2025 寒假前沿学科
科研实践项目

剑桥大学
网络安全与联邦学习模型

FEDERATED LEARNING IN CYBER SECURITY

上海安与教育科技有限公司

剑桥大学介绍

剑桥大学是一所享有盛誉的研究型大学，常年位居英国第一，有121位诺贝尔奖得主。

UNIVERSITY OF CAMBRIDGE

它采用传统的学院制度，并且是罗素大学集团和全球大学校长论坛的成员之一。剑桥大学被公认为英语世界中第二古老的大学，具有悠久的历史和卓越的学术传统。

- 剑桥大学排名：2025 QS排名全球第5名
- 剑桥大学是英语世界中第二古老的大学
- 剑桥大学目前有121名诺贝尔奖获得者，位列全球第二
- 剑桥大学优势学科包括机械工程、计算机、数学、人工智能等

剑桥大学在科技创新方面享有国际声誉，特别是在剑桥大学孕育了科技聚集地"硅沼"。

剑桥大学吸引了全英国最大且最重要的科技公司集群，这些公司的创新成果对世界产生了深远的影响。剑桥大学在许多引人注目的领域进行研究和开发，包括新型生物医药技术、新材料、新能源以及可持续发展科技等领域。

剑桥大学培养了许多杰出的校友，其中包括121位诺贝尔奖获得者、4位君主、15位英国首相，以及来自爱尔兰、澳大利亚、东南亚、韩国等国家或地区的至少30位总统和总理。

牛顿、达尔文、凯恩斯等近现代科学的开创者也是剑桥大学的校友。根据2024年的QS世界大学排名和Times世界大学排名，剑桥大学分别位列第2名，展示了其在全球高等教育中的卓越地位。

项目将在剑桥大学沃尔森学院（Wolfson College）、剑桥大学麦格达伦学院（Magdalene College）举办。

沃尔森学院（Wolfson College）

诞生于1965年，是剑桥大学比较年轻的综合型学院之一。学院具有浓厚的现代、创新的氛围，每年有800余位本科生、研究生在学院学习。沃尔森学院以其对包容性的承诺而著称，多元化而自豪，是来自70多个国家的代表使其成为最国际化的学术团体之一。

剑桥大学沃尔森学院

麦格达伦学院（Magdalene College）

是一所相对传统的学院，其“传统性”除了是如今唯一一个拥有烛光晚宴的学院外，还是牛津剑桥所有学院中最后一个开放面向女性招生的学院。每年招收 100 多名本科生，约有 350 名本科生和 200 名研究生。是全剑桥最小的学院之一。即便是一个小学院但是学术表现在剑桥所有学院中也名列前茅。它也是剑桥最美丽的学院之一，地理位置优越，校园坐落在卡姆河畔，拥有漂亮的花园。同时也拥有剑桥所有学院中最长的河岸。以传统的砖式建筑风格著称。校内既有历史悠久的建筑，也有一流的现代化设施。

剑桥大学麦格达伦学院

WHY THE PROGRAMME

学科背景

为了解决“数据保护”与“数据孤岛”这两大难题，Google公司于2016年提出了联邦学习（Federated Learning），旨在将“人工智能的重点转移到以保障安全隐私的大数据架构为中心的算法导向上”。目前，众多企业与研究机构都在积极地探索联邦学习的应用方式，它或许将成为下一个人工智能困境的解决之道。联邦学习是一种分布式机器学习技术，它允许多个参与方在不共享数据的情况下共同训练一个模型，从而提高模型的性能和保护数据隐私。当前的大环境下，人工智能的重点已经从以AI基础算法为中心的导向，转移到以保障安全及隐私的大数据架构为中心的导向上。这一重心的转移，推动了联邦学习的诞生，它为使用者带来了传统机器学习所不具有的优势。

剑桥大学的计算机科学和技术系（Department of Computer Science and Technology）在网络安全、密码学和相关领域享有卓越的学术声誉。

- 根据2024年的QS世界大学排名，剑桥大学计算机科学与信息系统专业在全球排名第8位。虽然该排名未专门列出网络安全，但它间接反映了该校在相关领域的研究和教育质量。

