

# Chapter 6

## Cloud Security Engineering

### Concept and Vision: Concept and Vision

**Shadi Aljawarneh**

*Jordan University of Science and Technology, Jordan*

#### **ABSTRACT**

*The research community found that a software system should be evolved once every few months to ensure it is adapted to the real-world environment. The system evolution requires regularly amendments that append, delete, or alter features. It also migrates or converts the software system from one operating platform to another. These amendments may result in requirements/ specifications that were satisfied in a previous release of a software system not being satisfied in the subsequent versions. As a result, software evolutionary changes violate security requirements, and then a system may become vulnerable to different kinds of attacks. In this paper, concepts and visions are presented to avoid/minimize the Cloud security issues.*

#### **INTRODUCTION**

Due to lack of control over the Cloud software, platform and/or infrastructure, several researchers stated that a security is a major challenge in the Cloud. In Cloud computing, the data will be virtualized across different distributed machines, hosted on the Web (M. Taylor, 2010), (R. Marchany, 2010). In business respective, the cloud introduces a channel to the service or platform in which it could operate (M. Taylor, 2010).

Thus, the security issue is the main risk that Cloud environment might be faced. This risk comes from the shortage of control over the Cloud environment. A number of practitioners described this point. For example, Stallman (Ch. Arthur, 2010) from the Free Software Foundation re-called the Cloud computing with Careless Computing because the Cloud customers will not control their own data and software and then there is no monitoring over the Cloud providers and subsequently the data owner may not recognize where data is geographically located at any particular time.

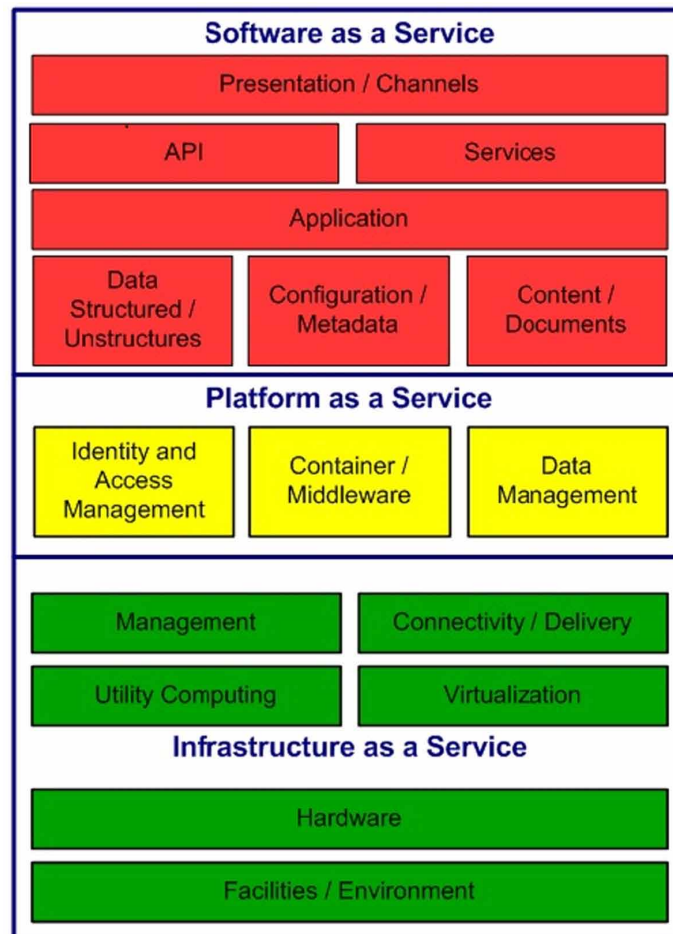
DOI: 10.4018/978-1-5225-5634-3.ch006

Threats in the Cloud computing might be resulted from the generic Cloud infrastructure which is available to the public; while it is possessed by organization selling Cloud services (R. Marchany, 2010), (R. Chow et al.,2009).

In Cloud computing, software and its data is created and managed virtually from its users and might only accessible via a certian cloud's software, platform or infrastructure. As shown in Figure 1, there are three Cloud models that describe the Cloud architecture for applications and services (M. Taylor, 2010), (R. Marchany, 2010):

1. **The Software as a Service (SaaS) Model:** The Cloud user rents/uses software for use on a paid subscription (Pay-As-You-Go).
2. **The Platform as a Service (PaaS) Model:** The user rents a development environment for application developers.
3. **The Infrastructure as a Service (IaaS) Model:** The user uses the hardware infrastructure on pay-per-use model, and the service can be expanded in relation to demands from customers.

Figure 1. Models of Cloud environment  
Taken from (M. Taylor, 2010)



7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/cloud-security-engineering-concept-and-vision/203499](http://www.igi-global.com/chapter/cloud-security-engineering-concept-and-vision/203499)

## Related Content

---

### Establishing Academic-Industry Partnerships: A Transdisciplinary Research Model for Distributed Usability Testing

Amber L. Lancaster and Dave Yeats (2021). *Research Anthology on Recent Trends, Tools, and Implications of Computer Programming* (pp. 1286-1303).

[www.irma-international.org/chapter/establishing-academic-industry-partnerships/261079](http://www.irma-international.org/chapter/establishing-academic-industry-partnerships/261079)

### High-Performance Computing for Theoretical Study of Nanoscale and Molecular Interconnects

Rasit O. Topaloglu, Swati R. Manjari and Saroj K. Nayak (2012). *Handbook of Research on Computational Science and Engineering: Theory and Practice* (pp. 78-97).

[www.irma-international.org/chapter/high-performance-computing-theoretical-study/60356](http://www.irma-international.org/chapter/high-performance-computing-theoretical-study/60356)

### Arts and Branches of Science Significantly Contributing to Cyber and Cyber Security: The West European and the Russian Views

Margarita Levin Jaitner and Áine MacDermott (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 977-994).

[www.irma-international.org/chapter/arts-and-branches-of-science-significantly-contributing-to-cyber-and-cyber-security/203544](http://www.irma-international.org/chapter/arts-and-branches-of-science-significantly-contributing-to-cyber-and-cyber-security/203544)

### An Enhanced Method for Running Embedded Applications in a Power-Efficient Manner

N. M. G. Kumar, Ayaz Ahmad, Dankan Gowda V., S. Lokesh and Kirti Rahul Rahul Kadam (2023). *Energy Systems Design for Low-Power Computing* (pp. 257-277).

[www.irma-international.org/chapter/an-enhanced-method-for-running-embedded-applications-in-a-power-efficient-manner/319999](http://www.irma-international.org/chapter/an-enhanced-method-for-running-embedded-applications-in-a-power-efficient-manner/319999)

### A Semantic Approach for Multi-Agent System Design

Rosario Girardi and Adriana Leite (2018). *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 941-968).

[www.irma-international.org/chapter/a-semantic-approach-for-multi-agent-system-design/192908](http://www.irma-international.org/chapter/a-semantic-approach-for-multi-agent-system-design/192908)