SECURITY CONCERNS AND COUNTERMEASURES IN CLOUD

PALLAVI SIDELLA

UNIVERSITY OF TENNESSEE, CHATTANOOGA

April 2012

ABSTRACT:

With the growing popularity of Cloud (*cloud computing and cloud service*), there is a growing concern for security risk for companies using them. Irrespective of the size of the companies, more and more companies are adopting this new economical computing resource in their environment. "Cloud computing as defined by NIST is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]" Understanding the risks, threats, vulnerabilities, and possible countermeasures before adopting this technology is important. In this paper I discussed the scope and control of cloud provider and cloud consumer on the cloud, security issues specific to 3rd party cloud provider, security risks and concerns in cloud and possible countermeasures.

Keywords: Cloud service, Cloud computing, Security concerns, and Counter measures.

1. INTRODUCTION:

Cloud is a general term which can refer to *cloud computing* or *cloud services*. Cloud computing is Information Technology (IT) model for computing which is composed of hardware, software, networking, and service components that enable the development and delivery of cloud services via Internet or private network.

"Cloud services are those services that are expressed, delivered and consumed over the internet or private network. [2]" Cloud service models are divided into three: (1)Infrastructure-as-a- Service (IaaS), (2)Platform-as-a-Service (PaaS), and (3)Software-as-a-Service (SaaS). These service models can be deployed as Private cloud, Public cloud, Community cloud or Hybrid Cloud. This paper discusses the security control in the cloud model by the consumer and provider of cloud, the threats, security issues specific to 3rd party cloud provider, risks and security concerns in cloud and possible countermeasures.

2. SECURITY CONTROL IN THE CLOUD MODEL:

Many organizations are seriously looking into cloud computing and services to cut down on costs and also to benefit greatly from the new alternatives and opportunities that were not available in the past. These new alternatives not only save millions of dollars, but also provide them with the choice to only rent the necessary computing power, storage space, and infrastructure from cloud providers. The choice of deployment model and the type of service model by the organizations/consumer plays an important role in scope and control over the computational environment. The scope and control between the cloud consumer and cloud provider for each of the service model is given in Figure 1. The higher the level of support the cloud provider has, the lower the scope and control the cloud consumer has over the cloud.

In **SaaS** the security burden is on the cloud provider as this model is based on a high degree of integrated functionality **with minimal consumer control** or, extensibility. The provider is responsible for most aspects of the security compliance and liabilities. The **PaaS** model has fewer higher-level features but offers greater extensibility and consumer control. The **security** provisions are split **between** the cloud provider and the cloud consumer in PaaS. **IaaS** offers **greater** tenant or consumer **control** over the security than the other two models.

The degree of control that a tenant or consumer has in a public cloud is minimal, whereas in a private cloud the tenant has maximum control. The degree of control for hybrid and community cloud is in between public and private.