剑桥的计算机科学系下设有多所研究机构，如安全工程实验室（Security Engineering Laboratory），专注于密码学、恶意软件分析、网络攻防策略等前沿技术研究。

- 剑桥与数学、工程、社会科学等多个学科领域紧密合作，这使得网络安全研究能从多角度审视问题，比如结合社会心理学探讨用户行为和攻击模式。

剑桥的计算机科学课程注重理论与实践相结合，培养出具备深厚理论基础和实战能力的安全专业人才，并与全球领先的科技公司有密切的合作。

- 如参与网络安全研究项目并将其应用于行业标准和解决方案的开发等，同时也有更多科研平台，如Dipartimento di Ingegneria Informatica、Cyber Security Centre等，汇集了最新的研究成果和技术发展动态。

PROGRAMME BACKGROUND

项目背景

随着技术的发展，网络安全趋势也在不断变化，数据泄露、勒索软件攻击和黑客攻击变得越来越普遍。近年来，全球范围内的隐私法规（如GDPR《通用数据保护条例》）对数据隐私保护提出了严格要求，本项目将充分利用剑桥大学在网络安全学科的学科优势，提高“黑客文化”和网络安全攻防实践，让学生深度参与网络安全的前沿实践。

用户对个人数据隐私的关注日益增加，传统的数据集中处理模式容易引发数据泄露风险。联邦学习允许数据在本地设备上处理，减少了数据传输和集中存储的需求，从而增强了隐私保护，降低了隐私风险。大型科技公司（如Google、Apple）和其他行业的公司（如医疗、金融）开始将联邦学习应用于实际场景，推动了其技术的成熟和普及。

在网络安全中，联邦学习可以应用在多个层面

包括隐私保护、恶意行为检测、去中心化安全防护、快速适应新威胁、协同分析等，这些应用展示了联邦学习在增强网络安全方面的潜力，同时也在数据隐私保护和跨组织协作中发挥了重要作用。

剑桥大学的计算机科学系有丰富的学术资源

包括安全工程实验室、网络安全中心等，专注在网络安全的前沿研究，同时也和其他学科进行联动，多方面多角度探讨网络安全在不同领域方面的应用以及影响。

剑桥大学在网络安全学科有多方面的优势

包括学术与产业实践相结合，与全球领先的科技公司有密切合作，如参与网络安全研究项目并将其应用于行业标准和解决方案的开发等。剑桥的研究成果常常被政府和国际组织采纳，作为制定网络安全政策和应对策略的重要依据，同时为政策制定者和企业人员提供培训。

PROGRAMME OBJECTIVE

项目目标

跨学科知识体系+学科研究前沿

- **跨学科知识体系**
  学生将学习网络安全的核心理论，包括加密学、网络协议、攻击防御技术和风险管理等，为解决实际问题提供坚实的基础。
- **学科研究前沿**
  项目内容涵盖最新的网络安全技术和工具，如先进的入侵检测系统、漏洞扫描器和渗透测试方法，使学生能够掌握行业前沿技能。

提升新工科跨学科人才全球胜任力

- **研究机会**
  剑桥大学项目通常包括研究导向的学习，学生有机会参与前沿的网络安全研究项目，深入探索特定的安全问题或技术。
- **跨学科视角**
  项目将结合计算机科学、法律、伦理学等多个学科的知识，帮助学生全面理解网络安全的多维度挑战。

问题解决能力

培养学生出色的分析和解决复杂安全问题的能力，学会如何设计、实施和评估安全策略。

项目目标

网络安全攻防模拟演练

通过实战模拟，学生将在受控环境中实践网络安全技术，提升实战能力和解决问题的技巧。

学生在项目中会分为两组，一方为黑客进攻组，另一方为防守组。在模拟场景中，黑客和防守者的互动不断推动网络安全领域的发展。攻击者寻找新的漏洞和攻击方式，而防守者则不断提升防御技术和策略，以应对这些新的威胁。

