



# PCL启智平台&北航启智重明项目调研

汇报人：胡锐

2023.1.4

# 一、启智平台介绍 – 人工智能开源开放平台和社区

## 关于启智社区 (OpenI)

启智社区 (简称OpenI) 是在国家实施新一代人工智能发展战略背景下, 新一代人工智能产业技术创新战略联盟 (AITISA) 组织产学研用协作共建共享的开源平台与社区, 以鹏城云脑科学装置及Trustie软件开发群体化方法为基础, 全面推动人工智能领域的开源开放与协同创新。社区在“开源开放、尊重创新”的原则下, 汇聚学术界、产业界及社会其他各界力量, 努力建设成具有国际影响力的**人工智能开源开放平台与社区**。

当前, OpenI启智社区已汇聚华为、百度、微众银行、商汤、旷视、京东、小米等人工智能龙头企业, 鹏城实验室、北京智源研究院、北京大学、国防科技大学、北京航空航天大学等顶级科研机构, 吸纳核心成员单位11家, 社区高级或普通成员均为国内顶级技术公司、一流研究机构或高校。形成了与国际顶级开源组织接轨的治理体系, 逐步形成完善的社区管理制度, 搭建可支撑社区全面运转的软硬件基础设施, 涵盖协同开发、**代码托管、数据分享、技术实训**等多个子系统的一体化支撑服务环境, 并在中国科学技术协会主办的2021年度“科创中国”开源创新榜中入选年度优秀开源社区。

立足长远发展, OpenI启智开源平台与社区已布局四个层次的建设, 即开源社区层、开源创新研究平台层、开放创新企业平台层和开源开放节点层。目前, 15个国家新一代人工智能开放创新平台正在有计划接入启智, 加入开放创新企业平台层; 鹏城实验室、北京智源人工智能研究院等新型科研机构在重大基础设施建设、社区发展等方面给予了大力支持, 在开源创新研究平台层发挥重要作用。



OpenI



大型开源  
项目社区



代码托管  
算力平台

# 大型开源项目社区

## ● 项目发起者一般是高校或科研机构

- ✓ 提供代码、数据集、模型
- ✓ 以及一些交流渠道



## 交流社区

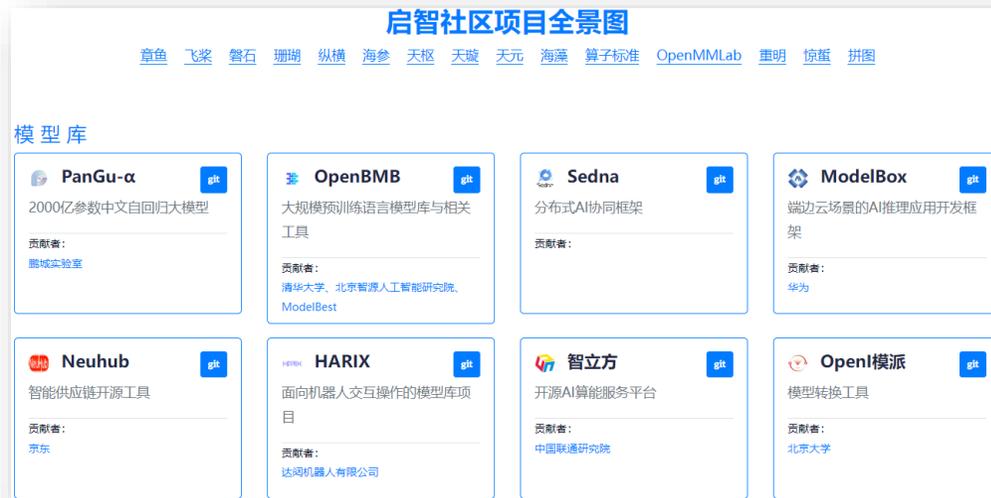
- 启智社区: <https://git.openi.org.cn/OpenBMB>
- GitHub: <https://github.com/OpenBMB>



