A Review on Security and Privacy in Cloud Infrastructures

Ms. Leena Patel
Lecturer, Computer Engineering, Gandhinagar Institute Of Technology, Gandhinagar

Abstract –

Cloud Computing is one of the powerful technology to be established within network for the benefits and profits of the enterprises and government too.This review paper describes categories of cloud architectures (cloud service delivery models), security and privacy concerns with challenges. It seeks to contribute a better understanding of emerging in trends and issues arise along with security and privacy for cloud infrastructures.

Keywords: Cloud computing, Cloud, security, privacy, challenges,

1. Introduction:

Cloud computing is defined as a model which is based on internet that enable convenient, on demand and pay per user access to gain access to applications and data in a web-based environment on demand (Australian Government, 2010). It satisfies user's requirement for computing resources like networks, storage, servers, services and applications, without physically acquiring them. (Choubey, 2011). Cloud service delivery models are "Software as a Service" (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). (Ponemon, 2011).

1.1 The Definition of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services which can be frequently provisioned and released with less management efforts or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (NIST, 2009).A cloud is incorporated with routers, firewalls, bridges, servers, modems and all other network devices.

1.2 CATEGORIES OF CLOUD SERVICES

David C. Chau's self portrait is-

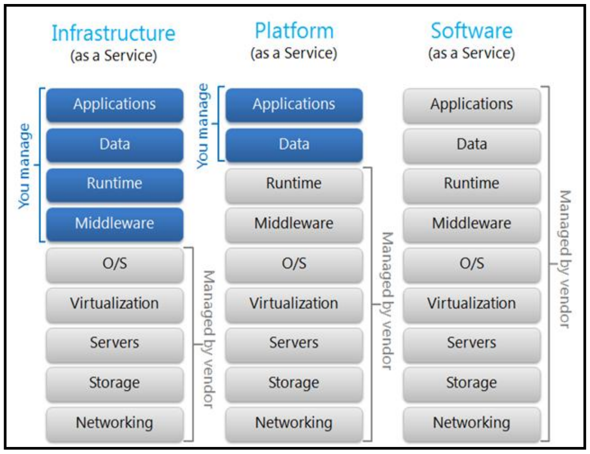

Figure.1 Cloud Service Models (C.Chau), 2010.

1. Infrastructure as a Service (IaaS) is the foundation of cloud services which provides clients with access to server hardware, storage, bandwidth and fundamental computing resources. E.g; Amazon EC2 allows individuals and businesses to rent machines preconfigured with selected operating system on which to run their own applications. (Australian Government, 2010). The capability provided to the consumer is to utilize the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as web-based email. (Mudge, 2010).

2. Platform as a Service (PaaS) builds upon IaaS and provides clients with access to the basic operating software and optional services to develop and use software applications within cloud. (Mudge, 2010).

3. Software as a Service (SaaS), builds upon the underlying IaaS and PaaS provides clients with integrated access to software applications. For example, Oracle SaaS Platform allows independent software vendors to build, deploy and manage SaaS and cloud-based applications using a licensing economic model. (Australian Government, 2010).The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. (Mudge, 2010).

1.3 TYPES OF CLOUDS

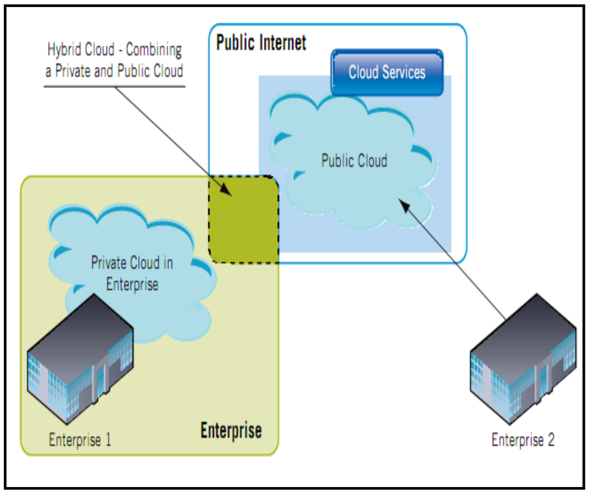
Hybrid Cloud - Combining a Private and Public Cloud
Public Internet
Cloud Services
Public Cloud
Private Cloud in Enterprise
Enterprise 1
Enterprise
Enterprise 2

Figure.2 Public, Private and Hybrid Cloud Deployment Example (Jim Machi, 2012)

1. Private cloud- The cloud infrastructure is operated for a specific organization. It may be managed by the organization or a third party and may be in house. (Jim Machi, 2012).
2. Community cloud- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns to the mission, security requirements, policy, and compliance considerations. (Mudge, 2010).
3. Public cloud- The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services. (Wyld,D C, 2010).

