1. Membership Inference against Generative Models

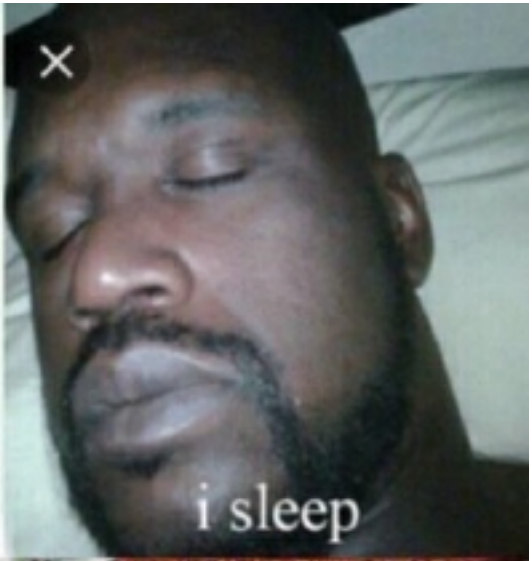
2. Property Inference in Collaborative/Federated ML

3. Backdoor Attacks in Federated ML

Agenda

10

Privacy



Memes

Agenda

1. Mem Ge inst
2. Property erated ML
3. Backdoc

Machine Learning as a Service