

Call for Contributions for

Submission:

1. Inform the Chair: with the Title of your Contribution.

2. Submission URL:

<https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=SECURWARE+2021+Special>

Please select Track Preference as **SSMCA**

3. Note: *For 2021, all events will be held in a hybrid mode: on site or virtual choices (live, prerecorded videos, voiced presentation slides, and .pdf slides). We hope for better times allowing us to return to the traditional on-site scientific events. However, we are ready to adapt any which way the conditions dictate.*

Special track

SSMCA: Security Solutions for Mission Critical Applications

Chairs

Adj. Prof. Dr. Fatima Hussain, Royal Bank of Canada and Ryerson University, Toronto, Canada
fatima.hussain@rbc.com

Assoc. Prof. Dr. Rasheed Hussain, Innopolis University, Russia
r.hussain@innopolis.ru

along with

SECURWARE 2021

The Fifteenth International Conference on Emerging Security Information, Systems and Technologies
<http://www.iaria.org/conferences2021/SECURWARE21.html>
November 14 - 18, 2021 - Athens, Greece

The development of smart applications holds the promise of creating today's intelligent and globally connected ecosystems. These may act as catalysts to produce a new generation of innovative technologies, which will drive the creation of new industries. Among other aspects, security of such applications is of paramount importance. User Behavior and Insider Threat is an emerging research paradigm and has deep impact on organization in terms of security and privacy.

However, a lot of work is still needed to develop and grow this user' behavior ecosystem. Insider threat has one of the many corners not in targeted organizational security, risk identification, and compliance initiatives, but also for partnered organizations.

Furthermore, Application Programming Interface (API) is considered as a new world connector and a gateway to automated, efficient, flexible and personalized user and business experience and application development. We have hardly started to address the design, development, and security issues of APIs, and smart applications, which are intricately entwined with the security and privacy challenges that impinge on the business and standardization domains.

Ubiquitous computing, context awareness, baseline behavior modeling, mobility and above all security are the core requirements for all critical applications. The track will highlight the recent developments in this evolving area from the perspective of design, computation, service, privacy and security. This track aims to bring together industrial and academic research to cover security and privacy aspects of critical applications in different domains such as online and mobile banking, public safety, and disaster response, automotive and transportation, IoT, and smart infrastructure.

Furthermore, this workshop will also highlight the recent developments in the security of such applications in the afore-mentioned domains. It will provide a platform for exchanging new ideas and research collaboration.

Topics include, but are not limited to:

- Insider threat and behavior modelling in mission critical applications
- User behavior and contextual security
- Emerging techniques for automotive (connected and autonomous cars) security
- Machine and Deep learning-based security techniques for critical applications
- Blockchain-based security in critical applications
- Internet of Things security through emerging techniques including, but not limited to, blockchain, machine learning, deep learning
- Security issues in finance and banking and solutions through emerging techniques
- Application Programming Interface (API) security for critical applications
- Communication and network security for critical applications using blockchain and machine/deep learning
- Authentication and identity management in smart applications
- Standardization activities for securing smart and critical applications

Important Datelines

Inform the Chairs: As soon as you decide to contribute.

Submission: September 4, 2021

Notification: September 20, 2021

Registration: October 1, 2021

Camera ready: October 15, 2021

Note: The submission deadline is somewhat flexible, providing arrangements are made ahead of time with the chairs.

Contribution Types

- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]
- Demos: two pages [posted on www.iaria.org]

Paper Format

- See: <http://www.iaria.org/format.html> [both LaTeX and .doc templates]
- Before submission, please check and comply with the editorial rules: <http://www.iaria.org/editorialrules.html>
- More information on camera ready preparations will be posted after the paper notifications are sent out.

Publications

- Extended versions of selected papers will be published in IARIA Journals: <http://www.iariajournals.org>
- Print proceedings will be available via Curran Associates, Inc.: <http://www.proceedings.com/9769.html>
- Articles will be archived in the free access ThinkMind Digital Library: <http://www.thinkmind.org>

Paper Submission

<https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=SECURWARE+2021+Special>

Please select Track Preference as **SSMCA**

Registration

- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.
- Registration fees are available at <http://www.iaria.org/registration.html>

Contacts

Chairs

Fatima Hussain: fatima.hussain@rbc.com

Rasheed Hussain: r.hussain@innopolis.ru

SECURWARE Logistics: steve@iaria.org
