International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

A Study on Security Issues and Challenges in Cloud IaaS

D. Sakthivel[1], Dr.B. Radha[2]
[1,2]*Department of Computer Science, Sree Saraswathi Thygaraja College, Pollachi, Tamilnadu - 642006*

Abstract: ***Cloud Computing has remarkable area in conceptual and infrastructural computing. Cloud computing provides user to access and keep their resources in cloud by Multi- tenant architecture. Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. In an IaaS model, a cloud provider hosts the infrastructure components traditionally present in an on-premises data center, including servers, storage and networking hardware, as well as the virtualization or hypervisor layer. Benefits of IaaS are it full control of the computing resources through administrative access to VMs, Flexible and efficient renting of computer hardware and Portability, interoperability with legacy applications. IaaS have some common issues such as Network dependence and browser based risks. It also has some specific issues such as Compatibility with legacy security vulnerabilities, Virtual Machine sprawl and Robustness of VM-level isolation and Data erase practices.***

Keywords: Cloud Computing, Cloud models, Infrastructure Security, Security Management

I. INTRODUCTION

In a general way, we can define computing to mean any goal-oriented activity requiring, benefiting from, or creating computers [1]. Thus, computing includes designing and building hardware and software systems for a wide range of purposes; processing, structuring, and managing various kinds of information; doing scientific studies using computers; making computer systems behave intelligently; creating and using communications and entertainment media; finding and gathering information relevant to any particular purpose, and so on. The list is virtually endless, and the possibilities are vast [7].

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [1]. (e.g networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [7].

A. Essential Characteristics

1) *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 each service provider [1]..
2) *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, tablets, laptops, and workstations) [1].
3) *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 [1]..
4) *Measured Service***:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [1].
5) *Rapid elasticity:* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time [1].
6) *Common Characteristics* [7]
7) Massive Scale
8) Resilient Computing
9) Homogeneity
10) Geographic Distribution
11) Virtualization
12) Service Orientation

13) Low Cost Software
14) Advanced Security

B. Cloud Services Models

1) *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 either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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 [2]. e.g: Google Spread Sheet
2) *Cloud Infrastructure as a Service (IaaS) :* The capability provided to provision processing, storage, networks, and other fundamental computing resources. Consumer can deploy and run arbitrary software [2]. Amazon Web Services and Flexi scale.
3) *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, libraries, services, 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 configuration settings for the application-hosting environment [2].

C. Types of Cloud (Deployment Models)

1) *Private cloud :* The cloud infrastructure is operated solely for an organization. e.g Window Server 'Hyper-V' [3].
2) *Community cloud :* The cloud infrastructure is shared by several organizations and supports a specific goal [3].
3) *Public cloud :* The cloud infrastructure is made available to the general public e.g Google Doc, Spread sheet [3].
4) *Hybrid cloud :* The cloud infrastructure is a composition of two or more clouds (private, community, or public) [3].e.g Cloud Bursting for load balancing between clouds.

II. INFRASTRUCTURE SECURITY

A. Infrastructure Security: The Network Level

With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. Although the organization's IT architecture may change with the implementation of a private cloud, the current network topology will probably not change significantly. There are four significant risk factors in this use case:[4]
Ensuring the confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
Ensuring the availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
Replacing the established model of network zones and tiers with domains

1) *Ensuring Data Confidentiality and Integrity:* Some resources and data previously confined to a private network are now exposed to the Internet, and to a shared public network belonging to a third-party cloud provider
2) *Ensuring Proper Access Control :* Since some subset of these resources (or maybe even all of them) is now exposed to the Internet, an organization using a public cloud faces a significant increase in risk to its data. The ability to audit the operations of your cloud provider's network (let alone to conduct any real time monitoring, such as on your own network), even after the fact, is probably non-existent. You will have decreased access to relevant network-level logs and data, and a limited ability to thoroughly conduct investigations and gather forensic data
3) *Ensuring the Availability of Internet-Facing Resources:* Reliance on network security has increased because an increased amount of data or an increased number of organizational personnel now depend on externally hosted devices to ensure the availability of cloud-provided resources. Consequently, the three risk factors enumerated in the preceding section must be acceptable to your organization.

