



THE SECOND

INTERNATIONAL WORKSHOP ON SECURE MOBILE CLOUD COMPUTING

IWoSeMC-21

May 10-13, 2021, Melbourne, Victoria, Australia

in conjunction with

The 21st IEEE/ACM International Symposium on Cluster,
Cloud and Internet Computing

WORKSHOP ORGANIZERS

Joanna Kolodziej – co-chair
NASK/ Cracow University of Technology, Poland

Martin Gilje Jaatun – co-chair
SINTEF Digital / University of Stavanger
Norway

Adrian Widlak – web administrator
Cracow University of Technology, Poland

IMPORTANT DATES

Paper Submissions
January 31, 2021

Acceptance Notification
February 22, 2021

**Camera Ready Papers and
Registration Due**
March 3, 2021

WORKSHOP PUBLICATION

All papers will be published in CCGrid 2021 proceedings.

As an additional incentive to attract participants, we will organize a special issue for distinguished workshop papers in one of the following journals: SIMPAT, IEEE Transactions on Service Computing, or CCPE.

LOCATION



Melbourne, Victoria, Australia

CALL FOR PAPERS

Cloud computing is recognized as a cost-effective paradigm in outsourcing infrastructure, platforms, and software. The problems related to privacy and security are still challenging especially in mobile cloud systems. Cloud end-users are now using mobile systems for applications that fall under the data intensive paradigm, such as Skyline queries, streaming information relays, and crowd sourced disaster management. However, the above paradigm shift has opened newer research directions in security, data interoperability, sustainable software development and many other areas.

This workshop primarily encompasses practical approaches that advance research in all aspects of handling large amounts of data in a secure manner in the cloud, mobile nodes and cloud connected Edge clusters such as in MANETs and Wireless Sensor Networks. Successful contributions may range from advanced technologies, applications, and innovative solutions for secure clouds, to development of methods, conceptual and theoretical models related to secure management, monitoring, scheduling and resource allocation.

Recommended topic areas include, but are not limited to:

- Mobile systems for security-aware data gathering and assimilation
- Mobile edge and fog secure models and infrastructures
- Mobile secure multi-agent systems
- Machine learning – based models and simulators of mobile clouds
- Advanced security and privacy mechanisms in smart phones and tablets
- Scalable identity and authentication protocols in mobile systems
- Security aware resource allocation and scheduling in mobile networks
- Secure communication in Smart Grid installations using Mobile Ad Hoc Network protocols
- Wireless Sensor Node applications for Smart Grid
- Secure 5G applications for Smart Grid
- Economical models in secure mobile networks
- Secure mobile network applications

Submission Guidelines:

The authors should submit their papers according the Author kit and submission Instructions available at the workshop webpage:

www.iwosemc.eu/paper-submissions