Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.707 – 711

RESEARCH ARTICLE

Infrastructure as a Service: Security Issues in Cloud Computing

P. R. Jaiswal[1], A. W. Rohankar[2]

[1]Sinhgad College of Engg, I.T. Department, University of Pune, India

[2]Sinhgad College of Engg, I.T. Department, University of Pune, India

[1] pavan.jaiswal85@gmail.com; [2] rohankar@sinhgad.edu

Abstract— Cloud computing is current trend in market. It allows resources to be leveraged on per-use basis. It reduces cost and complexity of service providers by means of capital and operational costs. It allows users to access applications remotely. On behalf of user, this construct directs cloud service provider to handle cost of servers, software updates, etc. For both, cloud providers and consumers; integrity, availability, confidentiality, authenticity and privacy are important concerns. Infrastructure as a Service (IaaS) serves as foundation layer for many other delivery models. This paper presents detailed study of IaaS and its components. We present how security at IaaS layer need to be handled carefully as delivery models- Platform as a Service (PaaS) and Software as a Service (SaaS) are built upon IaaS layer. We focus how IaaS security issues- data protection & usage monitoring, end-to-end logging & reporting, infrastructure hardening and end-to-end encryption need to be resolved.

Keywords – cloud computing; deployment models; service level agreement; utility computing; privacy

---

I. INTRODUCTION

Cloud is referred as large pool that holds easily accessible and usable virtualized resources [1]. To manage variable load and optimum usage, these resources are reconfigured dynamically. Cloud computing incorporates Internet delivery of services, virtualization, open source software, on demand deployment, etc. Cloud computing is a paradigm that uses Internet and central servers to maintain data and applications which in turns allows efficient computing.

In this paper, section II present cloud computing services, section III present cloud computing security issues, section IV describe cloud computing models, section V focus on IaaS components and section VI present IaaS security.

II. CLOUD COMPUTING SERVICES

A. Infrastructure as a Service

In IaaS model, Cloud Service Provider (CSP) outsources storage, servers, hardware, networking components, etc. to the consumer. CSP owns the equipment and responsible for housing, running and maintaining it. In this model, consumer pays on per-use basis. Characteristics and components of IaaS include: Policy-based services

1. Dynamic scaling
2. Automation of administrative tasks
3. Utility computing service and billing model
4. Internet connective
5. Desktop virtualization

Amazon Web Services (AWS) which gives IaaS also provides block of storage on demand and virtual server with unique IP addresses. AWS provides consumer an Application Program Interface (API) to start, stop, access, and configure the

virtual server and storage. Sometime IaaS is referred as Hardware as a Service (HaaS).

B. Platform as a Service

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over an Internet [1]. PaaS is an outgrowth of SaaS that allows hosted software applications to be made available to consumer over an Internet. Developer gets many advantages from PaaS. With PaaS, OS can be changed and upgraded as many times as needed. PaaS allows geographically distributed teams to work together on software development projects. CSP have crossed international boundaries for providing on-going and demanded services to consumers.

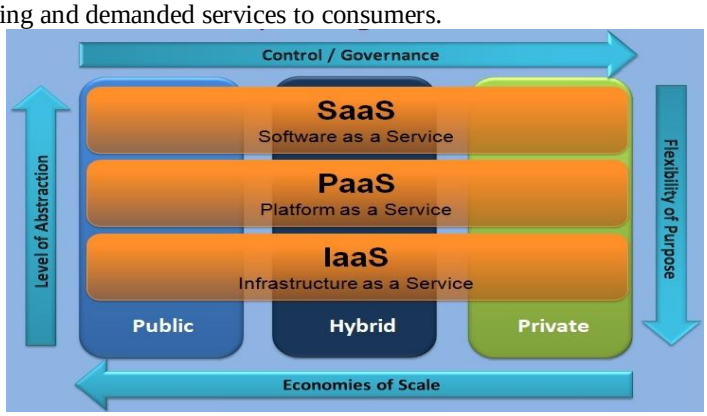

Fig. 1 Cloud computing service models

C. *Software as a Service*

Software as a service sometimes referred to as "software on demand," is software that is deployed over an Internet. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or at no charge. This approach is the part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service. SaaS was initially widely deployed for sales force automation and Customer Relationship Management (CRM). Now it has become commonplace for many business tasks, including computerized billing, invoicing, human resource management, financials, document management, service desk management and collaboration.

III. CLOUD COMPUTING SECURITY ISSUES

In past few years, cloud computing has grown to one of the fastest growing segments of IT industry. But this growth need cloud security to be intact. Below mentioned are few most important issues of cloud computing.

A. Privacy

Cloud computing utilizes virtual computing technology. In this, user's personal data is kept on various virtual data centres which may cross international boundaries. This is where data privacy protection may face controversy of various legal systems. There might be few chances that un-legitimate user may leak hidden information, which in turns compromises privacy of data.

