Part1:

（5W）

恶意文档（如pdf）的检测是工业界和学术界的难题，原因之一在于其结构与形式的多样，攻击者手段之丰富（如通过电子邮件的附件传播，钓鱼网站加密混淆等）（如：CVE的漏洞）。此研究项目的目标旨在为工业界（如蓝盾）和学术界提供一个基于AI的文档（PDF，word等）分类器，此分类器具有 准确度极高，误报率极低和抗逃逸能力强（？）三大特点。通过对文档领域特征的挖掘，并结合数据科学中的复杂建模，模型成功被构建。此模型可广泛应用于蓝盾多条产品线上，如在终端安全产品上加入此模组，又或者在邮件服务器上加入此模组，均是非常有意义的应用场景

AI文档分类器不仅限于pdf，如可扩展到word，execl，ppt等有结构的文档，但四大安全会议还是把重心放在pdf上。所以你的研究是非常重要的

特别是 样本的逃逸 和 分类器的抗逃逸，举个case study就能引人入胜了。

拿出一个pdf，他在沙箱里面的行为？他在文档分类器里面的评分以及原因？

Part2:

数据图表？

**图表1: 模型准确度，误报率以及 抗逃逸性（如果有）**

**图表2:** 4个算法，特征逐渐减1，准确率的变化。从99% 降到 ～50%（一个特征）。这个线段是平滑的吗？如果不平滑，为什么会bubble up（最好对特征的重要性进行排序）

**图表3（模型的抗逃逸）: 找出一个典型的PDF样本，能逃逸的，然后他具有恶意性的。**