Journal of Cloud Computing
a SpringerOpen Journal

EDITORIAL Open Access

Special issue on security in cloud computing

Martin Gilje Jaatun[1*], Costas Lambrinoudakis[2] and Chunming Rong[3]

* Correspondence: martin.g.jaatun@sintef.no
[1]Department of software engineering, safety and security, SINTEF ICT, Trondheim NO-7465, Norway
Full list of author information is available at the end of the article

Abstract

This special issue presents extended and revised versions of distinguished papers presented at the security & privacy track of the 3rd IEEE International Conference on Cloud Computing Technology and Science (IEEE Cloudcom 2011).

Guest editors' introduction

Cloud Computing may be considered as the next logical step in resource outsourcing, but security is recognized as the main stumbling block for wider cloud adoption. Although recent advances in cryptographic disciplines such as fully homomorphic encryption and secure multiparty computation are promising, it is clear that performance issues currently require us to cast a wider net to find practical solutions to cloud security that work with technology that is available today. In the following pages you will find a wide variety of approaches that contribute to this goal.

This is a special issue based on extended versions of papers invited from the security & privacy track of the 3rd IEEE international Conference on Cloud Computing Technology and Science (IEEE CloudCom), held in Athens, Greece from November 29th to December 1st 2011. The conference was organized jointly by the University of the Aegean and the University of Piraeus under the auspices of the IEEE TCSC with IEEE CS sponsorship.

The CloudCom conference series is steered by the Cloud Computing Association which was initiated in 2008 and formally registered in Norway in 2009. Since the first conference in this series, in 2009 in Beijing, one can notice a growing interest in the Cloud computing field, both in academia and industry. This was reflected both in the 2010 conference in Indianapolis and in the 2011 conference in Athens, where we have yet again noticed an increased number of submissions that reached 237. Acceptance rate was 24% with 58 high quality papers accepted for the main conference. Moreover, several work-in-progress and workshop papers were accepted. They reflect emerging work in new important areas on Cloud computing and shall provide a stimulus for further growth.

The papers in this special issue demonstrate the broad span of concerns in Cloud Computing security:

To lead off, Gonzalez et al. survey the state of the art in Cloud security in their article "*A quantitative analysis of current security concerns and solutions for cloud computing*". In their paper "*Implementation of a Secure Genome Sequence Search*

Platform on Public Cloud - Leveraging Open Source Solutions", Saxena et al. explore the challenges of using Cloud Computing to handle large amounts of potentially sensitive data. Watson exploits the fact that different parts of Cloud data may have different security levels in his article "*A Multi-Level Security Model for Partitioning Workflows over Federated Clouds*", showing how less sensitive data can be handled by cheaper, less secure providers, while data containing e.g. personal health information is restricted to providers with a defined security level. The idea of splitting up data to improve confidentiality when using public Cloud providers is taken to an extreme by Jaatun et al. in their article "*The Design of a Redundant Array of Independent Net-storages for Improved Confidentiality in Cloud Computing*". Virtualization is one of the pillars of Cloud Computing, and the security of virtual machines is therefore vital; this is tackled by Schwarzkopf et al. in their article "*Increasing Virtual Machine Security in Cloud Environments*". In "*Privacy preserving collaborative filtering for SaaS enabling PaaS clouds*", Basu et al. describe their experiences developing collaborative filtering in Google App Engine and Amazon Web Services to avoid individual user's preferences from being identified. Doelitzscher et al. introduce the concept of Security Audit as a Service (SAaaS) in their article "*An agent based business aware incident detection system for cloud environments*". Finally, Monfared and Jaatun present an approach for handling a compromised computing service in the OpenStack cloud platform in "*Handling Compromised Components in an IaaS Cloud Installation*".

CloudCom 2012 will be held on December 3rd in Taipei, Taiwan, and we are already looking forward to an exciting conference!

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Department of software engineering, safety and security, SINTEF ICT, Trondheim NO-7465, Norway. [2]Department of Digital Systems, University of Piraeus, 80, Karaoli & Dimitriou Str,, Piraeus 18534, Greece. [3]Center of IP-based Services Innovation (CIPSI), University of Stavanger, Stavanger NO-4036, Norway.

Received: 2 July 2012 Accepted: 11 July 2012
Published: 16 August 2012

doi:10.1186/2192-113X-1-17
Cite this article as: Jaatun *et al.*: Special issue on security in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications* 2012 **1**:17.