Compute Level Security Mechanisms in Public Cloud Environment

G. Vakula Rani* [1]

Asst. Prof. , Dept. of MCA ,
CMR Institute of Management Studies (Autonomous),
Bangalore, Karnataka , India
* Email : hodmca.ims@cmr.ac.in

P.K. Srimani[2]

[2]Former Chairman, Dept. of CS & Maths,
Bangalore University
Bangalore, Karnataka , India

Abstract - **Cloud computing has emerged as a new paradigm for hosting and delivering services over the Internet. It has an advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-and-use business model. Security is one of the major issues which hamper the growth of cloud computing. There are various risks associated with the security at different levels. One of the issue is the compute/Host level security i.e. securing a compute infrastructure includes security of the physical server, hypervisor, Virtual Machine (VM), guest OS and application security. This paper presents various key security issues and challenges which are currently faced in the Cloud computing and focuses mainly on compute level security considerations and preventive methods to provide cloud security solutions.**

Keywords : ***cloud computing, Application level, compute level, physical server hypervisor , Virtual Machine(VM), guest OS.***

I. INTRODUCTION

With the rapid development of processing and storage technologies and the success of the internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing. Cloud computing has gained large popularity in the recent years among a wide range of consumers, ranging from small start-ups to multinational companies. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. It enhances collaboration, agility, scaling, and availability. It provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down and provides an on-demand utility-like model of allocation and consumption of resoureces.

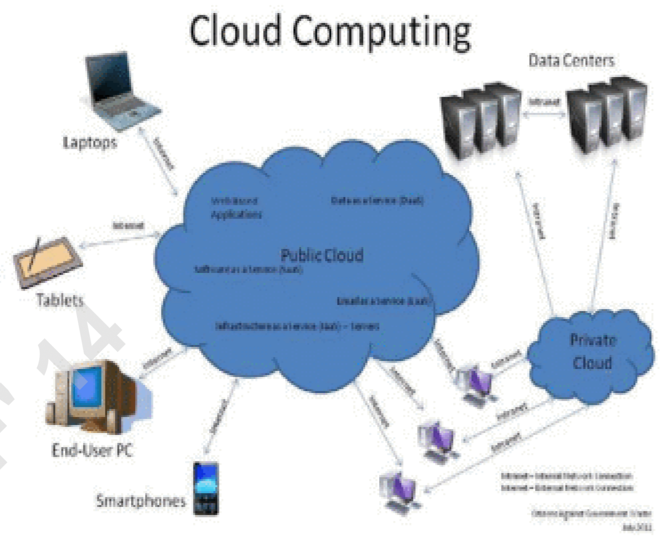

Figure 1 : Cloud Computing

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Few advantages of it include scalability, resilience, flexibility, efficiency and outsourcing non-core activities.

II. CLOUD COMPUTING

Cloud computing is a model for enabling 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. NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in figure 2.

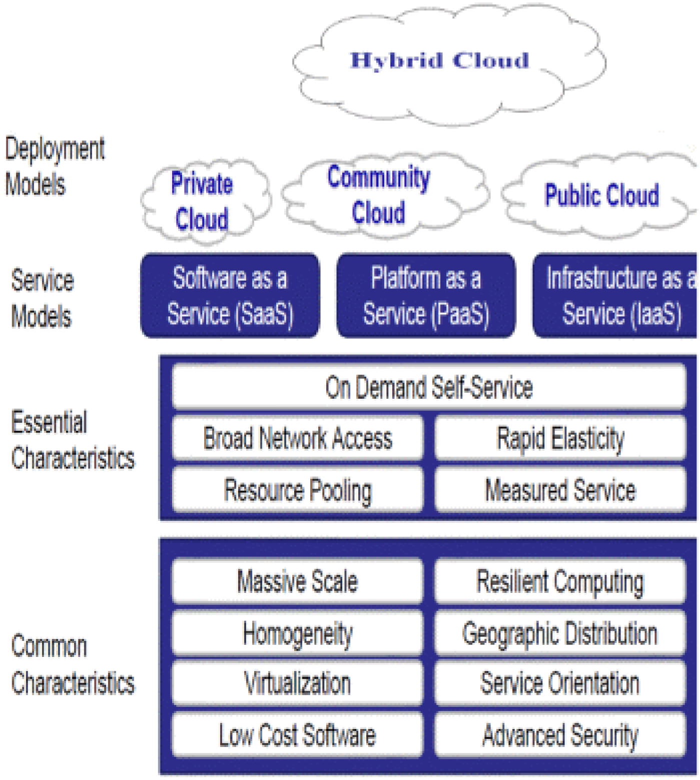

Figure2:Working Definition of Cloud Computing -NIST

A) Essential Characteristics of Cloud Computing

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.
- ***Broad network access*** : Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services.
- ***Resource pooling:*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- ***Rapid elasticity:*** Capabilities can be rapidly and elastically provisioned to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- ***Measured service*** : Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported.

