Paper Title: Towards Defenses Against DNN Model Stealing Attacks
Paper Link: https://arxiv.org/abs/1906.10908
Code Link: https://github.com/tribhuvanesh/prediction-poisoning

Software Requirements

You will need the following installation:

Environment Setup

Use Virtual Environment (Conda3)
Python 3.7
Pytorch 1.4+
conda env create -f environment.yml
cc install pip
pip install -r requirements.txt

Now set the knockoffnets packages –

cd knockoffnets pip install -e .
pip install pretrainedmodels
pip install matplotlib

Project Running Procedure

Use the Patch file attached in the project folder (prediction-poisoning) to update the changes to the original code.

Preparation

- Refer to the README.md file to learn about the dataset and model used.
- Believing, you have the required dataset and files with you. Modify the tesh.sh file with your model file path, dataset, and other details to test this project.
- Now use the tesh.sh script file to test the defense. (Refer to README.md to know more about the steps involved in defense)