4. Hybrid cloud- Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network (GNI, 2009).It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. (Kuyoro S.O, 2011).

2. Security

A number of the current applications of cloud computing involve consumer services, including e-mail, and social networks. The protection of personal data and management of privacy issues may well determine the success or failure of many cloud services. (Mudge, 2010).

As an OECD (Organization for Economic Cooperation and Development) paper has noted:

Companies that wish to provide Cloud services globally must adopt leading-edge security and auditing technologies and best-in-class practices. If they fail to earn the trust of their customers by adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments will come under increasing pressure to regulate privacy in the Cloud. And if government policy is poorly designed, it could stymie the growth of the Cloud and commercial Cloud services. (Prof M R Nelson, 2010).

2.1 Securing information within a cloud computing environment requires three levels of security:

a) Network security
b) Host security
c) Application security.

Encryption for the information security is not a complete solution because data needs to be decrypted in certain situations – so that computation can occur and the usual data management functions of indexing and sorting can be carried out. Thus although data in transit and data at rest are effectively encrypted, the need to decrypt, generally by the cloud service provider, can be a security concern. Nevertheless cloud services can be augmented by email filtering (including back-up, and spam), Web content filtering, and vulnerability management, all of which improve security. (Mudge, 2010).

2.2. SECURITY ON DEMAND

The Cloud Computing systems are secured if users can depend on them (i.e. DaaS, SaaS, PaaS,IaaS, and so on) to behave as users expect. Traditionally, it contains 5 goals, say availability, confidentiality, data integrity, control and audit, to achieve adequate security. They are integrated systematically, and none of them could be forfeited to achieve the adequate security.

A. Availability

The goal of availability for Cloud Computing systems is to ensure its users can use them at any time, at any place.

B. Confidentiality

Confidentiality means keeping users' data secret in the Cloud systems. The confidentiality in Cloud systems is a big obstacle for users to step into it, as many users said "My sensitive corporate data will never be in the Cloud" in the article named "Above the Cloud".

C. Data Integrity

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, keeping data integrity is a fundamental task. (M.Armbrust,A.Fox, 2009).

3. Privacy

Email, Instant messaging, business softwares and web content management are applications of the cloud environment. Many of them have been used remotely through internet. E.g. *Microsoft* recognizes privacy policies and protections to obtain trust of customers. Even secured systems and datacenters help to protect privacy and support. (Microsoft, 2009).

3.1 Privacy Questions in Cloud Computing

□ Are hosted data and applications within the cloud protected by suitably robust privacy policies?

□ Are the cloud computing provider's technical infrastructure, applications, and processes secure?

□ Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

Security is an essential component of strong privacy safeguards in all online computing environments, but security alone is not sufficient. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. (Microsoft, 2009).

4. Legal and Regulatory Challenges

Cloud services can thrive when companies are able to provide cloud services in an efficient way and assure customers that their data will remain private and secure. (Microsoft, 2009)

4.1 Challenges

The following are some of the notable challenges associated with cloud computing, some of them lead to the delay in services and some give the opportunity to be resolved with due care and focus :

- **Security and Privacy** —these challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment. (Dialogic, 2010).
- **Lack of Standards** — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services. (Dialogic, 2010).
- **Continuously Evolving** — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving. (Dialogic, 2010).

A Review on Security and Privacy in Cloud Infrastructures

Ms. Leena Patel
Lecturer, Computer Engineering, Gandhinagar Institute Of Technology, Gandhinagar

- **Compliance Concerns** —These challenges typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization. (Dialogic, 2010).

