Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Overview of Application Security in the Cloud

Sonali Ghodke
M.E. (CNIS) Student, Department of Computer Engineering,
Mumbai University, Maharashtra, India

***Abstract**: Cloud computing is the most recent emerging for accessing computing resources. Cloud is a collection of computer resources and provides a million of services to its user simultaneously. A Cloud provides a friendly environment to its user and various services such as Software as a service (SaaS), platform as a service (PaaS), and Infrastructure as a Service (IaaS). These services are used in Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Before you host home-grown or an industry-standard application on the cloud, there are several factors that need to be taken care of. Each of the SaaS, PaaS or IaaS (SPI) delivery models bring in security threats that the application never encountered when they were hosted within a corporate intranet. Integration of security into the Software Development Life Cycle has gained acceptance over the last decade. This paper describes the Software Development Life Cycle for SaaS, PaaS, and IaaS services.*

***Keywords**— Cloud Computing, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software Development Life Cycle (SDLC).*

I. INTRODUCTION

Cloud Computing is said to be the biggest thing since the Internet evolved. In other words Cloud Computing will become the greatest technical breakthrough in our lifetime. Cloud Computing is entering our life and changing the way people consume information. It is a technology that keeps up data and its application by using Internet and central remote servers. As per the definition of National Institute for STD Tech (NIST), Cloud Computing is a model for enabling ubiquitous, convenient, on demand N/W access to a shared pool. Configuring computing resources, for example N/W servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1] It is based on the concept of virtualization. In other words virtual computers are the components of the Cloud. It is also known as on demand computing, based on the internet based computing where shared resources, data and information provided to computer and other devices on demand[2].The figure 1 below shows the basic diagram of Cloud Computing.

Figure 1: Cloud Computing

Cloud Computing model is composed of
A. Service Model.
B. Deployment Model.
C. Characteristics.
The below figure 2 shows the Cloud Reference Model composed of three service models, four deployment models and five essential characteristics

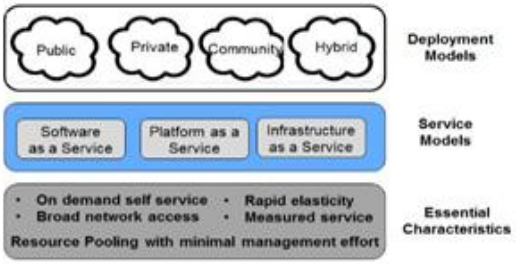

Figure 2: Cloud Computing Models

A. Service Models

1) ***Software as a Service (SaaS)*:** SaaS is the capability to use the provider's application running on Cloud infrastructure. The applications are accessible from various client devices through Web Browser. It is sometimes referred to as software on demand. In SAAS Cloud vendor supplies h/w infrastructure, software and application. The customer interacts with the application through portal in pay-per-use manner. The consumer does not need to manage or control the underlying Cloud infrastructure including N/W, OS, storage, servers etc. These are thus large number of Cloud providers such as Microsoft Live CRM, Google Apps such as Google mail, Google docs, and spread sheet.
2) ***Platform as a Service (PaaS)*:** It is the way to rent the h/w, OS, storage capacity over the internet. [3] Platforms are an abstraction layer between the software application (SAAS) and virtualized infrastructure (IAAS). [4] Consumer can write their application, specifications of a particular platform without needing to worry about the underlying h/w infrastructure. The consumer does not control, manage or own the underlying Cloud infrastructure including servers, OS, security devices, and has a control over the deployed application and possibly also the configuration of the hosting environment. It is particularly useful for small and medium sized enterprises (SME'S). Developers on the PaaS platform create applications on the Cloud platform using API'S website portal installed on Cloud server Force.com (a part of sales force.com), Microsoft Azure, and Google App engine are few leading PaaS providers.
3) ***Infrastructure as a Service (Iaas)*:** It is a model in which you as a customer pay for the resources such as memory, storage, h/w networking, devices kept at the provider's facility or where ever the provider keeps its h/w. IaaS like Amazon web services provides virtual server instances with unique IP adders and blocks of storage on demand. To start, stop or to access a provider's application, customer can use application programme interface (API). It is on the basis of pay-for-what-you-use. Examples are Amazon web services with elastic compute cloud (EC2), for processing and accessing simple storage service (S3) for storage.[5]

The below figure 3 shows the basic structure of Service Models.

