Agenda

1. Membership Inference against Generative Models

2. Property Inference in Collaborative/Federated ML

9

3. Backdoor Attacks in Federated ML

1

[redacted]

M

O

d

e

[redacted]

S

[redacted]

n

f

e

r

e

n

C

e

a

g

a

i

n

S

t

G

e

n

r

a

t

i

V

e

M

e

m

b

e

r

h

i

p

Inference

Collaborative/Federated

Property

2.

ML

in

Federated

Backdoor

ML

Attacks

3.

in

1

M

O

d

e

S

n

f

e

r

e

n

C

e

a

g

a

i

n

S

t

G

e

n

e

r

a

t

i

V

e

M

m

b

e

r

h

i

p

Inference

Collaborative/Federated

Property

2.

ML

in

10

Federated

Backdoor

ML

Attacks

3.

in