Security Aspects of Cloud Computing

Kunal Chadha
Scholar, CSE Department
University of Southern California, USA

Anvita Bajpai
X-Scholar, CSE Department
Marist College,
NY, USA

ABSTRACT

Cloud Computing is the new buzz word in today's computing world. Although there is huge buzz, many people are confused as to exactly what cloud computing is, especially as the term can be used to mean almost anything. The paper is categorized in three parts. The first part of this paper briefly explains the cloud computing model.

The second part of paper follows a discussion on what security threats and challenges pose in front of this technology.

While the final part focuses on how virtualization plays an important role in cloud computing and talks about techniques for securing the virtual machines over the cloud. The paper talks about what assumptions are made by existing kernel integrity-checking mechanisms which may not work in cloud environment and finally discuss an integrity discovery system using secure introspection [1] for virtual environments which ensures high security.

Keywords

Cloud computing, cloud delivery model, cloud deployment model, advantages of cloud, security concern in cloud, security measures in cloud, virtualization and secure introspection.

1. INTRODUCTION

The term cloud computing confuses many people, as the term can be used to mean almost anything. Broadly cloud computing technology describes highly scalable computing resources provided as an external service via the internet on a pay-as-you-go basis. These resources may be in form of servers, software, storage disks or a collection of processing resources.

To understand the cloud it is important to understand the model of cloud.

2. DEFINING THE CLOUD MODEL

NIST working definition of cloud model [5], defines it as a model for enabling omnipresent, 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.

The cloud model Comprises of

i. Essential characteristics.

ii. Delivery models.

iii. Deployment models.

2.1 Essential Characteristics:

Although NIST definition of cloud model defines five, there are broadly six essential characteristics defined for a cloud model:

i. On demand self services: Services such as software, email, server services can be provided without requiring human interaction with each service's provider.

ii. Ubiquitous network access: Cloud services are available over the network and accessed through standard mechanisms such as mobile phones, tablets, laptops and PDAs.

iii. Location independent resource pooling: The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, where different physical and virtual resources are dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services [5].

iv. Rapid elasticity: Cloud services can be rapidly and elastically provisioned. Cloud services can be provisioned to quickly scale up or scale down depending on demand for the service. To the consumer, these services available for provisioning appear to be unlimited and can be purchased in any quantity at any time.

v. Measured service: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Cloud computing services use a metering capability which enables to control and optimize resource use [5]. This implies that IT services are charged per usage metrics – pay per use. IT services such as network security, data hosting, data processing and even software services can be easily delivered as a contractual service.

vi. Multi Tenacity: It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

2.2 Delivery Model:

Delivery model [5] or the Service model of cloud computing defines how cloud services are provided to consumers. It includes:

i. Software as a Service (SaaS): SaaS is a software model provided by the vendor through an online service [4]. Software vendor or cloud's provider provides the infrastructure for running SaaS applications. User does not need to install SaaS application. User may buy license [4] for SaaS application, and access the application via network either mainly through web browser or sometimes other client application. SaaS vendor may charge user based on the product usage. SaaS model can save companies the expense on buying hardware and software and it removes the maintenance costs [4].

ii. Platform as a Service (PaaS): PaaS offers a high-level integrated environment to build, test, and deploy custom applications [3]. The consumer may use programming languages and tools supported by the provider's platform to build their own application in more efficient and quick manner. The provider is responsible for maintenance and control of the underlying cloud infrastructure including network, servers, and operating systems.

iii. Infrastructure as a Service (IaaS): "Iaas provisions hardware, software, and equipments (mostly at the unified resource layer, but can also include part of the fabric layer) to deliver software application environments with a resource usage-based pricing model" [3]. A cloud vendor providing IaaS can rent fundamental infrastructures which include computing resources and storing data to consumer. IaaS vendor may add or remove computing or storage resources instantly (rapid elasticity) when demanded by consumer.

A consumer may choose one or more of these three services simultaneously.

