Global Journal of Computer Science and Technology
Cloud and Distributed
Volume 13 Issue 1 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Multi Packed Security Addressing Challenges in Cloud Computing

By Dr. A. Ravi Prasad, J. Kishore Kumar & N. Jayanthi
Kurukshetra University, India

Abstract - Cloud computing efficiency, flexibility, greater agility, less capital expenditure is to overcome geographic limitations to compete in a global market. Most of the companies are shifting to Cloud based services, but at the same time they are concerned about the security risks. Hopefully after the definitions and illustrations of Cloud computing are given in this paper you will understand it better. This paper identifies security concerns arising in cloud computing environments and outlines methods to maintain compliance integrity and preserve security protection.

Keywords : *cloud computing, multi packed security, privacy.*

GJCST-B Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Multi Packed Security Addressing Challenges in Cloud Computing

Dr. A. Ravi Prasad [α], J. Kishore Kumar [σ] & N. Jayanthi [ρ]

Abstract - Cloud computing efficiency, flexibility, greater agility, less capital expenditure is to overcome geographic limitations to compete in a global market. Most of the companies are shifting to Cloud based services, but at the same time they are concerned about the security risks. Hopefully after the definitions and illustrations of Cloud computing are given in this paper you will understand it better.

This paper identifies security concerns arising in cloud computing environments and outlines methods to maintain compliance integrity and preserve security protection.

Keywords : cloud computing, multi packed security, privacy.

I. Introduction

Cloud computing use advanced computational power and improved storage capabilities. The main focus of cloud computing from the provider's view is extraneous hardware should be connected which can support downtime on any device in the network, without a change in the users' perspective. Also, the users' software image should be easily transferable from one cloud to another.

There are two characteristics of cloud model. They are Multi-tenancy and elasticity. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics helps in improving resource utilization, cost and service availability.

The Essential Cloud Characteristics are:

- Elasticity - this is useful for large and small organizations as it is pay-per-use basics and it will scale ITinfrastructure requirements.
- Pay-as-you-go versus install-and-own - capital requirements from the user to the service provider is equally attractive - again, to large and small organizations alike
- Savings - t is useful in terms of cost as one of the surveys reported that government agencies can save 25% to 50% of their IT costs and increase their business agility by migrating IT infrastructure to cloud services.
- Reduction in Market barrier - cloud computing services reduce IT barriers and lower infrastructure costs.
- Utilization of Infrastructure - because of its virtualizing hardware and software resources, which are provided as service work can happen between multiple users simultaneously. Because of good infrastructure this has better network efficiency which results in lower power consumption and smaller carbon footprints.
- Investment of Public - governments worldwide are investing to create economic regions of cloud technology development(e.g., China, Japan), are supporting cloud-related standards development (e.g., EU, US) or are migrating their own IT infrastructures to cloud services in an effort to lead by example (e.g., US, UK, Japan)
- Market research view - research points to ongoing rapid adoption of both public and private cloud services are assumed to be future prediction trend.
- Security - providing "security as a service" should be taken care yet.
- Standardization - improved standards are required to reduce or eliminate risk from many current problems which make difficult for cloud adoption
- Cloud Middleman - emerging cloud services brokers not only helps organization's that shift to the cloud to overcome specific security, privacy and compliance issues but also helps in achieve interoperability across multiple clouds and in-house IT infrastructure.
- Missing out - if organizations do not adopt cloud computing along with their competitors risk they are going to miss benefits such as the flexibility, agility and access to the latest versions of technologies.

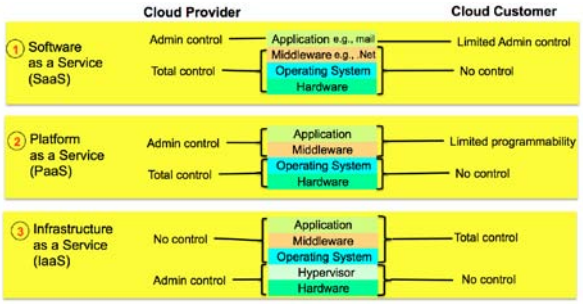
II. The Cloud Computing Architecture

There are certain characteristics of cloud computing. There are several definitions that stem from the three main categories of Cloud computing which are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

– Infrastructure-as-a-service (IaaS): providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. Amazon EC2 is the most IaaS provider.

Author α σ : Lecturer, S.G. Govt. Degree College, Piler, India.
Author ρ : M.Tech3 CSE Dept, SVCE, Tirupati.

– **Platform-as-a-service (PaaS):** providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known.
– **Software-as-a-service (SaaS):** Applications hosted on the cloud infrastructure as internet based service for end users, applications on the customer's computers be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. Sales Force CRM is an example of the provider.



III. Deployment Models

There are four deployment models, each with specific characteristics that support the needs of the services and users of the clouds in particular ways.

