 Editorial: Security and Dependability of Cloud Systems and Services

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

Service-based cloud computing systems are used nowadays in many business- and mission-critical scenarios. As the service-oriented paradigm increasingly spreads in a wide range of application fields, including big data, cloud storage, mobile cloud computing, and sensor cloud, there is a growing need for sound methodologies, algorithms and techniques for building services in which companies, organizations and citizens can trust and rely upon. Security and dependability are therefore becoming more and more relevant concerns for such systems, whose complexity, heterogeneity, and fast-changing dynamics bring difficult challenges to the research and industry communities.

We organized this Special Issue on Security and Dependability of Cloud Systems and Services to solicit novel results in these important and closely related research areas. As a result, the call received seventy-eight quality manuscripts from thirty-one different countries. All of them underwent a thorough review process, at the end of which we selected eleven manuscripts, with an acceptance rate of 14 percent.

The first part of the special issue focuses on security and trustworthiness aspects, including six papers that address relevant research issues from the perspective of both providers and users.

The first two articles deal with cloud trust management. The outsourcing of data and computation to the cloud leads users to pay attention to confidentiality and integrity issues. With the availability of many cloud service providers, customer decisions may depend on the level of trust that can be posed on them. Although cloud solutions today employ many security mechanisms, providers must give evidence that the advertised cloud services and security mechanisms are effectively enforced. Clearly, the management of such trust involves third parties, which users can query about the trustworthiness of the cloud service dependency for their cloud applications. In the article “RepCloud: Attesting to Cloud Service Dependency”, Anbang Ruan and Andrew Martin present an approach—named RepCloud—to manage cloud trust, which is based on reputation systems—a widely employed solution for modeling trust for peer-to-peer applications. RepCloud provides fine-grained attestations for the trust of a cloud computing base, exploiting a decentralized attestation scheme. The evaluation in a simulated Infrastructure-as-a-Service cloud environment shows that RepCloud exhibits much less overhead compared to existing attestation schemes, be they centralized or decentralized, but without the use of reputations systems.

Trust in cloud service providers is the problem faced also by Vincent Emeakaroha, Kaniz Fatema, Lisa van der Werff, Philip Healy, Theo Lynn, and John Morrison in the article “A Trust Label System for Communicating Trust in Cloud Services”. They address specifically the issue of communicating trust and trustworthiness, which is important to reduce the customers’ perception of uncertainty and of risks in the adoption of cloud solutions for the provisioning of their business services. The source of such uncertainty is the lack of transparency about the operational conditions and the quality of service offered by the diverse providers. The solution that the authors propose is the use of a trust label system, for which they show the technical implementation and its operationalization, and the evaluation using a real world use case scenario. The trust label system includes metrics and a data location model to inform consumers of their data location in clouds, as well as a service run-time monitoring framework to dynamically update the information displayed by the trust label interface. The metrics concern service execution, data management and contract conditions.

The next three articles cope with security of cloud storage systems, that is, the on-demand outsourcing of data by data owners to public cloud servers, while allowing intended data users to retrieve them through the cloud.

In the article “Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage”, Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen, and Jin Liu describe a public auditing scheme for strengthening trust of users (the data owners) in cloud storage service providers; this goal is pursued by checking data integrity remotely. In public auditing, an authorized third party auditor performs data integrity checks on behalf of data owners. The scheme supports privacy preservation, batch auditing and dynamic data operations, outperforming the previous schemes in computation complexity, storage costs and communication overhead.

The security of cloud storage systems is investigated by Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han in the article “KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage” from the perspective of the data access control. Attribute-based
encryption (ABE) is known to support fine-grained access control; and outsourced ABE allows users to access encrypted data stored in cloud. However, the amount of encrypted files stored in cloud nowadays is so large that query processing may become inefficient. The article proposes a novel ABE scheme, which outsources key-issuing and decryption, and supports keyword search. The proposed scheme is proved secure against chosen-plain text attacks.

Outsourced data access control is also the topic of the article “SecRBAC: Secure data in the Clouds”. To prevent unauthorized data access by the cloud service provider, and to ensure the provider is applying the access control policy defined by the user, Juan M. Marín Pérez, Gregorio Martínez Pérez, and Antonio F. Skarmeta Gómez propose to enrich the authorization model with increased role-based expressiveness. This is achieved by leveraging the logic formalism provided by semantic Web technologies. In their solution, data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. As a proof of concept, they describe a prototype integrated within Google services.

The last article of the first part of this Special Issue touches security aspects of Service Level Agreements (SLAs). SLAs are contracts between cloud service providers and customers specifying the characteristics of the provided services. Their enforcement poses several technical configuration issues to providers. In “Automatically Enforcing Security SLAs in the Cloud”, Valentina Casola, Alessandra De Benedictis, Madalina Erascu, Jolanda Modic, and Massimiliano Rak address the problem of automatic enforcement of SLAs related to security features. They propose a framework to manage the whole life cycle of security SLAs. Based on a security SLA model, the framework supports a security-driven planning process for automatically acquiring and configuring cloud resources for the optimal deployment of security-related software components in the cloud.

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

We wish to thank all authors who submitted their work for consideration for this special issue. With the high number of high quality manuscripts submitted to this Special Issue, we could not decide which of them to select without the valuable work of the about 230 reviewers from all over the world: 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 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.