 1$

Determine d such that $e.d \equiv 1 \bmod \varphi(n)$

Key:

Public key = (e, n)

Secret key= (d, n)

Encryption:

$c = me \bmod n$

where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. Given $ci = E(mi) = mie \bmod n$, then $(c1.\ c2) \bmod n = (m1\ .\ m2)e \bmod n$

H. Diffie- Hellman Key Exchange

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography.

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communication using a symmetric key cipher.

V. CONCLUSION

Cloud computing appears very useful service for many people; every third person is using cloud in different ways. Due to its flexibility, many persons are transferring their data to cloud. Cloud computing prove a very successful application for organisations. Because organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anywhere anytime easily. As people are saving their personal and important data to clouds, so it becomes a major issue to store that data safely. Many algorithms exist for the data security like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric, in which two different keys are used for encryption and decryption. These algorithms are not secure, there is need to enhance the security of algorithms.

VI. FUTURE SCOPE

Cloud computing opens several new trends, like using software that are not present on your computer, accessing data from anywhere. One of the big advantages of cloud computing is virtualization, but we can use cloud computing properly only if it provides reliable security. Cloud computing is mostly used because it provides much storage space to its user, so it becomes necessary to provide security to that data. There are many security algorithms, but security of all these algorithms can be broken by anyone. So it is very necessary to make security of cloud more strong.

REFERENCES

[1] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. **(2011)**.

[2] Anitha Y, "Security Issues in cloud computing", "International Journal of Thesis Projects and Dissertations "(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.

[3] Qi. Zhang ·Lu. Cheng, Raouf Boutaba, "Cloud computing: state-Of-the-art and research Challenges", "The Brazilian Computer Society", April 2010.

[4] Garima Saini, Gurgaon Naveen Sharma,"Triple Security of Data in Cloud Computing ", Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4) , 2014,

[5] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[6] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[7] Gurpreet Singh, Supriya Kinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[8] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha "Cryptography Algorithm Comparison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[9] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,"2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).