Major Cloud Computing Threats And Their Possible Solutions

Amanjot Kaur
A.P. CSE
MIMIT, Malout

Harjasdeep Singh
Lecturer CSE
MIMIT, Malout

Sukhwinder Bir
A. P. CSE
BCET, Gurdaspur

Abstract:

Cloud computing is everywhere. When you see a magazine or news related to technology you will definitely see cloud computing there. In recent years cloud computing becomes the hot topic in the field of information technology. Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Customers are both excited and nervous at the prospects of cloud computing. However, customers are also very concerned about the risks of cloud computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable. This paper analyses some threats in cloud computing and give some technical support for these threats.

Keywords: Cloud computing, security, threats.

1. Introduction:

The Cloud computing field offers so many advantages to the web connected devices. To handle the enormous data present in cloud and the popularity that gains cloud computing over the past few years, security becomes a major concern for all who are using it and also those who want to utilize it but would not

able to do so because no one can assure them in terms of security of their data on the cloud. In 2nd section we will give some introduction to cloud computing and its types. In 3rd section we will discuss about some security threats in cloud computing and in 4th section we will give some technical support to resolve those threats. In 5th section we will conclude the topic and give some future scope.

2. Types of Cloud Computing:

Cloud computing is a new concept of information technology that uses internet and remote services in order to maintain data and applications. There are different types of cloud computing. These are given below:

i)IAAS (Infrastructure As A Service):

The most basic cloud service is IAAS. In this service, cloud providers offer computers as physical or as virtual machines and other resources. Therefore Iaas is essentially a physical server box [4]. Rather than purchase servers, software, racks and having to pay for datacenter space for them, the datacenter rents those resources. The resources that you take on rent are:

- Server space
- Network Equipment
- Memory
- CPU Cycles
- Storage Space

ii) PAAS (Platform As A Service):

In this service, cloud providers deliver a computing platform including operating system, programming languages execution environment, database and web servers. The end users write their own codes and the PAAS providers upload that code and present it in the web. There are four types PAAS solutions:

- Social Application Platform
- Raw Compute Platform
- Web Application Platform

- Business Application Platform

Examples of PAAS are:

- Amazon
- Cloud Foundry
- Google App Engine
- Windows Azure

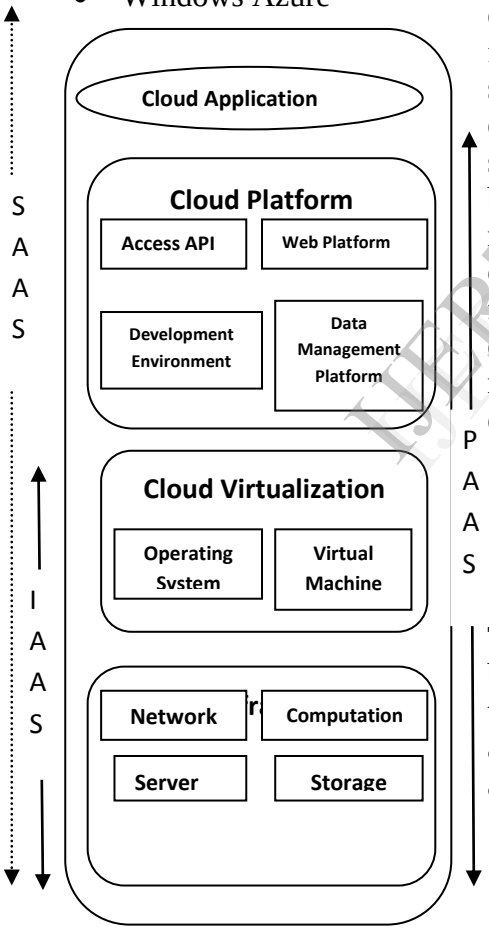

Fig.1: Types of Cloud Computing

iii) SAAS (Software As A Service):

In this service, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. This service is based on the concept of renting software from a service provider rather than buying it. It is currently the most popular type of cloud computing because of its high flexibility, great services, enhanced capability and less maintenance. Some instances of SAAS are:

- Yahoo Mail
- Google Docs
- CRM Applications

The service provider hosts both applications and data so that user can access these at any time. Common business areas in SAAS are:

- CRM
- ERP
- HRM

- SCM
- CMS
- Finance and Accounting

3. Security Threats:

When we talk about security in cloud, everyone asking, is their data is secure on the cloud? Here we are giving some vulnerable security threats which can enable both end users and vendors about these threats:

i) **Abuse and nefarious use of cloud computing:** IAAS attracts many cyber criminals due to some easiness of registration. Hosts know about their commands and control centres. In many cases the service providers offers a free trial period. Organizations should consider their risks due to unauthorized signup, lack of validation, service fraud and ad-hoc services.

ii) **Insecure Interfaces and APIs:** Application Programming Interfaces are used to establish, manage and monitor service. Security and availability of cloud service is dependent on the security of management, provisioning and monitoring interfaces.

iii) **Malicious Insider:** Cloud services are transparent to the customer. Organization does not need to know the background details e.g. how to deliver a service, provider's procedure, physical access to system etc.

iv) **Shared Technology Issues:** Multiple organizations can share and store large amount of data in cloud computing on servers. Shared technology is a way of life for IAAS. Mostly the essential components that are required to make this infrastructure were not designed to offer strong isolation properties for multi tenant architecture. To remove this gap, a virtualization hypervisor mediates access between guest operating system to gain inappropriate levels of control the underlying platform.

v) **Data loss and Leakage:** Data loss or leakage can happen

in many ways e.g. deletion without a backup, loss of the encoding key, unauthorised access etc. The threat of data compromise increases in the cloud due to a number of risks and challenges.

vi) **Account or Service Hijacking:** Organizations should aware of accounts and services hijacking. These attacks could be phishing, fraud, simple internet schemes and software vulnerabilities.

vii) **Unknown Risk Profile:** For most service providers, it is not a big concern to think about security, they just focus on functionality and benefits. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts and security design are important factors of estimating company's security profile.

4. **Methods to Resolve Threats**:

Abuse and nefarious use of cloud computing can be resolved by stricter initial registration and validation process, enhanced credit card fraud monitoring and coordination, monitoring public blacklist for one's own network blocks.

APIs can analyze the security model of cloud provider interfaces and understand the dependency chain associated with the APIs.

Malicious Insider can strict supply chain management and conduct a comprehensive supplier assessment specify human resources requirement as part of legal contracts and can determine security breach notification process.

Shared technologies can implement security for installation and configuration, monitor environment for unauthorized activity.

Data loss can encrypt and protect integrity of data in transit, analyzes data protection at both design and run time, contractually specify provider backup and retention strategies.

Service hijacking prohibit the sharing of account credentials between users and services, employ proactive monitoring to detect unauthorized activity. Accounts hijacking can be prohibit by sharing the account credentials between users and services and employ proactive monitoring to detect unauthorised activity.

Risk profile can be secure by discolouring applicable logs and data and monitoring and alerting on necessary information.

5. **Conclusion:**

This paper took information from CSA's March 2010 report, "Top Threats to Cloud Computing" and some other articles. This paper discussed seven threats specific to cloud computing. Internet cloud computing service provides both business and technical benefits. Risk management helps organizations to identify, manage and reduce their cloud computing risks so that they may achieve the greatest benefits at the lowest level of risk.

6. **References:**

1. HP "Top Threats to Cloud Computing" March 2010 issue.
2. http://www.altiusit.com/files/blog/Top10CloudComputingThreats.htm
3. http://ccskguide.org/top-threats-to-cloud-computing/
4. "Cloud Computing Basics" http://www.south.cattelecom.com/