網路多媒體實驗：Using model output to steal model from Machine Learning-as-a-Service platform

組員：林承德、趙冠豪、李羚毓　　指導助教：曾煒傑　　指導老師：林宗男教授

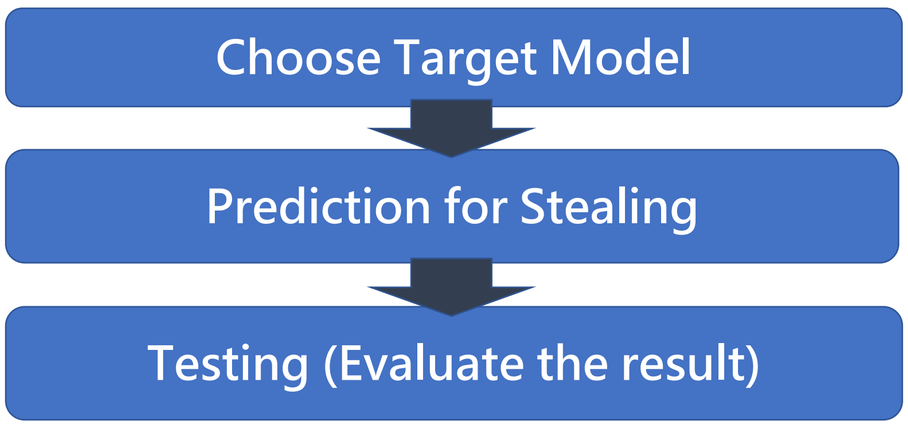
1. Aim：

1) Implement the method in ”Stealing Machine Learning Models via Prediction APIs” to steal model.

2) Try to steal different kinds of models using neural network.

