

Agenda

2 Private Data Release with Generative Neural Networks

3. Privacy Leakage from Generative Models as a Service

3. Privacy Leakage from Generative Models

asservice

1. Training (Distributed) ML Models with Privacy

4. Privacy Leakage in Collaborative ML

4. Privacy Leakage in Collaborative ML