OpenBMB QQ 交流群



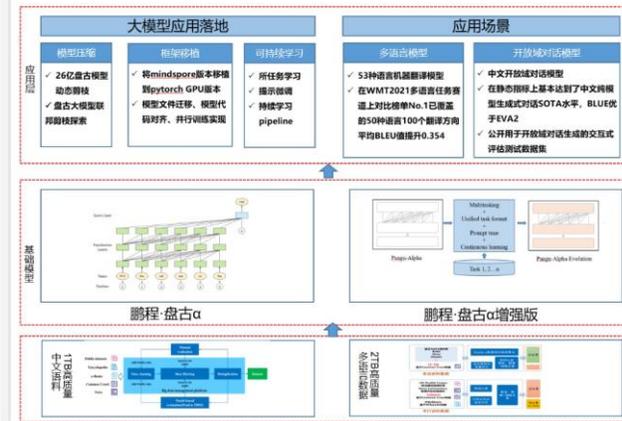
微信公众号: OpenBMB



## 项目简介

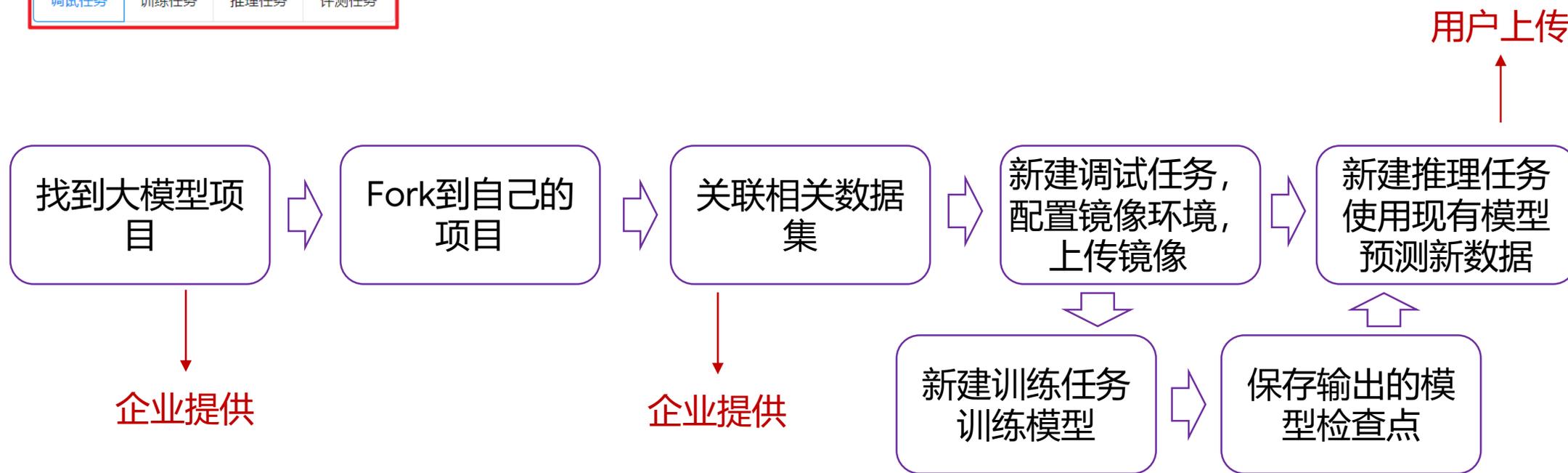
鹏程-盘古α是业界首个2000亿参数以中文为核心的预训练生成语言模型，目前开源了两个版本：鹏程-盘古α和鹏程-盘古α增强版，并支持NPU和GPU两个版本，支持丰富的场景应用，在知识问答、知识检索、知识推理、阅读理解等文本生成领域表现突出，具备较强的少样本学习的能力。