B) Cloud Service Models

Cloud service delivery is divided among three fundamental classifications and are often referred to as the "SPI Model," where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively.

- **Software as a Service (SaaS)** : The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email,). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. The Service Providers for SaaS are *Google Docs, Salesforce.com.*
- **Platform as a Service (PaaS)** : The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. The Service Providers for PaaS are *Google App Engine, Microsoft Azure Services, Amazon Elastic Map Reduce.*
- **Infrastructure as a Service (IaaS)** : 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. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). The Service Providers for IaaS are *Amazon EC2, Amazon S3, Linode and Rackspace.*

C) Cloud Deployment Models

When considering cloud computing options, good network connectivity is essential. Once the network is in place, the choices of how to create a cloud environment vary, but most fall into four different categories: private cloud, community cloud, public cloud, or hybrid cloud. Among the best known public cloud services are Amazon, Bing, Google, Yahoo, and others. However, these public clouds may not offer all of the security protections required by cloud users. A private cloud is one built for a specific customer – either in the corporate sector or government – with greater security protection for the customer's data. A community cloud allows several clients to share the same cloud to perform similar functions such as human resources or email. A hybrid cloud is a combination of two or more of the other three cloud infrastructure options.

D) *Benefits of Cloud Computing*

- Minimized capital expenditure
- Location and device independence
- Utilization and efficiency improvement
- Very high scalability
- High computing power

III. CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Cloud service provider faced many issues while implementing cloud services.

A) *Privacy issues:*

It is to secure private and sensitive information. The public cloud is one of the dominant architecture when cost reduction is concerned, but relying on a cloud service provider (CSP) to manage and hold customer information raises many privacy concerns as

a) *Lack of user control*: In software-as-a-service environment service provider is responsible to control data. Customer can retain its control on data when information is processed or stored. It is the legal requirement of the user and to make trust between customer and vendor. User sensitive data is processed in the cloud, they may have danger of misuse, theft or illegal resale.

b) *Unauthorized secondary usage*: Threats can occur if information is placed for illegal use. The possibility of vendor termination and if cloud computing provider is bankrupted or another company get the data as there are no technological barriers for secondary uses, the problem occurs.

B) *Security Issues*

Information assurance and data ownership

Data stored in cloud environment can be accessed by the hacker and the threat of access sensitive information. Information assurance concerns for cloud users involve Confidentiality, Integrity and Authenticity. Ensures that a user identity is genuine and there is no illegal access allowed.

Data ownership concerns the data belonging to a client is maintained by a cloud service provider, who has access to data, but is not the legal owner of it. This raises the concern of potential unauthorized data access and misuse.

C) *Multitenancy*

It is a key security concern in cloud. For cloud clients, co-location of multiple virtual machines (VM) in a single server and sharing the same resources increases the attack surface. Enforcing security controls and measure uniformly is difficult.

D) *Data privacy*

Potential for unauthorized disclosure of private data of a cloud client. Private data may include individual identity of the client, details of the services requested by the client, proprietary data of the client. CSP need to ensure that private data of its clients is protected from unauthorized disclosure.

E) *Denial of service attacks*

An attempt to prevent legal users from accessing a resource or service. DOS attack may affect software application/network components. A hacker can use a cloud to host a malicious application for achieve his object which may be a Distributed Denial of Service attacks against cloud itself or arranging another user in the cloud. Distributed Denial of Service (DDOS) attacks typically focus high quality of IP packets at specific network entry elements where infrastructure is shared by large number of clients. DDOS attacks are one of the powerful threats available especially with huge number of zombie machines. When a DDOS attack is launched, it sends a heavy flood of packets to a web server for multiple sources.

IV. BASIC INFORMATION SECURITY IN CLOUD

Cloud computing is an emerging technology with shared resources, lower cost according to the user demand. Security is the most important issues in cloud computing [15]. The fundamental basis for developing secure cloud environment is based on various information security principles:

A) *CIA triad*

A security framework for an information system has three primary goals: Confidentiality, Integrity, and Availability of physical and logical resources. This is commonly known as CIA triad.