产业实践能力

- **行业联系**
  通过与行业专家的互动、研讨会、讲座和实习机会建立宝贵的行业联系，增强职业发展机会。

PROJECT BASED LEARNING

项目模式--学术+攻防实践

学术前沿

该项目旨在让学生深入了解联邦学习的应用，包括隐私保护、恶意行为检测、去中心化安全防护、快速适应新威胁、协同分析等。

- 学生将深度学习如何利用联邦学习避免敏感信息的泄漏，如何进行恶意行为检测，以及不同组织的安全数据如何通过联邦学习模型进行协同分析，提升对复杂攻击的检测能力等。在该项目中，学生还将结合实践课题，了解联邦学习在实际应用中的模拟仿真过程，通过实践课题进一步提升理论认知以及实践能力。

攻防实践

在该项目中，学生将通过角色扮演网络安全的“攻击”与“防御”实战模拟攻防实践课题。

- 学生将自由选择攻守方，并进行组队，选择联邦学习框架和工具。在实践课题中，学生将开发用于网络安全威胁检测的初始机器学习模型，并为模型训练建立联邦学习环境，同时测试模型的准确性、效率和抵御网络威胁的能力，确保模型培训和评估期间的数据隐私和安全。在模拟场景中，攻击者寻找新的漏洞和攻击方式，而防守者则不断提升防御技术和策略，以应对这些新的威胁。通过实战模拟，黑客和防守者的互动不断推动网络安全领域的发展。学生也将在受控环境中实践网络安全技术，提升实战能力和解决问题的技巧。

ACADEMIC SYLLABUS

项目课程

01 联邦学习基础理论

- Overview of federated learning and its significance.
- Comparison with traditional centralized and distributed learning.
- Key concepts and terminologies.

02 联邦学习基础框架

- Types of federated learning: horizontal, vertical, and federated transfer learning.
- System architecture and components.
- Case studies and applications.

03 联邦学习中的数据隐私和安全问题

- Privacy-preserving techniques: differential privacy, secure multi-party computation.
- Data anonymization and encryption methods.
- Federated learning in regulated industries (healthcare, finance).

04 TensorFlow Federated (TFF) 开源框架介绍

- Overview of TensorFlow Federated.
- Setting up the development environment.
- Basic operations and building a simple federated learning model.

05 PySyft 学习及应用

- Overview of PySyft and its features.
- Setting up the development environment.
- Building federated learning models using PySyft.

06 联邦学习中的优化与交流

- Challenges in federated optimization.
- Communication efficiency and strategies.
- Model aggregation techniques.

07 处理非 IID 数据和系统异构性

- Understanding non-IID data distributions.
- Techniques to handle data heterogeneity.
- Federated learning with heterogeneous systems.

08 构建联邦学习模式

- Implementing a federated learning model from scratch.
- Training and evaluating the model on decentralized datasets.
- Addressing common issues and debugging.

09 高级隐私技术

- Homomorphic encryption and its application in federated learning.
- Secure aggregation protocols.
- Federated learning with differential privacy.

10 实际应用和案例研究

- Federated learning in healthcare: predictive modeling and diagnosis.
- Federated learning in finance: fraud detection and risk assessment.
- Other applications: smart cities, IoT, and more.

项目实践课题示例--网络安全的攻防实践

实践课题要点

联邦学习框架

利用 TensorFlow Federated 或 PySyft 等框架构建联合学习基础设施。

网络安全案例

重点关注特定的网络安全挑战，如入侵检测系统（IDS）、恶意软件检测和异常检测。

数据隐私与安全

采用差分隐私和同态加密等技术，确保训练过程中的数据安全。

实践课题所用工具及技能

01 框架

- TensorFlow Federated
- PySyft

02 编程语言

- Python

03 网络安全工具

- Snort（IDS）
- VirusTotal（恶意软件分析）

04 数据隐私技术

- 差分隐私
- 同态加密

PROJECT BASED LEARNING

项目实践课题示例--网络安全的攻防实践

第一阶段

构思和团队组建

Form teams and brainstorm ideas.

学生分为两组，一方为黑客进攻组，另一方为防守组，自由组建团队。

Define the scope of the cybersecurity challenge to address.

确定要应对的网络安全挑战的范围。

Select the federated learning framework and tools.