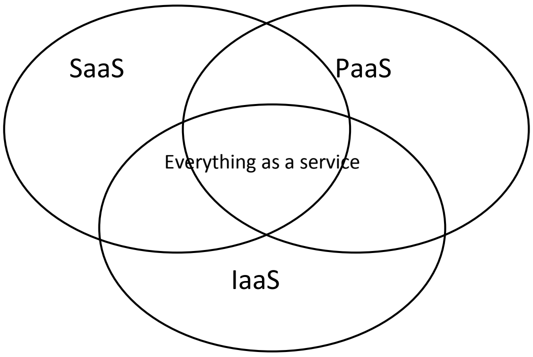

Figure 1: Delivery Model

2.3 Deployment Model:

The deployment model defines how cloud's services are delivered to consumers. It consists of:

i. Public Cloud: Also known as external cloud or multi-tenant cloud. "When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud" [4]. Services on public cloud are made available to the general public or a large industry group. Although service/data is owned by an organization selling the Cloud services, it may be managed by the organization or a third party who works as cloud vendor. Public clouds can host individual services or collections of services, allow for the deployment of service compositions and even entire service inventories.

ii. Private Cloud: Also referred to as internal cloud or on-premise cloud. In a private cloud only the consumers, who belong to the same organization that owns the cloud and have the access to its resources can access service [4]. In other words, the service is managed and operated for one organization only. This is primarily to maintain a consistent level of control over security, privacy and governance.

iii. Community Cloud: Also known as clouds for federated environments. In this cloud computing environments are shared and managed by a number of related organizations participating in a common domain or vertical market. In simple words, organizations that may want to work in collaboration may deploy shared services and data on community cloud. These services are only accessible to consumers who are part of participating organization.

iv. Hybrid cloud: "This cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)" [5].

2.4 Advantages of Cloud:

There are many reasons why organizations of all sizes and types are adopting cloud computing model of IT. It provides a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software [6]. Ultimately, it can save companies a considerable amount of money [6]. Some of the key points of advantage of cloud computing are:

i. Removal/reduction of capital expenditure: Consumers need not invest in infrastructure or buy applications. They may use such services from cloud's vendor.

ii. Reduced administration costs: IT solutions can be deployed extremely quickly and managed, maintained, patched and upgraded remotely by your service provider [6]. Even technical support can be provided by service provider.

iii. Improved resource utilization: Due to rapid elasticity [5] property of cloud computing, service provider may scale up or scale down resources allocated to any service if demand is increased or decreased.

iv. Economies of scale: Cloud computing customers can benefit from the economies of scale enjoyed by providers, who typically use very large-scale data centers operating at much higher efficiency levels, and multi-tenant architecture to share resources between many different customers [6]. This model of IT provision allows them to pass on savings to their customers [6].

v. Scalability on demand: Cloud computing enables customers to react quickly to changing IT needs, adding or subtracting capacity as and when required.

vi. Quick and easy implementation: Consumer may use vendor’s hardware and software resources to develop their solutions in more efficient manner.

vii. Helps smaller businesses compete: ‘Renting’ instead of investing in expensive infrastructures, enable smaller businesses to invest their resources elsewhere, this helps them to compete with big players in industry.

viii. Quality of service: Responsibility is shared between consumer company and cloud vendor.

ix. Guaranteed uptime.

x. Anywhere Access: Services on cloud are accessible everywhere where network can reach.

xi. Technical Support: Vendors may provide technical support, reducing burden from Consumer Company.

xii. Disaster recovery / backup: Also managed by vendor.

2.5 Concerns in Cloud:

Although cloud computing greatly benefits an organization, but cloud computing brings along itself concerns over security. The next section of this paper will discuss security concerns in cloud computing.

3. SECURITY CONCERN IN CLOUD COMPUTING

Cloud-based services and service-oriented solutions deployed on cloud platforms by cloud vendor can be designed to integrate with existing security frameworks of client. However, since some or all parts of the given service composition reside in vendor’s environment, which may not follow security policy as that of client, raises a security concern.

