Analysis of Cloud Computing Security Considerations for Platform as a Service

Keyur S. Mehta

***Abstract*—Cloud Computing is an IT model or computing environment which is composed of IT components (hardware, software, networking, and services) as well as the processes around the deployment of these elements that together enable us to develop and deliver cloud services via the Internet or a Private network. Cloud users no need to deploy the resources at their site because resources are available at the provider's side and they provide it and charged on usage basis. This paper focuses on the security of cloud computing considerations for Platform as a Service.**

***Index Terms*—Audit trial, cryptography, elasticity, hybrid cloud, private cloud, virtualization.**

I. Introduction

There are innumerous definitions of Cloud Computing and also huge disagreements about what it really is and means. In my opinion, one of the reasons why there is a lot of confusions because there is great mix-up of the concepts, namely technical and purely conceptual.

Cloud computing is an evolutionary process of prior computing approaches, which builds upon existing and new technologies. Even as cloud presents new opportunities around shared resources, the relative newness of the model makes it difficult to separate reasonable claims from hype. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

According to NIST, National Institute of Standards and Technology, Cloud Computing is:

"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, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [1]

II. Essential Characteristics

A. 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.

Manuscript received August 2, 2012; revised October 1, 2012.

Keyur S. Mehta is with the Department of Advanced Software and Computing Technology, International Institute of Information Technology, Pune, Maharashtra, India (e-mail: ksmehta2004@gmail.com).

B. Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms.

C. 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.

D. Elasticity

Elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

E. 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. [2]

F. Virtualization

It allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

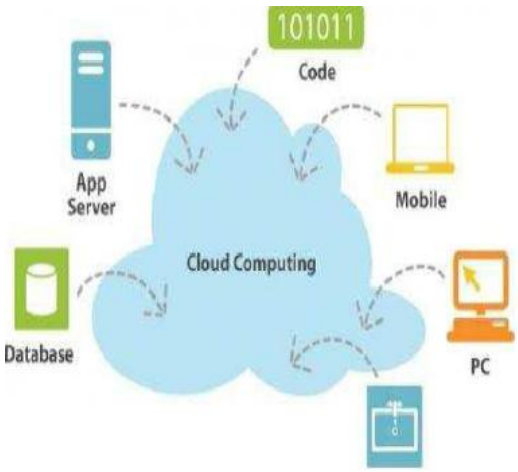

Fig. 1. General cloud diagram

G. Security

It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing

III. Service Models

Cloud Computing is distributed in three models according to their service.

- Infrastructure as a Service (IaaS)

- Platform as a Service (PaaS)
- Software as a Service (SaaS)

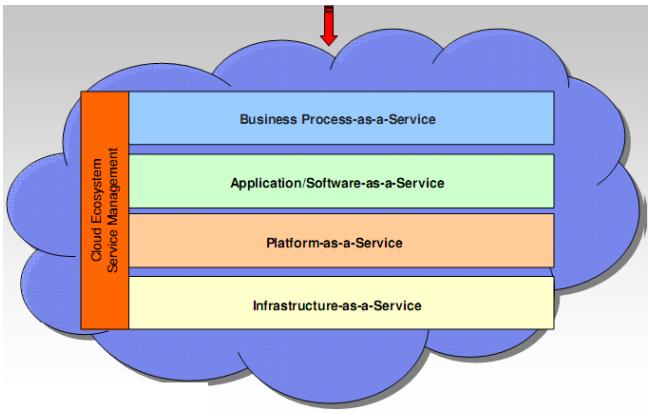

Fig. 2. Cloud computing service models

A. Infrastructure as a Service (IaaS)

In this most basic cloud service model, cloud providers offer computers – as physical or more often as virtual machines along with firewalls, load balancer and Network.

Examples of IaaS: Amazon Cloud Formation (EC2), Rack space Cloud, Google Compute Engine, and Right Scale.

B. Platform as a Service (PaaS)

It is a set of software and development tools hosted on the provider's servers. PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities.

Examples of PaaS: Amazon Elastic Beanstalk, Heroku, Engine Yard, Google App Engine, and Microsoft Azure.

C. Software as a Service (SaaS)

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. It is common to refer to special types of cloud based application software with a similar naming convention: desktop as a service, business process as a service, Test Environment as a Service, communication as a service.

Examples of SaaS: Google Apps, QuickBooks Online and Salesforce.com.

IV. Deployment Models

A. Private Cloud

It is cloud infrastructure operated only for a single organization, whether managed internally or by a third-party and hosted internally or externally. [2]

B. Community Cloud

It is infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. [2]

C. Public Cloud

Applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model. Generally, public cloud service providers like Microsoft and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered).[3]

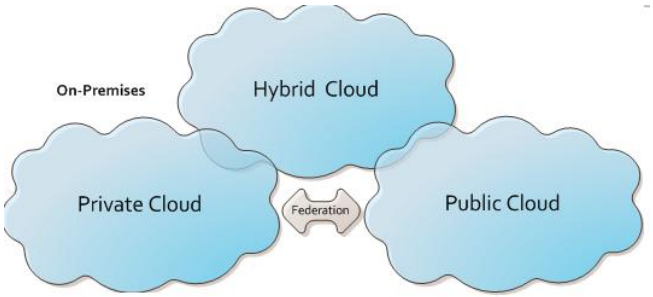

Fig. 3. Types of cloud

D. Hybrid Cloud

It is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. [3]

V. Platform as a Service (PAAS)

Platform as a Service (PaaS) is one of three main forms of cloud computing, where companies rent hardware and software from a third party. The platform is accessed across a private network or the internet and used to build applications rather than owning, running and developing on an internal IT infrastructure. [4]

PaaS sits in the middle of these two models: SaaS and IaaS. Essentially a company rents the hardware, operating systems, storage and network capacity that IaaS provides but also software servers and applications environments. This gives customers a platform on which they can load their data and start the developing applications they need.

