International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 10, Oct.-2014, pp: (113-117), Impact Factor: 1.252, Available online at: www.erpublications.com

Cloud Security and Algorithms: A Review

Divya saraswat[1], Dr. Pooja Tripathi[2]
[1] M.Tech Dept. of Computer Science, IPEC, Ghaziabad, U.P.
[2] Professor, Dept. of Computer science, IPEC, Ghaziabad, U.P.

Abstract: cloud computing is becoming an increasing enterprise model. It is an internet based computing includes the practice of using remote servers. The remote servers are hosted on internet to store, manage and process data rather than a local server or computer. Cloud computing offers the services that includes software, storage, data, applications, infrastructure and business process to the IT market place. These are the services that are provided to customers on leased basis. Despite all the potential gains in cloud computing there are some security issues and challenges. As applications move dynamically and organizations share the same remotely located physical hardware with strangers security is the basic concern. This paper introduces a detailed analysis of cloud computing security issues, challenges, algorithm for security.

Keywords: cloud computing, cloud services, scalability, SAAS, PAAS, deployment models, RSA, AES, Diffie-Hellman.

Introduction

Cloud computing is a latest extension in distributed computing. According to NIST[1] cloud computing is defined as: cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(e.g. network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to Garter [2] cloud computing is the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. Cloud computing provides collaboration, agility, scalability, availability, ability to change according to demand increase development work and provide potential for cost reduction. Cloud computing includes various computing concepts and technologies such as Web 2.0, service oriented architecture (SOA) and other technologies. These technologies provide online business applications with the help of web browsers for computing needs of users.

Although cloud computing offers various benefits to their users, it also has various security issues. In traditional data centers there are some procedures and controls on the server locations and organizations can utilize the resources. In cloud computing procedures and control reduces as the applications move dynamically and organizations share the same remotely located resources with strangers. According to the survey of IDC enterprise panel [3] in august 2008, security is the major challenge. According to IDC 75% of surveyed users are worried about the attacks on their critical business and IT systems. Cloud providers usually have direct access to stored data and they steal that data to gain profit which results in many security and privacy attacks occurs within cloud providers [4].security concerns are basically for risk areas such as external data storage, lack of control, multi-tenancy. So there is a strong need to secure the data. The rest of paper is organized as follows: Section 2. describes the related work, section 3. describes the computing service models, section 4. describes deployment models of cloud, section 5. describes some security issues, section 6. describes the security algorithm and finally we derive some conclusion.

Related work

There are many reviews on security and privacy in cloud. Popovi and Hocenski [5] discussed security issues which explain the problems encountered during implementation in cloud and also discuss challenges that CSP need to address. Maggi and Zanero [6] developed countermeasures which includes antivirus, intrusion detection system to mitigate well known security threats. Subhashini and Kavitha [7] outlines security risk faced in cloud computing. They give empirical evidence on security risk and issues encounter during deployment of service models. Md. Tanzim Khorshed et al [8] discussed that cloud computing helps to reduce cost of services and improve business outcomes. They also explore the security attacks and perform a survey to find out gaps and security concerns. Zhou [3] carried out study on privacy and security, work that

can be done to prevent privacy and security breaches and outlines that security laws should also be taken into consideration. Kresimir [9] explains high level security concerns such as data integrity.

Service models

Cloud services are delivered through three main service models. They are software as a service, infrastructure as a service and platform as a service. Figure 1 shows the main security concerns in these models and their examples.

a. Software as a service: The first and highest layer is known as SAAS. These are the services that are provided to users to use the software resources or applications running on cloud infrastructure. E.g. web based e-mail.
b. Platform as a service: The next layer is called PAAS. With the help of PAAS users can deploy their own applications without installing any platform or tools on their local machines. Services that can be done on PAAS are testing, collaborating, hosting and managing applications. E.g. amazon web services.
c. Infrastructure as a service: The final and lowest layer is IAAS. It provides users to provision processing, storage, network and other fundamental computing resources. E.g. amazon elastic compute cloud and eucalyptus.

Cloud deployment models

There are three deployment models for cloud. They are:

a. Public clouds: Also known as external clouds. This is an openly accessible model. In this type of cloud various enterprises can be used to deliver the services to users.
b. Private clouds: Also known as internal clouds. These types of clouds are privately owned by an organization to provide high level control over cloud services.
c. Hybrid clouds: Also known as virtual private cloud models. These clouds are combination of both public and private cloud.

Security issues

The classifications of security issues found within the cloud are:

a. Privacy and confidentiality: once data is stored in cloud it should be secure. Inappropriate or unauthorized access to the sensitive data is a risk that is posing on cloud.
b. Data integrity: Any modification on sensitive data by malicious users posing another risk on data security in cloud computing.
c. Data loss or leakage: Insecure API's lead to unwanted exposure of information.

