**Resilient Cyber-Physical Systems Through**

**Machine Learning Techniques**

Looking back at the 2023 cyber threat landscape, attackers focused on targeting cyber-physical systems, aiming to catch them unprepared and exploit sensitive data and resources. The **Cyber-Physical Systems Security** project focuses on addressing the security challenges associated with **Cyber-Physical Systems (CPS)** and **Internet of Things (IoT)** devices. These technologies play an essential role in critical infrastructure, government services, and everyday life. Examples of CPS include automobiles, medical devices, building automation systems, and the smart grid, each comprising intelligent, networked components with embedded sensors, processors, and actuators. These systems interact with the physical environment and are designed to support real-time, high-assurance operations in safety-critical scenarios.

Building on the foundation of CPS is a rapidly expanding field, driven by the increasing affordability and pervasiveness of sensor, platform, and networking technologies. Whether it is a vehicle's forward-collision prevention system, a real-time adaptive medical device, a smart agriculture decision-making system, or the latest IoT innovations, these systems offer significant competitive advantages and hold immense potential for supporting the country's financial and economic growth.

However, this rapid expansion of CPS also brings with it increased cybersecurity risks and a larger attack surface. The consequences of system failures can be severe, potentially affecting human lives and the environment due to unintentional faults or malicious attacks. The requirement for proactive, coordinated, and forward-looking efforts to ensure security and resilience has become more urgent than before.

*The objective of this workshop is to enhance participants' understanding of Cyber-Physical Systems (CPS) and equip them with practical skills to detect and prevent cybersecurity attacks using various machine learning (ML) techniques. A special focus will be given to Transformer-based approaches for network anomaly detection, offering an in-depth examination of their architecture and applications in CPS environments.*

*While ML-based methods have proven effective in identifying malicious network traffic, they remain vulnerable to adversarial attacks. One of the attacks is data poisoning, where an attacker manipulates the training data to compromise the performance of the ML model. This workshop will analyze how data poisoning attacks can compromise ML detectors, offering insights into the limitations and risks associated with ML-based security solutions.*

*The workshop will engage participants in hands-on exercises, gaining practical experience with the techniques relevant to protecting critical infrastructure. The workshop aims to bridge theoretical knowledge with real-world application, fostering a comprehensive understanding of CPS security challenges.*

The workshop is expected to cater for an audience including students, educators, university faculty, cybersecurity professionals, and researchers. Topics to be covered in the workshop will include:

* Introduction to cyber physical system
* Cyber physical Dataset and pre-processing
* ML based Network anomaly detection
* Transformer based Network anomaly detection
* Adversarial attack on Machine learning based Network anomaly detector

**Proposed Format and Tentative Agenda**

The registered attendees for this workshop will be provided Google colab link to be prepared with the code that will be used during the workshop. In addition, participants will be asked to download the dataset from google drive to be used during the session.

|  |  |
| --- | --- |
| **Timeline (3 hours)** | **Topics** |
| 10 minutes | Welcome Session and Overview of the project |
| 20 minutes | Introduction to cyberphysical system |
| 15 minutes | Dataset and pre-processing (Hands-on activity) |
| 45 minutes | ML based network anomaly detection (Hands-on activity) |
| 30 minutes | Transformer based Network anomaly detection  (Hands-on activity) |
| 40 minutes | Adversarial attack on Machine learning (Hands on Activity) |
| 20 minutes | Conclusion, future work and Q&A session |

**Workshop Organizer and Presenters**

1. Lopamudra Praharaj (*Graduate Research Assistant, Dept. of Computer Science, Tennessee Technological University*) (**Email** – [lpraharaj42@tntech.edu](mailto:lpraharaj42@tntech.edu))
2. Kshitiz Aryal (*Graduate Research Assistant, Dept. of Computer Science, Tennessee Technological University*) (**Email** – [karyal42@tntech.edu](mailto:karyal42@tntech.edu))
3. Shovan Roy (*Graduate Research Assistant, Dept. of Computer Science, Tennessee Technological University*) (**Email** – [sroy42@tntech.edu](mailto:sroy42@tntech.edu))
4. Maanak Gupta *(Associate Professor, Dept. of Computer Science, Tennessee Technological University)* (**Email** - [mgupta@tntech.edu](mailto:mgupta@tntech.edu))