基于盘古系列大模型提供大模型应用落地技术帮助用户高效的落地超大预训练模型到实际场景。整个框架特点如下：



# 代码托管算力平台

- 类似于Github，不过功能更丰富

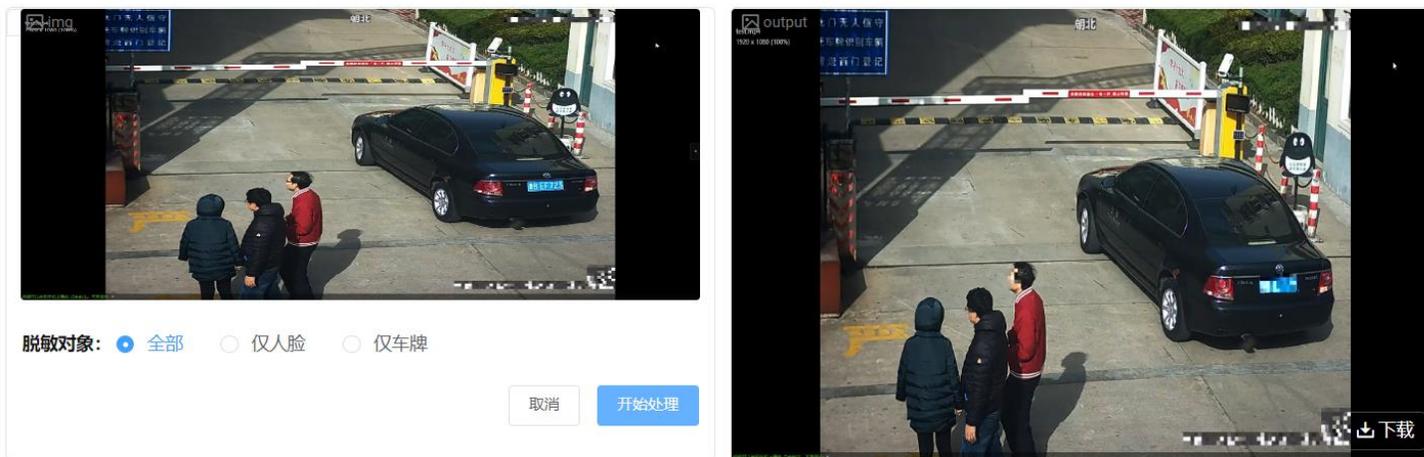


# 在线模型服务

- 和Huggingface类似，提供模型接口，在线服务

## 数据脱敏模型体验

利用人工智能AI技术，把图片中的人脸、车牌号码进行脱敏处理。该模型更多信息请访问项目 [tengxiao / tuomin](https://github.com/tengxiao/tuomin)



示例:

原始图片	脱敏图片	脱敏对象
		全部

## 二、北航“启智重明”项目

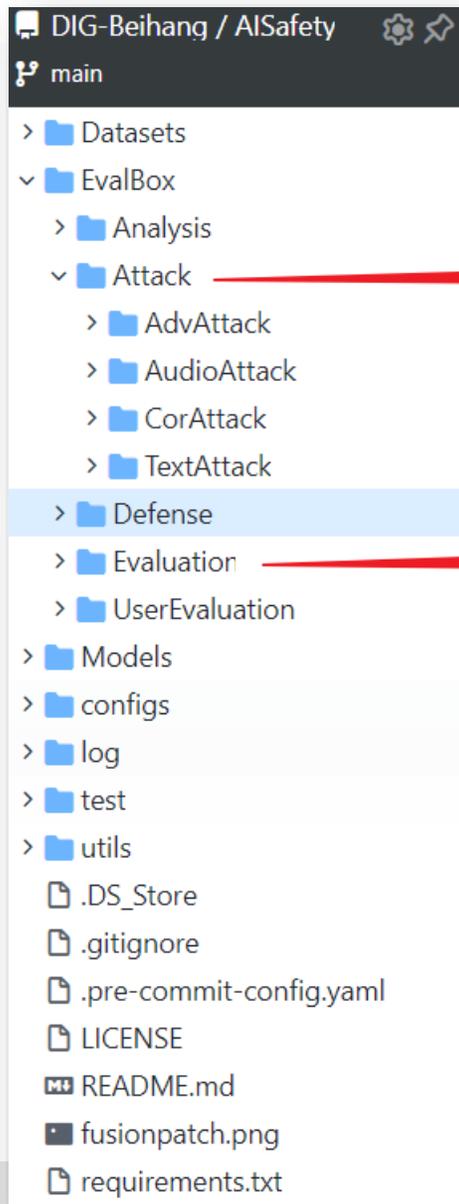
---



### 重明 (AISafety)

面向人工智能安全的评测评估平台“重明”，集成算法库、模型库、指标库、数据库等资源，包含20余种对抗样本攻击、19种噪声攻击、5大类30余种评测算法、覆盖60余种典型的计算机视觉模型以及30余种典型的自然语言处理模型；可支持一站式评测流程，以及可解释报生成。集成沙盒3D仿真验证环境集。核心代码开源并获得[首届OpenI启智社区优秀开源项目](#)。该平台已集成于工信部人工智能算法检验检测平台并服务揭榜评测，获得科技创新2030—“新一代人工智能”重大专项支持，已开展15家人工智能龙头企业的智能算法及系统的评测工作，推动人工智能产业生态的健康发展。