- **Private Cloud** - The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.
- **Community Cloud** - The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.
- **Public Cloud** - The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.
- **Hybrid Cloud** - The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud.

a) Benefits

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

- **Cost Savings** - Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities.
- **Scalability/Flexibility** - Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Companies to use extra resources at peak times, enabling them to satisfy consumer demands.
- **Reliability** - since there are services which use multiple redundant sites so user is supported with business continuity and disaster recovery.
- **Maintenance** - Cloud service providers reduces maintenance requirements as accessing is through APIs that do not require application installations onto PCs.
- **Mobile Accessible** - Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

b) Cloud Security Challenges

The following are some of the notable challenges associated with cloud computing they can be reduced with advanced services by planning.

- **Privacy and Security** -Two important issues that surround cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers.
- **Standards Improvement** - Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be operated in conjunction. Working is going on cloud computing standards and practices.
- **Continuously Evolving** - since cloud does not remain static as user requirements are continuously evolving, the requirements for interfaces, networking, and storage should also continuously evolve.

IV. Administrative Access to Servers and Applications

Cloud computing offers "self-service" access to computing power, most likely via internet. This increases exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in the system control.

V. Dynamic Virtual Machines: VM State and Sprawl

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily which makes difficult to achieve and maintain consistent security. In the cloud

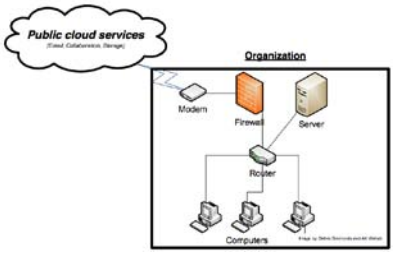
computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

a) Security, Privacy

Cloud computing present's specific challenges to privacy and security. When using cloud-based services, one is entrusting their data to a third-party for storage and security. Cloud-sourcing involves the use of many services, and many cloud based services provide services to each other, and thus cloud-based products may have to share your information with third parties if they are involved in processing or transferring of your information. They may share your information with advertisers as well, as many do to help cover the costs.

b) Public Cloud Computing

Public Cloud computing means relying on third parties to offer efficient IT services over the Internet as needed. The National Institute of Standards and Technology defines a public Cloud as a Cloud infrastructure that is made available to the general public or a large industry group. Public Clouds are owned by the organization(s) selling Cloud services



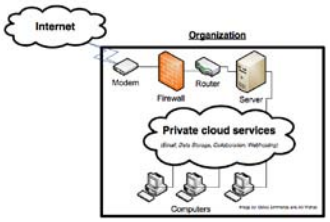
c) Public Cloud Security Issues

Public Clouds are hardened through continual hacking attempts. The NIST definition of public Clouds states that they are made available to the general public or a large industry group. Therefore, public Cloud providers are much larger targets for hackers than private Clouds. Public Clouds also attract the best security people available; the biggest and best Cloud service providers have millions of customers relying on them. They definitely would be meticulous about who they hire. Also public Cloud providers, especially larger companies like Google, Amazon, and Face book would get the latest security gear much easier than a small to midsize private company.

- Assessment of the CSP
- Security of the communication channels
- Transparency of security processes
  - Compliance with Regulations
  - Potentials of a single security breach
  - Access control mechanisms
  - Data Loss

d) Private Cloud Computing

According to the National Institute of Standards and Technology (NIST) a private Cloud is a Cloud infrastructure that is operated solely for an organization. The organization or a third party can manage it. Private Clouds can exist on-site or off-site (Grance, T., Mell, P., 2009). Typically private Clouds are used when sensitive data is involved.



e) Private Cloud Security Issues

Private Clouds have the same security concerns as public Clouds do, but typically on a smaller scale since private Clouds are operated solely for an organization.

- Security Architecture
- Perimeter Security and insider attacks
- Hypervisor vulnerabilities and network level authentication (IPSec, IPS/IDS)
- Security Zones

Solution approaches:

- Firewall
- Intrusion Detection and Prevention (IDS/IPS)
- Integrity Monitoring
- Log Inspection

f) Packed Security

This concept first concentrates on a agreement between customer, cloud provider and third party.

1. Customer training:
   - This indicates that first there should be a understanding between customer and service provider. So that a provider must train his/her customer about storing, updating and retrieving data.
   - If service provider is taking help of third party for services then there should be an understanding between provider and third party. So that third party train provider first then provider must train customer.
2. Double Jamming Algorithm:

a) Store data in encrypted form
b) Lock data
c) Encrypt the lock
d) Lock the lock
e) If data needed to be accessed or updated
f) First break all locks
g) Access/update data within specified attempts
h) Access/update data within specified time
i) If locks are not broken or

j) If locks are broken but not accessed/updated data with in particular attempts or
k) If locks are broken, accessed/updated data with in particular attempts but not with in particular time
l) Then it indicates threat to data.
m) Otherwise no problem

Advantages:

1. Very Secured

Disadvantage:

1. Proper choice of number of attempts
2. Proper choice of time interval

VI. Conclusion

In this paper we have provided a definition of Cloud computing and highlighted the security issues/concerns related to Clouds. As more businesses today utilize Cloud services and architectures, more threats and concerns arise. Both public and private Cloud models have their own advantages and challenges; therefore security will always be an issue.

Cloud computing is a v was ery wide subject area. Even though the scope scaled down to the security issues in Cloud computing it is still quite a challenge getting details on certain areas.