Speaker: Omar Tayeb O MONTASSER

Title: **Theoretical Foundations of Adversarially Robust Learning**

Abstract: Despite extraordinary progress, current machine learning systems have been shown to be brittle against adversarial examples: seemingly innocuous but carefully crafted perturbations of test examples that cause machine learning predictors to misclassify. Can we learn predictors robust to adversarial examples? and how? There has been much empirical interest in this major challenge in machine learning, and in this talk, we will present a theoretical perspective. We will illustrate the need to go beyond traditional approaches and principles, such as empirical (robust) risk minimization, and present new algorithmic ideas with stronger robust learning guarantees.