ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5, May 2014, Page No. 5764-5768

Cloud Computing and Security Issues

Mrs.R.Pushpalatha,
Assistant Professor,
Department of Computer Science(UG)
Kongu Arts And Science College,Erode.Tamil Nadu.
rpljour@gmail.com

Abstract: The cloud computing model for delivering computing services offers cheap access to a variety of standardized services from various providers. But after outsourcing a service to the cloud, the owner no longer controls the platform on which the service runs. The user is bound to trust the cloud provider for correctness, privacy, and integrity of its data and computations. Cryptographic mechanisms can reduce such trust by allowing the user to protect its data and computations, as well as to verify aspects of remote computation. Benefits of cloud storage are easy access, it means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. Each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the calculations and storage databases hosted by the Cloud provider. This paper describes different security issues to the cloud , different cryptographic algorithms adoptable to better security for the cloud.

Keywords: Cloud Computing Concepts, Security Algorithms, Security Issues.

1. Introduction

The definition of the Cloud computing is the set of resources or services offered through the internet to the users on their demand by cloud providers. Based on user demand , It conveys everything as a service over the internet, for instance operating system, network hardware, storage, resources, and software. Each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So ,there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments or calculations and storage ie databases hosted by the Cloud provider.. Security goals of data includes three main points namely:

- *Availability*
- *Confidentiality*
- *Integrity.*

Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are

- *Symmetric-key algorithms*
- *Asymmetric-key algorithms*
- *Hashing.*

Integrity of data is handled by hashing algorithms. Data cryptography means, it is the scrambling of the content of the data. It may be text, image, audio, video and so forth to make the data in the form of unreadable, invisible or meaningless, during transmission or storage it is termed Encryption. The aim of the cryptography is to take care of data secure from invaders. The opposite process, ie getting back the original data from encrypted data is called Decryption, which restores the original data. To encrypt data at cloud storage, use both symmetric-key and asymmetric-key algorithms. Cloud storage contains a large set of databases . Here asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

2. Security Issues to the Cloud

The data centre are similar for security requirements of a cloud and non-cloud. The Cloud Security initial report contains a different sort of taxonomy based on different security domains and processes that are followed in general cloud deployment. Some privacy and security-related issues that have long-term significance for cloud computing are:

- **Governance**
  Governance implies that the management and oversight by the organization over procedures, standards and policies for application development and data technology service acquirement, because the style, implementation, testing, use, and watching of engaged services.
- **Compliance**

Compliance refers to an association's responsibility to work in agreement with established laws, specifications and standards. Common compliance problems facing a company is an information location means storage of data or information

- **Malicious Insiders**
  'Malicious Insiders' impact on the organization is considerable. Malicious insiders are the threat which has access the data or information about the organization being a member of the organization. As cloud consumers application data is stored on cloud storage provided by cloud provider which also has the access to that data.
- **Account or service Hijacking**
  This threat occurs due to phishing, fraud and software vulnerabilities. In this type , attacker can get access to critical areas onto the cloud from where he can take permit and steeling important information leading to compromise of the availability, integrity, and also confidentiality to the services.
- **Hypervisor vulnerabilities**
  The Hypervisor is the main software component of Virtualization. There known security vulnerabilities for hypervisors and solutions are still limited.[2].
- **Insecure APIs**
- Anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities etc security threats may occur to organizations if the weak set of interfaces and APIs are used.

2.1. Security issues associated with the cloud

There are number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS) via the cloud) and security issues faced by their customers[3] .In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information[4].

2.2. Security issues faced by cloud providers

- **Infrastructure as a Service (IaaS)** Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.
  Characteristics and components of IaaS include:
  Utility computing service and billing model.
  Automation of administrative tasks.
  Dynamic scaling.
  Desktop virtualization.
  Policy-based services.
  Internet connectivity.

- **Platform as a Service (PaaS)** Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

- **Software as a Service (SaaS)**
  Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution.

  Benefits of the SaaS model include: easier administration automatic updates and patch management compatibility: All users will have the same version of software easier collaboration, for the same reason global accessibility. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service[5]. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured[6]. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist[7].