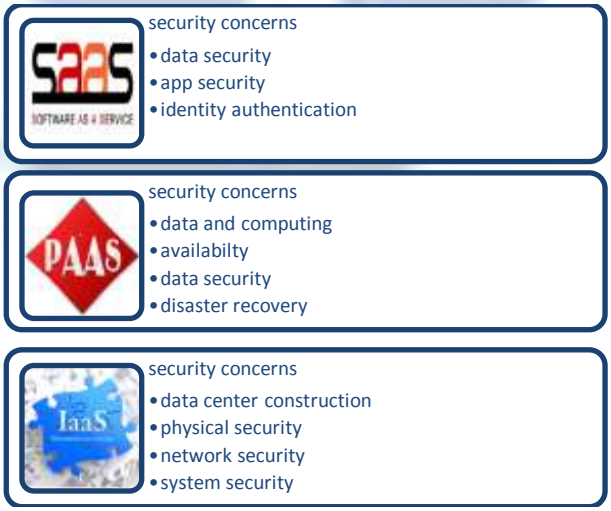

Figure 1.security concerns on cloud delivery models.

d. Data availability: Availability arises when user data becomes unavailable to users. Data are stored in different locations and servers. At this point data availability is a major issue as availability of uninterruptable and seamless provision becomes difficult.

e. Insecure interfaces: With the help of APIs we can access data that are placed in cloud. Malfunction and error in the software or the interface used to run in cloud, can lead to unwanted exposure of data.

Algorithms for security

There are various algorithms for the purpose of data security. They are symmetric key algorithms, asymmetric key algorithms, and combination key algorithm. Encryption using the cryptographic algorithms over data makes it more secure. Some of them are:

a. AES: Advance encryption scheme is a specification used for encrypting data. AES is developed by John Daemen and Vincent Rijmen. The algorithm is established by NIST in 2001. AES is based on symmetric encryption. Each of the ciphers has 128 bit block size and having key sizes of 128,192,256 bits respectively. Flowchart for AES algorithm is shown in figure 2.
b. RSA: Developed by Ron, Rivest, Shamir in 1977. RSA is a public key cryptography algorithm which involves a public key and a private key [10]. Public is the one which is known to everyone and is used for encryption of the data. For decrypting the data private key is used. RSA is used for secure data transmission. Algorithm for RSA is given in figure 3.
c. DES: DES stands for data encryption scheme. It operates on plaintext of fixed length string and after some operations returns the cipher text of same size. Mostly the block size is of 64 bits. The effective key length of DES is 56 bits.
d. MD5: MD5 is widely used cryptographic hash function. The hash value of 128 bit processes a variable length message into fixed length message of 128 bits. The input message is divided into blocks of 512 bits. The message is also padded so that its length is divisible by 512.public key of the receiver is used for encryption and private key of receiver is used for decryption.

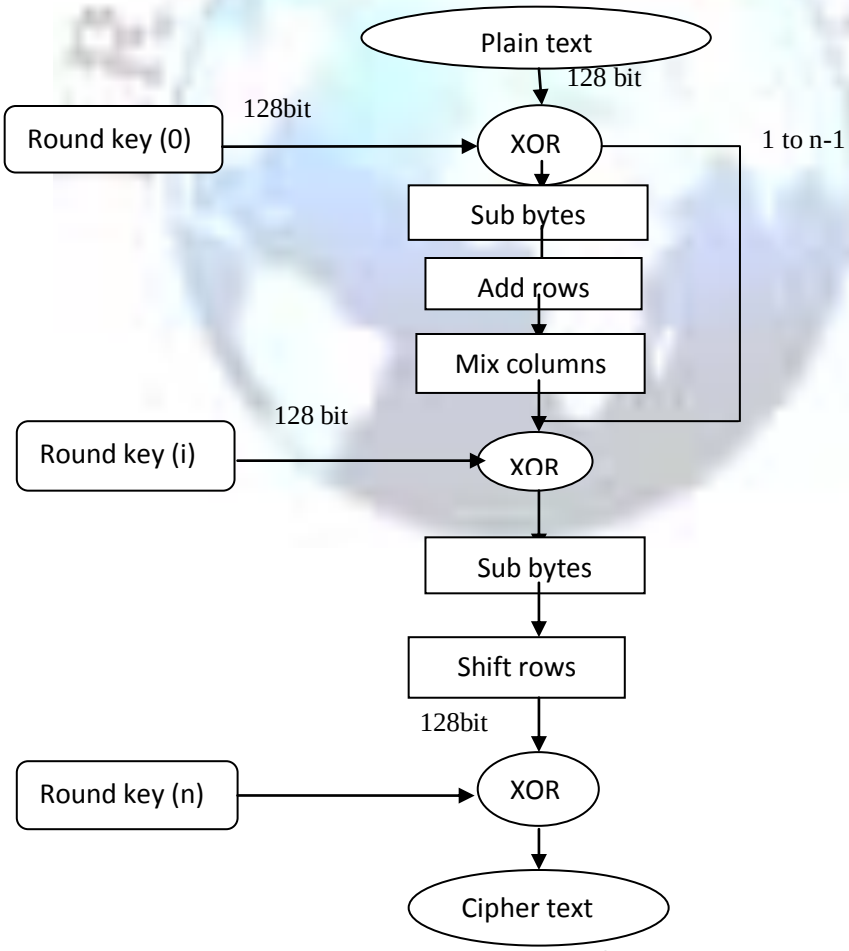

Figure 2: AES algorithm flowchart

e. Diffie-Hellman: The method was firstly developed by Whitefield Diffie and Martin Hellman in 1976. This algorithm is mostly used for key exchange between communicating parties. The two communicating parties agree upon same secret shared key that is used for encryption. Key exchange using Diffie- Hellman is shown in figure 4.