B. Infrastructure Security: The Host Level

When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models [4] (public, private, and hybrid). Although there are no known new threats to hosts that are specific to cloud

computing, some virtualization security threats—such as VM escape, system configuration drift, and insider threats by way of weak access control to the hypervisor—carry into the public cloud computing environment. The dynamic nature (elasticity) of cloud computing can bring new operational challenges from a security management perspective. The operational model motivates rapid provisioning and fleeting instances of VMs. Managing vulnerabilities and patches is therefore much harder than just running a scan, as the rate of change is much higher than in a traditional data center.

In addition, the fact that the clouds harness the power of thousands of compute nodes, combined with the homogeneity of the operating system employed by hosts, means the threats can be amplified quickly and easily—call it the "velocity of attack" factor in the cloud.

1) *SaaS and PaaS Host Security :* In general, CSPs do not publicly share information related to their host platforms, host operating systems, and the processes that are in place to secure the hosts, since hackers can exploit that information when they are trying to intrude into the cloud service. Hence, in the context of SaaS [4] (e.g., Salesforce.com, Workday.com) or PaaS (e.g., Google App Engine, Salesforce.com's Force.com) cloud services, host security is opaque to customers and the responsibility of securing the hosts is relegated to the CSP. To get assurance from the CSP on the security hygiene of its hosts, you should ask the vendor to share information under a nondisclosure agreement (NDA) or simply demand that the CSP share the information via a controls assessment framework such as SysTrust or ISO 27002. From a controls assurance perspective, the CSP has to ensure that appropriate preventive and detective controls are in place and will have to ensure the same via a third-party assessment or ISO 27002 type assessment framework. Since virtualization is a key enabling technology that improves host hardware utilization, among other benefits, it is common for CSPs to employ virtualization platforms, including Xen and VMware hypervisors, in their host computing platform architecture.
2) *IaaS Host Security :* Unlike PaaS and SaaS, IaaS customers are primarily responsible for securing the hosts provisioned in the cloud. Given that almost all IaaS services available today employ virtualization at the host layer, host security in IaaS should be categorized as follows: Virtualization software security the software layer that sits on top of bare metal and provides customers the ability to create and destroy virtual instances. Virtualization at the host level can be accomplished using any of the virtualization models, including OS-level virtualization (Solaris containers, BSD jails, Linux-VServer), paravirtualization (a combination of the hardware version and versions of Xen and VMware), or hardware-based virtualization (Xen, VMware, Microsoft Hyper-V). It is important to secure this layer of software that sits between the hardware and the virtual servers. In a public IaaS service, customers do not have access to this software layer; it is managed by the CSP only. Customer guest OS or virtual server security The virtual instance of an operating system that is provisioned on top of the virtualization layer and is visible to customers from the Internet; e.g., various flavors of Linux, Microsoft, and Solaris. Customers have full access to virtual servers
3) *Virtual Server Security :* Customers of IaaS have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology. Hence customers are responsible for securing and ongoing security management of the guest VM. A public IaaS, such as Amazon's Elastic Compute Cloud (EC2), offers a web services API to perform management functions such as provisioning, decommissioning, and replication of virtual servers on the IaaS platform. These system management functions, when orchestrated appropriately, can provide elasticity for resources to grow or shrink in line with workload demand. The dynamic life cycle of virtual servers can result in complexity if the process to manage the virtual servers is not automated with proper procedures. From an attack surface perspective, the virtual server (Windows, Solaris, or Linux) may be accessible to anyone on the Internet, so sufficient network access mitigation steps should be taken to restrict access to virtual instances. Typically, the CSP blocks all port access to virtual servers and recommends that customers use port 22 (Secure Shell or SSH) to administer virtual server instances. The cloud management API adds another layer of attack surface and must be included in the scope of securing virtual servers in the public cloud. Some of the new host security threats in the public IaaS include: • Stealing keys used to access and manage hosts (e.g., SSH private keys) Attacking unpatched, vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH) • Hijacking accounts that are not properly secured (i.e., weak or no passwords for standard accounts) Attacking systems that are not properly secured by host firewalls • Deploying Trojans embedded in the software component in the VM or within the VM image (the OS) itself.