5. Conclusion

The review concludes the aspects and dimensions for establishing security and privacy with challenges which would be leading-edge to more efficient and secured cloud services in the cloud infrastructures. By using a cloud system, your company's sensitive data and information will be stored on third-party servers. This article will be helpful to establish a future's powerful and efficient plus secured network through internet using cloud services. It will be the advanced new technology to the new era and future enhancement.

References

[1] Choubey, 2011. *A survey on cloud computing security, challenges and threats.* Bhopal, India: IJCSE.

[2] *Security of Cloud Computing Providers study*. Ponemon Institute, Researched report. Sponsered by CA Technologies.April, 2011.

[3] Kim-Kwang Raymond Choo, (2010). Cloud computing: *Challenges and future directions. Australian Government,.* Australian Institute of Criminology (Trends and Issues in crime and criminal justice). Page No.400.

[4] National Institute of Standards and Technology, December 2009, *Guidelines on security and privacy in public cloud comuting*. [online]. US, special publication 800-144, US department of commerce. Standard from Information Technology Laboratory (NIST), accessed on 14 May 2012 at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[5] Mudge, J C. (2010). CLOUD COMPUTING: Opportunities and Challenges for Australia.[online] Executive summery by *The australian academy of Technological sciences and engineering (ATSE)*. Last accessed on 15 May 2012 at http://www.egov.vic.gov.au/trends-and issues/information-and-communications technology/cloud-computing/cloud-computing-opportunities-and-challenges-for-australia-in-pdf-format-1367kb.html

[6] Wyld, D C, (2010). The cloudy future of government IT: *Cloud computing and the public sector around the world*. [online] International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010, Last accessed on 22 June 2010 at http://airccse.org/journal/ijwest/papers/0101w1.pdf

[7] Chou D C, 16th August 2010. Figure-1, self portrait. [Online image]. Last accessed at 9th May, 2012 at: http://blogs.msdn.com/b/johnalioto/archive/2010/08/16/10050822.aspx

[8] Nelson M R, (2009). Organization for Economic Cooperation and Development. Briefing paper for the ICCP Technology Foresight Forum: *Cloud computing and public policy*, Last accessed on 22 June 2010 at http://www.oecd.org/dataoecd/39/47/43933771.pdf

[9] Microsoft. (2009). Privacy in the Cloud Computing Era; *A Microsoft Perspective*, page.no.9 [online]. Lasr accessed on 16 May 2012 at http://download.microsoft.com/download/3/9/1/3912e37e-5d7a-4775-b677-b7c2baf10807/cloud_privacy_wp_102809.pdf

A Review on Security and Privacy in Cloud Infrastructures

Ms. Leena Patel
Lecturer, Computer Engineering, Gandhinagar Institute Of Technology, Gandhinagar

[10] Dialogic Corporation, (2010). White Paper: *Introduction to cloud computing*. [Online]. Last accessed on 14 May 2012 at www.dialogic.com.

[11] Machi J., 2010. Figure-2., Dialogoc Exchange Network, Corporate Blog [online image]. Last accessed on May 15, 2012 at http://blog.tmcnet.com/industry-insight/

[12] Department for Culture, Media and Sport (DCMS) and Department for Business, Innovation and Skills (DBIS), 2009, Digital Britain: Final Report, London.

[13] Kuyoro S. O., Ibikunle F. & Awodele O., 2011. Cloud Computing Security Issues and Challenges International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011,p249.

[14] Global Netoptex corporated.“Demystifying the cloud. Important opportunities, crucial choices.” pp4-14[online].Last accessed on May 15,2012 at: http://www.gni.com

*[15]*Minqi Zhou,Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, (2010). Security and Privacy in Cloud Computing [online]. In: *Sixth International Conference on Semantics, Knowledge and Grids*. Software Engineering Institute, East China Normal University, Shanghai 200062, p106. Last accessed on May 16, 2012 at {mqzhou,wxie,wnqian,ayzhou}@sei.ecnu.edu.cn, rongzhang@nict.go.jp.

[16] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson et al., “Above the clouds: A Berkeley view of cloud computing,” University of California, Berkeley,Tech. Rep, 2009.