Editorial: Security and Dependability of Cloud Systems and Services - Part II

Stefano Russo, *Senior Member, IEEE* and Marco Vieira, *Member, IEEE*

THIS is the second part of the Special Issue on Security and Dependability of Cloud Systems and Services, which we organized to solicit novel results in these important and closely related research areas. Indeed, security and dependability are increasingly important concerns for cloud systems and services, due to their spread in a large variety of application fields, including business- and mission-critical scenarios. This demands for innovative methodologies, algorithms and techniques for building services in which companies, organizations and citizens can trust and rely upon.

The call attracted seventy-eight submissions from thirty-one countries; all of them underwent a thorough review process, which resulted in eleven selected manuscripts, with an acceptance rate of 14 percent. The eleven articles were split into two parts.

The first part of the special issue focused on security aspects from the perspective of both providers and users. The six manuscripts addressed challenges in the areas of cloud trust management, secure cloud storage systems, and security-related service level agreements.

This second part includes five papers which address relevant dependability and security issues concerning services in federations of cloud platforms, in mobile cloud computing, in data centers and in sensor clouds.

Federations of cloud services and resources allow organizations to use a combination of different clouds—across different providers and tenants—to satisfy the needs of their applications, made up by a collection of diverse software components. Dependability and security are important concerns for such applications, but they are typically addressed separately. The first article, entitled "Cost Effective, Reliable and Secure Workflow Deployment over Federated Clouds" by Zhenyu Wen, Jacek Cala, Paul Watson, and Alexander Romanovsky, consider altogether issues of security, reliability and cost. The problem targeted is the deployment of workflow applications on federated clouds. The paper presents an algorithm which takes into account reliability, security and monetary cost of the deployment; the latter considers computing, storage and communication costs. The algorithm is shown to provide solutions which meet security requirements while providing reliability equivalent to two popular multi-criteria scheduling algorithms, at a cheaper cost.

In the second article, entitled "Risk Assessment in a Sensor Cloud Framework Using Attack Graphs", Amartya Sen and Sanjay Madria deal with security risk assessment in a sensor cloud. Sensor clouds are collections of heterogeneous wireless sensor networks (WSNs)—in general with different ownerships—whose sensing services are provided through a cloud platform. They may be subject to security threats both in the deployment areas, where sensors are not physically monitored for long periods or may even be hostile environments, and in the cloud integration environment. The authors propose a risk assessment framework for WSNs in a sensor cloud, based on attack graphs; the attacks may target confidentiality, integrity or availability. The framework supports security administrators in better comprehending the threats and take necessary actions, as well as to determine the efficiency of a security measure. It is validated by comparison with a variety of simulated attack scenarios.

The cloud computing paradigm has become popular also for mobile applications: indeed, with a market value currently estimated in several billion US dollars per year, Mobile Cloud Computing (MCC) is one of today's hottest new technologies. However MCC goes beyond the mere access to data storage and processing services outside the mobile device, and despite its rapid growth, many issues still need to be addressed. In the third article "A Context-Aware Architecture Supporting Service Availability in Mobile Cloud Computing", Gabriel Guerrero-Contreras, José Luis Garrido, Sara Balderas-Díaz, and Carlos Rodríguez-Domínguez explore the use of autonomic computing techniques to cope with disconnections and network partitions which are inherent to the dynamic nature of mobile networks, and may compromise service availability. In scenarios such as emergency situations and tourism, people may use local collaborative tools exploiting distributed resource pools provided by nearby mobile nodes. For such scenarios, the authors propose a reusable and adaptable service-oriented software architecture which uses a combination of service replication, self-configurable replicas' activation/hibernation, context-awareness and election mechanisms, to satisfy availability requirements of mobile clouds. The proposal has been evaluated through the simulation of some scenarios representative of emergency situations, where traditional network infrastructures may be unavailable, and it is necessary to support the collaboration between work groups through data storage and processing services.

