Course Relevance

In today's fast-moving world, machine learning (ML) models and systems are any and everywhere. Right from autonomous navigation of vehicles and UAVs, weather forecasting, biometric recognition, financial stocks, sports, and even predicting election trends and vote shares, ML models are now omnipresent. However, ML models and systems come with their own set of risks, which acts as a caveat for their omnipresence. Risks involve model understanding and accountability, vulnerability to unforeseen faults, adversarial manipulation, and concerns about following ethical norms in privacy and fairness. The focus of the workshops/boot camps will be specifically on educating the participants on the security aspects of autonomous vehicles and UAV's both from software and hardware point of view.

Course Objectives

- To familiarize participants about Cyber Physical Systems and the need for Machine Learning models to be Secure and Trustworthy.
- To familiarize participants with understanding the three pillars of Trustworthy ML models, namely i) Explainable ML models, ii) ML models inculcating fairness, iii) Secure ML models, i.e. privacy and robustness.
- To provide hands-on training using at least one framework, such as Tensorflow, Keras, and PyTorch.
- Training participants on Adversarial Machine and Deep learning using Foolbox package.

Workshop talks will be delivered by IIT/NIT/IIIT faculty along with Hands-on Laboratory sessions.

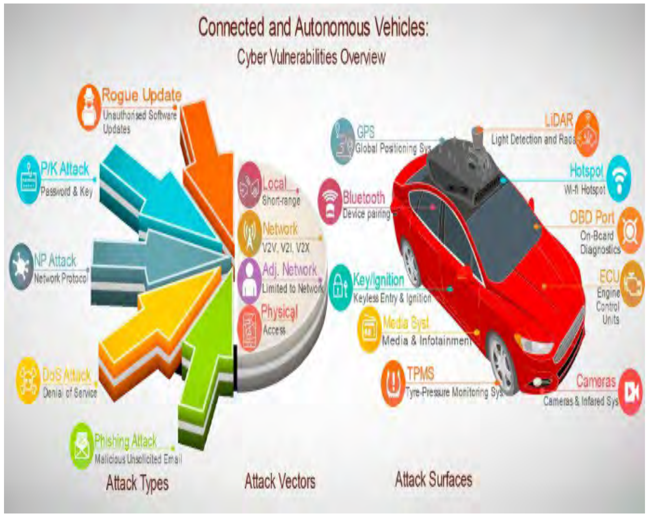
Queries can be sent on: isllabnitr@gmail.com

TiHAN, IIT Hyderabad sponsored

Skill Development Workshop on

Security Aspects of Cyber Physical Systems: UAV's & Driverless Cars

29th April-3rd May 2024



Co-ordinators:

Dr. MANISH OKADE

&

Dr. DIPTI PATRA

NIT Rourkela

ABOUT NIT ROURKELA

National Institute of Technology (NIT), Rourkela was founded as Regional Engineering College, Rourkela in 1961. It is a prestigious Institute with a reputation for excellence at both undergraduate and postgraduate levels, fostering the spirit of national integration among the students, a close interaction with industry and a strong emphasis on research, both basic and applied. Its been consistently ranked within TOP 20 engineering institutes for 8 consecutive years as per MoE’s NIRF, Govt. of India.

The city of Rourkela is a bustling industrial town, cosmopolitan by nature and is well connected to all parts of the country by road and rail. It is en-route Howrah-Mumbai main line of South-Eastern Railway. Nesting amidst greenery on all sides, NIT campus is approximately 7km from Rourkela railway station. The nearest airports are Jharsguda, Ranchi, Kolkata and Bhubaneswar.

Website: www.nitrkl.ac.in

Registration Details

Category	Registration Fees (Rs.)
Students (UG/PG/PhD)	500/-
Faculty	1500/-
Industry Participants	2500/-

ABOUT TiHAN, IIT Hyderabad

Department of Science and Technology (DST) under the National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS), “Govt. of India” has sanctioned the prestigious Technology Innovation Hub on Autonomous Navigation (TiHAN) and Data Acquisition Systems (UAVs, ROVs, etc.). The vision of this hub is to become a global destination for next-generation smart mobility technologies that utilize reliable and efficient autonomous navigation and data acquisition systems in the next five years. More details on https://tihan.iith.ac.in/

Module Details

(1) CPS introduction (2) UAV’s case study (3) ADAS introduction. (4) CAN bus (Controller Automation Network). (5)Fairness (6) Explainability & Role of Bias (7) Adversarial attacks (8) Adversarial defenses (9) Hands-on: Introduction to Foolbox software. Adversarial machine learning- Colab notebooks

Interested participants can register via the link.

https://forms.gle/gxyRBEKQQ5xNwrTy8

Shortlisted candidates will be given banking details so that they can pay the registration fee via online bank transfer/UPI pay