But being between IaaS and SaaS means that there is a great deal of overlap at both ends of the PaaS spectrum. There is no real agreement on what PaaS is and where these three forms start and stop so perhaps an example is the best way to get the idea across. [4]

VI. Difference Between PAAS and Traditional Development Platform

A. Multi-Tenant Development Tool

The traditional development tools are single user - a cloud-based studio must support multiple users, each with multiple active projects.

B. Multi-Tenant Deployment Architecture

A scalability is often not a concern of the initial development effort and is left instead for the System admin to deal with when the project deploys. In PaaS, scalability of the application and data tiers must be built-in (e.g., load

balancing, failover need to be basic elements of the dev platform itself).

C. Integrated Management

Traditional development solutions usually do not concern themselves with runtime monitoring, but in PaaS, the monitoring ability needs to be baked into the development platform.

D. Integrated billing

PaaS offerings require mechanisms for billing based on usage that are unique to the SaaS world. [5]

VII. Security Issues in PaaS

Cloud computing security is a sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

A. Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information**.**

B. Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

C. Abuse and Nefarious Use of Cloud Computing

By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. [6]

D. Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. [6]

Example: Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

E. Data Loss or Leakage

There are many ways to compromise data. For Example, deletion or alteration of records without a backup of the original content. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.

Example: Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures;

F. Malicious Insiders

This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. [6]

G. Account or Service Hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. [6]

H. Unknown Risk Profile

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications

I. Denial of Service (DoS) Attack

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009. We are creating a federation of different cloud provider, so this is consider as a major security issue in open cloud computing federation.

J. SLA (Service Level Agreement) Terms

The SLA services as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

VIII. Benefits of PaaS

As earlier I have mention security risks of Platform as a Service. But there are also many benefits to use cloud as a PaaS.

A. Reduces Operational Cost

Foremost advantage of using PaaS Service for running daily tasks of an organization smoothly and efficiently is the fact that daily operational costs get reduced to a huge percentage, while scaling up or raising the productivity levels of the organizations to a great extent. [7]

B. Low on Up-Front Costs

Second most important benefit of using PaaS is that it requires no up-front investments. This means if you wish to run your hardware and a software application on PaaS, only a negligible amount has to be paid for its start up.

C. Access to Information Round the Clock

Cloud computing has always encouraged easy access of information at any time of the hour and from anywhere. Sharing of Platform related applications can be done with

ease and without any hassle.

D. Integration with other Web Services

PaaS offers an integrated business environment. By stating this I mean that all the software as well as hardware applications that are running using PaaS area is compatible with most of the computer systems and telecommunication devices such as smart phones.

IX. Conclusion

Cloud computing has dramatically changed how custom, "Industry specific" business applications are built and run. Cloud computing has evolved to include platforms for building and running custom application. Cloud computing reduce the cost and complexity of evaluating, buying, configuring, and managing these complex environments. [8]

PaaS can reduce operational costs along with Up-Front costs. It also gives facility to access information round the clock user. Along with all these benefit of PaaS has its own disadvantages like: Low confidence in data security, service level agreements etc.

As per my analysis, PaaS which offers ease in use as is not that successful at present. If you strategically consider Platform as a Service, then you can achieve proper cost saving, lower risk and efficiency standard.

References

[1] M. S. Ribeiro. (February, 2010) Cloud computing: The New IT Paradigm. [Online]. Available: http://itechthoughts.wordpress.com/tag/paas/

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*. Retrieved 24 July 2011. Special publication 800-145

[3] F. Gens, (September, 2008), Defining Cloud Services and Cloud Computing. [Online]. Available: http://www.cloudreviews.com/blog/what-is-hot-in-cloud-computing cloud computing

[4] Platform as a Service. [Online]. Available: http://www.bestpricecomputers.co.uk/glossary/platform-as-a-service.htm

[5] C. Keene. (March, 2009). What is Platform as a Service. [Online]. Available: http://cloud.dzone.com/articles/what-platform-service-paas

[6] Cloud Security Alliance. (March 2012). Top Security Threads to Cloud Computing. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[7] J. Simth. (June, 2012). Benefits of Platform as a Service. [Online]. Available: http://www.hostreview.com/blog/120620-cloud-computing-with-benefits-of-paas-cloud-model

[8] J. R. Vic Winkler, "Securing the cloud," *Cloud Computing Security Techniques and Tactics*, vol. 5, pp. 150-152.

Keyur Mehta has completed his B.E. in Information Technology from Bhavnagar University, Bhavnagar, Gujarat, India in 2009. Now, he is pursuing his M.Tech in Software Technology from International Institute of Information and Technology (I2IT), Pune, Maharashtra, India. His research areas include: Information Security Management, Cloud Computing and Software Engineering.