Some of the most common distinct security considerations for cloud-based services and service compositions include the following:

i. Shared and virtualized resources- The service's physical infrastructure, may be shared among multiple tenants.

ii. Data privacy- As data is being hosted in vendor’s data center.

iii. Multi-tenancy- The service hosting processes and the exchanged data are executed and managed in shared environments.

It is also possible that organization’s data might be stored with competitor’s data in shared environment and if there is a bug in vendor’s execution environment, isolation of processes can be breached which may lead to stealing of data.

However cloud computing model uses security services to counter the security threats. The security services can be broadly be classified into Virtualization, Virtual Private Networks (VPN), Federated Identity Services and Policy Services.

The next part of paper will discuss the security measures that are adopted by cloud computing to tackle these security concerns.

3.1 Security Measures in Cloud Computing:

Security in cloud computing is provided broadly by the following services:

i. Virtualization: Each tenant may be given a completely isolated virtual environment to execute.

ii. Virtual Private Network (VPN): Data exchange between cloud provider and user may be secured by using VPN.

iii. Federated Identity: Federated identity is the ability to port data across security domains using claims and assertions from a digitally signed identity provider. Users who already authenticated themselves in the organization’s network should be authorized to services of organization that may be running over the cloud. This is provided by federated identity service, which ties identity management of organization and cloud service provider together.

iv. Policy Services: Defines policies that make assessment to decide which cloud service provider to choose depending of factors like reliability, security, etc.

Each of these services involve various techniques which boost security in cloud environment, the scope of this paper will only include a discussion on “virtualization”.

3.2 Security Measure: Virtualization:

Virtualization is the key to enabling a Cloud Computing environment [1]. In a multi-tenant environment it becomes vital that there is isolation between processes catering to different organizations. A bug in application or operating system can lead to isolation violation. The solution to such a problem to cater multiple organizations (tenants) is either by allocating separate physical machines or simply separate virtual machines.

Virtualization in this situation becomes a more cost effective solution as we may not require entire available resources rather we may only use slice of resources in particular machine.

Apart from isolation, virtualization in cloud also provides other advantages. One of the essential requirements of cloud provider is rapid elasticity, where resources can be added or removed depending on current demand by client organization. Cloud providers can add new virtual servers/machines or remove them easily. Another advantage of virtualization is portability. It is easy to move virtual machines from one physical machine to another, when maintenance work is required.

Un-doughtily, virtualization is adopted by cloud providers. Organizations may deploy security solutions over their virtual image which can provide some level of security even over public clouds. These can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications [7]. Some of these include:

i. Firewall
ii. Intrusion detection and prevention
iii. Integrity monitoring
iv. Log inspection

3.2.1 Firewall:

Firewall is a system designed to prevent unauthorized access to or from a private network. Firewall can help by decreasing the attack surface of virtualized servers in cloud computing environments [7].

Deploying firewall on VM with policies that map to security policy of organization, one may achieve the Virtual Machine isolation, data filtering at fine-grained level of ports, data segregation for analysis covering all IP-based protocols, frame types, etc.. Attacks like Denial of Services (DoS) can be prevented. Firewalls also allow setting different policies over different network interfaces.

3.2.2 Intrusion Detection and Prevention (IDS/IPS):

IDS/IPS can shield vulnerabilities in operating systems and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks [7].

An IDS/IPS can detect newly discovered vulnerabilities in both applications and operating system running in VM. This provides protection against exploits attempting to compromise virtual machines. There are IDS/IPS which are based on artificial intelligence techniques [8] which may learn about new vulnerabilities dynamically.

3.2.3 Integrity Monitoring:

It involves monitoring files, systems and registry for changes. Application files and critical system files (files, directories, registry keys and values, etc.) can be monitored for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

An integrity monitoring solution should enable [7]:

i. On-demand or scheduled detection.

ii. Extensive file property checking, including attributes (enables compliance with PCI 10.5.5)

iii. Directory-level monitoring.

iv. Flexible, practical monitoring through includes/excludes.

v. Auditable reports.

