International Journal of Computational Intelligence Techniques
ISSN: 0976-0466 & E-ISSN: 0976-0474, Volume 4, Issue 1, 2013, pp.-118-121.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000221

SECURITY RISK ASSOCIATED WITH CLOUD COMPUTING: KEY ISSUES AND A SURVEY

AL-DUBAI Y.F.*, AL-DUBAI A.F. AND KHAMITKAR S.D.

School of Computational Sciences, Swami Ramanand Teerth Marathwada University, Nanded- 431606, MS, India.
*Corresponding Author: Email- yaseraldubai@gmail.com

Received: June 14, 2013; Accepted: June 28, 2013

Abstract- These days not only large organizations, but companies even small and medium-size computing look forward to the adoption of economic resources for their application, either through the introduction of a new concept of cloud computing in their environment. Cloud computing improves the performance of organizations by using minimal resources and administrative support, with a common network, valuable resources, bandwidth, and software and hardware in an effective manner in terms of cost and service limited dealings provider. Basically it's a new concept to provide a virtual resource for consumers. Consumers can request a cloud services and applications, solutions and can store a large amount of data from a different location. But due to the constantly increasing in popularity of cloud computing there is a growing risk that security is a major issue and higher. This paper discusses some of the main security risk in cloud computing, and present the reference architectures of cloud security solutions that can be implemented to treat those attacks.

Keywords- Cloud computing, Risks, Security, Attacks

Citation: Al-Dubai Y.F., Al-Dubai A.F. and Khamitkar S.D. (2013) Security Risk Associated with Cloud Computing: Key Issues and A Survey. International Journal of Computational Intelligence Techniques, ISSN: 0976-0466 & E-ISSN: 0976-0474, Volume 4, Issue 1, pp.-118-121.

Introduction

"Cloud computing" simply means "Internet computing", and generally looked to the Internet and a collection of clouds, and thus can define the word cloud computing and take advantage of the Internet to provide Information Technology services as possible to the people and organizations. Cloud computing allows consumers to access resources on the Internet through the Internet, from anywhere at any time without having to worry about the technical management / material and resource conservation issues the original. Besides, cloud computing resources are dynamic and scalable [1][2]. Cloud computing is an independent computing it is entirely different from the network and computing services. Google Apps is the ultimate form of cloud computing, it can access to services via the browser and publish it on millions of devices over the Internet. Resources can be accessed from the cloud at any time and from any place all over the world using the internet. Cloud computing is less expensive than other computing models; and zero maintenance costs involved since the service provider is responsible for providing services and customers free of maintenance and management problems of hardware resources. Due to this property and also known as cloud computing service or that demand. "Scalability is a key attribute in the field of cloud computing and is achieved through virtualization for servers. Thus, the generation of a web of new computing uses remote servers are placed in data centers very secure and safe for the storage and management of data, so organizations do not need to pay for and take care of the internal solutions of information technology. After you create a cloud, cloud computing and publishing reference to the different requirements and for the purpose it will be used. The main service models that are being deployed as shown in [Fig-1]

- **Software as a Service (SaaS):** Software's are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server.
- **Platform as a Service (PaaS):** Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds.
- **Infrastructure as a Service (IaaS):** Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity.

There are four types of cloud computing models mentioned by NIST (2011): private cloud, public cloud, hybrid cloud and cloud community.

- **Public Cloud:** it is for the general public, where resources are provided, and web applications, and Internet services via the Internet, and any user can access services provided by the cloud,. Help public organizations in the provision of infrastructure for the implementation of the public cloud.

- **Private Cloud:** It is used internally by organizations and one organization, anyone within the organization to access data services and applications on the Internet, but users can not outside organizations access to the cloud. Evidence of a fully managed private cloud is maintained over the entire corporate data by the organization itself.
- **Hybrid Cloud:** Cloud is a combination of two or more clouds (public, private and community). Basically an environment that uses multiple suppliers internal or external cloud services. It is used by most organizations [9].
- **Community Cloud:** the cloud is basically a combination of one or more clouds public, private or mixed, which is shared by many organizations for one reason (mostly security) Infrastructured is to be shared by many organizations within a particular community with joint Security, compliance targets. Managed by a third party or managed cost internally. It is less than a public cloud, but more than a private cloud.

