CSCI 6708

Advanced Topics in Network Security

CRITICAL ANALYSIS OF I. Weber,

S. Nepal and L. Zhu, “Developing Dependable

and Secure Cloud Applications,” *IEEE Internet*

*Computing*, vol. 20, no. 3, pp. 74–79, 2016.

GROUP – 1

1. Sogra Bilal Memon (B00786252)
2. Faraaz Nizar Dhuka (B00784039)
3. Udaya Bhanu Lekhala (B00775670)
4. Choudhury Saadmaan Mahmid (B00751000)

**Summary of the Topic**

With the growing number of applications being provided as “Software-as-a-Service (SaaS)” [1] through cloud settings such as “Infrastructure-as-a-Service (IaaS)” [1] or “Platform-as-a-Service (PaaS)” [1], new techniques of deployment such as “DevOps” or “Development and Operations” [1] and “Continuous Deployment Pipeline (CDP)” [1] are being embraced by majority of the information technology industries. Consequently, new challenges to security (confidentiality, integrity and availability) and dependability (availability, reliability, safety, integrity and maintainability) have arisen as a result, which has created a tradeoff between speed and full-automation in deployment, and security of the deployment mechanisms. A better perspective about the various security challenges in cloud-based applications can be achieved through a thorough review of the “SaaS Security Life Cycle (SSLC)” [1]. SSLC consists of 5 phases – i. development, ii. delivery and deployment, iii. execution and maintenance, iv. termination and v. data storage [1]. Typically, SSLC is a combination of the standard Software Development Life Cycle (SDLC) and the standard “Data Security Life Cycle (DSLC)” [1]. Phases of a standard DSLC consists of “creating, storing, using, sharing, archiving and destroying” [1].

In the Development phase of SSLC, security and dependability requirements are specified through the “requirements gathering” and “design” steps of the integrated SDLC process. The “implementation” and “testing” steps of the SDLC can be executed in two ways: i. fully traditional or ii. fully in-cloud. Fully traditional strategy offers more control to the development team as they are typically performed in their local machines, while fully in-cloud relies entirely on cloud technologies rather than the developers themselves. The security challenges lie within the in-cloud strategy, where the stored components of the application are susceptible to attacks. Further, migration of applications from one cloud service provider to another is also subject to security risks.

Delivery and Deployment phase of SSLC can ensure maximized security and dependability by relying on “continuous delivery” [1] or “continuous deployment” [1]. Continuous delivery provides the confirmation about the completeness of the testing process and clearance to deploy the application. Continuous deployment automatically deploys the changes after each testing process. The researchers of the paper have introduced a solution to increase the dependability of the deployment process in cloud, which is called the “Process-Oriented Dependability (POD) Framework” [1], which mostly utilizes cloud metrics and logs from various operation tools in combination with the annotated model of the processes.

In the Execution and Operation phase of the SSLC, the biggest challenge to security is due to the nature of virtualization and the concept of multitenancy in cloud services [1]. Multitenancy exposes cloud servers, data and processes to threats that can emerge from both remote attackers and the tenants or administrators to the cloud services. Additionally, Virtual Machines (VMs) and their images are vulnerable to security risks especially when they are dormant, as a consequence of being left out or forgotten during security upgrades. Virtual Machine Monitors (VMMs) such as Hypervisors [1] are extremely effective in detecting attacks and vulnerabilities of deployed applications, however, VMMs often provide a “single-point of failure” [1] if the attacker takes control of the VMM itself.

Termination phase of the SSLC is concerned with the timely and secure termination of cloud applications. Essentially, the termination phase can face potential security challenges in the process of archiving and deleting data. Termination of a VM must ensure the security of VM images and that no data leakage has occurred. The researchers of the paper have proposed “TrustStore” [2], a “Key-Management Service (KMS)” [2] based solution to ensure secure data deletion.

Lastly, and most importantly, Data Storage phase deals with data security, which includes confidentiality, integrity and authenticity of the data. There are broadly three types of techniques to ensure confidentiality of data: i. architecture, ii. privacy and iii. security. One example of architecture for data confidentiality is a hybrid approach of storing sensitive data and processes in a private cloud and non-sensitive data and processes in a public cloud. Example of privacy measures for data confidentiality are “K-anonymization” [1] and “Differential Privacy” [1]. For security in data confidentiality, cryptographic techniques are used such as “homomorphic encryption” [1]. Data integrity techniques can be categorized into two types: i. Public auditing and ii. verification [1]. Data availability can be maximized through the use of multiple cloud service providers and data replication.

In conclusion, the entire SaaS life cycle including the generated data, needs to be secured by enforcing the Saas Security Life Cycle or SSLC. This will ensure non-repudiation, so that security violations can be audited and the person responsible can be held accountable. Each phase of SSLC may be subject to unique security challenges, and they need to be addressed and resolved in order to ensure security of cloud applications. Backup of cloud applications and the data is an effective way of ensuring dependability as well as availability in case of a service outage.