选择联邦学习框架和工具。

第二阶段

数据准备和模型开发

Collect and preprocess synthetic or publicly available cybersecurity datasets.

收集和预处理合成的或公开可用的网络安全数据集。

Develop initial machine learning models for cybersecurity threat detection.

开发用于网络安全威胁检测的初始机器学习模型。

Set up the federated learning environment for model training.

为模型训练建立联邦学习环境。

第三阶段

实施和测试

Implement federated learning to train models across distributed datasets.

实施联邦学习，跨分布式数据集训练模型。

Test the models for accuracy, efficiency, and robustness against cyber threats.

测试模型的准确性、效率和抵御网络威胁的能力。

Ensure data privacy and security during model training and evaluation.

确保模型培训和评估期间的数据隐私和安全。

第四阶段

部署和示范

Deploy the federated learning models in a simulated environment.

在模拟环境中部署联邦学习模型。

Demonstrate how the models detect and mitigate cybersecurity threats in real-time.

展示模型如何实时检测和缓解网络安全威胁。

Present the solution to a panel of judges, highlighting innovation, effectiveness, and potential impact.

进行现场演示以及答辩，向教授展示解决方案，突出创新性、 有效性和潜在影响。

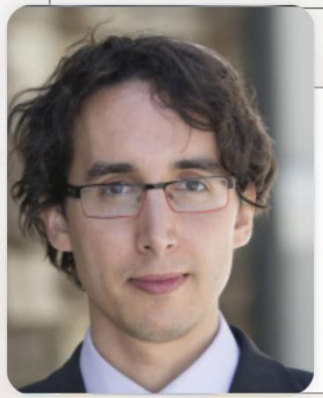
LEADING FACULTY
领衔师资

Prof. Nicolas Lane

- Prof. Lane 是英国皇家工程院新兴技术教席教授、剑桥大学计算机科学与技术系终身教授，并领导剑桥机器学习系统实验室（CaMLSys）。
- Prof. Lane同时也是剑桥大学圣约翰学院的研究员，在加入剑桥之前，Lane博士曾是牛津大学的副教授（2017年至2020年），也曾是伦敦大学的高级讲师（2016年至2017年）。
- Prof. Lane现在是Flower Labs的联合创始人兼首席科学家，Flower Labs是一家新兴人工智能公司（YCW23），致力于推动一种协作、开放和分布式的人工智能未来，旨在实现协作、开放和分布式的人工智能未来。

Dr. Filip Svoboda

- Dr. Filip Svoboda是 剑桥大学计算机科学与技术系的研究助理，同时也是牛津大学外聘讲师（AIMS CDT）。
- Dr. Filip Svoboda 致力于通过模型压缩和加速技术推动联邦学习，他是剑桥神经网络组的联合创始人和负责人。在加入剑桥之前，他曾在牛津大学机器学习系统实验室和牛津大学自治、智能机器和系统中心从事深度学习效率方面的工作。



Prof. Jose Hernandez-Lobato

- Prof. Jose Hernandez-Lobato 教授是剑桥大学工程系的机器学习教授，同时也是剑桥 ELLIS 部门的主任和剑桥医学人工智能中心的教员。
- 他的研究方向主要集中在基于模型的机器学习上，特别关注概率学习技术，如贝叶斯优化、矩阵分解方法、联结函数、高斯过程和稀疏线性模型。
- Prof. Jose Hernandez-Lobato 的研究成果多次发表在顶级机器学习期刊以及会议上，如机器学习研究杂志（Journal of Machine Learning Research）以及 NIPS 和 ICML 等会议。

*参访案例仅供参考，具体参访行程与内容以实际安排为准

NVIDIA Cambridge-1英伟达

是一座技术强大的超级计算机中心，也是英国最强大的超级计算机之一

它是各个领域开创性研究和进步的催化剂，特别是在加速与药物开发、疾病进展研究和物种保护计划相关的研究方面发挥着关键作用。凭借其强大的性能，赋予了英国顶尖医疗研究人员力量，促使了重大的发现和突破。学生有机会参观NVIDIA Cambridge-1并亲身见证这些理论概念的实际应用，与处于技术前沿的专业人士和研究人员互动。