# AI Safety 代码仓库



对抗攻击算法: FGSM、PGD等

评估指标

- 本质上是一个代码工具包, 提供了各种模型、攻击算法和评估指标
- 可以对应我们的“测试”部分, 比如针对多模态预训练大模型做一个类似的代码工具包

# AI Safety在启智平台的集成

代码 ▾ 任务 0 合并请求 0 数据集 模型 云脑 ? 项目设置

调试任务 训练任务 推理任务 评测任务 基准测试排行榜 新建评测任务

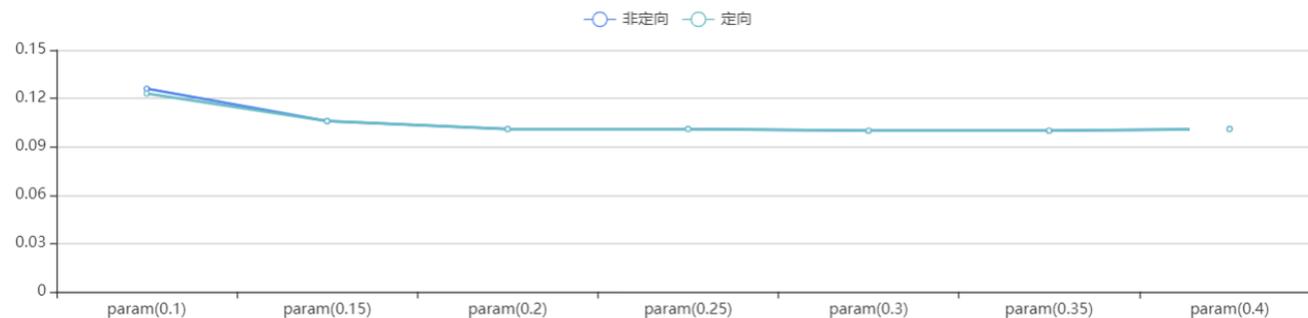
任务名称	状态	评测场景	评测类型	创建时间	运行时长	计算资源	创建者	操作
hhhu202301022270164	→ RUNNING	安全评测	Image Classification	20 秒前	00:01:38	CPU/GPU		停止 删除
hhhu202301021545978	✓ SUCCEEDED	安全评测	Image Classification	6 小时前	00:00:00	CPU/GPU		停止 删除



## ACC-fgsm\_cifar10\_1000

Accuracy: 精确度, 计算模型预测准确率, 该指标越高, 说明评测结果越好。

ACC	param(0.1)	param(0.15)	param(0.2)	param(0.25)	param(0.3)	param(0.35)	param(0.4)
非定向	0.126	0.106	0.101	0.101	0.100	0.100	0.101
定向	0.123	0.106	0.101	0.101	0.100	0.100	0.101



首页

新闻公告

检验检测

数据集和算法

资源中心

在线培训

成果展示

我的检测

关于我们



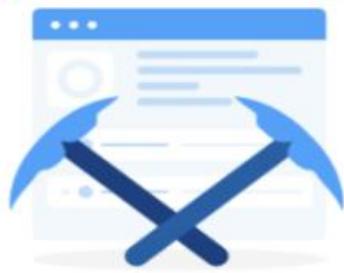
## 新闻信息

更多

- 人工智能标准化与产业创新发展前沿论坛在京召开
- 全国信标委人工智能分委会第一届委员会第二次全体会议在京召开
- 2021世界人工智能大会“共话标准，驱动产业——标准化分论坛”在...
- 重磅发布——《人工智能标准化白皮书（2021版）》
- 倒计时4天 | 2021世界人工智能大会“共话标准，驱动产业——标准...
- 《可信赖人工智能》白皮书启动会顺利召开

## 在线检测工具

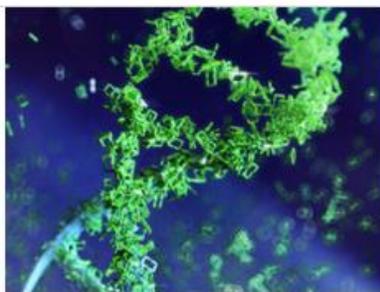
更多»



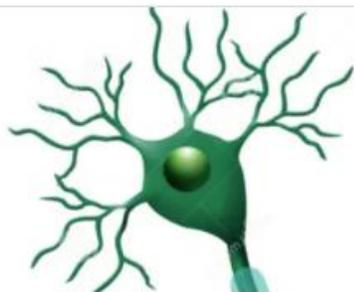
对抗性样本白盒生成工具



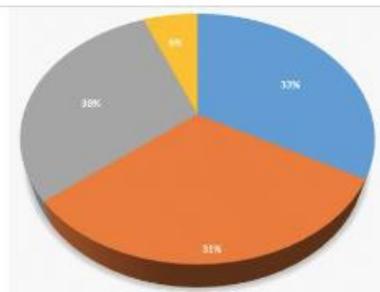
对抗性样本黑盒生成工具



神经网络鲁棒性验证工具



神经网络可解释性分析工具



神经网络可视化分析工具



神经网络代码覆盖率测试分析工具

谢谢!



北京交通大学