3.2.4 Log Inspection:

Log inspection collects and analyzes operating system and application logs for security events [7]. Rules are defined in log inspection which allows efficient extraction of security related events from multiple log-files. These logs can be sent to a stand-alone security system, or to a Security Information and Event Management (SIEM) system or centralized logging server for analysis [7]. Log inspection software on cloud resources enables suspicious behavior detection. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level.

3.2.5 Secure introspection:

In cloud computing users may move images from one cloud to another, thus an effective solution requires learning what guest operating system (OS) runs in each virtual machine (VM) and secure the guest OS without relying on the guest OS functionality or an initially secure guest VM state [1]. One such solution is secure introspection [1].

While virtualization plays key role in cloud computing, there are a few assumptions which cannot hold true in virtual environment over the cloud. Like for example it cannot be assumed that guest OS is known in advance, as VMs may be configured with any one or more guest OSes [1]. Similarly, assumption that system is monitored continuously from power-on and throughout its lifecycle also doesn’t hold as VMs can be created, cloned, reverted to snapshots and migrated arbitrarily throughout their lifetime [1]. Another assumption that guest system is clean when it starts being monitored doesn’t hold as VMs can come into existence already infected or compromised [1].

Secure introspection technique in [1] proposes an architecture that doesn’t assume any prior semantic knowledge of the guest OS, doesn’t require any prior trust assumptions into any state of the guest VM and has a dedicated guest VM which acts as centralized security manager for all VMs.

The proposed architecture in [1] includes the following:

i. A combination of discovery and integrity measurement of code and data starting from hardware state.

   Integrity measurements are done using whitelists [1] of code executing in the VM, which need to be generated offline once for every supported operating system.

   This technique learns the exact type and version of an operating system running inside a guest VM [1].

ii. As a second application of the secure-introspection infrastructure, there exists a root kit-detection and recovery service, which runs outside the guest VM and uses introspection to identify anomalous changes to guest-kernel data structures [1].

   When a rootkit is detected, it is rendered harmless by restoring the damaged kernel data structures to their valid state.

   This technique has been evaluated with its competing technologies and has been proved to be more efficient.

4. CONCLUSION

Cloud computing is the new buzz in computing world. Cloud-computing although brings lots of advantages to organizations, yet organizations need to carefully study and understand the security measures provided by the cloud service provider.

Virtualization plays a key role in cloud computing. While virtualization provide isolation in multi-tenant environment, some assumptions of virtual machine do not hold true in cloud environment. Such assumptions may pose a security threat. Techniques such as secure introspection [1], builds reliable security model for virtual environments without considering faulty assumptions.

5. REFERENCES

[1] M. Christodorescu, R. Sailer, D.L. Schales, D. Sgandurra, D. Zamboni. “Cloud Security Is Not (Just) Virtualization Security”. Conference on Computer and Communications Security Proceedings of the 2009 ACM workshop on Cloud computing security.

[2] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning. “Managing Security of Virtual Machine Images in a Cloud Environment”. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security

November 2009.Source: ACM Guide to Computing Literature.

[3] I. Foster, Y. Zhao, I.Raicu, S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, 2008.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10, 2009.

[5] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", Jan. 2011, U.S. Department of Commerce.

[6] R. Ferriman, "The benefits of Cloud Computing", White Paper.

[7] Third-Brigade. White Paper: Cloud Computing Secsurity: Making Virtual Machines Cloud-Ready.

[8] A. Kumar, Kunal Chadha, K. Asawa, "Framework for vulnerability reduction in real time intrusion detection and prevention systems using SOM based IDS with Netfilter-Iptables", IJCSIS Vol. 8 No. 4, July 2010 ISSN 1947-5500 International Journal of Computer Science & Information.