

Identity management in GRID computing and Service Oriented Architectures: research and practice

Theodora Varvarigou · Vassiliki Andronikou

Received: 7 January 2010 / Accepted: 22 January 2010 / Published online: 26 February 2010
© The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract Today, Service-Oriented Architecture (SOA) and Grid and Cloud computing comprise the key technologies in distributed systems. In systems following the SOA approach, functionalities are delivered and consumed as services. Given the variety of resources (i.e. data, computing capabilities, applications, etc) as well as the variation of user-requested Quality of Service (e.g., high performance, fast access, low cost, high media resolution, etc), there is a need for advanced user management, trust establishment and service management mechanisms which adjust, monitor and evaluate service provision according to the users' requirements and rights. Within this context, security and privacy requirements have become of great importance, as well the need for flexible and efficient identity management. This editorial of the special issue "Identity Management in Grid and SOA" discusses the importance of identity management within SOA and Grid environments. A number of techniques and existing systems addressing these issues are presented and evaluated. Identity management is considered in various contexts and at different levels, including service composition level, system level and inter-system communication level.

Keywords Identity · Grid · Cloud · Service Oriented Infrastructure · Service Oriented Architecture · Security · Privacy

Introduction: the trend towards SOA and SOI

Service Oriented Architecture (SOA) furnishes one of the key guiding principles in applications and systems development in many domains, including health, e-learning and financial among others (Kart et al. 2007; Pasatcha and Sunat 2008). SOA aims to simplify development and delivery of new business functionalities, enabling

T. Varvarigou (✉) · V. Andronikou
National Technical University of Athens, 9, Heroon Polutechniou Str., 15773 Athens, Greece
e-mail: dora@telecom.ntua.gr

V. Andronikou
e-mail: vandro@telecom.ntua.gr

service reusability and interoperability and reducing development and maintenance costs (Radhakrishnan and Sriraman 2007). Meanwhile, current business and scientific applications continuously pose stricter requirements for performance, availability, security, scalability, privacy, usability and flexibility. Within this context, Service Oriented Infrastructures (SOI) -in compliance with SOA—come to fill in these gaps by providing infrastructural resources as services.

Grid and Cloud computing comprise a heavily-researched and very promising attempt for SOI realisation both in the industrial (Thanos et al. 2007) and the scientific world. Although initially designed and developed for facilitating high performance computing applications, such as simulations, this new computing approach aims also at supporting highly collaborative applications across organisations and users of different expertise and varying levels of authorisation. The Grid infrastructure, and gradually the Cloud, is incorporating efficient mechanisms for aggregating, managing and orchestrating various resources (computational resources, data, storage, services, applications, knowledge, human expertise). These resources might be heterogeneous, distributed and dynamic, serving a continuously increasing number of users with differing requirements wanting Quality of Service (QoS) and who are subject to different access and service use policies.

Identity in Grid and SOA: questions and issues

Given the current trend of increasing complexity of collaboration among users and systems, there are two aspects of paramount importance to the implementation of SOI: First, the **heterogeneity**, the dynamic nature and the geographical dispersion of the resources (even across organisational boundaries) (Zhang et al. 2008) and second, the **nature** of business processes concerning complex policies for informational privacy, security and privacy comprise two aspects of paramount importance to the implementation of SOI (Mikkonen and Silander 2006), (Jana et al. 2009).

Important issues are raised that need to be properly handled such as *confidentiality, traceability, non-repudiation, data protection, informational privacy, access control* and *trust* and need to be properly handled. Failing to deal adequately with them may lead to serious consequences, such as sensitive information leak and unauthorised access to important business processes, and hence adopting Grid and Cloud computing requires extensive cooperation among the relevant experts.