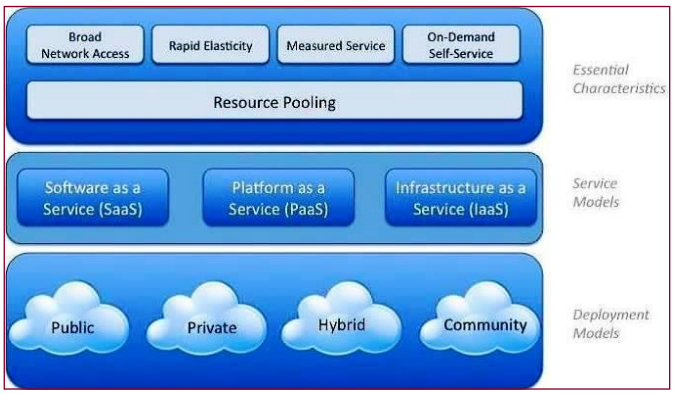

Fig. 1- NIST Visual Model of Cloud Computing

Cloud Computing Security Concern

Cloud computing concept is based on the concept of cloud computing in the remote storage of information or data outsourcing. Because the owner does not know where data is stored his/her data cannot be considered as hosts data can be completely reliable, data security is the most important concern among clients cloud [3-6].

- **Location Data:** When the owner sends data to the cloud, and he / she does not know where exactly the data is stored. Cloud keeps secret data storage location of the client. Besides that, you do not have to be stored on the same physical device. In other words, it can be distributed to several locations facility. In this scenario, the only option for the owner of the data is to trust and agree with the cloud service provider that the data stored in the cloud is safe and secured.
- **Access Policy:** There may be many users to access data in the same cloud that makes data security even more vulnerable. It all depends on cloud providers to the strength of the access control policies they impose to handle this situation.]
- **Regulatory Compliance:** Even if the cloud claims that it is safe enough from the attacks, the clients and the use of cloud services end up in the risks to which they are exposed only. Clients need to make sure that the cloud provider they are dealing with a certified or certified with a good security program. For example, in the health care sector, it is required for the cloud provider and staff development and support team, who are working on the data to take mandatory HIPPA (Health Insurance Portability and Accountability Act) test. This type of certification helps clients to make sure that their information is safe and is not lost. A few other examples of accreditation and ISO 27002 certification is a standard, safe haven, ITIL (IT Infrastructure Library Information Technology), and COBIT (control objectives for information and related technology).
- **Audit Permission:** Sometimes you may want to customers that there will be a third-party or cloud for review to ensure the protection of their own data. This requires that cloud providers agree to the review period.
- **Employees:** people who work in the cloud provider is the most important point of security concerns. Most of the time, the attackers insiders who know everything about this system. Customers must have the right to know how companies can take care of the provider this issue.
- **Data Classification and Transfer:** Usually many users use the same cloud to store their data. In other words, the cloud can have many users data 'stored in the same place. It is important to know how that data is kept separate for each user from the other. How data is encrypted and how data is transferred through the network. It is hard to make sure that the data is being transmitted safely because of the intricate designs of public and private clouds.
- **Service Level Agreement (SLA):** SLA is a contract between cloud service provider and client. This contract specifies the assurance and security level offered by the provider.
- **Reputation and Future of the Provider:** Before associating with a particular cloud provider, it is advised to inquire about provider's standing in the cloud market. One important thing for clients would be to know what will happen to their data if the cloud faces an outage. For instance, MediaMax went out of business in 2007 because of a faulty script and lost its customer's data. This incident raised a big question on the reliability of cloud computing [7].
- **Security Violation:** Even though cloud providers promise that their services are impregnable for any kind of attack, they cannot be thought as completely reliable. The concept of cloud computing is fairly new and a center of attraction for hackers. This makes clients more concerned about their data security.
- **Recovery Management:** Clients need to know about the assurance of their data in case of natural disasters. Also, they need to know if the cloud is taking care of the backup of their data regularly or not. For instance, on February 23rd, one of the databases of Nokia's contact on OVI service crashed and they were only able to recover the database from three week old. The clients had to suffer from the data loss between this time span. The world's leading Research and advisory company in information technology, Gartner, estimated that the business growth in cloud computing will rise to 150 billion dollars be the start of 2013. As more and more companies tend to shift towards cloud computing, hackers will try more to get information un-lawfully.