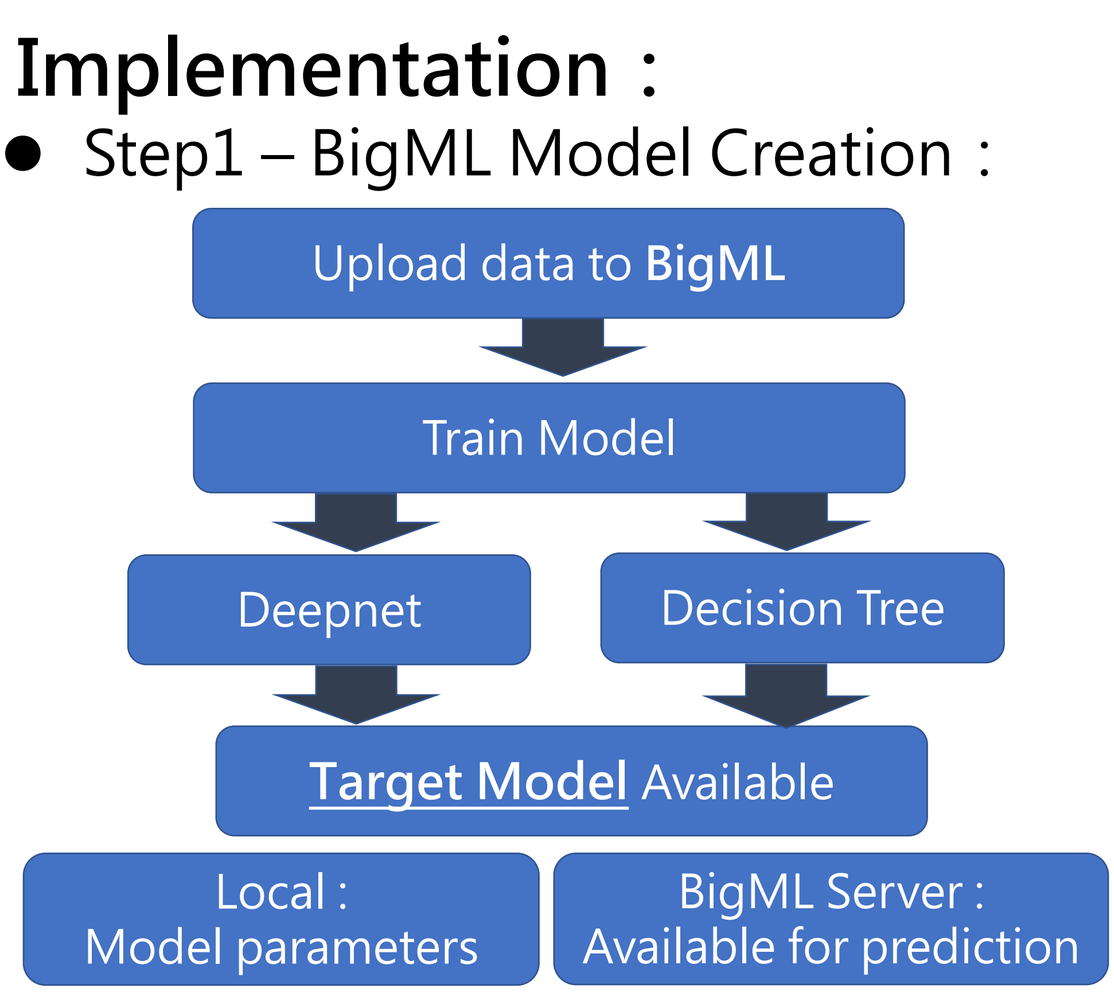
2. Introduction：

- Data：MNIST dataset
- Workflow：

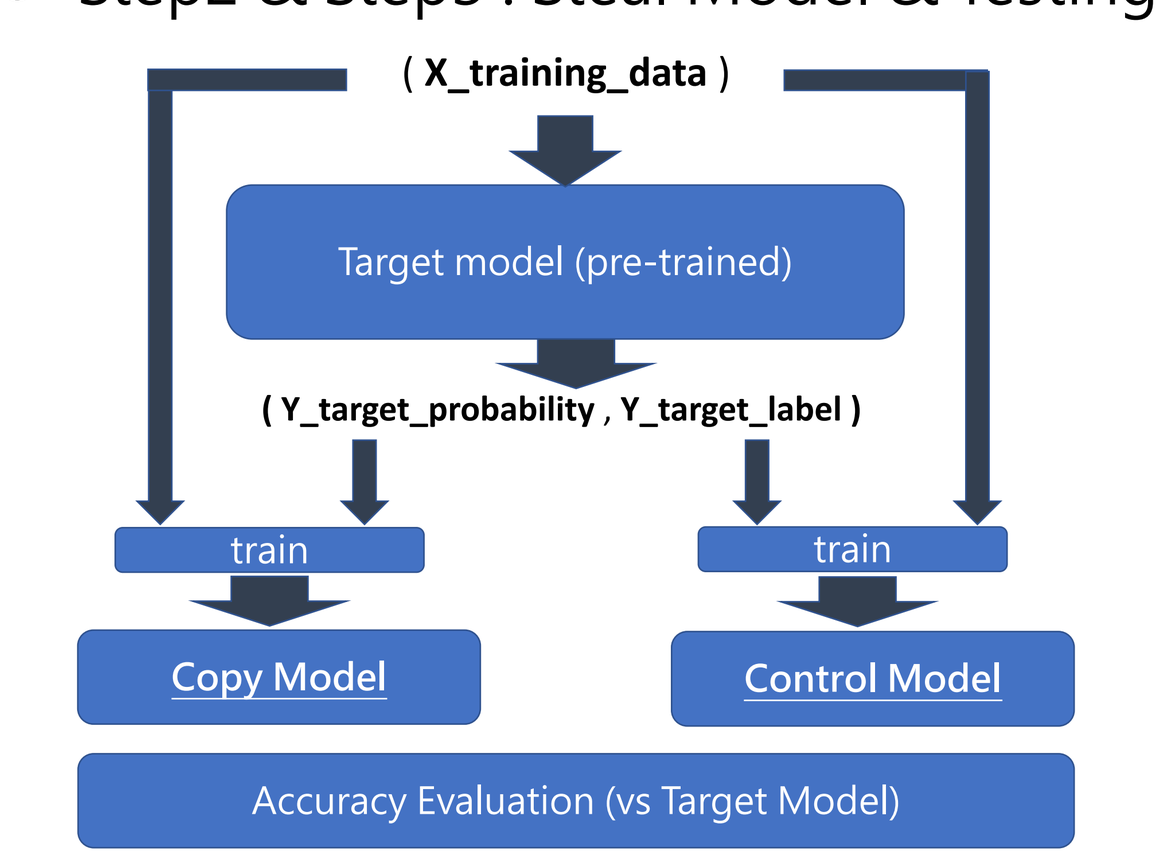


3. Implementation：

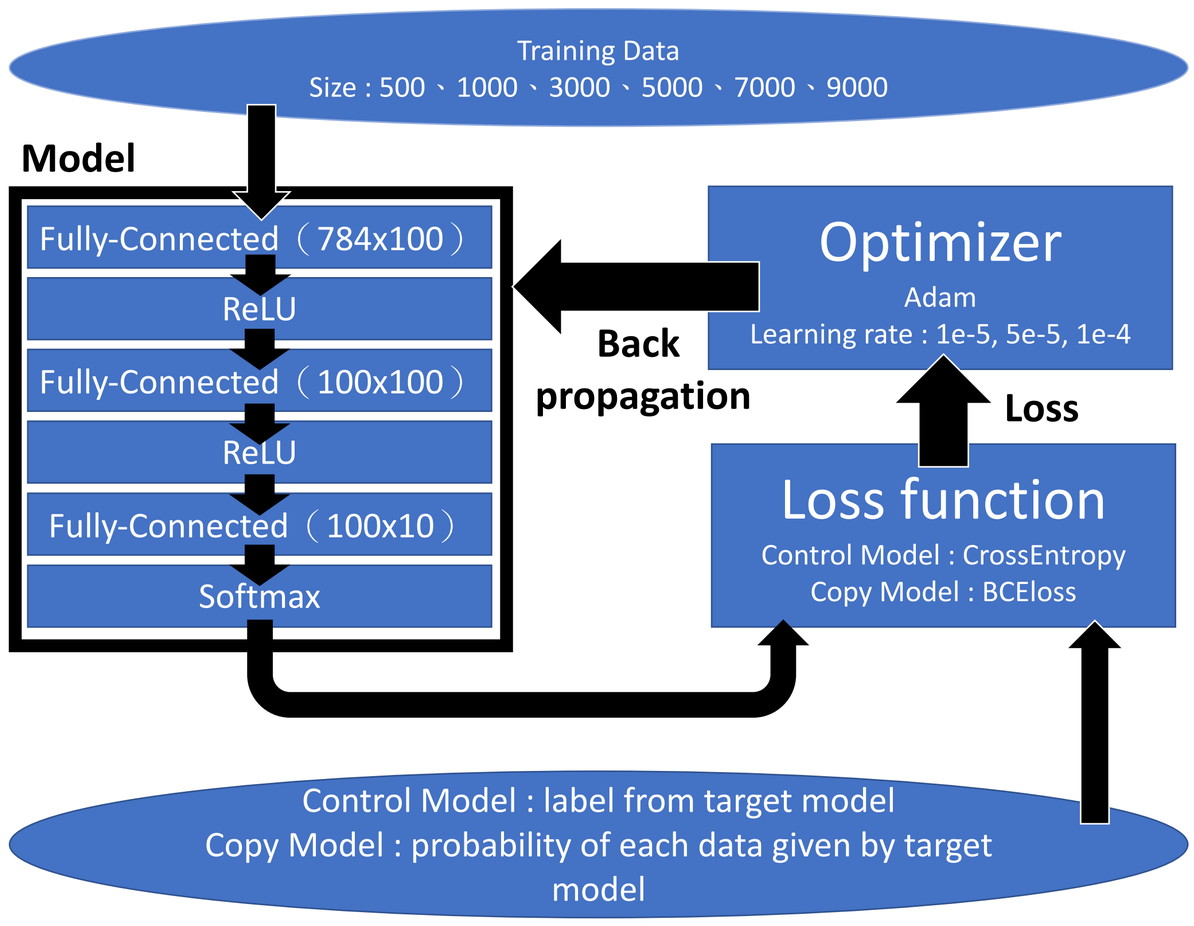
- Step1 – BigML Model Creation：



- Step2 & Step3 : Steal Model & Testing

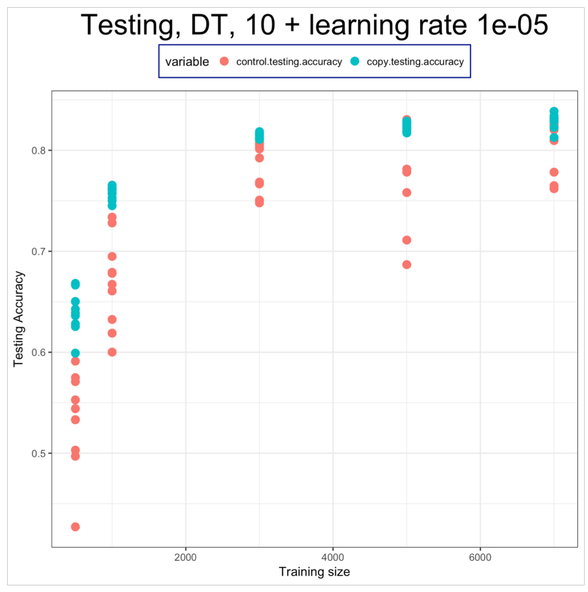


