Guest Editors' Introduction: Special Section on Cloud Computing Assessment: Metrics, Algorithms, Policies, Models, and Evaluation Techniques

Salvatore Distefano, *Member*, *IEEE*,
Antonio Puliafito, *Member*, *IEEE*, and Kishor S. Trivedi, *Fellow*, *IEEE*

CLOUD Computing is emerging as a promising computing, storage and sensing paradigm able to provide a flexible, dynamic, resilient, and cost effective reference architecture and processing infrastructure for both academic and business environments. It aims at raising the level of abstraction of physical resources toward a user-centric perspective, focused on the concept of service as the elementary unit for building any application. Both physical/hardware and logical/abstract (software, data, etc.) resources are therefore provided as a service and the whole Cloud design and the implementation choices follow a service oriented approach.

The Cloud paradigm is a real, operating and effective solution in commercial and business context, mainly offering data and computing resources and services according to a pay-per-use model, using the Web and the client-server paradigm and adopting specific Service Level Agreements (SLA). Several commercial solutions exist and a rising number of service and infrastructure providers operate in the business arena such as Amazon, Rackspace, Salesforces, Google, Microsoft, IBM, GoGrid, and so on. Cloud computing is quickly and widely spreading also in open contexts such as scientific, academic and social communities, due to the increasing demand of computing resources required by their users. As an example, there are several research activities and projects on Cloud, such as Nimbus, Eucalyptus, OpenNEbula, CLEVER, OpenCyrrus, OpenStack, OCCI, etc., aiming at implementing open infrastructures by providing specific middleware.

Apart from cost savings, other reasons of the success of the Cloud paradigm are: user-centric interfaces acting as unique, user friendly, points of access for users needs and requirements; on-demand service provisioning; Quality of Service (QoS) guaranteed offers, and autonomous systems for managing hardware, software and data transparently to users.

- *S. Distefano is with the Politecnico di Milano, Piazza L. da Vinci 32, 20133 Milano, Italy. E-mail: salvatore.distefano@polimi.it.*
- *A. Puliafito is with the University of Messina, Contrada di Dio, 98166 Messina, Italy. E-mail: apuliafito@unime.it.*
- *K.S. Trivedi is with the Duke University, 27708 Durham, NC, USA. E-mail: kst@ee.duke.edu.*

For information on obtaining reprints of this paper, please send e-mail to: tdsc@computer.org.

There are several open issues in the Cloud computing paradigm, mainly concerning information security (confidentiality and integrity), trustworthiness, interoperability, federation, reliability, availability, etc., which very often need to be evaluated altogether looking for performance and dependability indices and their correlation to SLA and QoS parameters, attributes only partially addressed, thus inhibiting the use the Cloud paradigm.

In particular, it is of primary importance in the Cloud computing context to adequately take into account problems related to SLA and QoS: effort is still required in order to formally specify attributes and requirements, to implement adequate protocols and policies, to model and investigate a Cloud infrastructure, to monitor and predict its behaviour.

This special issue deals with open problems related to Cloud computing assessment, and the interest raised in the scientific community is confirmed by the high quality of the papers received, which were selected after a review process started on July 2012 and ended on February 2013. Some relevant numbers are: 43 total submissions, nine papers accepted (approximately 0.2 acceptance ratio) after three rounds of reviews by more than 190 reviewers involved in the process. First of all we would like to thank the authors of all the submitted papers for the high quality of their scientific contributions, and the prompt and timely reaction to the continual requests from the editors.We also thank all reviewers for their dedication and timeless efforts, which allowed us to select very high quality papers and respect the strict deadlines we have imposed. Last but not least, special thanks go to Pam Gimzo and Ravi Sandhu for their prompt and valuable support in making the revision process as smooth as possible.

Different nonfunctional properties are considered in the special issue, mainly investigating Clouds behavior from the different perspectives of security and performance. For this reason we decided to split the special issue into two parts: the first that deals with security-related aspects (part I), and the second related to performance aspects (part II) of Cloud systems.

Part I of this special issue addresses security aspects of Cloud computing such as trustworthiness, privacy, security vulnerabilities, countermeasures and threats to both physical (hardware) and logical (software, applications, data) architecture and infrastructure.

1545-5971/13/$31.00 © 2013 IEEE Published by the IEEE Computer Society

Specifically four papers compose part I. The first paper, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," by Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, focuses on Infrastructure-as-a-Service (IaaS) Cloud security. In particular, it investigates the problem from the network perspective, dealing with issues arising from collaborative attacks such as the Distributed Denial-of-Service (DDoS). It proposes a defense-in-depth intrusion detection framework named NICE, aiming at detecting and predicting such kind of attacks. The approach adopted is based on the attack graph model as well as on software switch customization. The effectiveness of this solution is demonstrated through an in-depth experimentation on a private cloud environment, showing how NICE can reduce the risk of the Cloud system from being exploited and abused by internal and external attackers.