Cloud Computing Attacks

The hackers tried to attacks in the past and were also successful in achieving their goals. In this section we are described some of important types of attacks as shown below briefly

- **Denial of Service Attack (DOS):** A cloud is always at risk of denial of service attacks because sharing a cloud with several users makes it even more susceptible to Dos attacks. For example, on August 06, 2009 morning, the world's famous social networking site, twitter went down for 2 hours. When the media contacted the website owner, it was revealed that the website went down because of denial of service attack [7]. There were some problems in the network for other big websites also such as facebook.com and live journal. It was later revealed that the hacker used virus affected systems and generated un-wanted information to the twitter site, which couldn't handle the traffic.
- **Side Channel Attacks:** In this type of attack, the hacker places his virtual machine and sets up the environment he needs for the attack near the target machine. He places malicious code in the virtual machine which is initiated and the target machine is affected. This way it gets very easy for the hacker to understand the target machine and launch the attack. This type of attack is known as side-channel attack [10].
- **Authentication Attacks:** Authentication is also a center of attraction for attackers because the process is normally based on what a hacker knows about the target user. For example, a hacker can know the target date of birth, place where he is born, first name, last name and other details. Hacker can use such details to hack the user's email account, bank account as few of the email services just need to get these details to allow the user to sign in if the user forgets the password. In simple words, in this type of attack, the hacker searches for the weakest link of the target user and then initiates the attack [7].
- **Man in the Middle Attack:** In this type of attack, the hacker places himself in between two other people's communication channel and tries to grab the security credential or other details and then uses this information. The hacker may pretend to be the other guy in the communication channel and might block the other guy. He intercepts the communication channel and gets the information by decrypting the cipher text he gets from there [7].

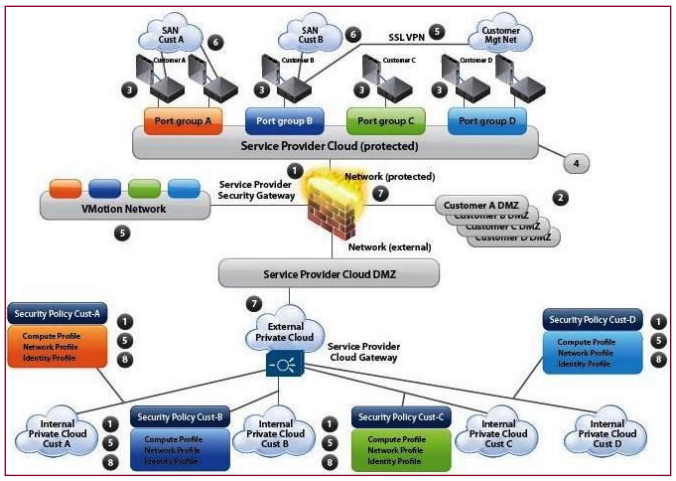

Fig. 2- Cloud Security Reference Architecture

Cloud Security Reference Architecture

In this section, [Fig-2] present reference architectures of cloud security, which are useful for understanding how various recommendations come together to provide a complete solution [8]. Enterprises that are interested in cloud computing models should consider the following reference architecture to ensure adequate security and optimal functionality.

As shown in [Fig-2], the diagram keys explain as:

