1. 题目： 基于属性基加密的细粒度模型授权控制

指导老师：杨文元

个人主页：<https://scst.sysu.edu.cn/members/members01/1402908.htm>

拥有丰富的本科生指导经验：<http://time--flies.gitee.io/periodical/pc>

（已指导多名本科生获得保研资格并录取于top高校，多名本科生录用或投稿国际论文）

课题简介：

随着人工智能模型应用于各大产业和人们生活，模型版权安全成为了人工智能数字资产中不可忽视的一个保障环节。主动授权控制技术作为模型版权的事前防御手段，能够限制未授权的用户正常使用模型，仅允许授权用户获得模型的高精度输出。但现有方案聚焦于粗粒度级别授权，授权用户具有模型全部功能使用权限，无法根据用户身份开放特定部分模型功能。

假设某医院开发了一种基于人工智能的医疗诊断模型，该模型能够诊断多种疾病（即不同的AI任务），如糖尿病、心脏病和癌症。不同级别的医疗人员（如全科医生、内科医生、肿瘤科医生）只能访问模型的特定部分功能，以确保模型使用的安全性和合规性。例如，全科医生仅能使用模型诊断常见慢性病，而内科医生和肿瘤科医生则分别能访问心脏病和癌症的诊断功能。

本课题将从现有模型授权控制技术出发，研究如何结合密码技术以支持细粒度的模型授权控制。本课题将尝试采用属性基加密（Attribute-Based Encryption, ABE）技术，通过为模型的不同功能模块（如不同层、分类功能等）定义属性集合，使用ABE对各模块的输出进行加密，使得具备相应属性的用户才能解密访问。本课题还将引入中心化的属性管理系统，根据用户身份和需求动态调整其属性集合，实现灵活且实时的AI模型权限控制。

（本课题为AI模型版权技术与密码学技术结合的创新性课题）

主要研究内容：

1. 研究细粒度模型授权控制技术，结合属性基加密等技术，实现基于用户属性的授权控制技术。
2. 实现一套中心化的属性管理系统，需要实时调整用户身份与属性集合 ，实现动态授权控制。
3. 题目：分布式跨模态实体认证接入层研究

指导老师：杨文元

个人主页：<https://scst.sysu.edu.cn/members/members01/1402908.htm>

拥有丰富的本科生指导经验：<http://time--flies.gitee.io/periodical/pc>

（已指导多名本科生获得保研资格并录取于top高校，多名本科生录用或投稿国际论文）

课题简介：

在数字化时代，我们每天都在与各种网络实体进行交互，从社交媒体到智能家居，再到工业物联网。随着各种网络技术的逐步发展，传统的IP网络架构愈发难以兼容愈发多样和复杂的新型网络技术。多模态网络因其对各网络技术良好的兼容性和拓展性成为了负载多种新型网络技术的可行方式。如何在多模态网络中实现安全、高效的跨模态实体接入和认证是目前多模态网络的一个研究方向。

本课题旨在为多模态网络构建一个安全可信的实体接入层，为跨模态实体入网认证搭建一座“信任桥梁”，确保网络交互的安全性和可靠性。本课题分为两个方向，一是为接入实体生成用于跨模态认证的身份标识，二是基于异构标识对入网实体进行动态认证。我们将利用分层编码、区块链防伪等前沿技术，设计一个适用于多模态网络的异构标识生成框架，解决多模态网络下异构标识的兼容性和扩展性问题。我们将实现动态的跨模态实体信任互证机制，基于二部图、分布式账本等技术构建信任互证异构池，实现跨模态实体间的信任传递，并根据网络实时安全态势动态调整信任度，实现智能的信任管理。

（本课题为国家重点项目研究内容之一，分布式跨模态实体认证接入层研究的创新性课题）

主要研究内容：

1. 基于分层编码、区块链防伪等前沿技术构建异构标识生成框架。
2. 基于二部图、分布式账本等技术构建信任互证异构池，实现跨模态实体信任互证机制。
3. 题目： 视频监控系统安全评价体系与安全知识图谱

指导老师：杨文元

个人主页：<https://scst.sysu.edu.cn/members/members01/1402908.htm>

（已指导多名本科生获得保研资格并录取于top高校，多名本科生录用或投稿国际论文）

拥有丰富的本科生指导经验：<http://time--flies.gitee.io/periodical/pc>

课题简介：

视频监控系统已被各国广泛部署以保卫公共安全，但若系统存在漏洞将导致严重的安全问题，利用智能感知和AI进行视频监控系统安全态势感知已成为保护国家安全，维护国家利益，提升国家安全管理的水平的重要手段。

在非协作条件下，评估视频监控系统的安全性尤为重要。因此，本课题结合人工智能技术，研究视频监控系统的安全态势感知理论与技术。

（本课题为重点项目研究内容之一，AI与网络安全融合的重要研究课题）

主要研究内容：

(1)构建多层次网络安全态势指标体系：针对视频监控系统安全指标不明确、难理解、覆盖不足的问题，本研究通过划分指标类别、量化参数和标准，从领导、管理、运维三个层次构建全面的安全态势指标体系。利用机器学习和数据分析技术进行数据收集和处理，通过智能算法提取和关联各层次指标，确保指标清晰全面。采用数据关联和知识图谱技术，建立动态、准确的安全态势评估模型，为不同层次用户提供全面、准确的安全评估和决策支持。

(2)利用多源数据探针采集数据，构建安全知识图谱：本课题利用多源数据探针采集视频监控系统的数据，构建设备图谱、威胁图谱和事件图谱。知识图谱是通过将实体（如设备、威胁、事件）及其关系（如连接、影响）系统化表示，构建动态、安全的知识网络。我们将使用数据预处理、命名实体识别和关系抽取技术，确保图谱的准确性和完整性。设备图谱展示设备信息，威胁图谱识别安全威胁，事件图谱重建安全事件过程。通过数据预处理、命名实体识别和关系抽取技术，确保图谱的完整性和动态更新，提升系统的安全态势感知和威胁检测能力。

本课题旨在通过安全态势感知等技术，提高视频监控系统的安全性评估水平，进而保障国家和公共安全。