	Who uses it?	*What services are available?*	*Why use it?*	*Examples*
SaaS	Business User	Email, Office, Automation, CRM, Website testing, Wiki, Blog, Virtual Desktop…..	To Complete Business Task	facebook
PaaS	Developer and Deployers	Service and application test, development, integration and deployment	Create or Deploy application and services for users	amazon webservices, Azure
IaaS	System Manager	Virtual machine, operating system, Message queue, Network, Storage,CPU, memory, backup service	Create platform for service application test, development, integration and deployment	

Figure 3: Service Models

B. Deployment Models

1) ***Private Cloud:*** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them. [6]
2) ***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 owned, managed and operated by commercial businessman, academic or government organization and exists in the premises of Cloud provider". [6]
3) ***Hybrid Cloud:*** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but can share data if required.
4) ***Community Cloud:*** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (Eg: mission, policy, security required). It may be managed by organization or trusted third party. [6]

The below figure 4 shows the basic structure of Deployment Models.

Figure 4: Deployment Models

C. Essential Characteristics

1) ***Rapid Elasticity:*** Resources are provisioned and released on demand and/or automated based on triggers or parameters. This will make sure your application will have exactly the capacity it needs at any point of time.
2) ***Measured Service:*** Resource usage are monitored, measured and reported transparently based on utilization (In short pay for use). Elastic computing resources are forced to keep the data within their capacitive internal data centres due to concerns over security, privacy, and corporate governance and compliance reasons. The Cloud infrastructure is operated solely for an organization or may be managed by an organization itself or by a third party.
3) ***On Demand Self Service:*** Users are able to provision Cloud Computing resources without requiring human interaction mostly done through a web based self-service portal thoughtsoncloud.com.
4) ***Resource Pooling:*** The cloud must have a large and flexible resource pool to meet consumer's needs, provide economies of scale, and meet service level requirements. The resources can be physically located at many geographic locations and assigned as virtual components of the computation as needed.
5) ***Broad Network Access:*** For cloud computing to be an effective alternative to in- house data centres, high-bandwidth communication links must be available to connect to the cloud services. Capabilities are available over the network and access through standard mechanisms that promote use by heterogeneous thin or thick client platforms.[7]

II. OBJECTIVES OF CLOUD INFORMATION SECURITY

In last few years Cloud Computing has grown from being a promising business to one of the fastest growing segments of IT industry. As each and every organization is moving their data to the Cloud, it means it uses the storage service provided by the Cloud provider. Hence there is a need to protect that data from unauthorized access, modified or denial of service attack etc. Developing secure software is based on applying the secure software design principles that form the fundamental basis for software assurance. The software security assurance report[2] defines software assurance as "the basis for gaining justifiable confidence that software will consistently exhibit all properties required to ensure that the software, in operation, will continue to operate dependably despite the presence of sponsored faults." Confidentiality, Integrity and availability are sometimes known as CIA triad of information system security, and are important pillars of software assurance. Additional factors that directly affect cloud software assurance include authentication, authorization, auditing, accountability, as summarized in following sections;

