A Secure System Development Framework for SaaS Applications in Cloud Computing

Eren TATAR, Emrah TOMUR

***Abstract*—The adoption of cloud computing is ever increasing through its economical and operational benefits. However, it also contains potential security issues in itself. Hence, while using cloud-based solutions, organizations need to be aware of these concerns and develop their solutions in a way that they include the information security management practices as a whole. In order to do that, a systematic development approach would be the most effective way to provide the necessary security controls at the beginning of the development life cycle. To handle with the security issues in the cloud computing and provide organizations a systematic way of integrating SaaS applications into their existing IT infrastructure, a secure system development framework will be developed and proposed within the scope of this study.**

***Index Terms*—Cloud Computing, SaaS, System Development Life Cycle, Secure System Development Framework**

I. Introduction

CLOUD computing has been defined several times differently by many leading experts working in IT sector. There is no just one description to be able to define all its characteristics, functionalities and architectural concept. However, all those interested in cloud computing somehow accept the definition of NIST: "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. This cloud model is composed of five essential characteristics, three service models, and four deployment models." [1]. In general, cloud computing, or just 'cloud', presents a paradigm shift in the whole traditional IT environment. With its service-oriented architecture, applications, system, and network, all of which can be offered as an on-demand self-service based on pay-per-use model. Hence, organizations can take advantage of both its economical and operational benefits. However, cloud also brings some security, privacy and trust issues up for discussion due to its unique aspects. Although most of these issues are not new, already exist in traditional IT environment, they need more consideration because of the dynamic nature of cloud computing platform. Depending upon literature and some private companies' surveys on cloud, security and privacy issues are thought as the key to adoption of cloud according to IT executives. Under these circumstances, before utilizing cloud-services, organizations should ensure that they understand the security and privacy risks in the cloud environment and their security and privacy requirements based on their business requirements are satisfied by the cloud service providers (CSPs).

Manuscript received July 15, 2013.

E. Tatar is with the department of Information Systems, Informatics Institute, Middle East Technical University, Ankara, TURKEY (e-mail: eren.tatar@metu.edu.tr).

E. Tomur is with the department of Information Systems, Informatics Institute, Middle East Technical University, Ankara, TURKEY (e-mail: emrah.tomur@gmail.com).

II. Cloud Service Models

The clear understanding of cloud architecture and features ,which are usually addressed under the title of deployment models, service models and service attributes, will help us better understand the security concerns in the cloud environment. The details of service models are given below:

Software as a Service (SaaS)

SaaS is described as publicly available services and applications on an on-demand basis. The customer's responsibility begins and ends with entering system and managing its data. Everything from application level down to the infrastructure level is under the responsibility of the provider.

Platform as a Service (PaaS)

PaaS is described as middleware which provides virtual machines, operating systems, applications, services, development frameworks. The customer is responsible for installing and managing the application that is being deployed. The service provider manages the cloud infrastructure, and operating system.

Infrastructure as a Service (IaaS)

IaaS is all the infrastructures that are offered to and can be provisioned by customers. It includes virtual machines, virtual storage, other virtual infrastructures, and other hardware assets. While the service provider manages all the infrastructure, the customer is responsible for all other aspects of the deployment.

III. Security Concerns in Cloud

With the advances in cloud computing, it continues to be significant changes in business manner and technology infrastructure of organizations. Its service-oriented

architecture changes the structure of applications and systems in terms of design, development and deploy. However, these advances also brings the existing traditional security issues and also new issues into question again. According to the CSA research [8], the cloud computing top nine threats in 2013 respectively are:

- Data Breaches
- Data Loss
- Account or Service Traffic Hijacking
- Insecure Interfaces and APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Vulnerabilities

These issues continue to be discussed today because of the highly dynamic nature of cloud computing. To deal with these security challenges precisely and properly, there needs to be a systematic approach covering all the information security management practices in order to provide essential security measures in each phases of a cloud-based solution development. Information security management can be defined as processes that enable organizations protect their IT operations and assets from unauthorized access, use, disclosure, disruption, modification, and destruction. It is not only a technical issue, but also a management issue. Hence, it is the responsibility of every member of the organization from the top to bottom. As cloud adoption increases, more confidentiality, integrity and availability, called as CIA triad, which forms the core of the information security, are demanded by cloud customers. Moreover, data security and system availability are considered the two most important service level agreement (SLA) parameters [9]. In order to respond all these issues properly, organizations should have a systematic way of integrating security practices into their development life cycle. Hence, it is possible with a security integrated system development life cycle.

