2022 年暑期英国剑桥大学短期科研项目——访学心得

蔡汉霖 梅努斯国际工程学院 2020 级自动化专业本科生

引言：2022 年 7 月 24 日—2022 年 10 月 24 日期间，我参与了由英国剑桥大学科文中心主办的本科生科研训练项目。期间，在导师 Pietro Lio'的指导下，我独立撰写了一篇题为 RIGMS Testbed for IoT Cybersecurity Research Using Machine Learning Based Approach 的学术论文。项目的最后，我取得了 3A（最高分）的优异成绩，并获得了导师的推荐信。下文，我将回顾本次暑期科研训练项目，谈谈自己的动机、收获与心得。

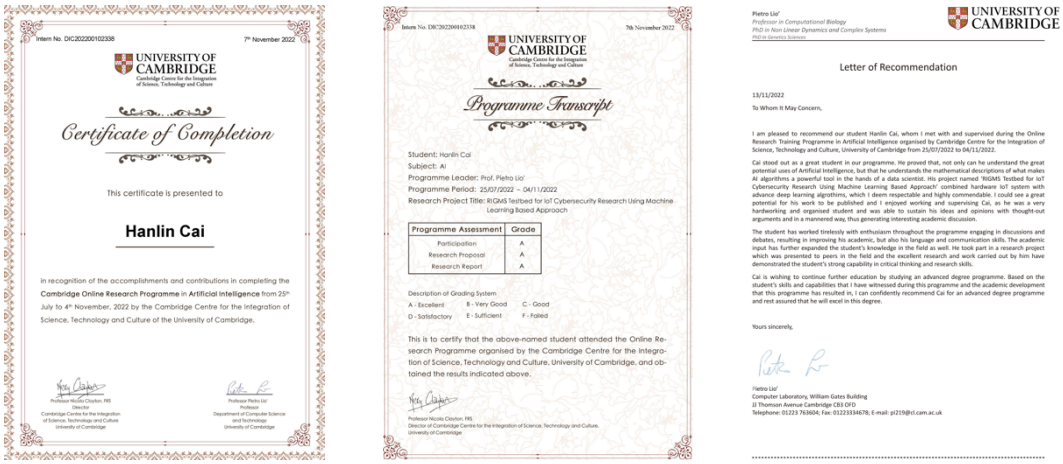

图 1 项目结业证书、成绩单与导师推荐信

我对于科研的动机与热爱，起源于大二学年的一门专业课 Ethics of modern intelligent device，当时我选择的课题是 Overdiagnosis and Overtreatment，在导师座谈会上，教授 Ms. Sinead 与我们分享了一个她自己身上的例子：

Sinead 的妈妈去年二次中风，当时她们一家收到医院通知，“你们的妈妈可能已经活不久了”，这时就需要家人做一个决定，要不要继续抢救——插鼻胃管来维持老人家的生命；还是“善终护理”——把老人接回家，等待生命最后一刻的到来。如果选择插管、戴上呼吸器，临终患者不会马上过世，她的生命可以用营养输液维持；当然她也没办法再恢复健康，因为身体的机能已经很大程度地衰竭了。

“有些人可能很孝顺，接受不了老人去世，她就想说，那先插管，延长生命总不会是错的”，Sinead 教授沉默了一会儿又说道：“但如果选择插管也会有其他的问题——首先，插管对于老人家来说是很痛苦的。其次，插着鼻胃管、带着呼吸器，度完生命最后一段日子的时候，老人家已经意识不清了，她没办法在生命终结的时候完成一些事情，比如她没有机会说她的临终遗言，没有机会跟亲友度过最后一段快乐的相处时光，也没有机会说一声再见，或者对她爱的人说一句“我爱你”。

最后，Sinead 和她的哥哥选择把母亲接回爱尔兰的老家，他们在那里一起度过了生命的最后一段时间。

在 Sinead 分享这个故事的时候，我可以很清楚地感受到一种情感的张力，这种感觉是很明显的，即使我们这群本科生们距离人生的那个“点”还颇为遥远，但我突然意识到，我们这群未来要成为工程师的家伙，我们设计出来的‘Intelligent devices’真的能够给使用者们带来福祉么？还是说这些设备从设计出来的那一刻就注定成为敛财的工具——掏空病人家属的口袋，却无法换得他们短暂的幸福？

至此，我萌生了改变这一切的决心，我开始能够思考技术革新背后的一些东西——没错，技术一定要越来越好，与此同时，也希望我们施加于技术之上的 ‘Humanity’，也能够给人们带来真切的幸福感。

在这基础上，我渴望更深入地探索专业的前沿领域，渴望立足世界一流学府来拓宽自己的学术视野与学术品位。于是我参与了本次剑桥大学科文中心主办的暑期科研训练项目，并希冀在项目过程中可以取得更深入的收获。

图 2 项目过程展示

科研训练项目中，我的导师 Pietro Lio'先生是意大利人，曾在剑桥大学取得了工程硕士的学位，后面回到意大利分别取得了 Systems Dynamics（系统动力学）和 Theoretical Genetics（遗传学）的两个哲学博士学位，目前在剑桥大学任职，主要从事于图神经网络和计算生物学方面的研究，而生命科学与系统工程的交叉领域正是我深感兴趣的。

