Paper ID: NITETCSE02

CLOUD INFRASTRUCTURE SECURITY AT DIFFERENT LAEVELS

Kavita M. Sunchu
ME *(Computer Science and Engineering)
Shriram Intitute of Engineering and Technology Center,
Paniv, Malshiras. India Kavita4.kamuni@gmail.com

Prof. Dhainje P.B.
Ph.D *(CSE) Shriram Intitute of Engineering and Technology Center,
Paniv, Malshiras, India dhainjeprakash@gmail.com

ABSTRACT

Cloud Computing is the collection of different types of hardware and software which delivers many services to the end-user over a network (typically the Internet). With cloud computing, users can access files and use applications from any device that can access the Internet. Now a day's cloud computing becomes more popular due to its few important attributes: multitenancy (single instance of software is used to run a service for multiple clients), massive scalability, elasticity, pay-per-use, and self-provisioning of resources. Cloud computing also delivers different types of services like Software-as-a-Service (SaaS), Platform-as-a-Services (PaaS) and Infrastructure-as-a-Services (IaaS). The current paper discussed infrastructure security at different levels: such as Application level, Host level and network level [1][6][9]l.

KEY WORDS — Saas, Paas, Iaas, Private, Public, Hybrid cloud, Application level, Network level, Host level, Computing, Cloud Computing Security.

INTRODUCTION

The cloud is a collection of different types of hardware and software resources that work combinelly to deliver many services of computing to the user as an online service (typically over the Internet). Through cloud computing, users can access any files and use different applications from any device that can connected to the Internet. Today's small and medium scale companies are moving towards cloud computing due to many reason like reduction in hardware, maintenance cost, pay-as-per-use, scalability, accessible location independent, on-demand security controls facility , fast deployment, flexibility and the highly motorized process [1].

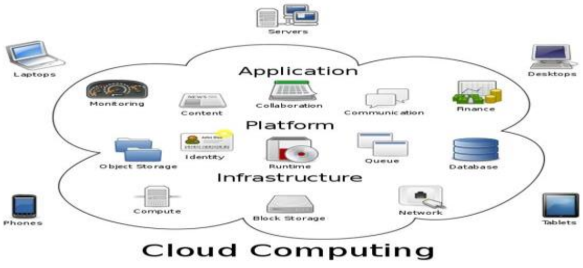

Fig 1: Cloud Computing

Cloud Computing refers to creating, organizing, and accessing the applications over a internet. It provides a facility of infrastructure, data storage, and application online [8].

CLOUD COMPUTING DEFINED

Our definition of cloud computing is based on five attributes:

1. Multitenancy : It is depends on a business model in which resources are shared i.e. Multiple users can use the same resource at the network, host, and application level [9].
2. Massive scalability: Many organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as it scales bandwidth and storage space [9] [6].
3. Elasticity : Users can rapidly add and remove their processing resources as per their need and release resources for other uses when they are no longer required [9] [6].
4. Pay-as-per-use: Users can pay for only the resources they are actually used and time they require resources [6] [9].
5. Self-provisioning of resources: Users add additional systems and network resources [9].

SPI FREAMEWORK

1. Software-as-a-service (SaaS)
2. Platform-as-a-service (PaaS)
3. Infrastructure-as-a-service (IaaS).

A. SOFTWARE-AS- A- SERVICE(SAAS)

This model provides software application as a service to the end users. There are several SaaS applications; some of them are listed below:

APPLICATIONS

- Billing and Invoicing System
- Customer Relationship Management (CRM)
- Help Desk Applications
- Human Resource (HR) Solutions [6]

