

Agenda

1. Training (Distributed) ML Models with Privacy
2. Private Data Release with Generative Neural Networks
3. Privacy Leakage from Generative Models
as a Service
4. Privacy Leakage in Collaborative/Federate ML

Machine Learning as a Service