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
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.467 – 471

Survey on Security Issues in Platform-as-a-Service Model

P Buddha Reddy, IT Department, Vardhaman College of Engineering
Vinod Bhupathi, IT Department, Vardhaman College of Engineering
Ch Sravan, CSE Department, Vardhaman College of Engineering

Abstract: Cloud computing is making a big revolution in the field of information technology thereby reducing capital expenditures spent. Computing is delivered as a service enabling effective utilization of computational resources. Certain security issues exist which prevents individuals and industries from using clouds despite its advantages. Resolving such problems may increase the usage of cloud thereby reducing the amount spent for resources. Platform-as-a-Service (PaaS). PaaS model, security issues encountered in PaaS clouds. The issues along with solutions discussed provide an insight into PaaS security for both providers and users which may help in future PaaS design and implementation.

Keywords: encryption, interoperability, multi-tenancy, trusted computing base, virtualization.

1 Introduction

Outsourcing of computational resources is possible with the advent of cloud computing. Sharing of resources reduces capital expenditure making it foreseen and can be observed as rising trend. Such sharing of resources may cause certain security issues despite of vast advantages of cloud like better utilization of resources, least time taken in deploying new services and so on. Three ways to deliver cloud computing capabilities (Figure 1) are Software as a Service (SaaS), Platform as a Service(PaaS) and Infrastructure as a Service (IaaS).

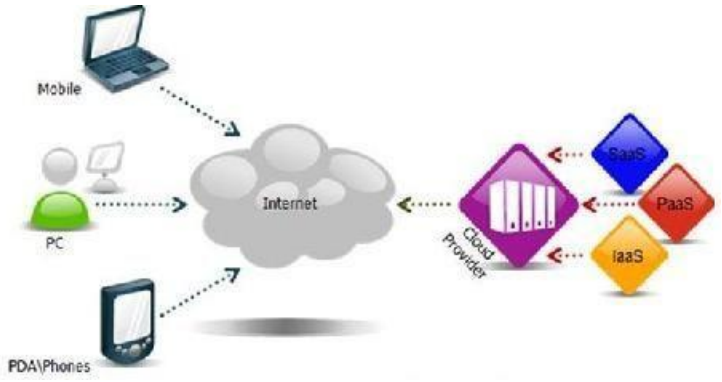

Fig 1 : Service model in Cloud Environment

Characteristics of cloud are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The various deployment models include private, public, hybrid and community cloud.

The paper focuses on basic PaaS model and also in identifying the security in PaaS environment along with the solutions. Section 2 gives a deep insight into PaaS mode. Section 3 discusses the security issues along with appropriate solutions. The paper is concluded in Section5.

2 PaaS Model

2.1 PaaS basic model

The two different constructs of PaaS model are Control space and App space (Figure2) serve different purposes. App space is fully wrapped within the Control space. Since control space operates on same infrastructure like the app space, control space shares some characteristics of app space. Control Space components are definitives built from primitives and sophisticates to provide the prescriptive approach to the App Space that makes PaaS an attractive alternative to traditional software builds, configuration and deployments.

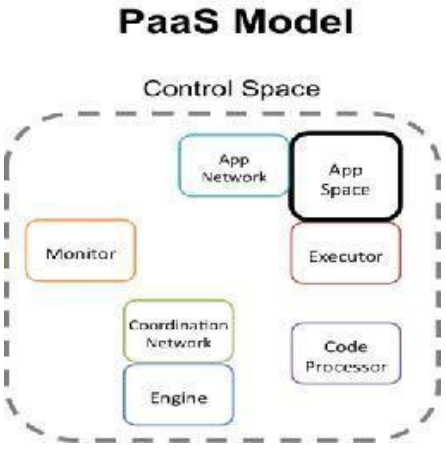

Fig. 2 : PaaS Model Control-space

2.1.1. Control Space

The functions of control space include automation, management and provisioning. It interacts to lo-level components with the help of API abstractions. The Control space determines what elements are exposed to App Space thereby maintaining coherency and dependencies of App Space. Several separate functions of control space can be combined in various manners based on PaaS implementation.

2.1.2. App Space

The applications of end-user/customer are deployed, updated and run in App Space which is being controlled by Control Space. Exposure of PaaS Element types by Control Space to App Space is one of the key differentiating factors between different PaaS implementations.

a) App network b) Executor c) Code Processor d) Coordination Network e) Engine f) Monitor

3 PaaS Security

3.1. PaaS Security Elements

Elements that characterize PaaS security platform are as follows:

a) Information processing: This is the stage where one is creating data and rest of the web uses it. Creation of data may happen live on remote server. So the document can be intercepted. PaaS provides security when this data is in stored format, which clearly states that the problem is during processing stage.

b) Information interactivity: This is the process of sharing data across the board. Interaction can go with personal computers, networks, devices like phones and so on. This interaction connects confidential data in local network with the web where most of them can access and hence security issue comes in.

c) Data Storage: This specifies the hosting aspect of Cloud. Several mechanisms in PaaS allow multiple applications to be encrypted to prevent data leakage. Verification is hard as data is in shared servers.

