SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
Faculty of Engineering
Website: https://www.eng.nus.edu.sg/ece/

Area: Control, Intelligent Systems and Robotics

Host: Assoc Prof Biplab Sikdar

TOPIC	**:**	**Adversarial Attack Against Deep Learning Models In IoT Applications**
SPEAKER	**:**	**Mr Abhijit Singh** **Graduate Student, ECE Dept, NUS**
DATE	**:**	**Wednesday, 10 February 2021**
TIME	**:**	**4.30PM to 5.00PM**
WEBINAR	**:**	**Join Zoom Meeting** **https://nus-sg.zoom.us/j/87867436840?pwd=TXpCZEJlK0c3N2lFa2ZPeGNnNTJPZz09**

ABSTRACT

Advancements in Machine Learning and Internet of Things have resulted in several interesting interdisciplinary applications, such as classification tasks based on data generated by smart devices for applications such as security, resource allocation, activity and task classification. However, these applications can be vulnerable to attacks by adversarial examples. In this seminar, we will discuss what Machine Learning is from a mathematical perspective, and how IoT fits in with Machine Learning. We will explain the concept of adversarial examples, and discuss some related literature in this area, and how that motivated our research. We will then explain the methodology of our research, and present our experimental results. The seminar will be concluded by a discussion on the significance of the results, and how we are planning on extending this work.

BIOGRAPHY

Abhijit is a PhD student in the ECE department, and is supervised by Dr Biplab Sikdar. His research area is Security and Privacy in Machine Learning. Before joining NUS, he graduated from the University of Edinburgh with an MSc degree in Artificial Intelligence, and worked for a few months as a Machine Learning Engineer at a FinTech start-up.