B. *Securit***y**

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Open Standard

In cloud computing, open standards are critical to grow. Many CSP provides well documented APIs which are unique to their implementation and thus difficult to interoperable. Towards the progress, there are many open standards are under development; OGF's Open Cloud Computing Interface is one of them. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

E. *Long-Term Viability*

should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

F. Freedom

In cloud computing, users are not permitted to physically possess storage of data, leaving data storage and control the data. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring .

G. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centres maintained by cloud providers may also be subject to compliance requirements.

IV. CLOUD COMPUTING MODELS

A. Public Cloud

Public cloud makes use of standard cloud computing model and makes resources available to public over an Internet. Public cloud services may be offered on pay-per-usage basis or may be free.

Benefits of public cloud:

1. Due to pay-per-usage, no wastage of resources.

2. Inexpensive setup as setup cost is managed by provider.

3. Easily accessible, etc.

B. Private Cloud

Private cloud is a cloud infrastructure operated for single organization [2]. It may be managed internally or by third party and hosted internally or externally. This kind of setup can grow business if security issues are handled carefully. It has significant footprint in terms of equipment setup and environmental controls. It costs additional capital expenditure as assets have to be refreshed periodically. Private cloud is also referred as internal cloud or corporate cloud.

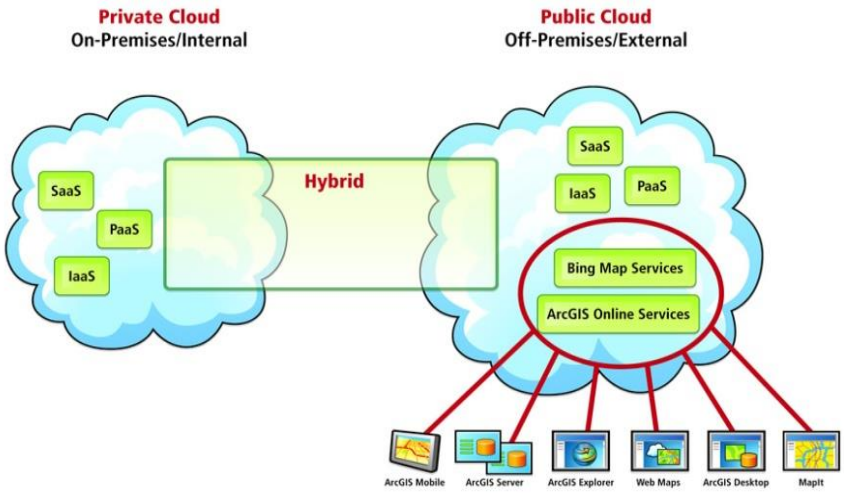

Fig. 2 Cloud computing types

C. Community Cloud

Community cloud is multi-tenant infrastructure shared amongst several organizations from specific group with common concerns. Concerns might be related to regulatory compliance, performance requirements, etc [3]. The goal of community cloud is to have participating organizations realize the benefits of public cloud with the added level of privacy which is usually associated with private cloud. It can be on-premises or off-premises and can be governed by participating organizations or by third party managed service provider (MSP).

D. Hybrid Cloud

Hybrid cloud is integrated cloud service utilizing both private and public clouds to perform distinct functions within organization [4]. In practice, an enterprise cloud implement hybrid cloud hosing to host their e-commerce website within a private cloud, where it is secure and scalable, but their brochure site is in public cloud, where it is more cost effective.

V. IAAS COMPONENTS

In past decade, several components of IaaS delivery model have been developed; nevertheless employing those components together in shared and outsourced environment carries multiple challenges. Security and privacy are most significant challenges amongst them. Breaching the security of any components may compromise the entire system's security. In this section we study the security issues of each component and discuss the proposed solutions and recommendations.

A. Service Level Agreement (SLA)

Cloud computing emerges a set of IT management complexities. SLA provides solution to these complexities, which in turns guarantees acceptable level of quality of service (QoS). SLA consists of SLA contract definition, SLA monitoring, SLA negotiation and SLA enforcement [5]. Contract definition and negotiation stage determines the benefits and responsibilities of each party. Any misunderstanding amongst the parties may affect the system's security and may leave client exposure to vulnerabilities. Apart from this, monitoring and enforcing SLA is crucial as it builds trust between provider and client.

To enforce SLA in dynamic environment, QoS attributes needs to be monitored continuously [6]. WSLA – Web Service Level Agreement, which manages SLA in cloud environment, was proposed by delegating SLA monitoring and enforcement tasks to third party to solve trust problems. Currently, client have to trust provider's SLA monitoring until standardizing cloud computing systems and delegating third parties to mediate SLA monitoring and enforcement.

B. Utility Computing

Utility computing played important role in grid computing deployment. It packages the resources, for e.g. hardware, bandwidth, storage, computation, etc., as metered services and delivers it to client. Firstly, it reduces total cost because of pay-per-usage basis and secondly, it has been developed to support scalable systems. Here scalability refers to rapid growing system in which owner need not to bother about denying services due to rapid increase of users or reaching peak in demands.

