

# 智能软件

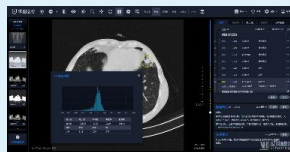
人脸识别



自动驾驶



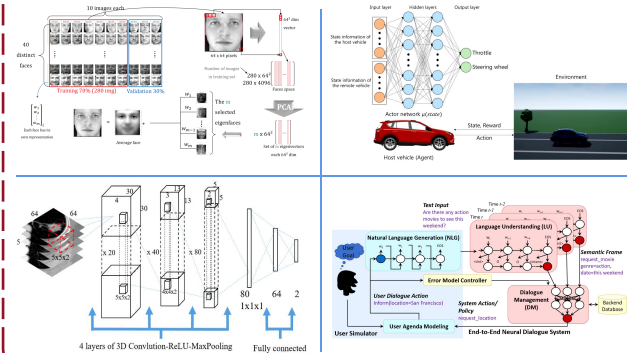
智能阅片



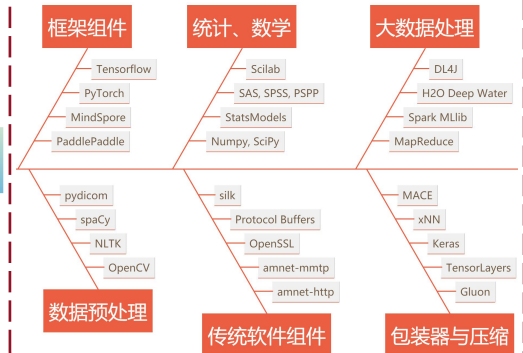
语音助手



## 智能组件



## 非智能组件



# 智能软件脆弱性分析报告

## 智能组件的脆弱性分析

该软件开发或依赖的智能组件是否易受噪声、异常数据的影响？应如何提高模型的鲁棒性？

## 非智能组件的脆弱性分析

该软件所引用的第三方组件之间的依赖关系是什么样的？哪些组件具有脆弱性？

## 跨组件的脆弱性分析

该软件是否可被跨组件攻击，尤其是利用第三方组件漏洞攻击智能组件？

反馈改进

测试分析