



【用户使用手册】docker 方式

原理

当用户无法提供模型给平台时，则可以采用 docker 方式进行黑盒评测。

其基本原理是，用户从平台上选择要推理的基础数据集（例如干净样本）和子数据集（例如对抗样本），用自己的模型去分别推理这两个数据集，将得到的推理结果（即 y）按格式保存成 JSON 文件，这个文件我们称作中间结果文件，平台再去按这个 JSON 文件的内容去评测指标。

Demo

<https://github.com/RayKr/aisafety-docker-demo>

使用手册

1. 执行文件，查看是否运行成功

```
python main.py
```

Bash

2. 本地编译 docker 镜像

```
docker build ./ -t demo:latest
```

Bash

注意：`opencv-python` 包，如果是在 macos 下编译，则需改成 `opencv-python-headless`。

3. 登录重明平台，点击菜单「模型管理」→「提交模型」→模型格式选择镜像，可以看到下方显示本用户的 docker 命令，例如：

The screenshot shows the AISafety platform interface. On the left is a sidebar with navigation items: 评测, 比赛, 仓库, 数据集管理, 模型管理 (highlighted with a red box), and 专区. The main content area is the 'Submit Model' form. It includes fields for 'Visible Range' (Public or Only Visible to Me), 'Scenario' (a dropdown menu), 'Model Type' (Non-comparison Model or Comparison Model), 'Model Format' (Source Code or Image, with Image selected and highlighted by a red box), 'Image Name' (a dropdown menu), and 'Image Tag' (a dropdown menu). Below these fields is a section for 'Image Description' with a red box highlighting the Docker commands: '登录命令: docker login 221.122.70.196:7005.' and '上传命令: docker push 221.122.70.196:7005/pro_10026/IMAGE:TAG.' At the bottom right are 'Cancel' and 'Submit' buttons.

4. 修改镜像 tag，这一步是为了保证可以正常 push 到远程仓库。

```
# 注意修改后的tag前半部分必须和步骤3中上传命令的一致 221.122.70.196:7005/pro_10026/  
docker tag demo:latest 221.122.70.196:7005/pro_10026/jzldemo:latest
```

Bash

5. 将镜像推送到重明平台仓库

```
# 先登录，使用重明平台账号密码  
docker login 221.122.70.196:7005
```

Bash

推送
docker push 221.122.70.196:7005/pro_10026/jzldemo:latest

6. 镜像推送成功后就可以在平台上新增模型了。

AI Safety

评测

比赛

仓库

数据集管理

模型管理

专区

模型管理->提交模型

仓库-模型管理

公开模型 我的模型

提交模型

模型名称

模型名称

场景: 请选择

查询

重置

模型名称	场景名称	模型类型	可生成对抗样本	数据格式	模型格式	操作
test-cifar-2	CV	非对比模型	是		源码	详情 更多
12121	CV	非对比模型	否		镜像	详情 更多

AI Safety

评测

比赛

仓库

数据集管理

模型管理

专区

仓库 / 模型管理 / 创建模型

帮助中心 testQA

* 模型名称:

我的docker模型

* 模型介绍:

B I H U S x² x₂

测试用的docker模型

* 可见范围:

公开 仅自己可见

* 模型类型:

非对比模型 对比模型

* 场景:

CV

* 模型格式:

源码 镜像

(请务必按照模型制作要求制作模型)

* 镜像名称

pro_10026/jzldemo

* 镜像标签

latest

下拉列表展示您已上传的镜像，若无可选镜像，请先将镜像上传。

Docker文档

登录命令: docker login 221.122.70.196:7005。

上传命令: docker push 221.122.70.196:7005/pro_10026/IMAGE:TAG。

取消

提交

镜像上传成功后，可以在镜像名称下拉列表中看到了，选择好名称和标签即可。

7. 创建评测任务，点击菜单栏「评测」→「创建评测」。

AI Safety

评测

比赛

仓库

数据集管理

模型管理

专区

首页 / 评测管理 / 创建评测任务

帮助中心testQA

创建评测任务

* 任务名称:

我的docker评测任务

* 任务简介:

我的docker评测任务

我的docker评测任务

* 模型:

我的docker模型 选择模型

* 可见范围:

公开

仅自己可见

* 评测类型:

白盒测试

黑盒测试

* 基础数据集:

jzl_cln_data 选择数据集

* 子数据集:

jzl_adv_data 选择子数据集

* 样本数:

1

* 抽取模式:

随机

顺序

* 评测指标:

ACC 选择评测指标

返回

提交

选择要评测的数据集，两个数据集可以通过环境变量传递给 docker 内的程序

8. 运行评测，查看日志结果。

我的docker评测任务	评测任务 - 创建	🕒 2022-09-20 15:21:16	未运行	运行更多
我的docker评测任务	完成	2022-09-20 15:21:56	00:00:11	查看结果更多

15 条10条/页

<12>

前往2页

查看日志

详情

删除

非目标攻击结果

评测进度: b'{"code":"0","msg":"","times":1663658515712}'

不存在target /childdataset/pgd/targets/pgd.txt

指标: ACC

IS_COMPARE_MODEL False

IS_PYTORCH_WHITE False

total 1

指标ACC: 0.0

非目标攻击结果

评测进度: b'{"code":"0","msg":"","times":1663658515722}'

使用 Demo 封装自定义模型

替换 main.py 中模型和参数，执行推理即可。

```
4 # 要评测的模型和参数文件
5 model = getModel()
6 ckpt = "models/example.pt"
7
8 # 执行推理，生成中间结果
9 inference(model, ckpt)
10
```