` **Cosmos** An International Journal of Management
A Refereed Research Journal
Vol 4 / No2 / Jan-Jun 2015 ISSN: 2278-1218

A QUICK REVIEW ON CLOUD COMPUTING AND RELATED SECURITY ISSUES

*Dr. Ramesh Maguri

Abstract

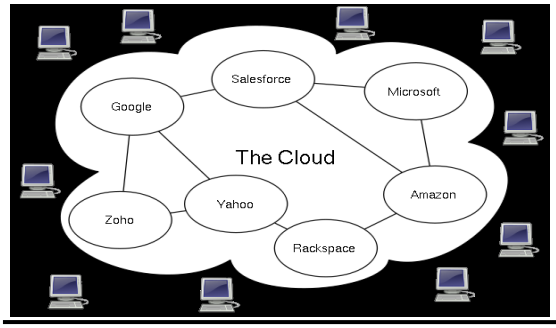
Cloud computing refers to provision of computational resources on demand via a computer network. The word "cloud computing" originated from the cloud symbol that is usually used by flow charts and diagrams to symbolize the internet. The principle behind the cloud is that any computer connected to the internet is connected to the same pool of computing power, applications, and files. In this review paper we discusse on cloud computing it,s Key Characteristics and related security issues.

I. Introduction

Cloud computing refers to provision of computational resources on demand via a computer network. In the traditional model of computing, both data and software are fully contained on the user's computer; in cloud computing, the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal for processes occurring on a network of computers far away. Common shorthand for a provider's cloud computing service (or even an aggregation of all existing cloud services) is "The Cloud".

The most common analogy to explain cloud computing is that of public utilities such as electricity, gas, and water. Just as centralized and standardized utilities free individuals from the vagaries of generating their own electricity or pumping their own water, cloud computing frees the user from having to deal with the physical, hardware aspects of a computer or the more mundane software maintenance tasks of possessing a physical computer in their home or office. Instead they use a share of a vast network of computers, reaping economies of scale.

The word ―cloud computing‖ originated from the cloud symbol that is usually used by flow charts and diagrams to symbolize the internet. The principle behind the cloud is that any computer connected to the internet is connected to the same pool of computing power, applications, and files. Users can store and access their own personal files such as music, pictures, videos, and bookmarks or play games or use



Productivity applications on a remote server rather than physically carrying around a storage medium such as a DVD or thumb drive. Almost all users of the internet may be using a form of cloud computing though few realize it. Those who use web-based email such as Gmail or Hotmail instead of receiving mail on their computer with Outlook or Entourage are the most common examples of such users

II. Key Characteristics

- **Agility** improves with users' ability to rapidly and inexpensively re-provision technological infrastructure resources
- **Application Programming Interface (API)** accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.
- **Cost** is claimed to be greatly reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This ostensibly lowers barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house)
- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- **Multi-tenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
  - o **Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  - o **Peak-load capacity** increases (users need not engineer for highest possible

*Lecturer, Department of Computer Science, JSS STC College Banhatti, Karnatak

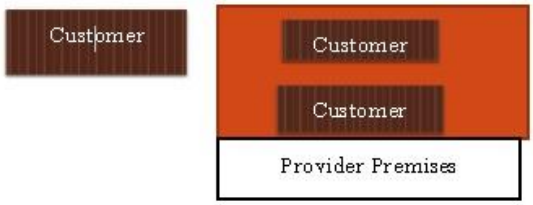
`

load-levels)

o **Utilization and efficiency** improvements for systems that are often only 10–20% utilized.

- **Reliability** is improved if multiple redundant sites are used, which makes well designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.
- **Performance** is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Security** could improve due to centralization of data increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than under traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems which are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
- **Maintenance of cloud computing applications** is easier, because they do not need to be installed on each user's computer. They are easier to support and to improve, as the changes reach the clients instantly.

III. Security Issues



- Security concerns arising because both customer data and program are residing in Provider Premises. Security is always a major concern in Open System Architectures

IV. Dangers and Vulnerabilities

Dangers to Security are

• Disrupts Services.
• Theft of Information.
• Loss of Privacy.
• Damage information.

Vulnerabilities are

• Hostile Program.
• Hostile people giving instructions to good programs.
• Bad guys corrupting or eavesdropping on communications

V. Security at Different Levels

We need Security at following levels:

- Server access security
- Internet access security
- Database access security
- Data privacy security
- Program access Security

At a Broad level, the major Questions are: One is How much secure is the Data? And second is How much secure is the Code?

We need to answer following Questions;-What is Data Security at Physical Layer? , What is Data Security at Network Layer? , What about investigation Support? And how much safe is data from Natural disaster

- Data can be redundantly store in multiple physical location.
- Physical location should be distributed across world.

Common Security Requirements

GOAL	DESCRIPTION
CONFIDENTIALITY	Ensuring that information is not disclosed to unauthorized persons.
INTEGRITY	Ensuring that information held in a system is a proper representation of the information intended and that it has not been modified by an unauthorized person.
AVAILABILITY	Ensuring that information processing resources are not made unavailable by malicious action.
NON-REPUDIATION	Ensuring that agreements made electronically can be proven to have been made.

