future internet

Editorial

Introduction to the Special Issue on Recent Advances in Web Services

Eduardo B. Fernandez

Department of Computer and Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL 33431, USA; E-mail: ed@cse.fau.edu; Tel.: +1-561-297-3466

Abstract: We have collected five papers describing different aspects of web services and cloud computing. Cloud computing is the next stage of application interoperability and it is a logical extension of web services, both approaches being a variety of Service-Oriented Architecture. The papers cover security, migration, certification, and application development. Together, these papers provide a useful panorama of some of the issues of these two technologies.

Keywords: web services; distributed systems; cloud computing; security; patterns; security patterns; cloud applications; cloud migration; SOA

Web services first appeared around the year 2000 in an effort to improve interoperability between applications, and both IBM and Microsoft adopted them as part of their main strategic objectives [1]. Web services introduced the possibility of using services that could be found in the Internet as part of user applications. This possibility enables the designer to concentrate on the core business aspects of the application; many ancillary services can simply be imported from the Internet. Web services were one of the first realizations of a Service-Oriented Architecture (SOA), where components present interfaces that can be invoked by other components. Their convenient interoperability was obtained at the cost of a variety of standards being developed by different institutions causing confusion for vendors and users. To make things worse, the standards were complex and kept evolving [2]. Security was an important objective, again spawning a variety of standards. Each standard comprises many pages of explanation and it is hard to understand all its points. This motivated Fernandez E.B. and his group to describe security standards as patterns where UML models made the descriptions clearer and more precise. The paper by Fernandez and his collaborators in this issue surveys their work in building patterns that describe web service security standards [3]. Their latest work is a standard for WS-Conversation, not included in this survey [4]. We believe that these patterns have contributed to make the web service security landscape much clearer. Our interest also comes from the need to have

pattern catalogs to build secure systems; we have proposed a methodology for this purpose which is based on patterns [5]. Although fast and dirty REST-based web services are very popular now, their lack of security and integrity precludes their use in any quality application; complex web services are still needed for more demanding applications. New standards, specific to cloud systems, are starting to appear and the existing web services standards can be used as guidelines for them. The same dilemma between speed and security is emerging in the cloud environment.

The paper by Anisetti *et al.* [6] considers another important security problem for those who use web services: how a consumer can specify the security properties they want in a service and how to verify, at execution time, if the service actually satisfies them. The approach is also useful for administrators in controlling their services.

Cloud computing is a new embodiment of SOA, where users access a variety of services to implement their functional needs, ranging from the basic use of the hardware to elaborated applications. Clouds are a generalization of web services where the services are grouped into three coarse sets based on the architectural level where they reside. Instead of providing users with application-oriented services as in conventional web services, now the users can access services on any architectural level.

Many existing legacy systems could migrate to the cloud in search of lower costs or better quality. The paper by Rosado *et al*. discusses migration problems and surveys current work as well as new directions for research in this area [7]. This aspect is particularly important because we need to understand the issues raised by this move: will a system which is reasonably secure in a controlled environment still be equally secure after being placed in a cloud system? The main conclusion of the paper is that this problem has not been studied in detail and more work is needed.

A designer trying to combine different cloud services in her application has a serious problem because the services usually come with low-level descriptions of their functions as seen by a particular provider. To solve this problem, Nguyen *et al.* [8] propose the concept of *cloud blueprints* which provide abstract descriptions of cloud services which allow combining services from different layers or different providers.

The paper by Fehling *et al.* [9] addresses how to build application flows, incorporating specific quality factors, using architectural patterns. Designers can in this way build automated management flows for applications.

Papers [2] and [9] are good examples of the value of patterns to describe and manipulate complex architectures. The patterns in [2] could be used to add security to the workflows of [9]. Papers [8] and [9] have some complementary objectives and it would be interesting to find ways to use both approaches together.

References

1. Levitt, J. From EDI to XML and UDDI: A Brief History of Web Services. 2012, IWK20010928S0006. Informationweek. Available online: http://www.informationweek.com/ news/6506480 (accessed on 17 June 2012).

2. Fernandez, E.B.; Hashizume, K.; Buckley, I.; Larrondo-Petrie, M.M.; VanHilst, M. Web services security: Standards and products. In *Web Services Security Development and Architecture: Theoretical and Practical Issues*; Gutierrez, C.A., Fernandez-Medina, E., Piattini, M., Eds.; IGI Global Group: Hershey, PA, USA, 2010; pp. 152–177.

3. Fernandez, E.B.; Ajaj, O.; Buckley, I.; Delessy-Gassant, N.; Hashizume, K.; Larrondo-Petrie, M.M. A Survey of Patterns for Web services security and reliability standards. *Future Internet* **2012**, *4*, 430–450.

4. Ajaj, O.; Fernandez, E.B. A pattern for the WS-SecureConversation standard for web services. *Pattern Lang. Programs*, submitted for publication, 2012.

5. Fernandez, E.B.; Larrondo-Petrie, M.M.; Sorgente, T.; VanHilst, M. A methodology to develop secure systems using patterns. In *Integrating Security and Software Engineering: Advances and Future Vision*; Mouratidis, H., Giorgini, P., Eds.; IGI Global Group: Hershey, PA, USA, 2006; pp. 107–126.

6. Anisetti, M.; Ardagna, C.A.; Damiani, E.; Frati, F.; Muller, H.A.; Pahlevan, A. Web service assurance: The notion and the issues. *Future Internet* **2012**, *4*, 92–109.

7. Rosado, D.G.; Gomez, R.; Mellado, D.; Fernandez-Medina, E. Security analysis in the migration to cloud environments. *Future Internet* **2012**, *4*, 469–487.

8. Nguyen, D.K.; Lelli, F.; Papazoglou, M.P.; van den Heuvel, W.J. Blueprinting approach in support of cloud computing. *Future Internet* **2012**, *4*, 322–346.

9. Fehling, C.; Leymann, F.; Rutschlin, J.; Schumm, D. Pattern-based development and management of cloud applications. *Future Internet* **2012**, *4*, 110–141.