IV. SYSTEM DEVELOPMENT LIFE CYCLE

The system development life cycle (SDLC) is a conceptual model including a sequence of processes followed to develop information systems. A typical SDLC phases are initiation, acquisition and development, implementation and assessment, operations and maintenance, and disposal. Although there are many SDLC models and methodologies such as the waterfall model, rapid application development (RAD), joint application development (JAD), spiral model, synchronize and stabilize, generally each of them consists of a series of defined steps or phases. Hence, integrating security activities into each phases of SDLC is an effective way to provide an appropriate level of security to protect critical assets in information systems development. Such an integration enables security to be planned, acquired, built in, and deployed as an integral part of a project or system [5]. It is also important to handle security practices in early stages of the SDLC. It plays a significant role in measuring and enforcing security requirements throughout the all phases of the life cycle. Also, the most effective way of integrating security into the SDLC is to plan and implement a detailed risk management program [5]. This will lead to identify, control, and minimize the security risks in information system by dealing with them in each phase of SDLC. Hence, an early attempt to control the risks can be accomplished in that way. The benefits of integrating security into an established SDLC are [5]:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation,
- Awareness of potential engineering challenges caused by mandatory security controls,
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques,
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner,
- Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases,
- Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment, and
- Improved systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

V. LITERATURE REVIEW

There are several studies on secure system development life cycle for cloud platform. These studies focus on addressing security and privacy risks in cloud and studying on taking precautions by integrating information security practices into each SDLC phases, generally including initiation, development or acquisition, implementation or assessment, operation or maintenance and disposal.

In order to develop a secure SDLC framework for integrating SaaS applications to built-in IT systems in organizations, the articles examined can be found below:

A. Secure System Development for Integrated Cloud Applications

The article [2] describes that integrating a SaaS application

Figure 1. Orange Model

into an existing IT infrastructure poses serious risks in terms of data and system security. According to the researchers, security issues related with integrating SaaS systems often occurs at individual integration or customization. To solve this problem, security enhancement controls are presented from the technical point of view. Besides, a model is proposed to help enterprises securely adopting a SaaS solution from the management point of view. The importance of enhancing the security controls before integrating the SaaS solutions into existing IT infrastructure is emphasized. Otherwise, it is claimed that systems will be vulnerable against high level of risks posed. In the article, SaaS solutions are classified into three categories which are stand-alone application, web based integration, and server based integration. Then, particular risks to those categories are defined in order to provide effective security controls against risks for secure integration of SaaS solutions. Afterwards, the secure integration of SaaS solutions is discussed and suggestions are offered for the defined three different types of SaaS solutions. According to the writer, in the field of IT process research, although there are many system development models, models focusing on SaaS integration security are rare. For example, SCoM [3] is shown as an example of one of those models addressing data security framework. However, its shortcoming is that it only focuses on stand-alone applications, one of the three types of SaaS solutions defined in the article. Hence, in order to help organizations enhance their security capabilities when using SaaS applications, a secure life cycle model called the Orange Model which is shown in Figure 1, is proposed. Orange Model created with reinforcing the SCoM model uses an incremental and iterative development approach. It is composed of a number of parts which are a core, pith, flesh, inner ring, peel and seeds. Each of them has its own specific meaning and function. For instance, the flesh of the model consists of eight parts representing the phases of SDLC. In the each those phases, the processes needed to be carried out, outputs of the process, and person in charge of the process are defined in detail. Business goals and risks

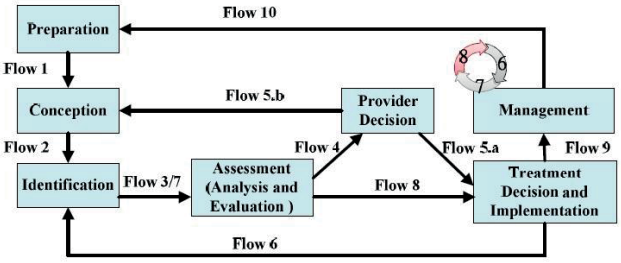

Figure 2. SCoRiM Framework

management forms the core of the Orange Model. The pith of the model covers all the phases existing in the flesh and its continuous policy improvement function and good communication with business and IT units function are defined as the key for success of secure management of the SaaS systems.

B. Enforcing Confidentiality in a SaaS Cloud Environment

The article [3] discusses that the top barriers to adoption of public cloud services (SaaS) in enterprises are losing control of systems, confidentiality issues, and rigid service level agreements (SLAs). To deal with confidentiality issues, on the basis of the idea of considering confidentiality in each phases of IT projects, a SaaS Confidentiality Risk Management Framework (SCoRiM) which is shown in Figure 2 is proposed. The framework consists of initiation, development and acquisition, implementation, operations and maintenance, disposition phases. It especially focuses on protecting critical data of small and medium sized enterprises (SMEs). Hence, it is claimed that framework enhances the client side confidentiality management on SMEs. It aims to enable SMEs gain capability of confidentiality risk analysis to determine which SaaS provider best suits their confidentiality needs. Also, the aim of the SCoRiM is cited as to enhance the data confidentiality with and without support from the service providers. However, there is no practical way offered in the article to implement confidentiality risk analysis. Without any checklist, it is quite difficult for SMEs to evaluate SaaS providers properly. In the article, SaaS applications are classified into two categories. The first one is complete applications like ERP, and CRM and the latter is custom applications like banking or customer tracking. Even if SCoRiM covers management of risks related with confidentiality issues in both categories, it especially focuses on the latter one.

C. Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle

The article [4] focuses to discuss the legal issues regarding protecting information and computer systems, laws and regulatory requirements. By its architecture, cloud computing centralizes the data storage in SaaS applications, thus, it causes data privacy and protection issues. This is why a cloud security self-governance deployment framework (Cloud SSDLC) which

Figure 3. Cloud SSDLC

is shown in Figure 3 is proposed in this article, especially from government and industry point of view. There are five main phases in proposed framework which are initiation, development, implementation, operation and destruction. Framework integrates SSDLC, cloud security domain guidelines and risk considerations. When it does that, the corresponding risks are integrated into each phase. The benefit of the model in practice is also supported by different cases from industry and government perspectives. The basic contribution of the framework is summarized as follows:

- Enhancing security in the cloud applications by integrating SSDLC and cloud,
- Identifying critical security issues in each system development life cycle phase,
- Being developed by working on a real case in a government cloud information system.

D.SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environment

In this article [7], it is described that security mechanisms are required in order to ensure the secure adoption of cloud computing since cloud gives rise to various security concerns including outsourcing, shared responsibility, virtualization, multi-tenancy, service level agreements, and heterogeneity. Consequently, a security framework for cloud computing environments is proposed to deal with different security challenges. The proposed framework consists of different modules to handle security and trust issues such as identity management, access control, policy integration among multiple clouds, trust management, secure services composition and integration. In fact, framework is based on multi-domain policy integration and secure service composition. While building the framework, security, policy and trust issues are being handled within the specified modules, not in the phases of SDLC as in the other frameworks discussed before.

E. Security Considerations in the System Development Life Cycle

The purpose of this guideline [5] is to help agencies in integrating security into their established IT system development life cycle. The guideline focuses on the information security components, not the implementation and development of SDLC. The base methodology is the waterfall SDLC in the document. For the successful integration of security into SDLC and for viability of it, the key security roles and responsibilities in SDLC are depicted. Each security activity in each phases of SDLC is defined by its description, its expected outputs including suggestions and further information for integration of other security activities, its synchronization to ensure its proper adaptation and its interdependencies with other tasks.

VI. FUTURE WORK

In order to provide such guarantees for requirements, organizations have relied on standards, guidelines and SLAs provided by cloud providers. There are some commonly accepted information security standards like ISO 27001-27006, 29361, 29362, 29363. However, although these standards are applicable to cloud [6], they should be reviewed and progressively developed for the cloud environment based on varying cloud security requirements. Moreover, the research and studies show that there are not any commonly accepted cloud standard. As well the developed models or frameworks do not present a comprehensive solution on how organizations will securely utilize application software offered as a service in their established IT system. The proposed models generally focus on a specific field of SaaS by categorizing SaaS solutions, and do not cover all core information security management practices. Currently, there are also variations in each element of the life cycle because there are no commonly accepted cloud standards. Hence, it is important to emphasize that standardization is required in order to make contribution to future development of cloud computing. Hence, we are planning to develop a comprehensive framework for organizations' system development life cycle to help them take the essential IT security issues regarding cloud computing into consideration when utilizing SaaS applications in their IT systems.

REFERENCES

[1] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145, September, 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Y. Chou, J. Oetting, *Secure System Development for Integrated Cloud Applications*, 2012 Second Symposium on Network Cloud Computing and Applications, IEEE, 2012.

[3] Y. Chou, J. Oetting, *Enforcing Confidentiality in a SaaS Cloud Environment*, 19th Telecommunications forum TELFOR 2011, Serbia, Belgrade, November 22-24, 2011, IEEE.

[4] T. Kao, C. Mao, C. Chang, K. Chang, *Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[5] R. Kissel, K. Stine, M. Scholl, H. Rossman, J. Fahlsing, J. Gulick, *Security Considerations in the System Development Life Cycle*, NIST, SP 800-64 Rev. 2, 2008.

[6] R. L. Krutz, R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley Publising, Inc. ,2010.

[7] H. Takabi, J. B. D. Joshi, G. Ahn, *SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments*, 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

[8] *CSA, The Notorious Nine: Cloud Computing Top Threats in 2013*, Top Threats Working Group, CSA, 2013. Available: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[9] Breaking through the cloud adoption barriers, KPMG Cloud Providers Survey, KPMG International, 2013. Available: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/cloud-service-providers-survey.pdf