World Wide Web (2016) 19:1–3
DOI 10.1007/s11280-015-0366-9

Guest editorial: large-scale Web virtualized environment

Ernesto Damiani[1] · **Kokou Yetongnon**[2] · **Richard Chbeir**[3]

Published online: 15 August 2015

Virtualization-based paradigms like cloud computing provide a powerful model that allows to simply and securely connect users to information resources on-demand and anywhere. Modern Web applications are increasingly hosted in a cloud-computing infrastructure, able to communicate and interact with external mobile devices. Such applications should dynamically scale in response to changes in the workload to guarantee service level agreements. This trend brought about a number of new modeling, design and implementation issues for Web applications.

Solving these key issues requires both first-class theoretical research and careful experimental evaluation to show that model predictions are faithful to observed application behavior. Results need to be validated in the context of hybrid provisioning on multiple, heterogeneous virtualized platforms and cloud stacks. In particular, Web-based information systems rely on models and tools for representing, integrating and linking data or resources from heterogeneous sources or platforms.

This special issue received many submissions from researchers and practitioners working on Web environments analyzing the impact of virtualization on them. After two rounds of review, eventually eight high quality papers were chosen.

The paper titled "MUBaaS: Mobile Ubiquitous Brokerage as a Service" presents a cloud-based application middleware, called Mobile Ubiquitous Brokerage as a Service (MUBaaS), which enables n-devices of a user to access multiple cloud services endpoints in soft-real time. This is achieved by proposing distributed brokers that coordinates the transactions of the user while taking load balancing into account. Pilot evaluations of the proposed architecture prove real-time application synchronization with reasonable scalability. The use of multiple

✉ Ernesto Damiani
ernesto.damiani@unimi.it

Kokou Yetongnon
kokou@u-bourgogne.fr

Richard Chbeir
richard.chbeir@univ-pau.fr

[1] Università degli Studi di Milano, 26013 Milan, Italy

[2] Université de Bourgogne, 21078 Dijon, France

[3] Université de Pau (UPPA), 64000 Anglet, France

personalized mobile devices (e.g., smartphones and tablets) is on the increase. As such, users expect to access several network-based services across their n-devices. Previous studies proposed Ubiquitous Cloud Computing (UCC) where a single user or service consumer is facilitated to access multiple services from n-devices. However, seamless synchronization of data between the multiple devices can be hindered by intermittent loss of connectivity in mobile wireless networks due to user mobility. Another source of latency is non-scalable architectures that tend to be overburdened during peak loads.

In "Behavior Evaluation for Trust Management based on Formal Distributed Network Monitoring" authors presents a technique for providing trust verdicts by evaluating the behaviors of different agents, making use of distributed network monitoring. This will provide trust management systems based on "soft trust" information regarding a trustee experience. They propose a formal distributed network monitoring approach to analyze the packets exchanged by the entities, in order to prove a system is acting in a trust-worthy manner. Based on formal "trust properties", authors analyze the systems behaviors, and then provide trust verdicts regarding those "trust properties". Furthermore, automatized testing is performed using a suite of tools we develop and finally, the methodology is applied to a real industrial DNS use case scenario.

In the paper titled "Access and Privacy Control Enforcement in RFID Middleware Systems: Proposal and Implementation on the Fosstrak Platform" authors describes novel techniques for automating the identification and storing of information in RFID tags. They provide a privacy policy-driven model using some enhanced contextual dimensions of the extended Role Based Access Control model, namely the purpose, the accuracy and the consent dimensions. Authors use the provisional context to model security rules whose activation depends on the history of previously performed actions. To show the feasibility of our privacy enforcement model, they first provide a proof-of-concept prototype integrated into the middleware of the Fosstrak platform, then evaluate the performance of the integrated module in terms of execution time.

The paper, titled "AcT: Accuracy-aware Crawling Techniques for Cloud-Crawler", presents The AcT framework, that supports two different accuracy-aware personalized crawling techniques to attain the optimal accuracy level of retrieving the information. Given the crawling frequency as a resource constraint, the first scheme aims to find the optimal schedule that maximizes the accuracy. In the second scheme, authors optimize the crawling frequency and the corresponding crawling schedule for a given accuracy level. They propose a supervised technique that monitors each news source for a particular time period and collect the news update patterns. The news update patterns are later analyzed using mixed integer programming to discover the optimal crawling schedule for the first scheme, whereas a greedy strategy is proposed to discover the optimal crawling frequency and crawling schedule for the second scheme.

In "Modeling Dynamic Recovery Strategy for Composite Web Services Execution" authors present an experimental study to evaluate the model and determine the impact on QoS parameters of different recovery strategies; and evaluate the intrusiveness of our strategy during the normal execution of Composite Web Services (CWS). In particular, during the execution of CWS, a component Web Service (WS) can fail and can be repaired with strategies such WS retry, substitution, compensation, roll-back, replication, or checkpointing. Each strategy behaves differently on different scenarios, impacting the CWS QoS. Authors propose a non intrusive dynamic fault tolerant model that analyses several levels of information: environment state, execution state, and QoS criteria, to dynamically decide the best recovery strategy when a failure occurs.

In “Context Respectful Counseling Agent virtualized on Web”, authors propose an analysis of workers distressing situations through a context-respectful counseling agent, presenting aa study of the feasibility and the effects of the tool in helping distressing persons in solving problems.

In the paper “Anonymizing Multimedia Documents” authors deal with the problem of Multimedia documents sharing and outsourcing, proposing the delinkability concept, a privacy-preserving constraint to bound the amount of information outsourced that can be used to re-identify individuals. Furthermore, authors present a set of experiments to demonstrate the efficiency of their approach.

The paper titled “Data Services with uncertain and correlated semantics” proposes a probabilistic approach to model the semantic uncertainty of data services. Services along with their possible semantic views are represented in probabilistic service registry. The correlations among service semantics are modeled through a directed probabilistic graphical model (Bayesian network). Based on this modeling, the authors study the problem of composing correlated data services to answer a user query, and propose an efficient method to compute the different possible compositions and their probabilities.

We would like to express our heartfelt thoughts to all authors who submitted manuscripts for consideration, and to the anonymous reviewers for their constructive criticism and help in making the final decisions. Our sincere gratitude will also go to the WWWJ EiC, Prof. Yanchun Zhang, as well as to Ms. Jennylyn Rosiento, and Mr. Hector Nazario from the Springer Journal Editorial Office for helping us to presenting this special issue to readers.