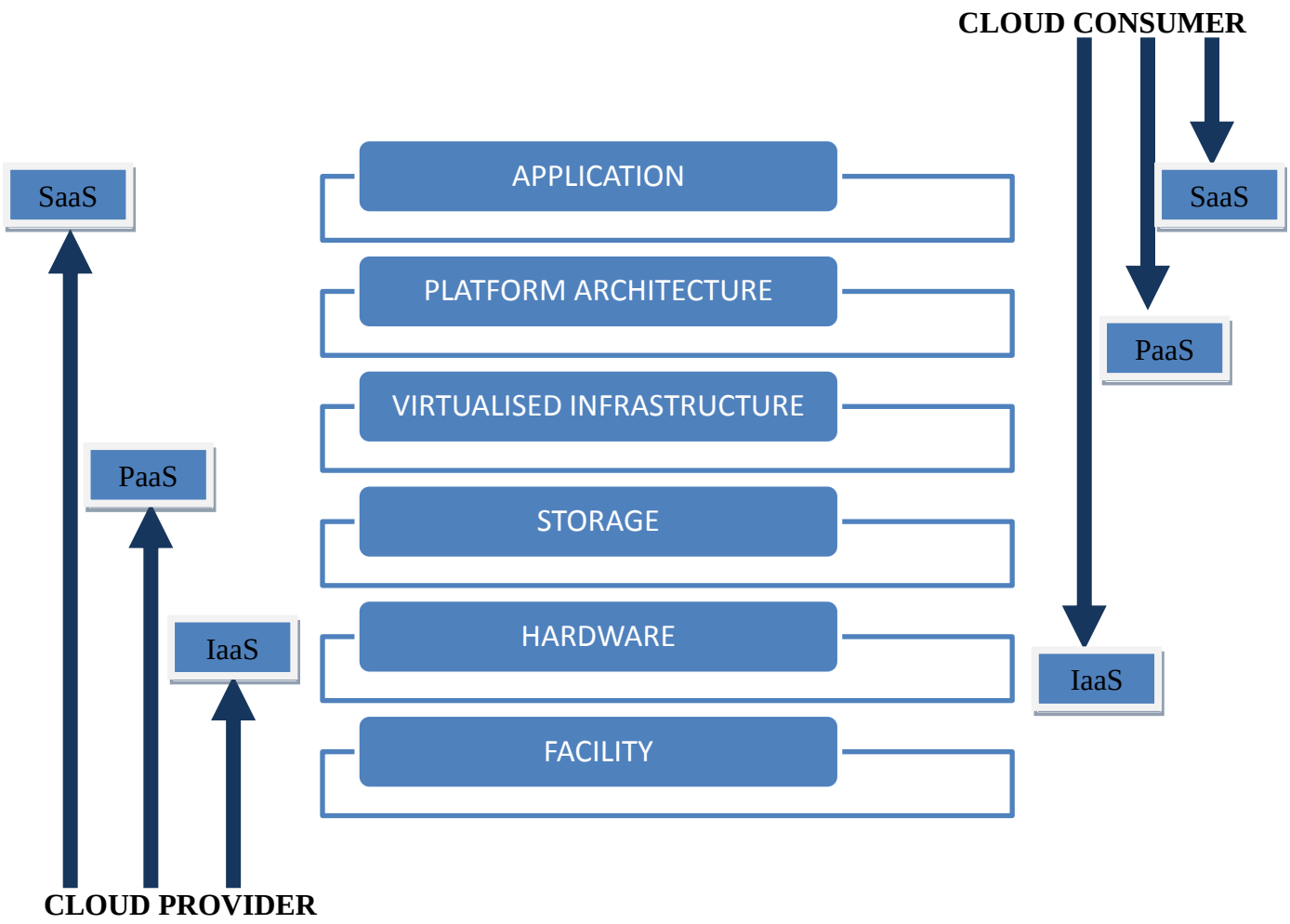

Figure 1: Scope and Control of Cloud Provider and Cloud Consumer[5].

3. SECURITY ISSUES SPECIFIC TO 3RD PARTY CLOUD PROVIDER:

Most security problems arise when provider is a third party. Self-managed clouds/private clouds still have security issues, except the issues mentioned below.

- Loss of control- over physical security of data, authentication techniques, policies, security monitoring , network management etc.,.
- Lack of trust – on resource availability from provider, policies, procedures and data storing and managing technique, on employees of the cloud provider etc.,.

- Multi-tenancy- sharing resources physically and logically with other consumers without knowing who they are.

4. MINIMIZING SECURITY ISSUES/RISKS WHEN CONSIDERING 3RD PARTY CLOUD PROVIDER:

The following are few security considerations that companies need to consider before selecting a cloud provider in order to reduce the risks:

- **Regulatory compliance: "** Provider must be willing to submit to external audits and security certifications.[6]"
- **Data location:** If the company requires the cloud provider to store and process data in specific geographic locations, provider should obey the privacy rules of those geographic locations.
- **Backup and recovery:** The backup and recovery policies and procedures of a cloud provider in case of a data loss or a disaster.
- **Shared environment:** "Public cloud services offered by providers have serious underlying complications- client organization typically share components and resources with other consumers." [2] Attackers can pose as a consumer and exploit the vulnerabilities within the environment and gain unauthorized access. The countermeasure for this is to use high level of assurance pertaining to the strength of security mechanism which is used for logical separation.
- **Provider's guarantee of availability**: "Does the Service Level Agreement (SLA) guarantee that the provider will provide the adequate system availability and quality of service?[7]" Availability can be affected due to various reasons like technical issues, denial of service attacks, poor software version control and poor change management processes.
- **Long-term viability:** If the cloud provider is going out of business or selling it to another company, "how can you get your data back? Will the data be in a format that could be easily imported into a replacement application?[6]"
- **Data encryption**: "Are hash algorithms, encryption algorithms and key lengths used to protect the data in transit and also in backup storage.[7]"