f. Homomorphic encryption: cloud service providers send their data to cloud after encryption. For the doing some calculations over data it is necessary to decrypt that data. For decryption, key is required. This might influence the confidentiality of data. Homomorphic encryption is a technique in which operations can be performed on the encrypted data without knowing the private (or decryption). The result of any operation after decryption is same as operation on plaintext. According to operations on data homomorphic encryption is categorized as additive homomorphic encryption and multiplicative homomorphic encryption [11].

a. Select two prime numbers randomly for security purpose of same bit length, a and b.
b. Compute n=p*q
c. F(n) = (p-1)*(q-1), where f(n) is Euler's totient function.
d. Choose an integer e, such that 1<e<f(n) and GCD (e,f(n))=1.e is now a public key.
e. Now, calculate d=e^{-1}mod f(n)
f. Now, d is private key d*e=1mod f(n)
g. Public key is (e,n)
h. Private key is (d,n)
i. Encryption:
$C=m^e \bmod n$
j. Decryption:
$M=c^e \bmod n$

Figure 3. RSA algorithm

g. Blowfish algorithm: It is a symmetric block cipher algorithm. It is used for the methods where the keys not change frequently. The block size for blowfish is 64 bits. When executed in 32 bit microprocessor with huge data caches this algorithm is consider most appropriate. Data encryption goes through 16 rounds of fiestal network [12].

Parameter selection	
Two parties A and B, agrees on two prime no. p and g.	
Computation	
Party 1	Party 2
Choose a secret integer a and compute: $A=g^a \bmod q$	Choose a secret integer b and compute: $B=g^b \bmod p$
Exchanging public numbers	
Party 1 sends A to party 2 Party 2 sends B to party 1	

Further computations	
Party 1	Party 2
Compute: $B^a \bmod p$	Compute: $A^b \bmod p$
The shared secret value is $B^a = (g^b)^a = g^{ba} = (g^a)^b = g^{ab}$	

Figure 4. Diffie-hellman key exchange

Conclusion

Cloud computing is an emerging trend in today's IT world. Many organizations moving towards the cloud but due to security reasons and issues it lacks. There are lots of security algorithms which can be implemented to cloud. These are symmetric and asymmetric algorithms including DES, AES, RSA, blowfish, MD5, Homomorphic, Diffie-Hellmen. Apart from all these algorithms there are many algorithms that can be developed by making some efficient enhancements to increase security levels. In future we will implement Diffie-Hellman algorithm by making some enhancements.

References

[1]. http://www.nist.gov//itl/cloud/
[2]. Gartnet Inc Gartner identifies the top 10 strategies technologies 2011. Online available: http://www.gartner.com/it/page.jsp?id=1454221.accessed: 15 july 2011.
[3]. Zhou M, Zhang R, Xiew, Qian W, Zhou A (2010)," Security and privacy in cloud computing: a survey" sixth international conferences on emantics knowledge and grid (SKG) 2010:105-112.
[4]. Rocha F, Abreu S, Correia M (2011), "The final frontier- confidentiality and privacy in cloud", pp 44-50.
[5]. Kresimir Popovic and Zeljko Hocenski,"Cloud computing security issues and challenges" in MIpro, 2010 proceedings of 33rd international convention, pages 344-349, 2010.
[6]. F.Maggi and S.Zanero,"Rethinking security in cloud world,"technical report, departimento di electtronica e informazion, polytecnico di Milano 2010 .
[7]. S.Subhashini and V.Kavitha, "A survey on security issues in service delivery models of cloud computing", journal of network and computer applications, 34(1):1-11, January 2011.
[8]. Md Tanzim Khorshed, A.B.M.Ali, and Saleh A.Wasimi, " A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", future generation computer systems,2012.
[9]. R.K Balachandra, P.V.Rakshit, "Cloud security issues", in PROC '09 IEEE international conference on services computing,2009,pp 517-520.
[10]. N.Padmaja and Priyanka Koduru," Providing data security in cloud computing using public key cryptography", international journal of engineering sciences and research, vol 04 issue 01-2013, ISSN:2230-8504;e-ISSN-2230-8512.
[11]. Maha Tebaa, Said El Hajji, Abdellatif El Ghazi, " Homomorphic encryption applied to cloud security", World congress on engineering Volume 1, july 4-6-2012, London, U.K, ISBN:978-988-19251-3-8, IISDN:2078-0958(print); ISSN:2078-0966.
[12]. G.Devi, M.Pramod kumar, "Cloud computing: a CRM service based on a separate encryption and decryption using blowfish algorithm", international journal of computer trends and technology, volume 3 issue 4,ISSN:2231-2803,2012,pp.592-596.