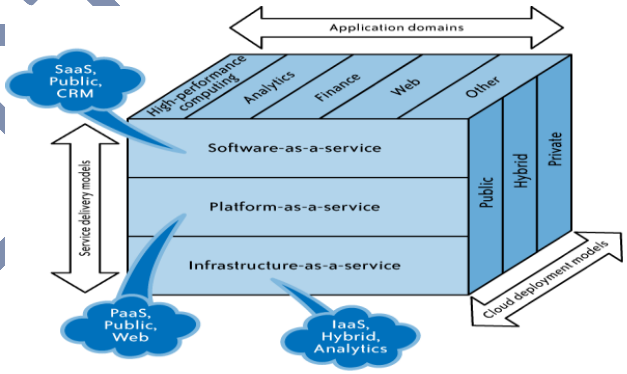

Fig 2: SPI service model

CHARACTERISTICS

- SaaS makes the software available over the Internet.
- The Software are maintained by the vendor rather than where they are running.
- The license to the software may be subscription based or usage based
- SaaS applications are cost effective since they do not require any maintenance at end user side.
- They are available on demand.

- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SaaS offers share data model. Therefore, multiple users can share single instance of infrastructure. All users are running same version of the software[1][6].

BENEFITS

SaaS provides benefits in terms of efficiency, scalability, performance and much more. Some of the benefits are as below:

- Modest Software Tools
- Efficient use of Software Licenses
- Centralized Management & Data
- Platform responsibilities managed by provider
- Multitenant solutions [1] [6].

B. PLATFORM-AS-A-SERVICE (PAAS)

PaaS offers the runtime environment for applications. It also offers development & deployment tools, required to develop applications [1] [6].

BENEFITS

- LOWER ADMINISTRATIVE OVERHEAD
- LOWER TOTAL COST OF OWNERSHIP
- SCALABLE SOLUTIONS
- MORE CURRENT SYSTEM SOFTWARE

TABLE 1: Cloud Service Delivery Model

Service Models	Services	Example	Service Providers	Advantage
Saas (Consume)	Software is offered as Service and delivered through a browser	Excel, WebPage, CRM, ERP Access, SQL Server	GoogleApps Salesforce.com	Reduce the cost Centralized control
Paas (build on it)	Enables developers to write applications without installing any tools in local system but run on the cloud.	Scripting Coding ,Coding and integration	AppEngine Azure Engine Yard Force.com	Scalability, Reliability and security Pay-per-use
Iaas (Migrate to it)	Computing infrastructure is rented to the user	Infrastructure Scalability & Availability	Amazon EC2,S3 GoGrid Linode Rackspace	Scalability Pay as you go Best-of-breed technology and resources

C. INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS provides access to necessary resources such as physical machines, virtual machines, virtual storage, etc., Apart from these resources, the IaaS also offers:

- Virtual machine disk storage
- Virtual local area network (VLANs) [1] [6] [9]

BENEFITS

- Full Control of the computing resources through Administrative Access to VMs.
- Flexible and Efficient renting of Computer Hardware.
- Portability, Interoperability with Legacy Applications [1] [6] [9].

DEPLOYMENT MODEL

A. Private Cloud: A private cloud involves a distinct and secure cloud based environment in which only the specified client can operate. However, private cloud model is only accessible by a single organization. So private clouds provides benefits like higher security and privacy, more control, cost and energy efficiency, improved reliability. [12]

B. Public Cloud: According to the document SP800-145, from NIST. “A public Cloud infrastructure is provisioned for open use by the general public which may be processed, managed and operated by commercial businessman, academic or government organization and exists in the place of cloud provider”[8].

C. Hybrid Cloud: This type of cloud is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but can share data if required.

D. Community Cloud: The cloud infrastructure is shared by many organizations and supports a specific community that has shared concerns (E.g.: mission, policy, security required). It may be managed by organization or trusted third party [8].
The below figure 4 shows the basic structure of Deployment Models [8].