**Research Problem**

The authors in the article discuss security as well as dependability challenges while developing secured and dependable cloud applications with respect to Software Development (SDLC) and Data Security (DSLC) Life Cycles. DevOps requires implementing a continuous deployment pipeline (CDP) which wants more security as well as error- checking, so that errors or any malicious code doesn’t spread. In testing and deployment, complete automation increases challenges on security, dependability and requires quick recovery, rollback, and resilience. [1]

SaaS Security Life Cycle (SSLC) combines SDLC and DSLC, with each phase having security and dependability issues. [1]

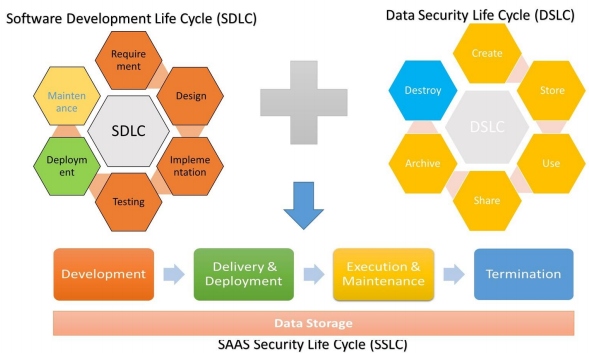


Fig 1. SaaS Security Life Cycle. Source [1]

In **Development phase**, the first two steps i.e. requirement gathering, and design includes security and dependability and last step i.e. testing has CDP activities. Fully in-cloud solutions have benefits like agility and distributed collaborative coding but, it also adds several threats and inability to port developed applications from one cloud provider to another. [1]

In **Delivery & Deployment phase,** dependability and security can be enhanced by using continuous delivery (ensures everything is tested) or continuous deployment (automatic deployment of changes). [1]

In **Execution & Operation phase,** use of Hypervisor enhances security and detects vulnerabilities of Virtual Machines (VM), but it is again a single point of failure. [1]

In **Termination,** the owner doesn’t have full control over data or storage media as the issue of secured deletion of data arises. [1]

**Data Storage-** the security of data is very important. Confidentiality is achieved through three criteria, architecture (uses Hybrid Cloud to separate sensitive- private and non-sensitive data- public cloud), privacy (K-anonymization and differential privacy), and security (homomorphic encryption). To achieve Integrity there are two categories, public auditing and verification but these approaches relies on storage service and efficiency problem. Availability is achieved by replicating data among several cloud service providers. So, in case of outage backups needs to be ready to minimize data loss and unavailability. [1]

**Proposed Solution - Bhanu**

**Critique**

The purpose of this research paper is to present a solution to the challenges faced in the development of secure and dependable cloud applications. This paper has a well-defined purpose and problem statement which have been communicated clearly to the readers. The paper follows a structured format: first, it defines the problem and then it defines the concepts required to understand the solution being proposed. The paper has been structured to provide the readers with an overview of what the paper contains: purpose of the paper, problem statement and the proposed solution. This is followed by a description of the phases involved in the Software Development Life Cycle (SDLC) and the Data Security Life Cycle (DSLC). The paper then introduces the SaaS Security Life Cycle which is a combination of the two development life cycles SDLC and DSLC). The relationship between the three life cycles have been clearly demonstrated through a well-structured diagram. The paper then highlights the necessity of following the SaaS Security Life Cycle (SSLC) for the development of dependable and secure cloud application. The challenges faced have been split across the different phases of SSLC. Each phase of SSLC is linked back to its equivalent phases in the SDLC and DSLC life cycles defining the procedures followed. It also describes how certain choices can cause a development convenience to security and dependability tradeoff. The paper defines the challenges faced in each of the phases and their possible solutions. The proposed solution has also been described clearly with the help of well-structured diagrams which contain references to other publications where readers can find more details.

However, the paper does not discuss the proposed solution in detail for the development phase. The solution proposed for the development phase is a pre-existing procedure which has simply been referenced. The solution this paper has proposed addresses the remaining three phases. The aspects of which have been discussed thoroughly in each of the relevant phases. This paper could also have included a section for future work which describes any limitations in their work that they plan on improving. This section could also provide readers with potential research topics to work on.

**References**

[1] I. Weber, S. Nepal and L. Zhu, “Developing Dependable and Secure Cloud Applications,” *IEEE Internet Computing*, vol. 20, no. 3, pp. 74–79, 2016

[2] J. Yao et al., “TrustStore: Making Amazon S3 Trustworthy with Services Composition,” *Proc. 10th IEEE/ACM Int’l Conf. Cluster, Cloud and Grid Computing*, 2010, pp. 600–605