- *S. Russo is with the Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione, Università di Napoli Federico II, Via Claudio 21, Napoli 80125, Italy. E-mail: stefano.russo@unina.it.*
- *M. Vieira is with the Departamento de Engenharia Informática, Universidad de Coimbra, Polo II - Pinhal de Marrocos, Coimbra 3030-290, Portugal. E-mail: mvieira@dei.ac.pt.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TSC.2017.2735818

1939-1374 © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Software and hardware failures cannot be considered rare exceptions in large datacenters. Service providers deal with them through redundancy and by enacting automatic failover mechanisms, which need to be carefully designed and configured to balance their overhead for real cost-effectiveness. In the fourth article, entitled "Reliable Computing Service in Massive-scale Systems through Rapid Low-cost Failover", Renyu Yang, Yang Zhang, Peter Garraghan, Yihui Feng, Jin Ouyang, Jie Xu, Zhuo Zhang, and Chao Li try to overcome some limitations of most common failover techniques in cloud datacenters, by considering timing failures and simultaneous failures—besides crash failures—and by minimizing unnecessary restarts, to reduce the overhead. This goal is achieved by means of soft-state inference for checkpoint-based state recovery. The experiments with Fuxi—a popular resource management and job execution system, deployed for instance within the Alibaba cloud—demonstrate the effectiveness of the proposed soft-state approach.

In the last article, Andrea Rosà, Lydia Chen, and Walter Binder cope with failures in today's multi-tenancy and multi-purpose datacenters running big-data applications. Failures are not infrequent in such large-scale datacenters, and have a significant impact on performance, which calls for a better comprehension of application failures and for the ability to predict them. In the paper titled "Failure Analysis and Prediction for Big-Data Systems", the authors present a study based in execution traces of a Google datacenter. They first analyze unsuccessful job and task executions, with particular reference to three types of failures, namely fail, kill, and eviction. They quantify the impact of failures on performance, and find patterns and interdependencies among unsuccessful jobs and tasks. They also explore failure root causes in relationship to workload and system attributes. Then, building on the observations resulting from the analysis, the authors propose on-line prediction models to classify unsuccessful executions in big-data systems. Six different classifiers are evaluated using the accuracy metric (i.e., the percentage of jobs or events correctly classified): linear and expanded linear discriminant analysis, quadratic discriminant analysis, logistic regression, support vector machines, neural networks. The latter provides the most accurate prediction of job and event outcomes.

We hope that the novel research contributions of the manuscripts in this special issue will provide interesting insights for further advances in the areas of security and dependability of cloud systems and services.

We wish to thank again all authors who submitted their work for consideration for this special issue, as well as the about 230 reviewers from all over the world, who helped us to select the eleven accepted papers: we are very grateful to all of them for providing timely and high-quality reviews. We due a special thank to the former Editor in Chief, Dr. Ling Liu, for her encouragement and wise suggestions throughout the whole long lasting process. Finally, we wish to thank once more the Editor in Chief, Dr. James Joshi, the Associate Editor in Chief, Rong N. Chang, and the Administrator, Ms. Christine Kurzawa of *IEEE Transactions on Services Computing* for their constant and valuable support.

Stefano Russo is a professor of computer engineering with Federico II University of Naples, where he teaches software engineering and distributed systems, and leads the DEpendable Systems and Software Engineering Research Team (www.dessert.unina.it). He co-authored more than 160 papers in the areas of software engineering, middleware technologies, and mobile computing. He is associate editor of the *IEEE Transactions on Services Computing*, and a senior member of the IEEE.

Marco Vieira received the PhD degree from the University of Coimbra. He is a full professor with the University of Coimbra, Portugal. He is an expert on dependability and security evaluation and benchmarking and his research interests include fault injection, robustness testing, software development processes, and software quality assurance, subjects in which he has authored or co-authored more than 150 papers in refereed conferences and journals. He is a member of the IEEE.