Dimensions of cloud security

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices[8]. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven[9] while the Cloud Security Alliance identifies fourteen areas of concern[10]) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues[11].

3. Cryptography

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host [12], and cryptography can resolve these issues to some extents. Encryption- converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text .

Consider an example, In the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data. This will helps us in reduction of Virtualization vulnerability. For secure communication between the host domain and the guest domain, or from hosts to management systems, encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking [13].

Security Algorithms

1.Symmetric-key algorithms

The most important type of the encryption is the symmetric key encryption. Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [14]. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of a symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit at a time is encrypted. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, at the decryption site, it takes a 64-bit ciphertext and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

Advanced Encryption Standard (AES)

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. AES is a non-Feistel cipher. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively [15]. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

Its algorithm is as follows:

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

Triple-DES

A quite simple way of increasing, the key size of DES is to use Triple DES, to guard it against attacks without the need to design a completely new block cipher algorithm. DES itself can be adapted and reused in a more secure scheme. Many former DES users can use Triple DES (TDES) which was described and analyzed by one of DES's patentees. It involves applying DES three times with two (2TDES) or three (3TDES)

different keys. TDES is quite slow but regarded as adequately secure.

Blowfish Algorithm

Blowfish is a symmetric block cipher algorithm. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches. Data encryption happens via a 16-round Feistel network [16] .

2.Asymmetric-key algorithms

Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA(Rivest-Shamir-Adleman), Diffie-Hellman Key Exchange.

Homomorphic Encryption

Cloud consumer encrypts its data before sending to the Cloud provider, But, each time he has to work on that will have to decrypt that data. The consumer will require giving the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud. Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption (without knowing the private key); only the consumer will have the secret key. When we decrypt the result of any operation, it is the same as if we had performed the calculation on the plaintext (or original data). The Homomorphic encryption is distinguishing, according to the operations that are performed on raw data [17].

- Additive Homomorphic encryption: additions of the raw data.
- Multiplicative Homomorphic encryption: products for raw data.

RSA

It is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.

Diffie-Hellman Key Exchange

In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel. To set up a key Alice chooses a random integer a [1; n] computes ga, similarly Bob computes gb for random b [1; n] and sends it to Alice. The secret key is gab, which Alice computes by computing (gb)a and Bob by computing (ga)b. The important concepts on which the security of the Diffie-Hellman key exchange protocol depends are [18]:

- Discrete Logarithm Problem (DLP): If from g and ga Eve, an adversary can compute a, then he can compute gab and the scheme is broken.
- Diffie-Hellman Problem (DHP): If from given the information g, ga and gb with or without solving the discrete logarithm problem, Eve can compute gab then the protocol is broken. It is still an open problem if DHP is equivalent to DLP.
- Decision Diffie-Hellman Problem (DDH): If we are given g; ga; gb and gc, DDH is to answer the question, deterministically or probabilistically, Is ab = c mod n?

3.Hashing Algorithm

MD5

Message-Digest algorithm 5 is 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.Widely used for file integrity checking.

4. Conclusion

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement than AES. RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for asymmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data. As discussed there are many security algorithms which are currently used in a cloud computing environment. Apart from this there are still there too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the environment.

References:

[1] Priyanka Arora, Arun Singh, Himanshu Tyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012

[2] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns

and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.

[3] ―"Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[4]""Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011-21-21.

[5] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[6] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[7]Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.

[8] "4 Cloud Computing Security Policies You Must Know". CloudComputingSec. 2011. Retrieved 2011-12-13.

[9] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.

[10] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

[11] "Cloud Security Front and Center". Forrester Research. 2009-11-18. Retrieved 2010-01-25

[12] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.

[13] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[14] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.

[15] M. Sudha , Dr.Bandaru Rama Krishna Rao , M. Monica ―A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment,‖ in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[16] 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.

[17] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering Volume I, July 4 - 6, 2012, London, U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online).

[18] Ayan Mahalanobis "Diffie-Hellman Key Exchange Protocol,Its Generalization and Nilpotent Groups.", August 2005, 40 pages.