1) ***Confidentiality:*** The principle of confidentiality specifies to keep the user data secret in the Cloud Computing system offerings (eg; application infrastructure) of essential public n/w. Therefore keeping all confidential data of users in the Cloud is a fundamental requirement which will attract even more users consequently. Encryption and Physical Isolation are the various techniques used to achieve confidentiality.
2) ***Integrity:*** Integrity means that changes need to be done by only authorized user through authorized mechanism. As data is the base for Cloud computing services such as SAAS, PAAS, and IAAS. Keeping data integrity is the fundamental task (i.e. information should not be modified by authorized users). Digital Signature is the technique used for marinating the Integrity.
3) ***Availability:*** The principle of availability states that resources or information should be available to the authorized parties at any time at any place. The information created and stored by an organization needs to be available to the user.
4) ***Access Control:*** It is the ability to control the access to host system and applications via common links. Control in system means to regulate the use of the system, including the applications on its structure and the data.
5) ***Authentication:*** Authentication is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be. [8]
6) ***Authorization:*** Authorization refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets. Once a user's identity and authentication are established, authorization levels determine the extent of system rights a user can hold. [8]
7) ***Auditing:*** To maintain operational assurance, organizations, use two basic methods: System audits and monitoring.
8) ***Accountability:*** Accountability is the ability to determine the actions and behaviours of a single individual within a cloud system and to identify that particular individual.

III. CLOUD APPLICATION SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

Since the beginning of software engineering era, security enable unity has been an integral part of traditional software development life cycle (SDLC) for internal applications. For example the Payment-Card-Industry-Data-Security-Standard (PCI-DSS) and several other organizations have been promoting security as a crucial and essential element within SDLC. Even when an internal application is moved to the Cloud, all implemented security features remain relevant and essential. Besides, the Clouds bring in numerous new issues. Instead of single uniform environment for development, testing and deployment, which are contained within the enterprise, cloud applications have at least two environments- one for development and other for deployment (which is the cloud). SDLC for cloud applications must have a well-defined trust relationship between the two environments, which depends on the cloud deployment mode in use. [5]

A. Security challenges in SaaS:

Major security issues in SaaS are listed as following:

1) ***Identity management in the cloud is immature***
2) ***Cloud standards are weak***
3) ***Access everywhere increases convenience, but also risk***
4) ***You don't always know where your data is***
5) ***Data Security***

Data security is one of the leading and most cited issues in SaaS delivery model. Data security may be a major concern for users who wants to introduce cloud computing. This technology needs proper security principles and mechanisms to eliminate users concerns. For example, most cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers [9]. The user data that need to be protected includes four parts which are: (i) usage data; information collected from computer devices (ii) sensitive information; information on health, bank account etc. (iii) Personally identifiable information; information that could be used to identify the individual (iv) Unique device identities; information that might be uniquely traceable e.g. IP addresses, unique hardware identities.

6) ***Availability***

The availability guarantees the reliable and timely access to cloud data or cloud computing resources by the suitable personnel. The SaaS application providers are necessary to make sure that the systems are running as it should be when desired and enterprises are provided with services almost all the time. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. Resiliency to hardware/software malfunction, as well as to defiance of service attacks, wants to be built from the ground up within the application.

7) ***Authentication & Authorization***

The authentication and authorization applications for enterprise environments may need to be changed, to work with a safe cloud environment. Forensics tasks may become much tougher since the investigators may not be able to access system hardware physically. Lio introduces two factor password authentication scheme based on having both the properties of discrete logarithm problem and secure one-way hash function [10]. There were some deficiencies in Lio [10] work; to overcome those insufficiencies Yang[11] introduce a mutual authentication scheme based on smart card and password. In which smart card user registers at the server firstly then chooses a right client to login and sends access request messages to the server. Then the server will complete mutual authentication with the user after receiving the messages.

