Agenda

1. Training (Distributed) ML Models with Privacy

with Privacy

1. Training (Distributed) ML Models

2. Private Data Release with Generative Neural Networks

4. Privacy Leakage in Collaborative/Federate ML

4. Privacy Leakage in Collaborative/Federated ML

3. Privacy Leakage from Generative Models as a Service

2. Private Data Release with Generative Neural Networks

3. Privacy Leakage from Generative Models as a Service