- **Security Profile per Compute Profile:** Administrators must communicate security policy projects for companies and server-class firewall rules that have been identified in a virtualApplication service provider. This should include levels of corporate server security patch, anti-virus status and restrictions on access to the file level. The VMware virtualCloud provides reference architecture and a way to communicate policies and firewall rules server layer of virtualApplication.
- **Security DMZ for VirtualApplication:** The service provider needs to validate the patch level and security level prior to bringing a virtual Application into the production environment. The VMware virtual Cloud reference architecture should include a DMZ area for validating the virtual Application and mitigating any security violations according to each enterprise's security profile.
- **Operating System Management:** It is important to understand the security hardening performed around the service provider's library of Operating Systems and patching policies. Administrators should update traditional security policies that govern the service provider's hosting environment to ensure that virtual machines are hardened and patched within the standard enterprise policies. Administrators should update virtual machines that are not at the correct patch level to the correct patch level through a DMZ, for example.
- **Resource Management:** The service provider needs to separate and isolate the resources each client virtual machine uses from other customers' virtual machine resources to prevent DDoS attacks. These attacks are usually caused by log files not having limits or CPU or memory utilization increasing on a single virtual machine through memory leaks or poorly behaving applications.
- **Security Profile per Network:** In addition to the virtual Application having a compute security profile, there should also be a network security profile to ensure perimeter and Web access security. This includes functionality like switch and router Access Control Lists (ACLs), perimeter firewall rules, or Web application security (Application Firewall, URL Filtering, white list and blacklists). The VMware virtual Cloud reference architecture provides a method to communicate the network security profile. A critical component of the reference architecture is the isolation of networks; enterprises need to ensure that service providers implement separate management networks and data networks per client. In other words, there needs to be complete isolation between each client's virtual machine and the data traffic connecting to their virtual machines. In addition, service providers should have a separate network for VMware VMotion and virtual machine ware virtual machine safe. Enterprises should request that service providers encrypt all management traffic, including VMware VMotion events. Many enterprises will require encryption of data packets through SSL/IPSec, or management connectivity through SSL or SSH. Some service providers offer only shared or open connectivity. At a minimum, all management connectivity should be provided through SSL.
- **Data Security:** Enterprises should request service providers provide access paths to only the physical servers that must

have access to maintain the desired functionality. Service providers should accomplish this through the use of zoning via SAN N-Port ID virtualization (NPIV), LUN masking, access lists and permission configurations.

- **Security Authentication, Authorization and Auditing :** Cloud service provider environments require tight integration with enterprise policies around individual and group access, authentication and auditing (AAA). This involves integrating corporate directories and group policies with the service provider's policies. Service providers should offer stronger authentication methods to enterprises, such as 2-factor hard or soft tokens or certificates. The enterprise should require a user access report, including administrative access as well as authentication failures, through the service provider portal or via a method that pulls this data back to the enterprise. The VMware virtual Cloud reference architecture provides a method to communicate the access controls and authentication needs to the service provider.
- **Identity Management (SSO, Entitlements) :** Cloud environments need control over user access. Cloud providers must define a virtual machine identity that ties each virtual machine to an asset identity within the provider's infrastructure. According to this identity, service providers are able to assign user, role and privilege access within the extended infrastructure to provide role-based access controls. Enterprises also want to prevent unauthorized data cloning or copying from a virtual machine to a USB device or CD. Service providers can prevent cloning and copying of virtual machines using a combination of virtual machine identity and server configuration management policies.

Conclusion

Cloud computing is a modern term that is offered in the business environment enables users to interact directly with virtual resources and secure. some of the security risks and counter-measures are discussed in this paper. It has many models to protect its own data for business users. An organization used private clouds within its organization to prevent from loss of data. Cloud computing have several deployment models that help in information retrieval. SAAS, PAAS, IAAS are three models of cloud computing. We present the key issue for cloud security risk concern and the important types of attacks. Also we explain reference architectures of cloud security to provide a complete solution.

References

[1] Mell P. and Grance T. (2011) *The NIST Definition of Cloud Computing*, Special Publication, 800-145

[2] Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R.H., Konwinski A., Lee G., Patterson D.A., Rabkin A., Stoica I. and Zaharia M. (2009) *UC Berkeley Technical Report UCB/EECS-2009-28*.

[3] Jerry Archer, Dave Cullinane and Nils Puhlmann (2011) *Security Guidance for Critical Areas of Focus in Cloud Computing* V3.0.

[4] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham (2010) *International Journal of Information Security and Privacy*, 4(2), 39-51.

[5] Daniele Catteddu and Giles Hogben (2009) *European Network and Information Security Agency*.

[6] Wang Zhijun, Zhang Ni, Qiao Zizhi, Lin Min (2012) *IEEE International Conference on Oxide Materials for Electronic Engineering*.

[7] Kifayat K., Merabti M., and Shi Q. (2010) *International Journal of Multimedia Intelligence and Security*, 1(4), 428-442.

[8] Kandukuri B.R., Paturi R., Rakshit A. (2009) *IEEE International Conference on Services Computing*, 517-520.

[9] Casassa-Mont M., Pearson S. and Bramhall P. (2013) *Proc. DEXA*, *IEEE Computer Society*, 377-382.

[10] Shuo Chen, Rui Wang, Xiao Feng Wang and Kehuan Zhang (2010) *IEEE Symposium on Security & Privacy*.