The first challenge to the utility computing is the complexity of cloud computing. For example, the higher provider as Amazon must offers its services as metered services. These services can be used by second level providers and provided as metered services to client. Amazon DevPay5 allows second level provider to meter the usage of AWS services and bill the client accordingly. The second challenge is that, utility computing systems can be attractive targets of attackers. Attacker may aim to access services without paying or can go further to drive specific client bill to unmanageable level. In such cases, keeping system healthy and well-functioning is a responsibility of provider.

C. Cloud Software

There are many open source cloud software implementations are available in the market, for e.g. Eucalyptus, Nimbus 6, etc., which joins the cloud component together. Cloud software can be either open source or commercially close source. In the both the cases we cannot ensure vulnerabilities and bugs in available software. Furthermost to perform most management functions, cloud providers have furnished APIs. For example, to consume the services by implementing own application, one can use Amazon's EC2 toolkits or simply use web interfaces offered by provider. In both cases, client uses web service protocols. SOAP is one of the most supported protocols for web services. Many SOAP based security solutions are researched, developed and implemented. WS-Security, a standard extension for security in SOAP, addresses the security for web services. It determines SOAP header that carried WS-Security extensions and determines how existing XML security standards like XML signature and XML encryption are applied to SOAP massages. Indeed, there are attacks those belong to web service world, but as a technology used in cloud computing, web services security strongly influences the cloud service's security.

D. Platform Virtualization

Virtualization a fundamental technology platform for cloud computing services, facilitates aggregation of multiple standalone systems into a single hardware platform by virtualizing the computing resources. Virtualization provides multi tenancy and scalability, which are significant characteristics of cloud computing. As hypervisor is responsible for virtual machine (VM) isolation, no VM is able to access directly any others virtual disk or memory or application on the same host. IaaS, a shared environment, demands an accurate configuration to maintain strong isolation. CSP undertakes substantial efforts to reduce threats resulting from monitoring, communication, notification, migration, mobility and DOS.

VI. IAAS SECURITY

Till this section, we understood cloud computing and its models. Now in this section we present security in regard to IaaS. Most admins will be comfortable and familiar with IaaS because it is similar to work that we do in data centres [7]. We save on energy cost by deploying server consolidation plan to reduce physical server footprint in data centre. After server consolidation, cloud features like – self-service, automation is used. But before these features are actually used, various security implications of IaaS need to be considered. Security issues are varied depending on whether we use public cloud or private cloud implementation of IaaS. With private cloud, we have control over solutions from top to bottom. With IaaS in public cloud, we control VMs and services running on VMs. For both scenarios, we consider the following security issues:

A. Data Leakage Protection and Usage Monitoring

Data stored in IaaS infrastructure in both private and public cloud needs to be monitored closely [8]. This is essential when IaaS is deployed in public cloud. In this, it should be known that who is accessing the information, how it is accessed, location from where it is accessed and what happened to accessed information later. These problems can be solved by using modern Rights Management services applying restriction to business critical data. Policies for information need to be created and deployed. In addition, transparent process can be created that monitors information usage.

B. End to End Logging and Reporting

The effective deployment of IaaS demands comprehensive logging and reporting in place. Robust logging and reporting solutions helps to keep track of where the information is, who accesses it, which machines are handling it and which storage arrays are responsible for it. These solutions are important for service management and optimization.

C. Authentication and Authorization

Robust authentication and authorization helps to get effective Data Loss Prevention (DLP) solution. For every application, just user name and password is not most secure authentication mechanism. Sometime two factor or multi-factor authentication is needed [9]. We need to consider tiering access policies based on level of trust.

D. Infrastructure Hardening

"Golden-image" VM and VM templates need to be hardened and cleaned [10]. This can be done while images are created. On regular basis, testing of these master images need to be done.

E. End to end encryption

IaaS as a service, both in public and private clouds, needs to take advantage of encryption from end-to-end. We can make use of whole disk encryption to encrypt all the data including user files on the disk. This prevents offline attacks. In addition to disk encryption, all communications to host OS and VMs in the IaaS infrastructure are encrypted. This can be done over SSL/TLS or IPSec.

VII. CONCLUSION

In this paper we presented that cloud computing is more than just server virtualization. There are service models for cloud computing: SaaS, PaaS and IaaS and there are (at least) three deployment models: public cloud, private cloud and hybrid cloud. We presented IaaS components: SLA, utility computing, cloud software and platform virtualization. When deploying IaaS solution, there are a number of security issues that need to be considered for both private cloud IaaS and public cloud IaaS that we highlighted in this paper.

RFERENCES

[1]http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html

[2]http://en.wikipedia.org/wiki/Cloud_computing#Private_cloud

[3]http://searchcloudstorage.techtarget.com/definition/community-cloud

[4] http://www.interoute.com/cloud-article/what-hybrid-cloud

[5] F. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[6] "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009.

[7] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, *On Technical Security Issues in Cloud Computing*. IEEE, 2009.

[8] Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009.

[9] E. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud- Computing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.

[10] T. Garfinkel and M. Rosenblum, "When virtual is harder than real:security challenges in virtual machine based computing environments," Proceedings of the 10th conference on Hot Topics in Operating Systems –Volume 10, 2005.

