Prefix and Course Number

EE P ____

Course Title (120 character maximum)

Privacy Preserving Machine Learning

Abbreviated Title; Must be ALL CAPS (Max 20 characters)

PRIVCY PRESERVNG ML

Catalog course description (450 character maximum)

Focuses on the theoretical and applied aspects of Privacy Preserving Machine Learning. Considers statistical and information-theoretic notion of privacy and privacy attacks against machine learning models. Covers prevention and mitigation of privacy attacks, including multi-party secure computation (MPC), differential privacy (DP), federated learning, robust federated learning, and split learning.

Justification for adding course

The ECE Professional Masters Program (PMP) proposes the creation of a new permanent course, EE P ____: Privacy Preserving Machine Learning. This course was successfully piloted in Spring 2023 under the special topics number EE P 596.

EE P ____will be offered as part of PMP's standard MSEE degree program and the Certificate in Machine Learning and Deep Learning: Application Frontiers.

Evaluation details

- Readings and discussion: 15%
- Labs: 25%
- Project: 60%

Learning Objectives

By the end of this course, students will demonstrate the ability to:

- Understand statistical and information-theoretic notion of privacy.
- Develop an understanding of privacy attacks against machine learning models.
- Utilize privacy engineering techniques, including secure multiparty computation (MPC), and differential privacy.

- Understand privacy preserving approaches, including federated learning and split learning.
- Gain familiarity with federated learning in adversarial attacks, privacy attacks against machine learning systems, and privacy engineering techniques, including secure multi-party computation (MPC), and differential privacy, and their applications to machine learning systems.
- Utilize state-of-the-art Python libraries and tools used for PPML, such as PySyft.