Requirements Eng (2013) 18:297–298
DOI 10.1007/s00766-013-0177-4

EDITORIAL

Requirements Engineering for Security, Privacy and Services in Cloud Environments

Stefanos Gritzalis · Lin Liu

Published online: 3 July 2013

Being one of the most versatile technologies innovated till date, cloud computing and its managed services have brought about drastic changes to improvise and enhance the existing IT infrastructures. A critical issue that has been raised as a result of the rapid employment of Cloud services and the distributed nature of the enabling Cloud architecture is the satisfaction of new security requirements and the protection of users' privacy. Specifically, the distinct architectural and functional characteristics of cloud computing raise a number of security and privacy challenges that need to be identified, analysed and modelled. The aim is to design and develop secure, trustworthy and privacy preserving Cloud Systems Application Services.

Software engineering in cloud computing is an essential aspect for obtaining a systematic, disciplined and quantifiable approach to the development, operation and maintenance of software services. Incorporating security and privacy during the engineering process is of vital importance for assuring the development of reliable, correct, robust and trustful systems as well as adaptive and evolving software services that satisfy users' requirements. To this extent, the need to investigate methods and tools that will assist developers in constructing more reliable privacy-oriented information systems and services in Cloud environments is fully justified.

S. Gritzalis (✉)
Department of Information and Communication Systems Engineering, University of the Aegean, Mytilene, Greece
e-mail: sgritz@aegean.gr
URL: http://www.icsd.aegean.gr/sgritz

L. Liu
School of Software, Tsinghua University, Beijing, China
e-mail: linliu@tsinghua.edu.cn
URL: http://www.thss.tsinghua.edu.cn/linliu

This special issue of the Requirements Engineering journal aims at providing researchers and professionals with insights into the state-of-the-art in Requirements Engineering for Security, Privacy and Services in Cloud Environments from the views of modelling language, design framework and policy compliance knowledge patterns.

1 The content of this special issue

The papers presented in this special issue contribute to the afore-mentioned research directions. The three papers presented in this special issue have been selected following a thorough review process of eight submissions that responded to the Call for Papers which was distributed. Each of the papers was reviewed by at least three reviewers, all established requirements engineering researchers, in two review stages.

In their paper entitled "*Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements*", C. Kalloniatis, H. Mouratidis and S. Islam provide a framework for the elicitation and analysis of security and privacy requirements for cloud-based system, which integrates the *Secure Tropos* and *PRiS* modelling languages. Actors, their related attributes and associations were introduced in the modelling language so that the cloud computing migration needs and security, privacy requirements can be elicited, and the appropriate deployment and service models can be selected based on the elicited security and privacy requirements. Finally, a real-world case study, based on the Greek National Gazette, is given to demonstrate the applicability of the approach.

F. Moyano, C. Fernandez-Gago and J. Lopez in their paper entitled "*A Framework for Enabling Trust*

Requirements in Social Cloud Applications" present a trust and reputation framework to support the development of trust-aware social cloud applications. The paper argues that when social and cloud applications are put together, trust and reputation considerations become especially relevant that deserves attention of developers. It uses an example scenario of implementing a social website for cloud providers. The suggested approach is a callable framework that can be adapted by developers to their application-specific needs. Instead of proposing a new trust or reputation model, the paper is providing mechanisms to implement any trust model of the developer's choice.

The paper by K. Beckers, I. Côté, S. Faßbender and S. Hofbauer, "*A Pattern-based Method for Establishing a Cloud-specific Information Security Management System*" presents a requirements patterns-based approach for designing a cloud-based information security management system in accordance with ISO 27001 standard. The authors analysed that the challenges of design and implementing an ISO 27001 standard compliance system include: asset identification, threat and risk analysis and security reasoning. Then a method that adopts several existing requirements engineering methods and patterns in response to security-specific tasks, e.g. context descriptions, threat analysis and policy definition, is given in detail. It eases the effort of establishing an information security management system and can produce the necessary documentation for an ISO 27001 compliance procedure. The proposed approach is illustrated using an online banking example.

Acknowledgments We would like to thank a number of people that contributed to the preparation of this special issue. First, we would like to thank Prof. P. Loucopoulos and Prof. W. Robinson, *Requirements Engineering* Editors-in-Chief, for giving us the opportunity to prepare this special issue. In addition, we would like to thank numerous reviewers for their professional effort to select the articles to reflect the essence of this special issue and all authors for their contributions and for undertaking two-cycle revision of their manuscripts.