भारतीय प्रौद्योगिकी संस्थान तिरुपति
TIRUPATI

INDIAN INSTITUTE OF TECHNOLOGY TIRUPATI
भारतीय प्रौद्योगिकी संस्थान तिरुपति
Yerpedu-Venkatagiri Road, Yerpedu Post, Tirupati District, Andhra Pradesh - 517 619

1.	Title of the course	Adversarial Deep Learning
2.	Course number	CS547L
3.	Structure of credits (L-T-P-C)	2-0-0-2
4.	New course/modification to	New
5.	To be offered by	Computer Science and Engineering
6.	Proposed by	Chalavadi Vishnu
7.	Prerequisite	CoT
8.	**Course Objective(s):** To develop a critical analysis framework on attacks and defense using robust privacy conscious architectures for deep learning models that are currently used in the real world.	
9.	**Course Content:** Introduction to backpropagation; Review of loss functions and distance measures in deep networks; Introduction to generative adversarial networks: generative modeling, discriminative learning; Adversarial learning: quantization, adversarial attacks, transferability of attacks; Adversarial defense: defense mechanisms, privacy preserving models, federated learning.	
10.	**Textbook(s):** 1. Warr K, Strengthening Deep Neural Networks: Making AI Less Susceptible to Adversarial Trickery, O'Reilly Media (2019). 2. Miller D J, Xiang Z and Kesidis G, Adversarial Learning and Secure AI, Cambridge University Press (2023).	
11.	**Reference(s):** 1. Foster D, Generative Deep Learning, O'Reilly Media (2022). 2. Vorobeychik Y, Kantarcioglu M, Brachman R, Stone P and Rossi F, Adversarial Machine Learning, Springer (2018).	