



Guest Editors

Stefanos Gritzalis

University of the Aegean, Greece

sgritz@aegean.gr

<http://www.icsd.aegean.gr/sgritz>

Chris Mitchell

Royal Holloway, University of London, UK

C.Mitchell@rhul.ac.uk

<http://www.chrismitchell.net/>

Bhavani Thuraisingham

University of Texas at Dallas, USA

bhavani.thuraisingham@utdallas.edu

<http://www.utdallas.edu/~bxt043000>

Jianying Zhou

Institute for Infocomm Research, Singapore

jyzhou@i2R.a-star.edu.sg

<http://icsd.i2r.a-star.edu.sg/staff/jianying/>

Aims and Scope

Cloud Computing (CC) is the new trend in computing and resource management. The architectural shift towards thin clients and the conveniently centralized provision of computing resources that the CC paradigm introduces, offer significant economic benefits to its users.

However, the remarkable CC benefits are not offered at no cost. As clients' lack of direct resource control, new security and privacy risks are introduced. The whole IT infrastructure is under the control of the cloud provider and the clients have to trust the security protection mechanisms that the cloud and the service providers offer. At the same time, the centralization of resources constitutes the cloud provider a very tempting target. The CC technology is evolving rapidly and the security and privacy protection mechanisms must keep this quick pace in order to support the acceptance of the cloud model. New security solutions are required, while well-established practices must be revisited.

This special issue of the **International Journal of Information Security** aims at providing researchers and professionals with insights on the state-of-the-art in **Security in Cloud Computing**. It will publish original, novel and high quality research contributions from industry, government, business, and academia.

The topics of interest include, but are not limited, to:

- Auditing in Cloud Computing
- Business and security risk models
- Cloud Infrastructure Security
- Cloud-centric security modeling and threats
- Copyright protection in the Cloud era
- Cryptography in the Cloud era
- Emerging threats in Cloud-based services
- Forensics in Cloud environments
- Legal and regulatory issues in the Cloud era
- Multi-tenancy related security/privacy issues
- Performance evaluation for security solutions
- Privacy in Cloud computing
- Secure identity management mechanisms
- Secure job deployment and scheduling
- Secure virtualization and resource allocation mechanisms
- Securing distributed data storage in the Cloud
- Security and privacy in big data management
- Security and privacy in mobile Cloud
- Security and privacy requirements engineering in the Cloud
- Security for emerging Cloud programming models
- Security management in the Cloud
- Security modelling and threats in Cloud computing
- Trust and policy management in the Cloud
- User authentication and access control in Cloud-aware services

Schedule

- Submission deadline: December 23, 2012
- Author notification - review comments: February 20, 2013
- Revised submissions: March 30, 2013
- Final decision: April 30, 2013
- Final manuscripts due: May 10, 2013
- Tentative Publication: Fall 2013

Submission Information

Submit your manuscript, through the Springer reviewing system available at:

<http://www.editorialmanager.com/ijis/>

(select for article type: Special Issue "SI: Security in Cloud Computing")

Authors are invited to submit original high quality manuscripts that should be written in grammatically correct and coherent English with a very precise and concise presentation. A single-blinded review process will be followed, which means that authors' names and other information should be shown in the first page of your manuscript