

CALL FOR PAPERS

5th IEEE Workshop on Security and Privacy in the Cloud (SPC 2019)

Washington, DC, USA, June 12, 2019

Cloud computing is today the reference paradigm for large-scale data storage and processing due to the convenient and efficient network access to configurable resources that can be easily adjusted according to the users needs. Although the benefits of cloud computing are tremendous, security and privacy concerns have still a detrimental impact on the adoption and acceptability of cloud services. In fact, users as well as companies that rely on cloud storage and computation services lose the direct control over the systems managing their data and applications, thus putting the confidentiality, integrity and availability of the data at risk. The goal of this workshop is to bring together researchers and practitioners who are interested in discussing the security, privacy, and data protection issues emerging in cloud scenarios, and possible solutions to them.

SPC 2019 is the fifth workshop in this series and will be held in Washington, DC, USA, on June 12, in conjunction with the IEEE Conference on Communications and Network Security (IEEE CNS 2019).

The workshop seeks submissions from academia, industry, and government presenting novel research, as well as experimental studies, on all theoretical and practical aspects of security, privacy, and data protection in cloud scenarios. Topics of interest include, but are not limited to:

Anonymity in cloud scenarios	Key management in cloud scenarios	Security and privacy in the Internet of Things
Applied cryptography in cloud scenarios	Privacy	Security and privacy of big data
Cloud-based biometric systems	Privacy of accesses	Security and privacy of distributed computations
Data and application security	Secure computation over encrypted data	Security and privacy of fog computing
Data and system integrity	Security and trust metrics	Security and privacy policies
Data availability in outsourcing scenarios	Security and privacy in crowdsourcing	Selective information sharing
Data protection	Security and privacy in multi/federated clouds	Threats, vulnerabilities, and risk management
Efficient access to outsourced data	Security and privacy in data outsourcing	

Paper submissions. Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Submissions should be at most 9 pages in the IEEE 8,5"x11" two-column format (<http://cns2019.ieee-cns.org/authors/submission-instructions>). Font size should be no smaller than 10 points. Submissions should not be anonymized. The workshop will also consider short submissions of up to 4 pages for results that are preliminary or that simply require few pages.

Papers should be submitted for review through EDAS (<https://edas.info/>). Only PDF files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. Papers must be received by the deadline of *March 7, 2019* (11:59 p.m. American Samoa time). Authors of accepted papers must guarantee that their papers will be presented at the workshop. Accepted and presented papers will be included in the IEEE CNS 2019 conference proceedings and also in IEEE Xplore as well as other Abstracting and Indexing (A&I) databases.

Program Chairs

Massimiliano Albanese

George Mason University, USA

Pierangela Samarati

Università degli Studi di Milano, Italy

Important dates

Paper Submission due: **March 7, 2019**

Notification to authors: **April 5, 2019**

Camera ready due: **April 12, 2019**

Program Committee

TBA