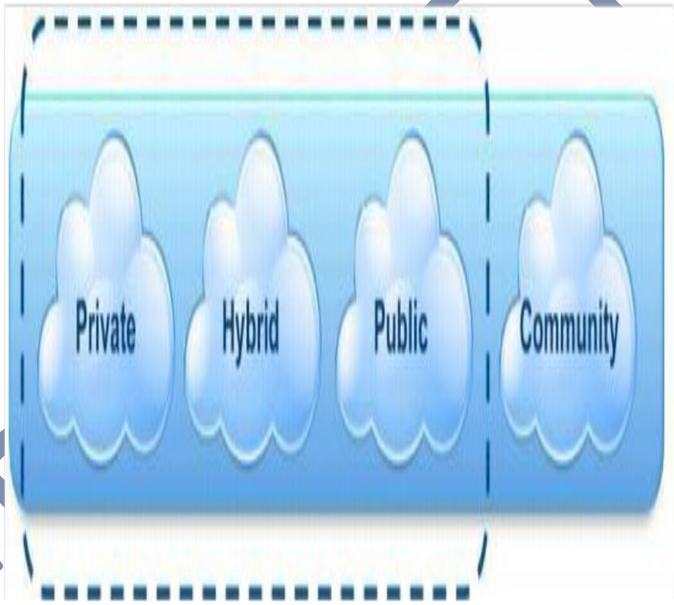

Figure 4: Cloud Deployment Models

INFRASTRUCTURE SECURITY AT DIFFERENT LEVELS

A. The network level

B. The host level

C. The application level

TABLE II: Different types of attack and preventive method

Security problem	Attacks	Attack type	Preventive Method
Network Level	DNS attack	Sender and a receiver get rerouted through some evil connection.	Domain name system security Extensions (DNSSEC) reduces the effects of DNS threats.
	Eavesdropping	Attacker monitor network traffic in transit then interprets all unprotected data	Methods of preventing intruders are Internet protocol security(IP sec) Implement security policies and procedures install anti-virus software
	Dos Attack	Prevent the authorized user to accessing services on network	DoS attacks can be prevented with a firewall but they have configured properly Enforce strong password policies
	DDoS	Attack against a single network from multiple computers or systems	Limit the number of ICMP and SYN packets on router interfaces.
	Sniffer Attack	Data is not encrypted & flowing in network, and chance to read the vital Information.	Detect based on ARP and RTT. Implement Internet Protocol Security (IPSec) to encrypt network traffic System administrator can prevent this attack to be tight on security, i.e one time password or ticketing authentication
	Issues of reused IP addresses	IP address is reassigned and reused by other customer. The address still exists in the DNS cache.	Old ARP addresses are cleared from cache
	BGP Prefix Hijacking	network attack in which wrong announcement on IP address associated with a autonomous system.	Filtering and MD5/TTL protection(preventing the source of most attacks)
Host Level	hypervisor .	Single hardware unit is difficult to monitor multiple operating systems. code get control of the system and block other guest OS	Malicious Hook safe that can provide generic protection against kernel mode root kits
	Securing virtual server	Self-provisioning new virtual servers on an IaaS platform creates a risk that insecure virtual servers	Operational security procedures need to be followed
	Cookie Poisoning	Unauthorized person can change or modify the content of cookies	Cookie should be avoided, or regular Cookie Cleanup is necessary.
	Backdoor and debug options	Debug options are left enabled unnoticed, it provide an easy entry to a hacker into the web-site and let him make changes at the web-site level	Scan the system periodically for SUID/SGID files Permissions and ownership of important files and directories periodically
Application level	Hidden field manipulation	Certain fields are hidden in the web-site and it's used by the developers. Hacker can easily modify on the web page.	Avoid putting parameters into a query string
	Dos Attack	Services used by the authorized user unable to be used by them.	Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks .Preventive tools are Firewalls,Switches,Routers,
	DDoS	DDoS attack results in making the service unavailable to the authorized.	Preventive tools are firewalls, Switches, Routers, Application front-end hardware, IPS based Prevention, etc.
	Google Hacking:-	Google search engine Best option for the hacker to access the sensitive information	Prevent sharing of any sensitive information Software solution such as Web Vulnerability Scanner
	SQL injection	Malicious code is inserted into a standard SQL code and gain unauthorized access to a database	Avoiding the usage of dynamically generated SQL in the code
	Cross site Scripting attak attacks	Inject the malicious scripts into web contents.	Various techniques to detect the security flaws like: Active Content Filtering, Content Based Data Leakage Prevention Technology.