剑桥科技园

英国剑桥科技园是世界上公认的最重要的技术中心之一

该地区的GDP占全英国比重的15.8%，研发开支占该区GDP比重的3.4%，形成了以大学、新兴公司和大型跨国公司密切协作的产业网络中开展业务的极具创新特色的经济形态，并不断吸引着来自全世界的投资。剑桥科技园区的经济发展创造了“剑桥现象”，如今已成为整个英格兰东部地区的发展中心。

R&R罗罗航空发动机中心

罗罗航空发动机中心是位于英国的全球顶尖的发动机制造厂商之一

罗罗航空发动机中心已有100多年的创新历史，致力于推动现代世界。同学们将参访该工厂，了解其在航空领域的领先地位和创新能力。目前，他们正在进行为期多年的转型，以建立高效、有竞争力且不断增长的罗罗航空发动机中心。

剑桥计算机历史中心

剑桥计算机历史中心也是剑桥重要的计算机实践基地

拥有超过 40,000 件关于古董电脑、文件等藏品。核心藏品包括一千多台历史悠久的计算机，以及手机、游戏机、计算器，最重要的是还有对先驱者的采访，并拥有世界上最大的里昂电子办公室文物收藏。

CULTURAL IMMERSION

项目文化活动

*活动案例仅供参考，具体参访行程与内容以实际安排为准

剑河撑船

打卡剑桥最受欢迎的文化活动之一剑河撑船，沿岸欣赏剑桥风光。

伦敦、牛津游览

游览世界级城市，感受传统英伦风情，打卡泰晤士河、牛津大学、大本钟等英国地标性建筑。

剑桥赛艇体验课

在剑桥获得独一无二的赛艇体验，深度感受赛艇运动的魅力。

国王学院参访

前往剑桥最负盛名的老牌学院——国王学院，探寻徐志摩的脚步，感受剑桥古老的学院气息

剑桥大学图书馆体验

注册成为剑桥大学图书馆一员，持有实名注册的图书馆卡，沉浸式体验作为剑桥学子的一天。

高桌晚宴

剑桥大学的正式晚宴（Formal Dinner）是一项传统且隆重的活动，通常在学院的大厅或宴会厅举行。学员们将打卡哈利波特同款学院晚宴，身着正装体验剑桥Formal Dinner，感受严肃又神秘的传统英式餐桌文化。

WHAT YOU WILL GAIN

项目预期收获

网络安全领域前沿学科

- 学生将在该项目中了解并学习网络安全方向最前沿的学术动态、技术发展以及最新的应用，旨在让学生深入探索联邦学习的应用，并学习剑桥大学在联邦学习方向的最新研究。

皇家工程院院士领衔顶级师资

- 剑桥大学在计算机科学、人工智能领域有着享誉世界的学术声誉和科研实力，由剑桥大学工程系资深教授、英国皇家工程院院士领衔的教学团队将结合最新的应用案例为学生教授网络安全的前沿科技应用。

网络安全攻防实践与“黑客文化”