3.2. PaaS Security Issues

3.2.1. Interoperability

Interoperability is the ability for different cloud to talk to each other at three different levels (SaaS, PaaS and IaaS). It is actually the ability to write code that works with more than one cloud provider

simultaneously, regardless of the differences between the providers [15]. Application written to use specific services from a vendor's PaaS will require changes to use similar services from another vendor's PaaS. Efforts are taken on development of open and proprietary standard API's to enable cloud management, security, and interoperability. Common container formats like DMTF'S Open Virtualization Format (OVF) can be used. Application written to those standards is far more likely to be interoperable and portable. Interoperability can be maintained by providing common interfaces to objects for resource access.

3.2.2. Host Vulnerability

Vulnerability may be described in terms of resistance to a certain type of attack. Multi-tenancy allows user objects to be spread over interconnected multi-user hosts. Hosts have to be protected from attacks in such an environment. If this protection fails, an attacker can easily access the resources of host and also tenant objects. Provider has to take necessary security measures. TCB serves as solution for host vulnerability also.

3.2.3. Object Vulnerability

Service providers can access and modify user objects. Three ways by which security of an object can be breached in PaaS clouds are: a) Provider may access any user object that resides on its hosts. A fully homomorphic encryption can be employed as a cryptographic defense for user objects during execution, but it is computationally expensive. Hence, this type of attack is unavoidable and can be avoided to some extent by trust relations between user and provider. b) Users may mutually attack each other's objects that are tenants of same host because tenant objects synchronously share the same resources. c) Third party may directly attack a user object. Secure coding enables objects to defend themselves.

3.2.4. Access Control

Network communications must be confidential and access of remote entities should be controlled. Three major concepts of access control are: authentication, authorization and traceability. Some of the attacks in such cloud-based environments are impersonation, phishing attacks, brute force attacks and password reset attacks. Two-factor authentication like smart cards and biometric mechanisms can protect from such attacks. Solutions to access control problems are as follows: a) Encapsulation b) Policy enforcement points (PEPs)

3.2.5. Privacy-Aware Authentication

For authentication, user reveals most of the details regarding him. Proxy certificates help to reduce the risk associated with revealing of these attributes. Proxy certificate is actually an electronic certificate that includes only the required attributes of the corresponding identity. Requirements to be met during privacy-

aware authentication with proxy certificates are: a) Based on access control policies defined by both service providers and users, hosts and objects should not request more attributes than the required amount. If more attributes are requested, then the service is negotiated. b) With the help of trusted third party, easily configurable credentials which reveal data that the identity owners permit can be achieved.

4. Conclusion

Secure PaaS cloud can be achieved by understanding the PaaS model, its types and the issues related to security as described in the paper. The various features of PaaS can be utilized in an efficient manner based on the deeper understanding of PaaS environment in cloud. The characteristics of PaaS along with the evaluation criteria in choosing a provider for PaaS has also been identified along with PaaS security elements. Finally, security issues in PaaS with their appropriate solutions have been discussed to provide a clear insight in data security issues and other challenges while running application on PaaS platform. With the solutions and also by knowing these issues, customers can be precautionary while using PaaS.

References

1. Devi T, Ganesan R. Platform-as-a-Service (PaaS): Model and Security Issues. TELKOMNIKA Vol. 15, No. 1, July 2015 : 151 – 161
2. LM Kaufman. Data security in the world of cloud computing. IEEE Security & Privacy. 2009; 7(4): 61-64.
3. D Catteddu, G Hogben. Cloud computing: Benefits, risks and recommendations for information security. Technical report, ENISA. 2009.
4. S Subashini, V Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011; 34(1): 1-11.
5. VJR Winkler. Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham: Syngress. 2011.
6. National Institute of Standards and Technology (NIST). http://www.nist.gov.
7. Google app engine. 2012. https://developers.google.com/ appengine/.
8. Windows azure platform. 2012. http://www.windowsazure.com/ en-us/.
9. D Zissis, D Lekkas. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; 28(3): 583-592.
10. M Almorsy, J Grundy, AS Ibrahim. Collaboration-Based Cloud Computing Security Management Framework. IEEE 4th International Conference on Cloud Computing. 2011: 364-371.
11. A Bessani, M Correia, B Quaresma, F Andr´e,P Sousa. Depsky: dependable and secure storage in a cloud-of-clouds. In Proceedings of the sixth conference on Computer systems, EuroSys ’11. New York, NY, USA. 2011. 31-46.

