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+2025+Special
Please select Track Preference as **AICLOUDSEC**
3. Note: *For 2025, 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

2nd AICLOUDSEC: Securing the Future - Navigating the Intersections of AI, Cloud, and IoT

Chairs

Prof. Dr. Andreas Aßmuth, Fachhochschule Kiel, Germany
andreas.assmuth@fh-kiel.de

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

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

along with

CLOUD COMPUTING 2025: The Sixteenth International Conference on Cloud Computing, GRIDs, and Virtualization
https://www.iaria.org/conferences2025/CLOUDCOMPUTING25.html
April 6 - 10, 2025 - Valencia, Spain

In the digital age, where Artificial Intelligence (AI) has evolved from a distant vision to a ubiquitous force shaping our daily lives and work, the challenges and dangers accompanying this technological revolution have also intensified. The proliferation of AI services across the Internet has ushered in a new era of convenience for users, ranging from text translation to the generation of computer graphics based on simple text descriptions. However, with this widespread use, these systems and the computing systems in the cloud that are used to provide them have become interesting targets for cyber criminals.

We are now witnessing an increasingly sophisticated landscape of targeted attacks against AI systems. These attacks range from manipulating artificial intelligence to achieve desired, often malicious outcomes, to model stealing attacks, to misusing generative AI technology for creating phishing emails, forging voices, or producing convincingly real images and videos (deepfakes) boosting social engineering attacks. In February 2024, for example, a company in Hong Kong was tricked into sending a multimillion-dollar transfer after an employee participated in a video call. What the employee didn't realize was that the other 'people' in the call, including someone who looked and sounded like the CFO, were actually fake, created using generative AI.

IoT devices are often interconnected with cloud services, and successful attacks against these cloud services can have significant repercussions for the IoT devices themselves. Similarly, attacks on or manipulations of

(numerous) IoT devices can also have consequences for the associated cloud services – even if it's only in terms of receiving incorrect sensor data. This, in turn, could invalidate calculations in the cloud aimed at optimizing the operating parameters of the IoT devices, essentially rendering them useless, for instance. Thus, it is essential to also focus on attacks targeting IoT devices or cloud services connected to these devices. These attacks can be AI-powered or traditional, underscoring the importance of comprehensive security strategies that consider both, the cloud and the IoT ecosystem.

This special track continues the reflections and discussions from CLOUD COMPUTING 2024. It aims to explore the intersections between cloud computing, security, and artificial intelligence. We invite researchers, practitioners, and experts to submit contributions on all topics related to this convergence.

Contributors are invited to submit original papers on topics including, but not limited to

- Cloud Security
- Cloud Privacy
- (AI-based) Attacks on Cloud Services, Infrastructures, or Plattforms
- (AI-based) Detection or Countermeasures Against Cloud Attacks
- AI-driven Threat Detection and Response
- AI-enhanced Identity and Access Management
- Trustworthy AI
- AI Robustness and Resilience
- AI-Driven Security Operation Centers (SOCs)
- Attacks on Cloud-based AI Services or Models
- Privacy-preserving Machine Learning (in the Cloud)
- Cloud Forensics
- Cloud Encryption
- Post-Quantum Migration: Quantum-resistant Security Protocols
- Cloud Risks, especially through AI
- Cloud Threat Environment
- AI Governance and Compliance
- Cloud Governance Challenges
- Cloud and Big Data
- Cloud and Data Analytics
- Cloud-connected IoT Systems
- Trust and Privacy in AI-powered IoT
- IoT Security
- Cloud Zero Trust Models
- Cloud Challenges for SMEs
- Cloud-Based Password Managers
- Accessibility Challenges of Cloud Usage
- User Perceptions of Cloud-Based Backups as Ransomware Mitigation
- Management Approaches to Cloud Security and Privacy
- Security Challenges to Cloud, Fog or Edge Computing and Potential Solutions
- 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.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]

- Demos: two pages [posted on www.iaria.org]

Important Deadlines
Inform the Chair or Coordinator: As soon as you decide to contribute
Submission: Feb 15, 2025
Notification: March 7, 2025
Registration: March 19, 2025
Camera-ready: March 19, 2025
Note: *The submission deadline is somewhat flexible, providing arrangements are made ahead of time with the chairs.*

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 Open Access ThinkMind Digital Library: http://www.thinkmind.org

Paper Submission
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CLOUD+COMPUTING+2025+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.iaria.org/registration.html

Contacts
Chairs
Andreas Aßmuth, andreas.assmuth@fh-kiel.de
Sebastian Fischer, sebastian.fischer@oth-regensburg.de
Christoph P. Neumann, c.neumann@oth-aw.de
Logistics (Steve McGuire): steve@iaria.org