III.SECURITY MANAGEMENT IN IAAS CLOUD

Security management focus areas for securing services in the cloud:

Availability management

Access control

Vulnerability management
Patch management
Configuration management
Incident response
System use and access monitoring

A. IaaS Availability Management

Availability considerations for the IaaS delivery model should include both a computing and storage (persistent and ephemeral) infrastructure in the cloud. IaaS providers may also offer other services such as account management, a message queue service, an identity and authentication service, a database service, a billing service, and monitoring services. Hence, availability management should take into consideration all the services that you depend on for your IT and business needs. Customers are responsible for all aspects of availability management since they are responsible for provisioning and managing the life cycle of virtual servers[4].

Managing your IaaS virtual infrastructure in the cloud depends on five factors:

1) Availability of a CSP network, host, storage, and support application infrastructure. This factor depends on the following:
2) CSP data center architecture, including a geographically diverse and fault-tolerance architecture.
3) Reliability, diversity, and redundancy of Internet connectivity used by the customer and the CSP.
4) Reliability and redundancy architecture of the hardware and software components used for delivering compute and storage services.
5) Availability management process and procedures, including business continuity processes established by the CSP.
6) Web console or API service availability. The web console and API are required to manage the life cycle of the virtual servers. When those services become unavailable, customers are unable to provision, start, stop, and deprovision virtual servers.
7) SLA. Because this factor varies across CSPs, the SLA should be reviewed and reconciled, including exclusion clauses.
8) Availability of your virtual servers and the attached storage (persistent and ephemeral) for compute services (e.g., Amazon Web Services' S3† and Amazon Elastic Block Store).
9) Availability of virtual storage that your users and virtual server depend on for storage service. This includes both synchronous and asynchronous storage access use cases. Synchronous storage access use cases demand low data access latency and continuous availability, whereas asynchronous use cases are more tolerant to latency and availability.
10) Examples for synchronous storage use cases include database transactions, video streaming, and user authentication. Inconsistency or disruptions to storage in synchronous storage has a higher impact on overall server and application availability. A common example of an asynchronous use case is a cloud-based storage service for backing up your computer over the Internet.
11) Availability of your network connectivity to the Internet or virtual network connectivity to IaaS services. In some cases, this can involve virtual private network (VPN) connectivity between your internal private data center and the public IaaS cloud (e.g., hybrid clouds).
12) Availability of network services, including a DNS, routing services, and authentication services required to connect to the IaaS service.

B. IaaS Health Monitoring

The following options are available to IaaS customers for managing the health of their service:

Service health dashboard published by the CSP [4].

CID (this database is generally community-supported, and may not reflect all CSPs and all incidents that have occurred).• CSP customer mailing list that notifies customers of occurring and recently occurred outages.

Internal or third-party-based service monitoring tools (e.g., Nagios) that periodically check the health of your IaaS virtual server. For example, Amazon Web Services (AWS) is offering a cloud monitoring service called Cloud Watch. This web service provides monitoring for AWS cloud resources, including Amazon's Elastic Compute Cloud (EC2).

It also provides customers with visibility into resource utilization, operational performance, and overall demand patterns, including metrics such as CPU utilization, disk reads and writes, and network traffic.

Web console or API that publishes the current health status of your virtual servers and network.

Similar to SaaS service monitoring, customers who are hosting applications on an IaaS platform should take additional steps to monitor the health of the hosted application. For example, if you are hosting an e-commerce application on your Amazon EC2 virtual cloud, you should monitor the health of both the e-commerce application and the virtual server instances.

C. Access Control: IaaS

IaaS customers are entirely responsible for managing all aspects of access control to their resources in the cloud. Access to the virtual servers, virtual network, virtual storage, and applications hosted on an IaaS platform will have to be designed and managed by the customer [5]. In an IaaS delivery model, access control management falls into one of the following two categories:

CSP infrastructure access control

Access control management to the host, network, and management applications that are owned and managed by the CSP

Customer virtual infrastructure access control

Access control management to your virtual server (virtual machines or VMs), virtual storage, virtual networks, and applications hosted on virtual servers

