INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1355 - 1360
RECEIVED : 29/10/2016. PUBLISHED: 16/11/2016
November 16, 2016

SURVEY ON CLOUD TAAS IN PUBLIC CLOUD SERVER

[1]R.Yaminipriya, [2]Dr.S.V.Sudha,
[1]PG Scholar, Dept of Computer Science and Engineering, Dr.N.G.P Institute of Technology, Coimbatore,
[2]Professor & Head, Dept of Computer Science and Engineering, Dr.N.G.P Institute of Technology, Coimbatore.

Abstract:

Software Testing is a challenging activity for many software engineering projects and it is one of the five main technical activity areas of the software engineering lifecycle that still poses substantial challenges. Testing software requires enough resources and budget to complete it successfully. But most of the organizations face the challenges to provide enough resources to test their software in distributed environment, with different loading level. This leads to severe problem when the software deployed into different client environment and varying user load. Cloud computing is a one of the emerging technology which opens new door for software testing. This paper investigates the software testing in cloud platform which includes cloud testing models, recent research work, commercial tools and research issues.

Keywords : Software Testing, Cloud Testing, Testing Tools

1. INTRODUCTION

Software testing is an integral and important phase of the software development process. Testing requires expensive dedicated infrastructure and resources that were only used sporadically which scrutinizes the application's performance, reliability, speed, security and functionality. Since, business applications are growing in complexity, it is somewhat difficult for organizations to build and maintain in-house testing facilities that imitate real-time environments. This is where cloud testing has emerged as a fresh approach to testing where cloud computing environments are leveraged to simulate real-world user traffic by significantly decreasing costs [1].

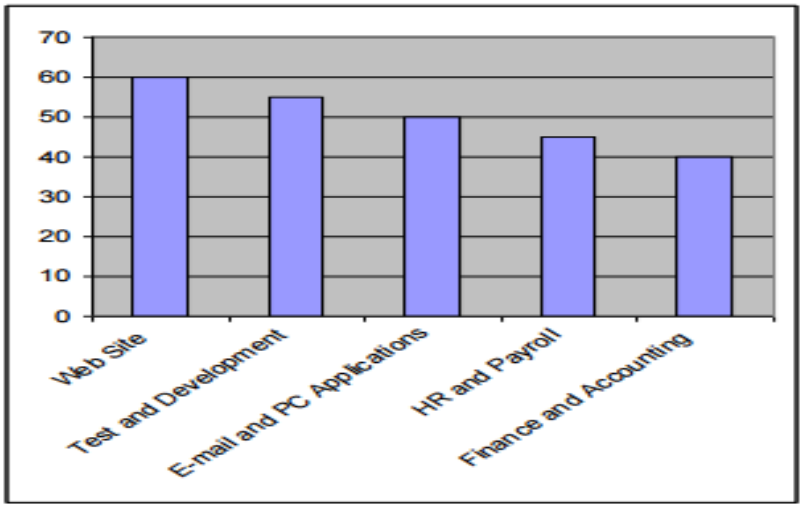

Fig.1. TOP Applications in Cloud

This can also be extended to classical functional, regression and other testing of regular products in a product development cycle from a perspective of cost. In essence, cloud testing is a form of software

testing wherein testing is done using resources, machines or servers from the cloud infrastructure. Besides, the entire testing environments can be obtained from the cloud on- demand at a cost that is practical and reasonable due to the pay- for-use nature of cloud computing and with a lead-time that is near impossible within a company's own data center. Now remote machines in the cloud are used to provide a common ground for testers to test and developers to isolate and resolve the observed software defects. Apparently, cloud testing has traditionally been used to refer to load and performance testing of Web sites. However, with increasing maturity of technology, all kinds of enterprise software can be tested for functional and performance issues before going in for full fledged enterprise deployment. The below figure 1 indicates that testing and application development rank second (57%) as the most likely workload to be put into the cloud after Web sites (61%)[2]. Hence the cloud platform provides cost effective solution to the software testing, still it poses the some challenges.

2. LITERATURE SURVEY

Cloud computing environments seek to simulate the real world user traffic as we load testing and stress testing websites. Compared to software testing cloud testing has several advantages: Reduce the cost leveraging the resources of the cloud computing operations present in the real time applications[2]. A. Forms of Cloud Testing There are three different type of cloud testing environments present in the real time cloud applications [5].