在项目过程中，导师首先和我确定了大体的研究方向，立足于我先前的研究基础进行深入拓展，即以“实时智能环境管理系统”为基础（如下图 3 所示），探索一种更加安全、用户友好的系统模式——**旨在预防网络安全攻击，保障用户隐私安全。**

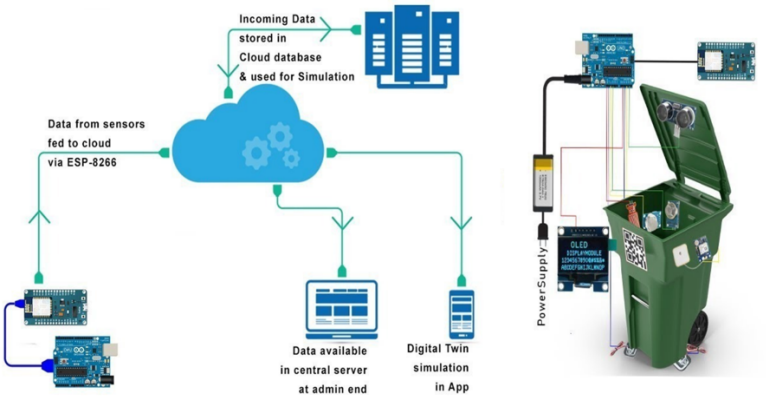

Figure 3 Real-time intelligent garbage monitoring system

图 3 实时智能环境管理系统示意图

上文提到的“实时智能环境管理系统”，是我在大二时期的课设工作，在梅努斯学院的 Dr. Chin Hong Wong 指导下，我们致力于搭建一个能与“经济社会可持续性发展”、“市政垃圾处理需求”有机结合的新型智能环境监管系统。（相关工作发表了 IEEE 国际会议论文 1 篇，并获得第 15 届中国大学生计算机设计大赛的国家三等奖与福建省二等奖。）

基于该系统，我们进一步开展了系统模式的改进工作，考虑到原有的系统主要关注于嵌入式设备的应用与拓展，而缺乏关注系统本身的安全性与可持续性，因此，Prof. Lio'建议我针对系统的用户安全模块进行探索与改进。

经过详细的文献综述与初步实验测试，我们发现使用机器学习的模型对系统进行安全分析可以取得较优的结果，但目前绝大多数基于监督式学习算法模型的安全攻击检测方案，所采用的攻击场景与数据集大多存在场景片面、数据集有偏的缺陷。因此我们采用目前最优的五类算法模型，立足于真实的物联网硬件环境，对更广泛的攻击场景进行了详细具体的实验与分析（如下图 4 所示）。

实验表明，我们所提出的物联网安全测试床所产生数据集具有非常高的可靠性，进一步，我们通过对比五类算法模式所取得的不同结果，对机器学习模型进行了改进分析与参数调整。最后，我们的工作将对物联网系统的安全分析研究与网络安全领域的机器学习应用产生有利的推动与影响。

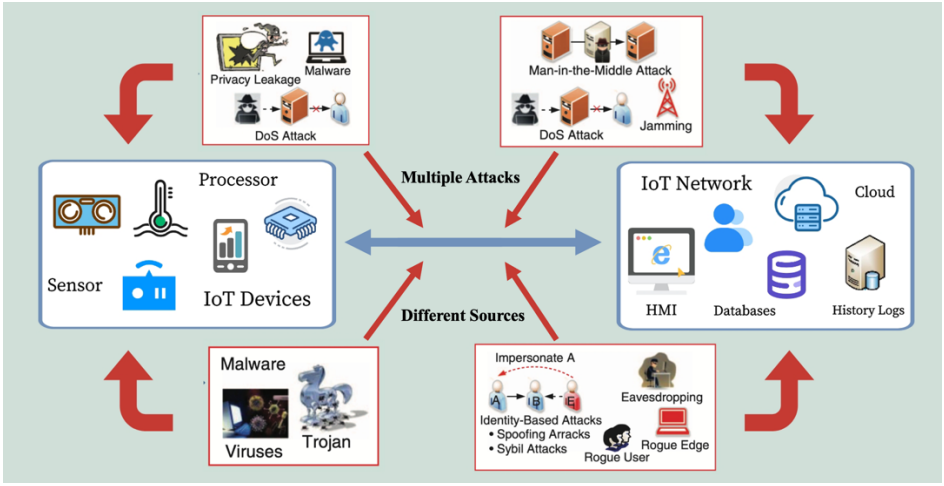

Figure 4 An illustration of IoT security attacks

图 4 物联网安全攻击场景

项目的最后，Prof. Lio'给予我所取得的研究成果极高的评价：I could see a great potential for his work to be published and I deem respectable and highly commendable.与此同时，经过项目评议组的审核与评分，我最终以项目全 A 的优异成绩为本次暑期科研训练项目话上了完满的句号。当然，项目的结束不会是学习交流的结束，在未来，我将继续秉承谦逊、钻研的初心，继续学习、不断进步！

在本文最后，我由衷地感谢福州大学对学生科研交流的支持与帮助，感谢梅努斯国际工程学院的领导老师对我的鼓励与引导。正因为学校治学的开放、包容、多元，才让我们一众莘莘学子有机会在更广阔的世界舞台上拓展学术视野，增添青春风采！感谢！