5. SECURITY THREATS IN CLOUD COMPUTING:

One of the top security concern for companies is the physical location of data, as it is spread across geographic area with cloud computing. If the data is located in another country the laws of the host country of the equipment apply to the data and on the machines [3], which can be a big issue if the country does not have adequate laws to protect sensitive data.

Cloud computing security threats are almost same as those found in existing computing platforms. The Cloud Security Alliance [4] did a research on the threats facing cloud computing and it identified the following seven major threats:

- **Abuse and Nefarious Use of Cloud Computing**
- **Insecure Application Programming Interface**
- **Malicious Insiders**
- **Shared Technology Vulnerabilities**
- **Data Loss/Leakage**
- **Account, Service & Traffic Hijacking**
- **Unknown Risk Profile**

Attackers can pose as a legitimate customer and purchase the services of cloud computing and use it for nefarious purpose like password cracking and launching other types of attacks like download of exploits, Trojans, host botnets, etc. The cloud consumers interact with cloud services using software interfaces or API's; vulnerability in the cloud can increase as third parties build new software. The counter measure [8] for the above mentioned **Abuse and Nefarious Use of Cloud Computing** attack is to toughen up the registration process and monitor the network traffic. **Insecure API's** can be protected by thorough analysis of the interfaces and quality implementation of the security mechanism like authentication, access control, and encryption. The countermeasure for **Malicious insiders** is, applying the access control matrix model and thus reducing the access to the resources and keeping it bare minimum to function properly in their roles. **Shared Technology issues** can be addressed by monitoring and applying high level of assurance pertaining to the strength of security mechanism which is used for logical separation. **Data loss or leakage -** data loss threat can be addressed using quality disaster recovery and backup; and data leakage can be remedied using strong encryption algorithm for storing data and accessing the data. **Account or service hijacking** is generally carried out by phishing site or social engineering

approach where attacker can gather the information, falsify transactions and also redirect to malicious websites. Again strong authentication techniques and security policies can prevent these types of attacks.

6. CONCLUSION:

Cloud provider offers cloud as service or as cloud computing. Companies/ Organizations are adopting this new technology to save cost and benefit greatly from the new alternatives but they need to also analyze the security risk associated with it. Cloud services are offered as Infrastructure-as-a- Service (Iaas), Platform-as-a-Service (Paas) and Software-as-a-Service (SaaS). These service models can be deployed as Private cloud, Public cloud, Community cloud or Hybrid Cloud. The Companies/ Organizations should also understand the threats involved and scope of control in the cloud model before transitioning to the cloud.

7. REFERENCES:

[1] The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Securing the Cloud: Cloud Computer Security Techniques and Tactics by Graham Speake, Vic (J.R.) Winkler. Syngress publications.

[3]Smith, R. (2009) - Computing in the cloud. Research Technology Management, 52(5), 65-68, ABI/INFORM Global. (Document ID: 1864072981).

[4] Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance - http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[5] Guidelines on Security and Privacy in Public Cloud Computing- http://nvlpubs.nist.gov/nistpubs/sp/2011/sp800-144.pdf

[6] Edwards, J. (2009) Cutting through the fog of cloud security: Computerworld. Framingham: Vol. 43, Issue 8; page26, 3 pages.

[7] Cloud Computing Security Considerations - http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

[8]Top 7 threats to cloud computing- http://www.net-security.org/secworld.php?id=8943
[9] An overview of the security concerns in enterprise cloud computing- http://arxiv.org/ftp/arxiv/papers/1101/1101.5613.pdf