8) ***Network Security***

In a SaaS deployment model, susceptible data is gained from the enterprises, processed by the SaaS application and stores at the SaaS vendor end. All data flow across the network wants to be protected in order to evade outflow of perceptive information. This involves the use of strong network traffic encryption techniques such as Transport Layer Security (TLS)and Secure Socket Layer (SSL) for security. In case of Amazon Web Services (AWS), the network layer provides significant protection against traditional network security issues, such as scanning, IP spoofing, port packet sniffing, etc. For highest protection, Amazon S3 is reachable via SSL encrypted endpoints. The encrypted end points are reachable from both the Internet and from within AmazonEC2, making it sure that data is transferred securely both within AWS and from sources outside of AWS [12]. However, malevolent users can exploit weak point in network security configuration to sniff network packets.

9) ***Web application security***

B. Application Security in a SaaS Environment:

SaaS vendors provide the infrastructure and applications to users on the pay-per-use model. The cost per month paid to the SaaS provider is based on the modules selected, number of user accounts, and amount of utilization of the application. [5]

C. SDLC for SaaS Environment:

A closer analysis on the controls and security provided by the SaaS vendor is needed because users have the least control in this delivery mechanism. As shown in the figure below, the SaaS provider evaluates the user requirements to select the application and necessary modules to meet the requirements. The SaaS provider is responsible for all other phases of SDLC. The user needs to be concerned about how the enterprise SDLC practices match with those of the SaaS provider. The security built-in the application directly impacts the users and its employees, partners and customers. The SaaS vendors provides API'S to exchange data with your enterprise applications on those residing at another cloud vendor, as shown in the figure 5 below.[5]

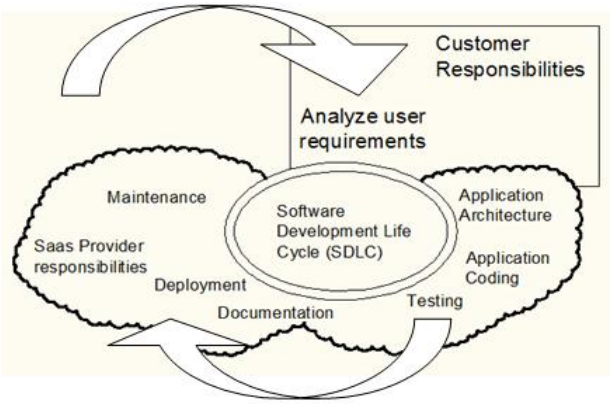

Figure 5: SDLC for SaaS Environment

A. Security Challenges in a PaaS:

There are several security challenges in a PaaS, which are as follows;

1) ***Data Distributed across multiple servers:*** PaaS provides development environment, which is spread across groups of clustered hosts. It is not possible to identify a host as the owner of user data because it is a platform and not a single host. The absence of a single host makes it difficult to secure user data, as hardening a host is a lot easier than a platform.
2) ***Data Distributed across geographical locations:*** For disaster recovery, PaaS provider replicates customer data to multiple geographic. The presence of data at various sites makes it more difficult to secure. Each data centres or geography has multiple images. Even if older images are deleted, it is a pointer that is deleted. The actual data continues to stay on the media. This brings a new security issue and data exposure.
3) ***Risk from Debugging Privileges:*** PaaS provides a built-in debugger to walk-through problematic areas in the code. It allows developers to access memory locations, which are necessary for quick problem identification, but exposes the environment to hackers and viruses.
4) ***Risk of having several open TCP codes:*** PaaS uses distributed file system, a common implementation being the Hadoop distributed file system (HDFS). It uses a few TCP ports. These ports can be used for DoS or other attack vectors.