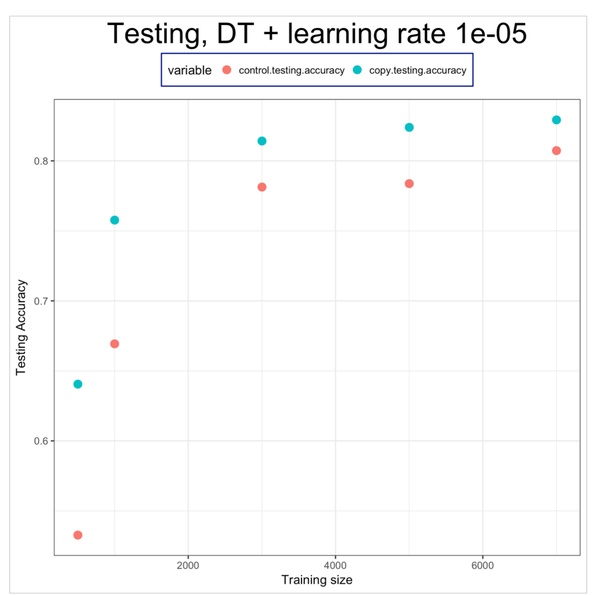
- Step2 & Step3 : Steal Model & Testing



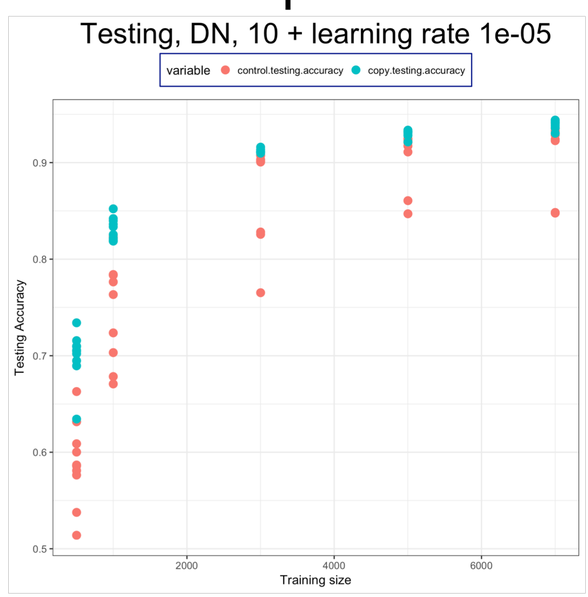
4.Results

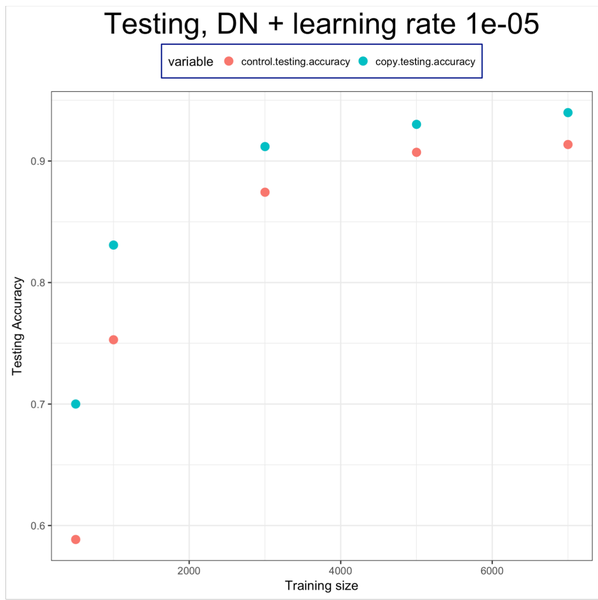
- Decision Tree：





- Deepnet：





5. Conclusion

1. In different training size, learning rate with fixed loss function, BCEloss as well as 200 epoch, the precision of copy model is higher than control model

2. Neural Network is a good way to steal both decision tree model and deepnet model created by BigML.

3. The precision of copy model is higher than control model in limited training data (about 10% higher).