

Normal learning

Dataset



Poisoning attack

Learning
algorithm