B. Application Security in PaaS Environment:

PaaS vendors provide the h/infrastructure, application building blocks, compilers, and a runtime environment to develop and host applications. These blocks could be similar to those used internally within an enterprise; however, one needs to code certain security in applications in order to cover multi-tenancy and thousands of users who have potential access to the platform. [5] Application security has been a problem long before the arrival of PaaS. Some of the ways to protect data in a PaaS environment are as follows;

1) ***Testing for vulnerabilities:*** Several tools have been developed to identify application vulnerabilities. Some good ones are described at the Open Web Application Security Project (OWASP) site (http:/www.owasp.org). It lists several, battle tested tools, to protect the web based applications from security threats. These can be effectively used to harden the cloud applications. OWASP is a non-profit organization, dedicated to improving application security by providing tools and best practices to discover design and implementation defects and to protect against the flaws.
2) ***Tools:*** The cloud provider should be able to provide tools to identify security issues and scan web pages. You must continuously scan web pages for common security issues such as XSS and SQL injections.
3) ***Logs:*** All activity and security events must be logged and the data must be protected through encryption. The log must be regularly scanned for indications of security threats.
4) **Application Keys:** All API calls to the platform or services within must require an application key. The cloud application must have provisions to maintain and secure the key along with the other credentials.
5) ***Secure Protocols:*** For Simple Object Access Protocol (SOAP) based messages, secure protocols such as web services security must be used. It provides a foundation for implementing security functions such as confidentiality and integrity for web based application. It is maintained by OASIS (Organization for the Advancement of Structured Information Standards), an international, non-profit consortium, which is focused on open standards adoption for applications. Cloud applications must use Secure Sockets Layer (SSL), whenever possible.

C. SDLC for PaaS Environment:

One must have a mature and well established SDLC with a body of secure design and coding rules. The user needs to adopt specific security tools and standards to enable security in all SDLC phases. All software architects, developers, and testers in the organization must be familiar with the API'S and the security measures implemented by SaaS provider. All PaaS platforms have their own set of security challenges. The customer needs to develop close familiarity with the platform tools and the environment. Some PaaS providers offer a set of best practices or trainings to their customers.

Application security has been a key concern long before the arrival of PaaS. Many organizations have internally developed a strong development practice, with distinct processes for development, testing and production. For them PaaS security should be a familiar terrain. However several organizations do not have strong and tested security policies for application development. The figure 6 below shows the structure. [5]

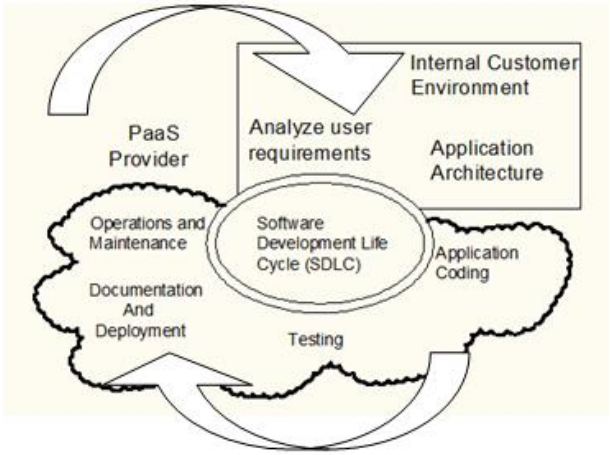

Figure 6: SDLC for PaaS Environment

A. Application Security in an IaaS Environment:

For application within an enterprise, several internal controls exist to protect the data. In a cloud, the corresponding security controls must be coded within the application. This section describes the security aspects for application developed in an IaaS environment. In this service providers create virtual machines (VM's) with internal or external storage devices. [5] To meet the various types of security requirements, and mitigate incessant threats, IaaS providers offer special security tools to help application developers improve security and meet compliance requirements. These tools can be used to identify and block several threats. These include the following [5]

1) **dWAF: -** It allows a set of rules to be applied to web-based communication to accept or drop packets based on port number, source, destination IP addresses, and other parameters.
2) **Host-based Intrusion detection systems (HIDS):-** It monitors and reports if any user or application has circumvented the IaaS host security policy.
3) **Host-based Intrusion prevention systems (HIPS):-** It monitors each IaaS host for suspicious activities by analysing the events within the host and takes steps to stop such activity. It blocks the malicious activity by dropping the bad packets, resetting the connection, or entirely blocking traffic from the offending IP address or network to and from the IaaS host.

