Chapter 35
A Conceptual Security Framework for Cloud Computing Issues

Shadi Aljawarneh
Jordan University of Science and Technology, Jordan

Muneer Bani Yassein
Jordan University of Science and Technology, Jordan

ABSTRACT

In this article, perspectives from Cloud computing practitioners are shown in order to address clients concerns and bring about awareness of the measures that put in place to ensure software security of the client services running in the Cloud. In addition, the authors have investigated the impacts of a number of the existing approaches and techniques to put a systematic survey of the current software security issues in the Cloud environment. Based on such perspectives and survey, a generic framework conceptually is designed to outline the possible current solutions of software security issues in the Cloud and to present a preferred software security approach to investigate the Cloud research community. As a potential enhancement on the proposed Cloud software security framework, the concepts of fuzzy systems might be used to solve a large numbers of issues in the Cloud security on different framework levels.

1. INTRODUCTION

Cloud computing is a new concept in the era of technology. This concept adds new paradigms, techniques and approaches to computing science. In Cloud, software and its data are created and maintained virtually for the users and only accessible via a particular Cloud's software, platform or infrastructure (Aljawarneh, 2011). Before 2005, clients imagined renting resources, information and software in order to operate, run and enhance their devices and programs. Currently, it is possible to rent whatever resources you like so that this dream is now realized. In general, Cloud has four basic characteristics:

DOI: 10.4018/978-1-5225-5634-3.ch035

1. **Scalability:** Cloud opts to use scalable architecture. Scalability means that hardware units are added to bring more resources to the Cloud system (David, et al., 2015). However, this feature is in trade-off with the software security. Therefore, scalability might ease to depict the Cloud and it might increase criminals who would access the Cloud storage and Datacenters illegitimately (Aljawarneh, 2011). Vaquero et al (Vaquero, et al., 2012) aimed to make the reader's acquaintance with this problem in distributed systems: user-oriented service-level scalability. Scalability issues are analysed from the Infrastructure as a Service (IaaS) and the Platform as a Service (PaaS) point of view, as they deal with different functions and abstraction levels (Vaquero, et al., 2012).
2. **Availability:** The services, platform and data are accessible at any time and place. Cloud exposes potentially to greater software security threats, principally when the Cloud is based on the Internet rather than an organization's own platform (David, et al., 2015).
3. **Automatic Backup:** Day after day, a lot of manufacturers of electronic devices rely on the model of Cloud computing and they are progressively more including this paradigm in their products since it brings the characteristics of communication and automatic backup of the information (Sessions, 2009).
4. Adding value and additional services to the user such as the ability to synchronise among friends on social networking sites such as Facebook and friends on phones registered the same names in the Palm phones (Aljawarneh, 2011).

Currently, academic world requires sharing, distributing, integrating and changing information, linking applications and other resources within and among organizations (Wang, Zhang, & Cao, 2009). Due to openness, virtualization and distribution interconnection, software security becomes a crucial challenge in order to ensure the integrity, confidentially and authenticity of digitized data in Clouds (Aljawarneh, et al., 2010; Aljawarneh, et al., 2015).

In this paper, we have attempted to put the readers in the current state of software security issues and levels in Cloud by presenting a generic framework that might assist in the protection of their Cloud services and Datacenters. This paper provides a survey of software security tools and techniques in the area of Cloud Computing. It analyses the major vendors solutions and practitioners approaches, and then provides a general layered framework aimed at providing organizations with a roadmap of the different perspectives from which software security issues in Cloud-based systems can be faced. Such paper contribution plays an unquestionable central role in the adoption of Cloud-based solutions by organizations.

Software security is the main issue that might be faced the practitioners of Cloud applications and systems. The owners of data might be concerned because the data and coupled with software are not under their control but rather possessed by the Cloud. In addition, the data owner may not be aware of where the data is geographically located at any particular time. So our research statement in this study is to question how to secure the data contained in the Cloud (Aljawarneh, et al., 2015).

The rest of the paper is organized as follows. Section 2 states six reasons of increasing client's suspicions during the use of Cloud services and describes the current Cloud software security tools. Section 3 describes the scenarios of the Cloud threats. In Section 4, we have conceptually presented a generic framework consisting of components and levels in the Clouds. Thus we have reviewed the existing solutions and discussed a number of practitioners' perspectives correlated to the client's suspicions against using Cloud software security. A case study about the health software security has been discussed in Section 5. Finally, we have drawn the conclusions and future work.