A. Data centre Security

Professional Security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked. All physical and electronic access to data centers by employees should be logged and audited routinely. **Audit tools** so that users can easily determine how their

`

data is stored, protected, used, and verify policy enforcement.

B. Data Location

When user use the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in? Data should be stored and processed only in specific jurisdictions as define by user. Provider should also make a contractual commitment to obey local privacy requirements on behalf of their customers, Data-centered policies that are generated when a user provides personal or sensitive information, that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy

C. Backups of Data

Data store in database of provider should be redundantly store in multiple physical location. Data that is generated during running of program on instances is all customer data and therefore provider should not perform backups. Control of Administrator on Databases.

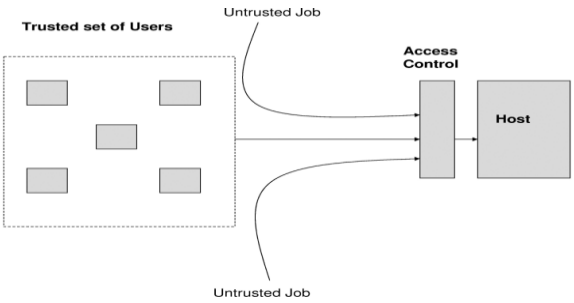
D. Data Sanitization

Sanitization is the process of removing sensitive information from a storage device.

What happens to data stored in a cloud computing environment once it has passed its user‘s ―use by date‖ What data sanitization practices does the cloud computing service provider propose to implement for redundant and retiring data storage devices as and when these devices are retired or taken out of service

E. Host Security Issues

The host running the job, the job may well be a virus or a worm which can destroy the system From malicious users



F. Information Security

Security related to the information exchanged between different hosts or between hosts and users. This issues pertaining to ***secure communication***, ***authentication***, *and issues* concerning ***single sign on*** *and* ***delegation***. Secure communication issues include those security concerns that arise during the communication between two entities. These include confidentiality and integrity issues. Confidentiality indicates that all data sent by users should be accessible to only ―legitimate‖ receivers, and integrity indicates that all data received should only be sent/modified by ―legitimate‖ senders.

Solution: public key encryption, X.509 certificates, and the Secure Sockets Layer (SSL) enables secure authentication and communication over computer networks.

G. Network Security

- Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service.
- Like DNS Hacking, Routing Table ―Poisoning‖, XDoS attacks
- QoS Violation : through congestion, delaying or dropping packets, or through resource hacking.
- Man in the Middle Attack: To overcome it always use SSL
- IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address.
- Solution: Infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning:**
- If the customer configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan.
- When Port scanning is detected it should be stopped and blocked.
- **ARP Cache Attack**: To find out the MAC address associated with a particular IP address, a computer simply sends an **ARP** request broadcast.
- An attacker sitting on the same Ethernet network (i.e., LAN), can easily sniff the network traffic of a victim on his Ethernet network by sending spoofed **ARP** messages to the victim.

VI. Security Issues from Virtualization

Type of virtualization provider is using- Para Virtualization or full system virtualization.

Instance Isolation: ensuring that Different instances running on the same physical machine are isolated from each other. Control of Administrator on Host O/s and Guest o/s. Current VMMs do not offer perfect isolation: Many bugs have been found in all popular VMMs that allow to escape from

`

VM! Virtual machine monitor should be ‗root secure', meaning that no level of privilege within the virtualized guest environment permits interference with the host system.

A. Vulnerability in Virtualization

Some vulnerabilities have been found in all virtualization software, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges. For ex.

- The vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system.(**Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege**) .A vulnerability was found in VMware's shared folders mechanism that grants users of a Guest system read and write access to any portion of the Host's file system including the system folder and other security-sensitive files. A vulnerability in Xen is caused due to an input validation error in tools/pygrub/src/GrubConf.py. This can be exploited by "root" users of a guest domain to execute arbitrary commands in domain via specially crafted entries in grub.conf when the guest system is booted.

B. How secure is encryption Scheme

Solution: A trusted set of users is defined through the distribution of digital certification, passwords, keys etc. and then access control policies are defined to allow the trusted users to access the resources of the hosts.

- Is it possible for all of my data to be fully encrypted?
- What algorithms are used?
- Who holds, maintains and issues the keys?

Problem:

- Encryption accidents can make data totally unusable.
- Encryption can complicate availability

Solution

- The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

C. How to ensure Users that both

Data and Code are safe?

Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe.

Solution:

- Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

Conclusion

This is basically a review paper in which we discussed on security issues related to cloud computing. Today it is an emerging technology. A lot research is still going on.

References

1. Sean Marstona; Zhi Lia; Subhajyoti Bandyopadhyaya; Juheng Zhanga; Anand Ghalsasib. "Cloud computing — The business perspective".. Retrieved 10 April 2011.
2. M. Armbrust; A. Fox; R. Griffith; A.D. Joseph; R.H. Katz; A. Konwinski; G. Lee; D.A. Patterson; A. Rabkin; I. Stoica and M. Zaharia. "Above the Clouds: A Berkeley View of cloud computing". University of California at Berkeley. Retrieved 10 April 2011.