B. SDLC for IaaS Environment:

When an application runs in IaaS environment, its development and initial testing could have potentially been within an internal enterprise environment. However some SDLC phases such as testing, deployment and maintenance are done in the IaaS cloud as shown in the figure 7 below.

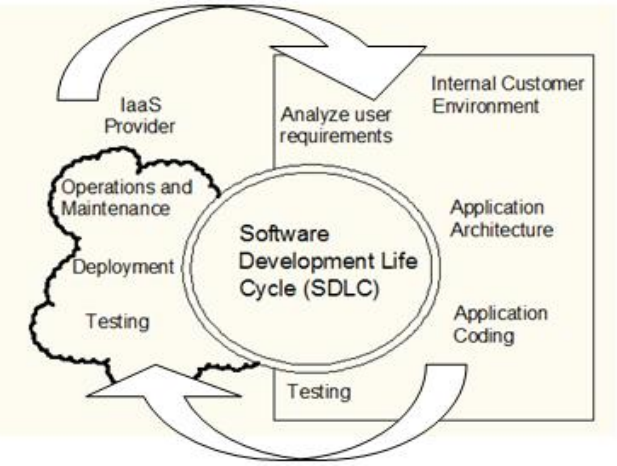

Figure 7: SDLC for IaaS Environment

IV. CONCLUSION

- In this paper we discuss about various services in cloud computing, its characteristics, security issues and models.
- In this paper we discuss the use of Software Development Life Cycle in various cloud services such SaaS, PaaS, IaaS.

- For cloud computing, additional activities must be added to the SDLC in order to build security into the application.
- New security techniques need to be developed, so that it will be easy to work with the clouds architecture.
- The development of cloud computing technology is still in the early stage. Hence new enhanced software architectures need to be developing for security purposes.

REFERENCES

[1] National Institute Of Standard and Technology. Esrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc,2009
[2] https://en.m.wikipedia.org/wiki/cloud-computing
[3] Pankaj Arora, Rubal Chaudhry Wadhawan, Satinder Pal Ahuja."Cloud computing Security Issues in Infrastructure as a Service". Volume-2, Issue 1, January 2012, ISSN: 2277 128X
[4] Sachin R Desale, Kadambari V. Vanmali, Brajendra Singh Rajput, "Distributed Versus Cloud Computing and data security issues and new trends-Fog Computing", IJETR, ISSN: 2321-0869, Volume-2,Issue-11,November 2014
[5] Kailash Jayaswal, JagannathKallakurchi, Donald J.Houde, Dr.Deven Shah, Cloud Computing Black Book.
[6] NIST special publications 800-145. The NIST definition. A Cloud Computing by Peter Mell & Timothy Grance
[7] www.thoughtsoncloud.com/2014/01/cloud-computing-defined-charachteristics-service-levels/
[8] Russel Dean Vines, Cloud Security-A comprehensive guide to Cloud Computing.
[9] T. Elahi and S. Pearson, "Privacy Assurance: Bridging the Gap between Preference and Practice," in Trust, Privacy and Security in Digital Business. vol. 4657, C. Lambrinoudakis, et al., Eds., ed: Springer Berlin Heidelberg, 2007, pp. 65-74.
[10] I. E. Liao, et al., "A password authentication scheme over insecure networks , in " Journal of Computer and System Sciences, vol. 72, pp. 727-740, 2006.
[11] G. Yang, *et al.*, "Two-factor mutual authentication based on smart cards and passwords," in *Journal of Computer and System Sciences*, vol. 74, pp. 1160-1172, 2008.
[12] Amazon. —"Amazon Elastic Compute Cloud (EC2)" [0nline] 2010, http://www.amazon.com/ec2/S (Accessed: 20 November2013).
[13] Soofi, Aized Amin, et al. "Security Issues in SaaS Delivery Model of Cloud Computing." (2014).

