How Can We Defend?

30

Differentially Private Synthetic Data?

How Can We Defend?

Differentially Private Synthetic Data?

Neural Networks

Input

Data vector $x = (x_1, \ldots, x_n)$

Output

Linear function of x