- 学生将通过实践课题，沉浸式体验网络安全的进攻和防守。在模拟场景中，学生将通过黑客进攻以及防守者的体验，进一步学习并探索网络安全技术和策略的不断进步。

剑桥大学学院项目官方认证

- 学生完成项目考核后将获得由剑桥大学副校长在结业仪式亲自颁发的项目官方证书，项目录取后注册剑桥大学图书馆学生卡，可使用剑桥大学图书馆等资源。

直通剑桥大学招生官

- 剑桥大学招生官将为学生讲解剑桥大学最新的申请要求以及案例，同时为学生进一步解答关于剑桥大学的最新动态，提供各类申请机会。

跨文化体验

- 沉浸式体验剑桥大学学子的校园生活，锻炼学生跨文化交流的能力，体验当地人文特色，更加全面客观的了解剑桥顶尖学府的学习以及日常生活。

PROGRAMME SCHEDULE

项目计划日程安排

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
Morning Session 9-12	乘机抵达伦敦，指定时间内集中安排接机，伦敦-剑桥，办理入住	开营仪式	学术课程	学术课程	学术课程	剑桥-伦敦-剑桥 伦敦参访	剑桥-牛津-剑桥 牛津大学参访
Afternoon Session 2-5		剑桥大学学院参访	学术课程	产业参访	项目实践		
Fellow’s Night		小组项目	小组项目	小组项目	文化活动		
	Day 8	**Day 9**	**Day 10**	**Day 11**	**Day 12**	**Day 13**	**Day 14**
Morning Session 9-12	学术课程	学术课程	学术课程	网络安全攻防实践 项目颁奖仪式 Formal Hall高桌晚宴	小组点评	剑桥-伦敦机场 离开剑桥，指定时间内集中安排送机	抵达国内
Afternoon Session 2-5	学术课程	产业参访	学术课程		结业仪式		
Fellow’s Night	项目实践	文化活动	小组项目		自由活动		

*此项目日程为计划安排示例，实际安排可能会有调整。

PROJECT COST DESCRIPTION

项目费用说明

项目时间：2025年 • 1月13日-1月26日 • 2月1日-2月14日

线下项目	费用内容
32800 元 / 人	包括项目课程、文化活动、机构探访、住宿、餐饮、当地通勤及接送机、项目服务管理费用、签证服务及保险费用，明细如下。

项目课程费用

- 课程费用；
- Workshops费用；
- 教学课件、书籍、资料费用；
- 教学场地相关费用；
- 项目申请费用；
- 助教费用。

签证服务及保险

- 个人境外旅行意外保险；
- 英国签证咨询及协助申请服务。

住宿与活动费用

01. 食、住、行服务

部分早餐及部分午餐；住宿费用（单人间）；接送机送机费用；城市间通勤交通费用。

02. 文化实践及参访费用

全程4个机构探访费用；全程6个文化体验探访费用。

03. 生活服务费用

大学区域及房间网络服务；First-Aid 紧急治疗包和支援服务；英国当地医院医疗保险服务。

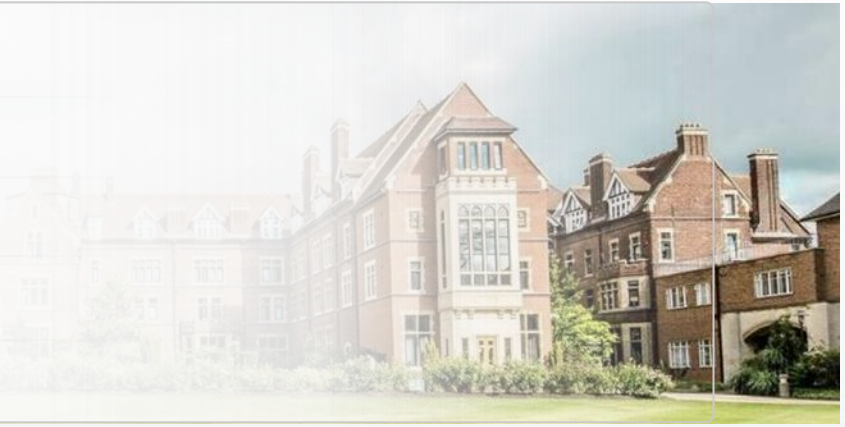
04. 项目管理费用

项目方管理费用；外方院校管理费用。

项目申请及咨询服务

项目申请条件

1. 满足学校国际交流派出要求；
2. 本科生、研究生，年满18岁；
3. 具备一定的专业课程基础知识，各项目专业基础课程要求详询Cindy老师；
4. 具备一定的学术英语能力、海外生活能力、开放积极的交流心态，参与项目期间遵纪守法，尊重项目组安排；
5. 本项目也欢迎高校创新创业指导老师，高校创新创业竞赛组织管理人员等报名。



申 请 流 程

1. 填写报名提交材料 → 2. 等待审核结果 → 3. 收到录取通知后签署项目合约 → 4. 完成缴费
5. 获得官方邀请函 → 6. 办理签证 → 7. 购买往返机票 → 8. 参加线上/线下行前培训 → 9. 出境

注：申请过程中我们将为学生提供全程的指导服务。

项目咨询Cindy老师