© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 09 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Security enhancement in Cloud Computing

Pooja Bansal

Email id poojasinghal273@gmail.com

Abstract— Cloud computing makes it possible to use Internet-based apps as utilities. It gives us the ability to design, configure, and personalise our apps in real time through the internet. Using cloud computing, customers may store and execute programmes on a virtual computer infrastructure. Because cloud service providers may access and modify client data without their knowledge or consent, there are additional security risks associated with using the service. We're working to balance security, efficiency, and usability while developing cryptographic primitives and protocols for the cloud. Using cryptography, data may be encoded such that only the intended recipients can access it and process it.

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

I.

I. “Cloud Computing: An Overview [8]

Cloud computing is a kind of utility computing in computer networking, in which a large number of computers are linked together over a communication network, such the Internet.

A. What is a Cloud?

Internet or Network is what the word Cloud alludes to. Another way of putting it is that anything in the Cloud is present at a distant place. WAN, LAN, and VPN are all methods through which the cloud may provide services across both public and private networks. It is possible to run applications such as email and CRM on a cloud-based platform.

B. What is Cloud Computing, exactly?

Software and physical resources may be configured and accessed remotely in Cloud Computing. Online data storage, infrastructure and application are all provided by this service.

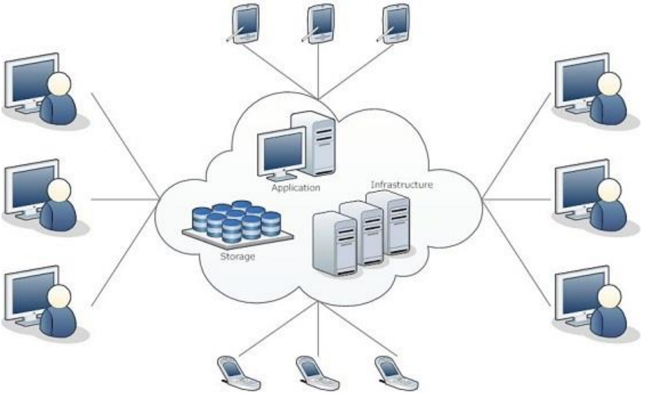

Fig 1.

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.**

A. *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.

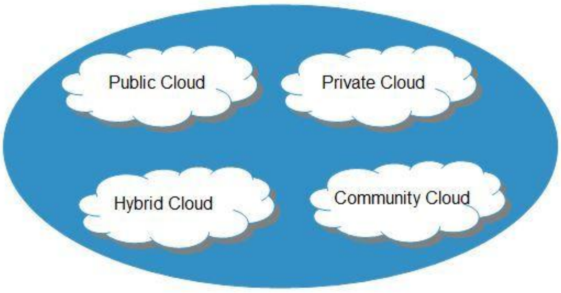

Fig 2.

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:

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.

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.

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 **Cryptography***

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other?s identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

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

In an attempt to save money, time, and resources, businesses and the government will continue to shift to a cloud-based environment. Using the Cloud to provide IT services is expected to save time, money, and increase efficiency. The advantages of this new computing paradigm are many, but so are the security threats.

Elastic, on-demand, and user-friendly, the Cloud makes computer resources readily accessible to users. In order to deliver services at a cheaper cost than in a typical data centre, data centre virtualization is crucial, but it is not required. Because the attack surface of a Cloud service expands, virtualization eliminates certain security threats
Even on the Cloud, traditional security measures are still necessary, even if they are done virtually. Security zones are created for each client in a virtualized Cloud architecture termed multi-tenancy. Multi-tenant environments are made possible via virtual NICs, virtual switches, and port groups.

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.