A. Cloud/SaaS-oriented testing

This type of testing applications arrives specified with semantic relations in cloud testing operations. This testing can be performed inside the cloud by user and other SaaS service venders[1]. The primary objective is to assure the quality of the provided service functions offered in a cloud. Since clouds and SaaS usually provide certain service APIs and connectivity interfaces to their customers, it is required task for engineers to validate these APIs and connectivity in a cloud environment [4]. In addition, testing cloud-based or SaaS-based security services and functional features must be tested.

B. Online-based application testing on a cloud

This type of testing activities is performed to check online application on cloud by using with cloud-based large-scale traffic and user accesses[7].

C. Cloud-based application testing over clouds

This type of testing refers to the engineering activities performed to assure the quality of a cloud-based application crossing different clouds. This suggests that the system-level integration, function validation, performance evaluation, and scalability measurement scope with different cloud technologies[7].

3. CLOUD COMPUTING MODELS

Cloud computing, to put it simply, means "Internet Computing." The Internet is commonly visualized as clouds; hence the term "cloud computing" for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides,

databases in cloud are very dynamic and scalable.“ 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, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

A. Software-as-a-Service (SaaS).

The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The cloud provider is responsible for the management the application, operating systems and underlying infrastructure. The consumer can only control some of the user-specific application configuration settings. Example: Yahoo!, Gmail, Google Diocs, etc.

B. Platform-as-a-Service (PaaS)

The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. “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”. Example: Google Aps, SQL Azure, etc.

C. Infrastructure-as-a-Service (IaaS)

The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can the use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. “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)”. Example: Amazon (S3, EC2), Windows Azure, etc.

D. Cloud Deployment Models

Regardless of which delivery model is utilized, cloud offerings can be deployed in four primary ways, each with their own characteristics. The characteristics to describe the deployment models are; (i) who owns the infrastructure; (ii) who manages the infrastructure; (iii) where is the infrastructure located; (iv) and who accesses the cloud services.

4. THE SECURITY MODELS OF CLOUD COMPUTING

A. The Cloud Multiple-Tenancy Model of NIST

Multiple-tenancy [4] is an important function characteristic of cloud computing that allows multiple applications of cloud service providers currently running in a physical server to offer cloud service for customers. This physical server partitions and processes different customer demands with virtualization. Virtualization possesses good capability of sharing and isolation, and is a right core technology of cloud computing. By running multiple virtual machines (VMs) [5] in a physical machine, virtualization enables to share computing resource such as processor, memory, storage, and I/O among different customers‟ applications, and improves the utilization of cloud resources.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1355 - 1360
RECEIVED : 29/10/2016. PUBLISHED: 16/11/2016
November 16, 2016

By hosting different customers‟ applications into different virtual machines, virtualization enables to isolate fault, virus, and intrusion of one from other virtual machines and hardware, and reduce the damage of malicious applications. The technology difficulties of multiple-tenancy model include data isolation, architecture extension, configuration self-definition, and performance customization. Data isolation means that the business data of multiple customers do not intervene mutually. Architecture extension means that multipletenancy should provide a basic framework to implement high flexibility and scalability. Configuration self definition means that cloud computing should support different customers‟ respective demands on its service platform configuration. Performance customization means that cloud computing should assure different customers‟ demands on the performance of multiple-tenancy platform under different workload. The impact of multiple-tenancy model is different corresponding to different cloud deployment models. Taking SaaS as an example, SaaS with multiple-tenancy function characteristic has two basic features. First, it is easy to scale-out and scale-up to serve for a mass of customers based on Web service. Second, it can present additional business logic that enables customers to extend its service platform and satisfy larger enterprises‟ demands. Multipletenancy model of cloud computing implemented by virtualization offers a method to satisfy different customer demands on security, segmentation, isolation, governance, SLA and billing/chargeback etc.

B. The Cloud Risk Accumulation Model of CSA

Understanding the layer dependency of cloud service models is very critical to analyze the security risks of cloud computing. IaaS is the foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is an inherited relation between the service capability of different layers in cloud computing. Similar to the inheritance of cloud service capability, the security risks of cloud computing is also inherited between different service layers [4]. IaaS provides no distinctive function similar to application service but maximum extensibility for customers, meaning that IaaS holds little security functions and capabilities except for the infrastructure‟s own security functions and capabilities. IaaS demands that customers take charge of the security of operating systems, software applications and contents etc. PaaS offers the capability of developing customized applications based on the PaaS platform for customers and more extensibility than SaaS, at the cost of reducing those available distinctive functions of SaaS. Similarly, the intrinsic security function and capability of PaaS are not complete, but customers possess more flexibility to implement additional security. SaaS presents the least customer extensibility.

