© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 06 Issue: 02 | May-June 2015

Enhancement of Security in Cloud Computing

Meenaxi Kumari
Computer Science Engineering
CBS Group of Institution(MDU)
Bhiwani, India
e-mail: meenaxikdn@gmail.com

Rajiv Mishra
Computer Science Engineering
CBS Group of Institution)
Jhajjar,India
email: mishrarajiv99@gmail.com

Abstract— Cloud Computing provides us means of accessing the applications as utilities over the Internet. It allows us to create, configure, and customize the applications online.

Keywords- *Cloud Server,Encryption,Deployment Model,*

*****

I. Introduction to Cloud Computing [8]

In computer networking, **cloud computing** is computing that involves a large number of computers connected through a communication network such as the Internet, similar to utility computing.

A. What is Cloud?

The term **Cloud** refers to a **Network** or **Internet.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

B. What is Cloud Computing?

Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

Fig 1.

Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.**

C. Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

II. Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

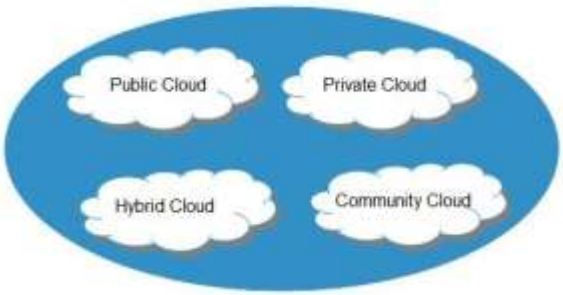

Fig 2.

a) Public Cloud

The **public cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

b) Private Cloud

The **private cloud** allows systems and services to be accessible within an organization. It is more secured because of its private nature.

c) Community Cloud

The **community cloud** allows systems and services to be accessible by a group of organizations.

d) Hybrid Cloud

The **hybrid cloud** is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

2) Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Anything-as-a-Service (XaaS) is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

The **Infrastructure-as-a-Service (IaaS)** is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model, as shown in the following diagram:

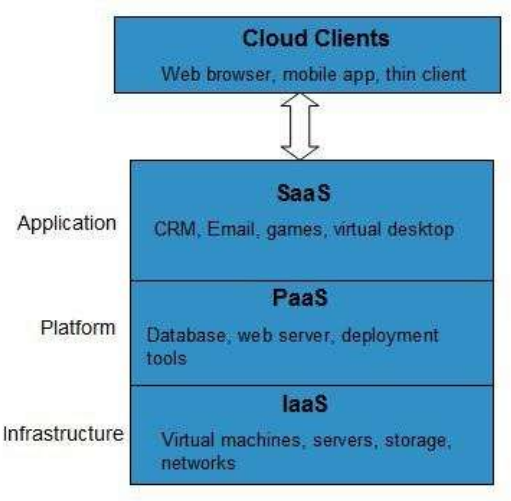

Fig 3.

a) Infrastructure-as-a-Service (IaaS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

b) Platform-as-a-Service (PaaS)

PaaS provides the runtime environment for applications, development and deployment tools, etc.

c) Software-as-a-Service (SaaS)

SaaS model allows to use software applications as a service to end-users.

III Security in the Cloud [9]

Security in the world of information technology has become a popular topic within the industry and within the media. It is not uncommon to read about successful hacker exploits against consumers, business or government. As witnessed by the July, 2012 Dropbox security breach (Strauss, 2012) or the 6 million passwords that were stolen from eHarmony and LinkedIn, risks associated with Cloud computing are not necessarily reduced.

Virtual switches and the hypervisor are two examples of points of attack that are not present in the traditional data center. The attack surface can be defined as our exposure.
Exposures are the vulnerabilities that are exploitable by the attacker (Northcutt, 2012).
Consequently, an increased attack surface may increase security risks of Cloud security [7] providers if the risks are not properly managed.

Risks can be decreased for small and medium sized business because there may be a lack of staff with specialization in information security whereas Cloud Service Providers (CSP) will have specialized staff that focus on information security. Because of economies of scale, it is cheaper to utilize a CSP than to design a high availability data center.

IV Existing security Mechanism

Much of the theoretical work in cryptography[4] concerns cryptographic *primitives*—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called *cryptosystems* or *cryptographic protocols*, which guarantee one or more high-level security properties.