The second paper "Security and Privacy-Enhancing Multicloud Architectures," by Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, addresses security and privacy issues. It proposes to use multiple Cloud providers for gaining security and privacy, comparing ten different techniques grouped into four categories by the specific approach they implement. This paper therefore provides an interesting classification of such techniques and on the metrics to consider in their evaluation. The assessment of the multi-Cloud techniques properties thus identified shows that there is no optimal approach to foster both security and legal compliance. Specific rules and guidelines are therefore provided starting from an in depth comparison of such techniques.

The third paper "Entrusting Private Computation and Data to Untrusted Networks," by Yuriy Brun and Nenad Medvidovic, investigates trustiness of information and computing operations. The paper proposes sTile, a technique for distributing trust-needing computation onto insecure network computing infrastructure. The problem and the solution technique are formally specified, theoretically demonstrating the effectiveness of the technique in preserving privacy in an efficient and scalable way. Furthermore, specific experiments on real infrastructure were performed aiming at verifying and validating the sTile approach also against different approaches such as the ones based on homomorphic encryption.

Homomorphic encryption is adopted in the last paper of this special issue, "Towards Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data," by Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue and Minglu Li, to secure data in Cloud environments. Specifically, the problem of securing multikeyword top-k retrieval over encrypted cloud data is addressed, starting from a server-side ranking SSE scheme. To this end, the authors propose a two-round searchable encryption algorithm. The paper provides an in depth security analysis, demonstrating the effectiveness of the proposed solution in ensuring data privacy with good performance and low overhead.

Overall, we believe that part I of this special issue has achieved its primary purpose of collecting state-of-the-art research on Cloud computing security, addressing several open issues on the topic. The papers included in this issue not only represent important theoretical advances, which offer opportunities for further research, but also describe interesting and effective applications in real domains.

Salvatore Distefano
Antonio Puliafito
Kishor S. Trivedi
Guest Editors

Salvatore Distefano received, in October 2001, the master's degree in computer engineering from the University of Catania. In 2006 he achieved the PhD degree on advanced technologies for the information engineering from the University of Messina. His research interests include stochastic modeling, performance evaluation, reliability techniques, parallel and distributed computing and software engineering. During his research activity he participated to the development of the WebSPN, ArgoPerformance and GS3 tools. He has been involved in several national and international research projects. He is member of international conference committees and he is on the editorial boards of several international journals on dependability and distributed computing topics. At this time, he is an assistant professor at Politecnico di Milano. He is a member of the IEEE.

Antonio Puliafito is a full professor of computer engineering at the University of Messina, Italy. His interests include parallel and distributed systems, networking, wireless and Cloud computing. He has contributed to the development of the software tools WebSPN and ArgoPerformance. He is coauthor (with R. Sahner and K.S. Trivedi) of the text entitled Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package, edited by Kluwer Academic Publishers. He is also the responsible of two big Grid Projects (TriGrid VL and PI2S2) funded by the Sicilian Regional Government and by the Italian MIUR, respectively. He is currently a member of the general assembly and of the technical committee of the Reservoir and Vision, IP projects funded from the EU to explore the deployment and management of IT services and data across different administrative domains. He is also the main investigator of the Italian PRIN2008 project Cloud@Home, trying to combine cloud and volunteer computing. He is a member of the IEEE.

Kishor S. Trivedi holds the Hudson Chair in the Department of Electrical and Computer Engineering at Duke University, Durham, North Carolina. He was the Duke-Site Director of an National Science Foundation Industry-University Cooperative Research Center between NC State University and Duke University for carrying out applied research in computing and communications. He has served as a principal investigator on various AFOSR, ARO, Burroughs, DARPA, Draper Lab, NEC, IBM, DEC, Alcatel, Telcordia, Motorola, NASA, NIH, ONR, NSWC, Boeing, Union Switch and Signals, NSF, Cisco, Huawei, NATO, JPL and SPC funded projects and as a consultant to industry and research laboratories. He was an editor of the *IEEE Transactions on Computers* from 1983-1987. He was on the editorial board of the *IEEE Transactions on Dependable and Secure Systems*. He is a codesigner of NASA's HARP, IBM's SAVE, SHARPE, SPNP, Boeing's IRAP and SREPT modeling packages. He is the author of a well known text entitled, Probability and Statistics with Reliability, Queuing and Computer Science Applications. He is a fellow of the IEEE.