CENTER FOR COMPUTATIONAL SCIENCES
2024 – 2025 SEMINAR SERIES

AI in Practice

Hosted Jointly by CCS/ITSRCI, IBI/CAAI, &
UK AI/ML Hub Seminar Series

In person attendance: 327 McVey Hall 12:15pm – 1:15
Remote attendance: https://uky.zoom.us/j/82467171189

Seminar website: https://www.ccs.uky.edu/ccs-seminar-series-on-ai-in-practice/

THURSDAY November 21, 2024 at 12:15 PM – 1:15 PM

Cohen Archbold, Electrical and Computer Engineering
and Usman Hassan, Computer Science

AI–in-Practice – Private Machine Learning

In this presentation, we'll explore the key tools and methodologies for bringing privacy and security to distributed machine learning (ML). With the increasing need to protect sensitive data in collaborative and decentralized environments, privacy-preserving techniques have become critical. The talk will be structured around two major approaches: (1) federated learning, (2) differential privacy. Federated Learning allows machine learning models to be trained across decentralized devices without sharing sensitive data, ensuring that personal information remains local while only model updates are aggregated. We will demonstrate Flower, a federated learning framework, in our talk to showcase its capabilities for decentralized model training. Differential Privacy (DP) protects individual records by making them indistinguishable within a dataset through controlled noise. This technique has become popular in ML for safeguarding training data while enabling useful statistical analysis. Our talk will include a demo using TensorFlow Privacy and PyTorch-Opacus, illustrating how DP can be integrated into machine learning models for privacy-preserving training. Lastly, we will discuss the privacy risks associated with ML models and demonstrate how to measure a model's susceptibility to attack. This talk is aimed at machine learning practitioners, data scientists, and researchers interested in applying privacy-preserving technologies in distributed environments.