

Call for Contributions

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

2. Submission URL:

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

Please select Track Preference as **IoTSCEC**

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

IoTSCEC: IoT Security in the Cloud through Edge Computing

Chair

Dr. Mamadou H. Diallo, Naval Information Warfare Center (NIWC) Pacific, U.S. Department of Defense,
San Diego, CA, USA
mamadou.h.diallo@navy.mil

Coordinator

Michael August, Naval Information Warfare Center (NIWC) Pacific, U.S. Department of Defense, San
Diego, CA, USA
michael.august@navy.mil

along with

ALLDATA 2021, The Seventh International Conference on Big Data, Small Data, Linked Data and Open Data
<https://www.iaria.org/conferences2021/ALLDATA21.html>
April 18, 2021 to April 22, 2021 - Porto, Portugal

In recent years, significant research efforts have been conducted to address the security of cloud-based IoT (internet of Things) systems. However, securing IoT systems end-to-end remains a significant challenge resulting in lack of trust for IoT data. This difficulty is attributed to the various challenges in securing IoT devices including severe resource constraints, diverse dedicated communication standards, and insufficient security design.

The emerging edge computing, which extends cloud resources closer to the devices, provides a promising paradigm for developing and deploying novel, reconfigurable security techniques and approaches for IoT systems in the cloud. Edge-based security techniques have the potential to increase the trustworthiness of the data collected by IoT devices.

While edge-based security for IoT is promising, the edge layer increases the attack surfaces because this layer itself needs security protection. This special track focuses on techniques and approaches that make use of the rich edge resources to provide security and trust to IoT systems deployed in the cloud.

Topics include, but not limited to:

- Edge-based security architecture design for IoT
- Edge-based, privacy-preserving mechanisms for IoT
- Trustworthy security framework for IoT based on edge computing
- IoT security based on edge computing and secure computing including homomorphic encryption and multiparty computation
- Distributed and cross-domain machine learning or data mining algorithms for IoT security
- Edge-based artificial intelligence for securing IoT
- Firewalls at the edge layer
- Intrusion Detection Systems (IDS) at the edge layer
- Edge-based authentication and authorization mechanisms
- Edge-based privacy-preserving design and algorithms

- Lightweight protocols for end device-edge communications
- Secure operating systems and lightweight virtual machines
- Data quality at the edge for IoT security
- Security approaches for untrusted edge layers

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]

Important Datelines

Inform the Chair or Coordinator: As soon as you decide to contribute

Submission: March 4, 2021

Notification: March 20, 2021

Registration: April 1, 2021

Camera ready: April 1, 2021

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

Paper Format

- See: <http://www.iaria.org/format.html>
- Before submission, please check and comply with the editorial rules:
<http://www.iaria.org/editorialrules.html>

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=ALLDATA+2021+Special>

Please select Track Preference as **IoTSCEC**

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

Mamadou H. Diallo mamadou.h.diallo@navy.mil

Michael August michael.august@navy.mil

Logistics: steve@iaria.org