Confidentiality
Availability
Integrity

Figure 3: CIA triad

- *Confidentiality* Provides the required secrecy of information and ensures that only authorized users have access to data. In addition, it restricts unauthorized users from accessing information.
- *Integrity* Ensures that unauthorized changes to information are not allowed. The objective of this goal is to detect and protect against unauthorized alteration or deletion of information.
- *Availability* Ensures that authorized users have reliable and timely access to the compute, storage, and network resources. Availability also requires transferring data to different location(s) to ensure its availability if a failure occurs in any location.

B) AAA(Authentication, Authorization, and Auditing)

The security framework for an information system should provide authentication and authorization capabilities that are required to ensure legitimate access to data.

- *Authentication* ensure that a user's are genuine so that no illegitimate access to information is allowed. Multi-factor authentication is a special method for authentication, which considers multiple factors together for authenticating a user.
- *Authorization* is to grant specific access rights to a user on resources. Authorization defines the limits of the access rights of a user on a resource; for example, read-only access or read-write access on a file.
- *Auditing* is a process to evaluate the effectiveness of security enforcement mechanisms.

C) Encryption:

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized users. Decryption is the process of converting encrypted data back into its original form. Encryption is used to enforce confidentiality, privacy, and integrity. The non encrypted data, which is given to the encryption process as an input, is called plaintext (clear text) and the encrypted data, which is an outcome of the encryption process, is called cipher text. Encryption and decryption requires keys to apply on data. When the keys for encryption and decryption are the same, it is known as symmetric encryption. When these keys are different (but related), it is known as asymmetric encryption. For data encryption, most often, symmetric encryption is used. Asymmetric encryption is most commonly used to secure separate end points of a connection, for example, Web browser and Web server (using https), VPN client and server, or for transferring a symmetric key.

D) Defense-in-Depth

It is a risk management strategy which provides multiple layers of defense against attacks. Defense-in-depth represents the use of multiple security defenses to help mitigate the risk of security threats if one component of the defense is being compromised. An example could be an antivirus software installed on individual VM when there is already a virus protection on the firewalls within the same environment. Different security products from multiple vendors may be deployed to defend different potential vulnerable resources within the network. Defense-in-depth is an information assurance strategy in which multiple layers of defense are placed throughout the system. For this reason, it is also known as a "layered approach to security". Because there are multiple measures for security at different levels, defense-in-depth gives additional time to detect and respond to an attack. This reduces the scope of a security breach. However, the overall cost of deploying defense-in-depth is often higher, compared to single-layered security mechanisms.

V. Levels of Security

There are several security challenges associated with cloud computing at different levels ie. at the physical, network, host/ compute , application and data levels. The main issues relate to defining which parties are responsible for which aspects of security.

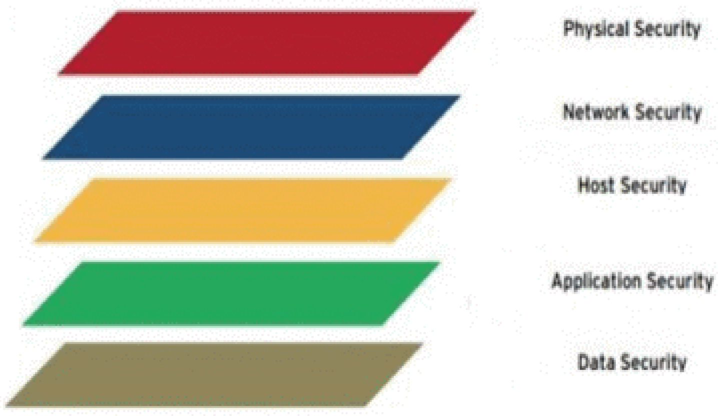

Figure 4: Levels of Security

Security	***Mechanisms***
Physical Security	Guards, Locks, Access Controls, Environmental Safeguards
Network Security	Network Segmentation, Network Based IDS/ IPS, Virtual Firewall, Demilitarized Zone.
Compute/ Host Security	Server Hardening , Host Based Fire Wall, Virus Protection, Patch Management Intrusion Prevention, File Integrity, And Logs Monitoring.
Application Security	Intrusion Prevention, Vulnerability Assessments and Penetration Testing.
Data Security	Data Encryption, Data-at-rest , Data shredding and Secure Communication (SSL).

A) Security mechanisms at Compute/ Host Level

Securing a compute infrastructure includes enforcing security of the physical server, hypervisor, VM, and guest OS. Security at the hypervisor level primarily aims at securing hypervisor from the root kits and malware based attacks and protection of the hypervisor management system. VM isolation and hardening are two key techniques for securing VMs. Security at the guest OS level uses sandboxing and hardening as two key methods. Application hardening is used to reduce vulnerability of the applications from getting exploited by malicious attackers.