Managing *identity* in the Grid and SOA

This special issue aims at presenting current practices, trends and mechanisms on identity management in Grid and Cloud environments. The paper titled “*A Security Framework for Dynamic Collaborative Working Environments*” by Matthias Assel, Stefan Wesner and Alexander Kipp (DOI:10.1007/s12394-009-0027-1) presents the application of the Grid-related security concepts into collaborative working environments and results in a security model that enables dynamic, trust-enabled and secure collaborations. Within this context, scenarios from the health and the engineering domains offering real-world experience are described. The paper titled “*Delegation of Access Rights in Multi-Domain Service Compositions*” by Laurent

Bussard, Anna Nano and Ulrich Pinsdorf underlines that delegation of access rights across trust domains will become essential in service composition scenarios. The authors propose a framework supporting abstract delegation that harmonises the management of heterogeneous access control mechanisms and offers a unified user experience independent of these mechanisms.

In the paper entitled “*Quantifying Privacy in Terms of Entropy for Context Aware Services*” (DOI:10.1007/s12394-009-0026-2) Athanasios S. Voulodimos and Charalampos Z. Patrikakis propose a framework through which the users of Location Based Services are able to configure the level of privacy they wish according to the desired balance between privacy and quality of services offered. They use entropy as a means of measuring the capability of locating a user’s whereabouts and identifying personal selections. In the paper entitled “*Information Exchange in Business Collaboration using Grid Technologies*” by Fotis Aisopos, Konstantinos Tserpes, Magdalini Kardara, George Panousopoulos, Stephen Phillips and Spyridon Salamouras (DOI:10.1007/s12394-009-0028-0), the authors describe a novel Grid-based Anti-Money Laundering (AML) system, which allows for trusted, secure and efficient communication of appropriate information among banks in order for money laundering activities to be detected. Their research approach focuses on identity management and trust establishment, and more specifically Service Level Agreements (SLAs).

The basis of the presented research of authors of the paper “*Trusting third-parties storage providers for holding personal information. A context-based approach to protecting identity-related data in untrusted domains*” by Giulio Galiero and Gabriele Giammatteo lies on the encryption of data before they are uploaded to an untrusted domain. In this paper the authors further extend this approach by introducing dynamic adaptation of the encryption process through the EncryptMe tool.

This special editorial issue also includes the paper titled “*Federated Identity Management in Mobile Dynamic Virtual Organizations*” by Matteo Gaeta, Juergen Jaehnert, Kleopatra Konstanteli, Sergio Miranda, Pierluigi Ritrovato and Theodora Varvarigou which presents the identity management mechanisms developed within the context of a Mobile Grid infrastructure.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

- Jana D, Chaudhuri A, Bhaumik BB. Privacy and Anonymity Protection in Computational Grid Services. *IJCSA*. 2009;6(1):98–107.
- Kart F, Gengxin Miao, Moser, LE, Melliar-Smith PM. A Distributed e-Healthcare System Based on the Service Oriented Architecture, *Services Computing*, 2007. SCC 2007, IEEE International Conference on 9–13 July 2007, Page(s):652–659.
- Mikkonen H, Silander M. Federated Identity Management for Grids, *Networking and Services*, 2006. ICNS. International conference on, 2006.
- Pasatcha P, Sunat K. A distributed e-education system based on the service oriented architecture, *Management of Innovation and Technology*, 2008. ICMIT 2008. 4th IEEE International Conference on 21–24 Sept. 2008, Page(s):1282–1285.

- Radhakrishnan R, Sriraman B. Aligning Architectural Approaches towards an SOA-Based Enterprise Architecture, *Software Architecture 2007. WICSA '07. The Working IEEE/IFIP Conference on 6–9 Jan. 2007*, Page(s):38–38.
- Thanos GA, Courcoubetis C, Stamloulis GD. Adopting the Grid for Business Purposes -The Main Objectives and the Associated Economic Issues, In: *Lecture Notes in Computer Science -Grid Economics and Business Models*, Springer Berlin / Heidelberg, Volume 4685/2007, Pages: 1–15.
- Zhang W, Zhang H, Zhang B, Yang Y. “An Identity-Based Authentication Model for Multi-domain in Grid Environment,” *2008 International Conference on Computer Science and Software Engineering*, Volume 3, Pages: 165–169, 2008.