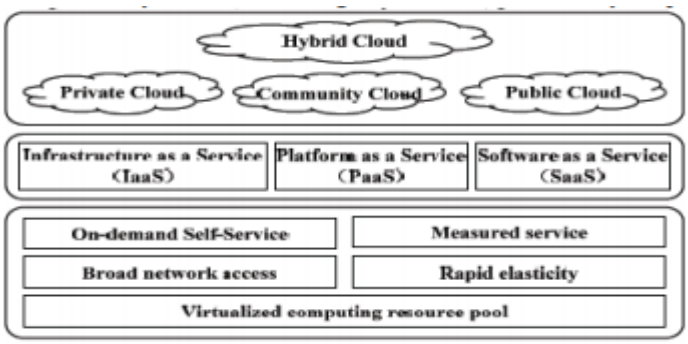

Fig.2. The NIST,s definition model of cloud computing

In SaaS, cloud service providers take charge of more security responsibilities, and customers pay for little security effort on the SaaS platform. One critical feature of cloud security architecture is that the lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of. In SaaS, cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc. In PaaS and IaaS, the above demands are charged by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform.

C. Jerico Forum's Cloud Cube Model

Jerico formu‟s cloud cube model is a figuration description of security attribute information implied in the service and deployment models of cloud computing and the location, manager and owner of computing resources and so on as figure 3 shown. In cloud cube model, the definitions of model parameters are as follows, a model parameter to define the physical location of data storage. If the physical location of data storage is inside of the data owner‟s boundary, then the model parameter value is internal. Contrariwise, the model parameter value is external. For example, the data center of a private enterprise cloud is internal, and the data center of Amazon‟s SC3 is external. Note: the cloud with internal data storage is not more secure than the one with external data storage. The combination of internal and external data storage maybe present more secure usage model. a model parameter to describe the "architectural mindset" of security protection, i.e. a customer‟s application is inside or outside of traditional security boundary? Perimeterised means that a customer‟s application operates within traditional IT security boundary signaled by firewall that blocks the incorporation of different security zones. In fact, customers running some applications inside of security zone can extend/shrink their application perimeter to/back from external cloud environment by VPN. De-perimeterised means that the fadeway of traditional IT security boundary and the exposure of a customer‟s application operation. For the security protection of deperimeterised environment, Jerico Forum uses the metadata and mechanisms in their commandments and Collaboration Oriented Architectures Framework (COA) to encapsulate a customer‟s data.

CONCLUSION

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. However, the prevalence of cloud computing is blocked by its security to a great extent. To contribute some effort to improving the security of cloud computing, finally, we surveyed the main existing security models of cloud computing, and summarized the main security risks of cloud computing from different Organizations. In the future, we will give and implement some security strategies with technology and management ways.

REFERENCES

[1] Wikipedia, http:// en.wikipedia.org/ wiki/ Cloud Computing.

[2] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). Decemeber,2009

[3] Cloud Security Alliance. Top Threats to Cloud Computing, 2010.http://www.cloudsecurityalliance.org [accessed on: March, 2010].

[4] K., Thirupathi Rao et al., "Secure multi-tenancy cloud storage in cloud computing" Global Journal of Mech., Engg. & Comp. Sciences, review paper, Pp.79-82 (2012).

[5] J. Gao, X. Bai, and W. T. Tsai, "Cloud-Testing Issues, Challenges, Needs and Practice," Software Engineering: An International Journal, vol. 1, no. 1, pp. 9–23, 2011.

[6] Pat Hyek (2011)," Cloud Computing Issues and Impacts", Global Technology Industry Discussion Series.

[7] IXIA (2011), "Testing the Cloud: Definitions, Requirements and Solutions", August 2011, CA, URL: http://www.ixiacom.com

[8] Neha Mehrotra (2011), "Cloud Testing Vs Testing a Cloud", Infosys Viewpoint.

[9] Prince Jain, Dr. Gurdev Singh & Isha Gulati (2011), "Process Model for Cloud Service Engineering", International Journal of Computer Applications, Vol. 36, No. 8.