A SERVEY OF SECURITY ALGORITHMS IN CLOUD COMPUTING

SONIA SINDHU[1]

Jind, Haryana,India

Abstract: **Recently, there has been a dramatic increase in the popularity of cloud computing systems that rent computing resources on-demand, bill on a pay-as-you-go basis, and multiplex many users on the same physical infrastructure. It is a virtual pool of resources which are provided to users via Internet. It gives users virtually unlimited pay-per-use computing resources without the burden of managing the underlying infrastructure Due to cost-efficiency and less hands-on management, data owners are outsourcing their data to the cloud which can provide access to the data as a service. However, by outsourcing their data to the cloud, the data owners lose control over their data as the cloud provider becomes a third party. At first, encrypting the data by the owner and then exporting it to the cloud seems to be a good approach.In this paper we have discussed about cloud computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of various security algorithms. In this paper, we discuss a number of existing techniques used to provide security in the field of cloud computing on the basis of different parameters.**

Keywords–Cloud computing; data confidentiality

I. INTRODUCTION

"Cloud computing is a model enabling ubiquitous, ,convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." In Cloud Computing the term Cloud is used for the service provider, which holds all types of resources for storage, computing etc. Mainly three types of services are provided by the cloud. First is Infrastructure as a Service (IaaS), which provides cloud users the infrastructure for various purposes like the storage system and computation resources. Second is Platform as a Service (PaaS), which provides the platform to the clients so that they can make their applications on this platform. Third is Software as a Service (SaaS), which provides the software to the users; so users don't need to install the software on their own machines and they can use the software directly from the cloud. Due to the wide range of facilities provided by the cloud computing, the Cloud Computing is becoming the need of the IT industries. The services of the Cloud are provided through the Internet. The devices that want to access the services of the Cloud should have the Internet accessing capability. Devices need to have very less memory, a very light operating system and browser. Cloud Computing provides many benefits: it results in cost savings because there is no need of initial installation of much resource; it provides scalability and flexibility, the users can increase or decrease the number of services as per requirement; maintenance cost is very less because all the resources are managed by the Cloud providers.

Fig.1 Evolution of Calculation Mode

Cloud computing is a product from mixing traditional computer techniques and network technologies, such as grid computing, distributed computing, parallel computing, utility computing, network storage, virtualization, load balancing, etc[1].

Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment.

ISSN: 2278 – 1323

II. SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING

The security requirements in service oriented cloud computing model are as follows:

A. Data security

The provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. [3]

B. Privacy

The providers should ensure that all critical data are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

C. Data confidentiality

The cloud users want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. [4]

D. Fine-grained access control

The provider should facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. [7]

The effective implementation for the above mentioned security issues would be encrypting data by using certain encryption techniques, which allows flexibility in specifying differential access rights of individual users in a feasible way.

III. SECURITY ALGORITHM USED IN CLOUD COMPUTING

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption. Some of the symmetric & asymmetric algorithms are followings : [6].

RSA ALGORITHM

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone. How RSA is going to work in cloud environment is explained as: RSA algorithm is used to ensure the security of data in cloud computing. In RSA algorithm we have encrypted our data to provide security. The purpose of securing data is that only concerned and authorized users can access it. After encryption data is stored in the cloud. So that when it is required then a request can be placed to cloud provider. Cloud provider authenticates the user and delivers the data to user. As RSA is a Block Cipher in which every message is mapped to an integer. In the proposed cloud environment, Public key is known to all, whereas Private Key known only to user who originally owns the data. Thus encryption is done by the cloud service provider and decryption is done by the cloud user or consumer. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only.

Algorithm

Key Generation: KeyGen(p, q)

Input:

Two large primes – p, q

Compute $n = p \cdot q$

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

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

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

Key:

public key = (e, n)

secret key= (d, n)

Encryption:

$c = m^E \bmod n$

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 multi-plying the cipher texts. The result of the operation will be the cipher text of the product.

Given $c_i = E(m_i) = m_i^e \bmod n$, then

$(c1 \cdot c2) \bmod n = (m1 \cdot m2)^e \bmod n$ [8].

DES ALGORITHM

The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm.

Algorithm:

function DES_Encrypt (M, K) where M = (L, R)

M ← IP(M)

ISSN: 2278 – 1323

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

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. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications [9][10].

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds
5. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows
12. Add Round Key

MD5

(Message-Digest algorithm 5), a widely used cryptographic hash function with a 128 bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks . the message is padded so that its length is divisible by 512. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

DSA

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standards for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [10]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break .With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [10]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [11].

IV. CONCLUSION AND FUTURE PROSPECTS

In this paper encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES, and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers. In the future, we will extend our research by providing implementations and producingresults to justify our concepts of security for cloud computing.

REFERENCES

[1] Mohammad Hamdaqa and Ladan Tahvildari , "Cloud Computing Uncovered: A Research Landscape". Elsevier Press. pp. 41–85. ISBN 0-12-396535-7.
[2] Huang Q.Y., Huang T.L.,"An Optimistic Job Scheduling Strat egy based on QoS for Cloud Comput ing", IEEE Int ernat ional Conference on Intelligent Comput ing and Integrated Systems (ICISS), 2010, Guilin, pp. 673-675, 2010
[3] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International
[4] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009

ISSN: 2278 – 1323

[5] Ronald L. Krutz, Russell Dean Vines "Cloud SecurityA Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010

[6] Otero, A. R., Otero, C. E., Qureshi, A.(2010). Securing data transfer in the cloud through introducing identification packet and UDT – authentication option field: a characterization. International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

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

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

[9] 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.

[10] 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.

[11] 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).

ISSN: 2278 – 1323