# Membership Attack Defense

Membership Attack 利用差分隐私来避免攻击者很容易的通过分类结果找到攻击目标的训练属性。

主要有以下几个数据集被我们使用：

UCI Adult(Census Income)数据集

<http://archive.ics.uci.edu/ml/datasets/Census+Income>

Texas hospital stays 德州医院数据集

<http://www.dshs.texas.gov/THCIC/Hospitals/Download.shtm>

Kaggle 用户购买记录数据集：

<https://www.kaggle.com/c/acquire-valued-shoppers-challenge/data>

CIFAR10和CIFAR100数据集：

<http://www.cs.toronto.edu/~kriz/cifar.html>

四个数据集中，只有最后一个是图像相关的的识别工作。

## UCI Adult数据集

我们首先分析UCI Adult中的数据集中的内容。UCI Adult数据集中包含用户的各种信息，然后利用这些信息判断用户的年工资收入是否大于50k。Prediction task is to determine whether a person makes over 50K a year.