Call for Contributions for SIAS

Note: Onsite and Online Options
In order to accommodate a large number of situations, we are offering the option for either physical presence or virtual participation. We would be delighted if all authors manage to attend in person, but are aware that special circumstances are best handled by having flexible options.

Submission:
1. Inform the Chair: with the Title of your Contribution
2. Submission URL:
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CYBER+2020+Special
Please select Track Preference as **SIAS**

Special track

SIAS: Security of Intelligent Autonomous Systems

Chair and Coordinator
Ramesh Kumar Rakesh, Researcher, R&D Centre, Hitachi Ltd, India
ramesh.rakesh@hitachi.co.in

Co-Chair
Prof. Dr. Chiranjib Bhattacharya, Indian Institute of Science, Bangalore, India
chiru@iisc.ac.in

along with

CYBER 2020, The Fifth International Conference on Cyber-Technologies and Cyber-Systems
https://www.iaria.org/conferences2020/CYBER20.html
October 25-29, 2020 - Nice, French Riviera, France

Deep learning in AI (Artifical Intelligence) technology stack has emerged as an efficient technology to build solutions to the problems which were not possible using conventional learning techniques. With the evolution of high-performance hardware to train complex models, deep learning model is being adopted in the traditional fields of image classification, speech recognition, language processing etc to advanced areas like prediction of protein structure, analysis of drug molecules, reconstruction of brain circuits, analysing particle accelerator data, impact of mutations in DNA, etc.

With their high accuracy, Deep learning networks are widely adopted by major industrial players in AI-based services on Internet, cloud computing and other service platforms. Extensive use of deep learning is observed across wide spectrum of security and safety critical intelligent systems. Self-driving cars, malware detection, drones and robotics are examples of the safety critical systems where deep learning systems are extensively used. Some of these systems are directly impacting human life. At the same time, advancements in face-recognition systems has propelled security critical ATMs and mobile phones to use biometric authentication as a security feature. At the same time, Automatic Speech Recognition (ASR) models and Voice Controllable systems (VCS) made it possible to realize voice-based authentication in banks as well as many voice-based products like Siri by Apple, Alexa by Amazon, Cortana by Microsoft and Google Assistant.

However, recent research reports have proven that Deep neural networks are vulnerable to attack through carefully crafted adversarial examples. These adversarial examples are imperceptible to the human eye but can lead the model to misclassify the output. Recent studies show that adversarial examples can be applied to real world applications. For example, an adversary can confuse autonomous vehicles by manipulating the stop sign in a traffic sign recognition system or remove the segmentation of pedestrians in an object recognition system. Voice recognition system can be attacked by generating adversarial commands.

The vulnerability to adversarial examples becomes one of the major risks for applying AI technologies in security and safety-critical environments. Objective of this track is to explore the landscape of security and safety challenges of AI systems and research efforts to detect and prevent AI systems from such challenges.

The topics include, but are not limited to the following subtopics:

- Safety and security challenges of AI applications
- Adversarial robustness
- Adversarial attack detection
- Adversarial attack prevention
- Framework for secured AI applications
- Adversarial safe systems

Important Datelines

Inform the Chair: As soon as you decide to contribute
Submission: August 1, 2020
Notification: August 21, 2020
Registration: September 1, 2020
Camera-ready: September 1, 2020

Note: *These deadlines are somewhat flexible, providing arrangements are made ahead of time with the chair.*

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=CYBER+2020+Special

Please select Track Preference as **SIAS**

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

Ramesh Rakesh: ramesh.rakesh@hitachi.co.in
CYBER Logistics: steve@iaria.org