A. INFRASTRUCTURE SECURITY: THE NETWORK LEVEL

As network level of infrastructure security is concerned , it is important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. If public cloud services are chosen, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account [2].

There are four significant risk factors in this use case:

1. Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider
2. Ensuring proper access control
3. Ensuring the availability of the Internet-facing resources
4. Replacing the established model of network zones and tiers with domains.[2]

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 public, private, and hybrid) should be considered [2]. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services. IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (virtualization software security, customer guest OS or virtual server security) [2].

C. INFRASTRUCTURE SECURITY - THE APPLICATION LEVEL

Software security or applications should be a crucial element of a security program. Most enterprises with information security programs have yet to introduce an application security program to address this domain. Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reexamine current practices and standards. The application security spectrum ranges from single-user applications to multiuser e-commerce applications used by many users.

The level is responsible for managing [7], [`10],[11]:
_ Application-level security threats;
_ End user security;
_ SaaS application security;
_ PaaS application security;
_ Customer-deployed application security
_ IaaS application security
_ Public cloud security limitations

THE IMPACT OF CLOUD COMPUTING ON USERS

This section describes the impact of cloud computing on different types of users:

- Individual consumers
- Individual businesses
- Start-ups
- Small and medium-size businesses (SMBs)
- Enterprise businesses [9]

CLOUD COMPUTING APPLICATIONS

A. Business Applications: Mail Chimp, Chatter, Google Apps for business, and Quickbooks.
B. Data Storage and Backup : Box.com, Mozy, Joukuu
C. Management Applications:time tracking, organizing notes.
D. Social Applications: Facebook, Twitter, etc.
E. Entertainment Applications :Audio box.fm, music files
F. Art Applications: Moo offers art services such as designing and printing business cards, postcards and mini cards. [7]

CONCLUSION

This paper discussed about various services provided by cloud and Infrastructure security at different levels. In order to provide security to cloud at different levels the security threads must be controlled. Today, security is mainly considered due to increasing availability of cloud. Security in cloud computing covers security threats and challenges in network level, host level and application level are identified and finds the solution to prevent from the attacks. So regularly checking should be performed to secure the cloud from external attacks. Table II listed different types of attacks at different levels and their preventive methods.

REFERENCES

[1] R. Charanya, M.Aramudhan, K. Mohan, S. Nithya, “Levels of Security Issues in Cloud Computing” International Journal of Engineering and Technology (IJET), ISSN: 0975-4024, Vol 5 No 2 Apr-May 2013,Page-1912.
[2] Dimiter Velev1 and Plamena Zlateva2,” Cloud Infrastructure Security”,page 1- 9.
[3] Sonali Ghodke,” An Overview of Application Security in the Cloud “,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015 ISSN: 2277 128X.
[4] Raj Kumar,” Research on Cloud Computing Security Threats using Data Transmission”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015 ISSN: 2277 128X.
[5] Pankaj Arora, Rubal Chaudhry Wadhawan ,Er. Satinder Pal Ahuja,” Cloud Computing Security Issues in Infrastructure as a Service “, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X .
[6] http://www.tutorialspoint.com//cloud_computing/index.htm.
[7]http://www.tutorialspoint.com/cloud_computing/cloud_computing _applications.htm.
[8]http://www.tutorialspoint.com/cloud_computing/cloud_computing_quick_guide.htm.
[9] Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.
[10] Reese, G.: Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly Media, Inc., 2009.
[11] Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management and Security. CRC Press, 2009.
[12]http://www.interoute.com/cloud-article/what-private-cloud.