Note however, that the distinction between cryptographic *primitives* and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

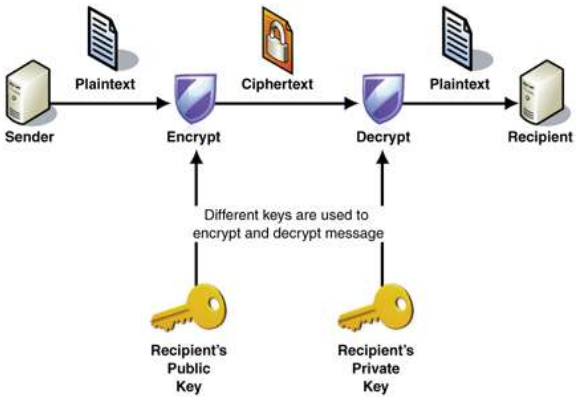

Fig 4.

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or *cryptosystem*.

Cryptosystems are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties. Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties.

Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems.

Key generation

When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys.

However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past.

Therefore, it is essential that an implementation uses a source of high entropy for its initialization.

Basic algorithm and terminology

RSA encryption and decryption are essentially mathematical operations. They are what are termed *exponentiation*, *modulo* a particular number.

Because of this, RSA keys actually consist of numbers involved in this calculation, as follows:

- the public key consists of the modulus and a public exponent;
- the private key consists of that same modulus plus a private exponent.

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$
Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig 5.

V Challenges

- Intruders: those who capture the packet and alter the information
- Users with limited privileges should not be able to access unauthorized information
- Crypto analyst: those who decrypt cipher text into plain text without key

VI Objective and Methodology

There are multiple enhancements in security mechanism.

1. The presence of intruder should be detected to prevent an unauthorized access of information by adding some delimiter at the end of encrypted text and same delimiter should be used during decryption.
2. Some time information to be sent are multiple and merged using delimiter into plain text then at the time of decryption plain text is split again in multiple pieces of information.
3. Allow authentic access to the information on the basis of privilege levels of user.
4. To protect information from cryptanalyst IP Filter would be attached in decryption module

VII Future scope and Conclusion

Business and government will continue to move a Cloud environment in an effort to reduce costs, improve efficiencies and reduce administrative overhead. Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This new paradigm of computing offers many benefits but it also increases security risks.

The delivery of computing resources in a Cloud environment is elastic, available on demand and convenient for the customer. While not mandatory, virtualization of the data center is important to achieve economies of scale that enable services to

be provided at a lower cost than a traditional data center. While virtualization reduces some security risks, others are increased because the attack surface in a Cloud service increases.

Traditional security methods are still relevant in the Cloud but are implemented in a virtual means. In a virtualized Cloud environment customers are segregated into separate security zones called multi-tenancy. Virtual NICs, virtual switches and port groups add complexity but allow a multi-tenant environment.

Reference

[1] Amazon. (2011). Amazon Web Services: Overview of Security Processes. Retrieved from http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

[2]Arora, P., Biyani, R. and Dave, S. (2011). To the cloud:Cloud powering an enterprise. McGraw-Hill. Buck, K. and Hanf, D. (2009).

[3]Mitre cloud computing series, Cloud SLA considerations for the government consumer. Retrieved from http://www.mitre.org/work/tech_papers/2010/10_2902/cloud_sla_considerations_government.pdf

[4] Introduction to Cryptography http://en.wikipedia.org/wiki/Cryptography

[5]Traditional Cloud server security http://cloudsecuritythreats.blogspot.in/2011/11/traditional-security.html

[6] Fundamentals of Cryptography: Algorithm and Security Services by Professor Guevara Noubir

http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06/cryptography.pdf

[7] Logik Bomb: Hacker's Encyclopedia (1997)

[8] Hafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster. ISBN 0-671-68322-5.

[9] Sterling, Bruce (1992). *The Hacker Crackdown*. Bantam. ISBN 0-553-08058-X.

[10] Slatalla, Michelle; Joshua Quittner (1995). *Masters of Deception: The Gang That Ruled Cyberspace*. HarperCollins. ISBN 0-06-017030-1.

[11] Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.

[12] Verton, Dan (2002). *The Hacker Diaries : Confessions of Teenage Hackers*. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.

[13] Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.

[14] Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge. ISBN 978-0-415-18072-6.

[15] Levy, Steven (2002). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.

[16] Ventre, Daniel (2009). *Information Warfare*. Wiley - ISTE. ISBN 978-1-84821-094-3.