

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=CLOUD+COMPUTING+2024+Special>

Please select Track Preference as **AICLOUDSEC**

3. Note: *For 2024, 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

AICLOUDSEC: AI - Curse or Blessing for the Security of Cloud Services?

Chairs

Prof. Dr. Andreas Aßmuth, Ostbayerische Technische Hochschule Amberg-Weiden
a.assmuth@oth-aw.de

Prof. Dr. Sebastian Fischer, Ostbayerische Technische Hochschule Regensburg
sebastian.fischer@oth-regensburg.de

Prof. Dr. Christoph P. Neumann, Ostbayerische Technische Hochschule Amberg-Weiden
c.neumann@oth-aw.de

along with

CLOUD COMPUTING 2024: The Fifteenth International Conference on Cloud Computing, GRIDs, and Virtualization

<https://www.iaria.org/conferences2024/CLOUDCOMPUTING24.html>

April 14 - 18, 2024 - Venice, Italy

Artificial Intelligence (AI) is currently a hype topic that has long been discussed beyond a circle of experts to the general public. More and more AI services are being made available via the Internet, enabling users to translate their texts or generate computer graphics based on simple text-based descriptions. Additionally, methods of machine learning have already been used in industry to optimize processes and process parameters or to optimally plan the maintenance of the machines used through predictive maintenance. So, Cloud-based AI services are already available, which is reason enough to think about their security.

This special track would like to address all topics related to the intersection of cloud computing, security, and AI. Contributions describing how AI methods can be used to better detect or prevent attacks against cloud services or cloud-based AI services are just as relevant as novel attack techniques against cloud services in which AI methods are used to prepare or conduct the attacks. Another topic is attacks against AI models themselves, i.e. questions such as how can AI models be manipulated so that their output corresponds to what an attacker wants, or how can such attacks be detected and prevented.

As in previous years, devices and services connected to cloud services will also be considered, which could also be affected by the attacks described, i.e., attacks against IoT devices of any kind that can have an impact on cloud services are also of interest to the special track.

Suitable research topics for this special track include, but are not limited to, the following areas:

- Cloud Security
- Cloud Privacy
- AI-based Attacks on Cloud Services, Infrastructures or Platforms
- AI-based Detection or Countermeasures against Cloud Attacks
- Attacks on Cloud-based AI services or models
- Blockchain and Artificial Intelligence
- Privacy-preserving Machine Learning in the Cloud

- Cloud Forensics
- Cloud Encryption
- Cloud Risks, especially through AI
- Cloud Threat Environment
- Cloud Database Issues, such as lack of immutability and poor security
- Cloud Governance Challenges
- Cloud and Big Data
- Cloud and Data Analytics
- Cloud-connected IoT Systems
- Cloud Zero Trust Models
- Cloud Challenges for SMEs
- Cloud-Based Password Managers
- IoT Security
- Accessibility Challenges of Cloud Usage
- User Perceptions of Cloud-Based Backups as Ransomware Mitigation
- Management Approach to Cloud Security and Privacy
- Security Challenges to Cloud, Fog or Edge Computing and Potential Solutions
- Security-oriented Task Scheduling for Cloud and Fog Computing
- Services Computing and Security/Privacy Challenges
- Any individual elements which may be contributed towards a complete solution.

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.aria.org]
- Presentations: slide only [slide-deck posted on www.aria.org]
- Demos: two pages [posted on www.aria.org]

Important Datelines

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

- Submission: Feb 28, 2024 (earlier, better)
- Notification: Mar 17, 2024
- Registration: Mar 27, 2024
- Camera ready: Mar 27, 2024

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

Paper Format

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

Publications

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

Paper Submission

<https://www.ariasubmit.org/conferences/submit/newcontribution.php?event=CLOUD+COMPUTING+2024+Special>

Please select Track Preference as **AICLOUDSEC**

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.iaia.org/registration.html>

Contact

Chairs:

Andreas Aßmuth, a.assmuth@oth-aw.de

Sebastian Fischer, sebastian.fischer@oth-regensburg.de

Christoph P. Neumann, c.neumann@oth-aw.de

Logistics (Steve McGuire): steve@iaia.org