Security Consider -ation	***Preventive Method***
Physical Server Security	i) Determine user authentication and authorization mechanisms. ii) If the server has unused hardware components such as NICs, USB ports, or drives, they should be removed or disabled. This should also be done in the VM (template). iii) Adequate physical security protection including safety of the premises where the server will be housed. iv) Explore the efficacy and feasibility of segregating VMs and creating security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data on separate physical hardware components such as servers, storage, etc. v) Run a host firewall and open only the minimum ports necessary to support the services on an instance.
Hypervi-sor Security	i) security-critical hypervisor updates should be installed at the earliest and the VMs hosted on it should be hardened ii) Hypervisor services like clipboard, if not used, should be disabled. iii) Disable access to the management console to prevent unauthorized access. iv) There must be a separate firewall with strong security installed between the management system and the rest of the network. v)Levels of access should be restricted to selected administrators. vi) VM-specific security mechanisms embedded in hypervisor APIs must be utilized to provide granular monitoring of traffic crossing VM backplanes, which will be opaque to traditional network security controls.
VM Security	i)VM isolation helps in preventing a compromised guest OS from impacting other guest OSs. ii)VMs should be hardened against security threats. Hardening is a process of changing the default configuration in order to achieve greater security iii)Use VM templates to deploy VMs. iv)To avoid DoS attacks, the VM management software should limit the VM's resources so that a single VM is not allowed to consume all of the server's resources. v)Disable unneeded functions and unused devices. vi)Take VM backups on a regular basis and schedule point-in-time snapshots to restore a VM to a safe state, in case of an attack. vii) Perform vulnerability scanning of the guest OS regularly to identify existing vulnerabilities. viii) Validate the history and integrity of any VM image or template originating from the cloud provider before using.
Guest OS and Applicati on Security	i) Hardening will effectively safeguard guest OS and the applications running on it. ii)Disallowing the application from spawning executable files iii) Disallowing the application from creating or modifying executable files iv) Disallowing the application from modifying sensitive areas v)Sandboxing for guest OS and application security. Sandboxing involves isolating execution of an application from other applications in order to restrict the resources that the application can access and the privileges vi) Administrative access and control of virtualized operating systems is crucial, and should include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.

B) *General Recommendations for Compute Level security are*

i) Protect the integrity of the image from unauthorized users.
ii) Secure the private keys in the public cloud.
iii) Keep the decryption keys away from the cloud
iv) Secure the log events to a dedicated log server.
v) Keep the log server separate with higher security protection, including accessing controls.
vi) Have a reporting mechanism in place that provides evidence of isolation and raises alerts if there is a breach of isolation.
vii) Be aware of multi-tenancy situations with VMs where regulatory concerns may warrant segregation.
viii) The access control mechanisms, including role based access control and identity management techniques such as one-time password, identity federation, and OpenID are recommended .
ix) Operational security procedures need to be followed.

VI. CONCLUSIONS

Cloud computing has gained large popularity in the recent years among a wide range of consumers, ranging from small start-ups to multinational companies because of the potential cost savings and gains in IT flexibility. There are a number of security issues in cloud and these depend upon the service provision and deployment models. In order to keep the cloud secure, the security threats need to be controlled at various levels. This paper has highlighted various key security issues and challenges which are currently faced in the cloud computing. It has mainly focused on the compute level security considerations and preventive methods to provide cloud security solutions which prevent the attacks.

REFERENCES

[1] Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* "Cloud Computing Security: From Single to Multi-Clouds"
[2] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Prepared by the Cloud Security Alliance, December 2009.
[3] Rajesh Piplode* Umesh Kumar Singh, *IJARCSSE All Rights Reserved Page | 115* Volume 2, Issue 9, September 2012 ISSN: 2277 128X International Journal of Advanced© *2012.*
[4] Research in Computer Science and Software Engineering; Research Paper " An Overview and Study of Security Issues & Challenges in Cloud Computing"
[5] Security Guidance for Critical Areas of Focus in Cloud Computing V3, Prepared by the Cloud Security Alliance, 2011.
[6] Levels of Security Issues in Cloud Computing, R. Charanya et al. / International Journal of Engineering and Technology (IJET) 2014
[7] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].
[8] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.
[9] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[10] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.
[11] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]
[12] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].
[13] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.
[14] "EMC IT's Journey to the Private Cloud: A Practitioner's Guide"
[15] "Cloud Infrastructure and Services Student Guide", EMC Education Services, May 2, 2013
[16] Anthony T. Velte , "Cloud Computing: A Practical Approach", 1st Edition, Tata Mcgraw Hill Education Private Limited, 2009