1) *CSP infrastructure access control:* The CSP is responsible for managing access control to the administrative network that is used to perform administrator functions. This includes access control to administrative processes, such as backups, host (hypervisor) and network maintenance, router and firewall policy management, and system monitoring and management. Access to administrative functions should be protected using strong authentication and role-based access control. Strong operational procedures should be implemented to support the provisioning and revocation of administrative privileges. Periodic access control audits and administrative user certifications should be implemented to validate least privileges and separation of duties. In this regard, the aforementioned AWS security white paper states that: Amazon. com's Information Security Policies, followed by AWS, are guided by the fundamental principle of least privilege. Least privilege protects customer information assets by requiring that no individual, program or system is granted more access privileges than are necessary to perform the task. Any employee found to have violated this policy may be subject to disciplinary action, including termination [5].
2) *Customer virtual infrastructure access control:* To start with, IaaS customers must understand the virtual resources (network, host, firewall, load balancers, management console, etc.) and the available protection mechanisms to restrict access to authorized users. It is not uncommon for CSPs to provide customers with full root access and administrative control over rented virtual servers. In addition, customers can be assigned privileges to manage network access policies for both the ingress and egress of their virtual network and virtual servers. Hence, the customer is responsible for taking the necessary steps to protect access to virtual resources.

D. Network Access Control

Check with the provider on the default configuration of the network access that is typically enforced by a firewall managed by the CSP. It is customary for CSPs to deny all access to your virtual servers by default (factory settings), which automatically denies all inbound traffic to your virtual servers. This forces you to explicitly add new rules to allow access to your virtual servers in the cloud—for example, allow access to IP 10.0.0.1 from 192.168.0.1 to port 22 (Secure Shell or SSH), where 10.0.0.1 is the IP address of the virtual server and 192.168.0.1 is the trusted IP address from which 10.0.0.1 can be accessed using SSH. Amazon EC2 offers network group features that allow the creation of multiple security groups to enforce different ingress policies as needed. According to Amazon, a customer can control each security group with a PEM-encoded X.509 certificate and restrict traffic to each EC2 instance by protocol, service port, or source IP address.

E. Virtual Server Access Control

Virtual servers running your preferred OS [6](Linux, Solaris, or Windows) should be protected with access controls, such as OS authentication mechanisms. It is a standard practice to configure Unix servers with SSH-based logins with strong authentication. Strong authentication protects against several security threats (e.g., IP spoofing, fake routes, man-in-the-middle, and DNS spoofing). The authentication methods include Rivest-Shamir-Adleman (RSA) encryption algorithm-based host authentication, pure RSA authentication, one-time passwords with S/Key, and authentication using Kerberos. When using RSA keys, it is recommended that the keys are stored in a secure form of media and that they are secured with a passphrase. These measures help to protect your keys from unauthorized users.

F. Cloud Management Station

Management of your virtual resources on the cloud is usually accomplished from a client system with applications that manipulate remote resources using a CSP-proprietary API [6](REST, SOAP, or HTTP with XML/JSON). A client management toolkit (supplied by the CSP) is installed on the management station, which interacts with the CSP management service via the published API. Because the station contains sensitive information, including host and user keys, and firewall policies, the cloud management station should be viewed as a command and control center for the cloud infrastructure. Hence, access to the management station should be protected with strong authentication and sound access provisioning procedures.

G. Web-Based Console

Some CSPs supplement the cloud management station with a web-based console feature by which customers can manage access to their virtual infrastructure in the cloud [6]. The console offers an alternative means to the cloud management station for managing the cloud infrastructure. Similar to the management station, the console offers access to sensitive information, including access to your host keys and firewall policies with just a few mouse clicks; it acts as a management station for your cloud infrastructure. Because the web console is a powerful tool that can control your virtual network and virtual server instances, you should adequately protect console access. For example, the web console should be accessed only with HTTPS protocol.

IV. CONCLUSION AND FUTURE WORK

Ensuring security of cloud data is still a challenging problem. Cloud service providers as well as other third parties use different various techniques to acquire valuable information from user data hosted on the cloud. In this paper, we have discussed the impact of Infrastructure security and management of security in Iaas. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has bright future.

REFERENCES

[1] Cloud Computing Principles and paradigm by A.John Wiley & sons,Inc.,201
[2] Introduction to Cloud Computing Architecture by Sun Microsystems,Inc., june 2009
[3] Amazon Web Services: Overview of Security Processes, may 2011.
[4] Cloud Security and Privacy by O'Reily,Inc.,September 2009
[5] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-molina, K. Kenthapadi,R. Motwani, U. Srivastava, D. Thomas, and Y. Xu. Two can keep a secret: A distributed architecture for secure database services. In In Proc. CIDR, 2005
[6] Wikipedia, "Cloud computing," http://en.wikipedia.org/wiki/ Cloud_computing
[7] Tutorialspoint, "Cloud computing," https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm

.