Agenda

1. Membership Inference against Generative Models

2. Property Inference in Collaborative/Federated ML

3. Backdoor Attacks in Federated ML

Robustness in FL