Chapter 29
Runtime Reusable Weaving Model for Cloud Services Using Aspect-Oriented Programming:
The Security-Related Aspect

Anas M.R. Alsobeh
Yarmouk University, Jordan

Aws Abed Al Raheem Magableh
Yarmouk University, Jordan

Emad M. AlSukhni
Yarmouk University, Jordan

ABSTRACT

Cloud computing technology has opened an avenue to meet the critical need to securely share distributed resources and web services, and especially those that belong to clients who have sensitive data and applications. However, implementing crosscutting concerns for cloud-based applications is a challenge. This challenge stems from the nature of distributed Web-based technology architecture and infrastructure. One of the key concerns is security logic, which is scattered and tangled across all the cloud service layers. In addition, maintenance and modification of the security aspect is a difficult task. Therefore, cloud services need to be extended by enriching them with features to support adaptation so that these services can become better structured and less complex. Aspect-oriented programming is the right technical solution for this problem as it enables the required separation when implementing security features without the need to change the core code of the server or client in the cloud. Therefore, this article proposes a Runtime Reusable Weaving Model for weaving security-related crosscutting concerns through layers of cloud computing architecture. The proposed model does not require access to the source code of a cloud service and this can make it easier for the client to reuse the needed security-related crosscutting concerns. The proposed model is implemented using aspect orientation techniques to integrate cloud security solutions at the software-as-a-service layer.

DOI: 10.4018/978-1-5225-8176-5.ch029

1. INTRODUCTION

Cloud Computing environment is accessed via the internet, which enables end-users to access a range of distributed resources and web services over a network. It can give several clients access to secure shared data at the same time by tokenizing the data during transmission or when it is processed (Zhang, Cheng & Boutaba, 2010; Asma, Chaurasia & Mokhtar, 2012). Cloud vendors (providers) provide a certain level of security for client data; however, clients of cloud services may also need to implement their own security features for peace of mind. When clients add their own security features, this obviously increases the complexity of each application logic in the cloud computing environment as well as that of the physical distributed system itself. There are several security aspects that are in place/time that attempt to ensure the security of cloud services (Look, 2011; The Apache Software Foundation, 2016; Apache Axis, 2016), but access to the base code of the services being protected is required and these aspects are usually controlled by the cloud services vendor (e.g., Amazon Web Service (AWS), Microsoft Azure, etc.)

Cloud computing offers a variety of ways to manage how data flows across a plethora of applications on the web. Cloud computing is relatively new and the range of cloud services is still growing but there is already a wide range of tools available that support the development and deployment of web applications. However, these tools have some serious drawbacks, particularly with respect to ensuring the security aspect of client applications. They are almost completely static and thus do not support the dynamic adaptation of cloud services (Powell, Stembridge and Yuan, 2012). This is unfortunate to say the least as the cloud computing environment is very dynamic. However, due to the quality of the existing support tools, it cannot easily take on new features and it is difficult to reuse some applications or crosscutting concerns already on the cloud logic for different purposes. Cloud computing has to deal with a number of security aspects related to encryption, authentication, denial-of-services attacks, access control and privacy threats (Alani, 2014). The ways in which these are dealt with are usually defined and set when developing or deploying a cloud application and this means that they cannot be altered when the application is running in the cloud. Additionally, cloud services are tightly coupled to cloud applications logic. For instance, when data security involves encrypting the data there is also a need for suitable and well-defined security aspects to be in place for safe and effective data sharing. Ensuring that this is the case, is made more complicated by the highly complex nature of the cloud.

Aspect-oriented software development (AOSD) and aspect-oriented programming languages (AOPL) have been developed to handle such limitations. They can capture new crosscutting concerns and new changes that relate to security. In fact, AOP weaving, as it is commonly known, is a relatively easy way to separate and the scattered or tangled crosscutting concerns logic between modules of the core cloud service with constituting a new cloud service layer. This research aims to propose an approach to enhance the security of applications in the cloud environment. It proposes the utilization of Reusable Service Layer (RSL) to improve the implementation of security-related crosscutting concerns in cloud services and proposes a way in which these concerns can be integrated into the cloud environment at runtime. The proposed approach provides an adequate amount of cloud service metadata (i.e., context information) so that the requisite information can be obtained for effective implementation of security aspects. This is based-on employ AOP to decouple and isolate the security characteristics from the core cloud service.

This research introduces an aspect-oriented cloud reusable security service (ACRSS) model, which can be used for several security scenarios in distributed cloud applications. The main objective of ACRSS