教育研究
Education Research
第 9 卷◆第 1 期◆版本 1.0◆2026 年
文章类型：论文 | 刊号（ISSN）：2630-4686 /（中图刊号）：380GL020

人工智能赋能信息安全专业课程教学研究

杨蒙蒙 唐俊 刘天舒 张米 赵丽梅*
绵阳职业技术学院
DOI:10.12238/er.v9i1.6739

[摘　要] 网络安全是数字中国建设的重要基础，对高素质信息安全人才的需求呈爆发式增长。然而，传统信息安全专业课程教学具有理论与实践脱节、教学资源滞后、因材施教不足等痛点，不能够满足对“实战型”“创新型”人才的要求。人工智能（AI）技术的快速发展为解决以上的痛点有了新思路——它在智能资源生成、个性化学习、虚拟仿真实验等方面的优势，能够和教学中需要的实践性、实时性需求相融合。本文基于信息安全专业教学现状，利用 AI 技术针对面临的挑战提出对策，为推动信息安全教学改革提供参考。
[关键词] 人工智能；信息安全；高等教育
中图分类号：TP309-4 文献标识码：A

Research on AI-Empowered Teaching in Information Security Programs

Mengmeng Yang, Jun Tang, Tianshu Liu, Mi Zhang, Limei Zhao*
Mianyang Vocational and Technical College

Abstract: Cybersecurity serves as a vital foundation for building a Digital China, driving explosive growth in demand for highly skilled information security professionals. However, traditional information security curricula suffer from disconnects between theory and practice, outdated teaching resources, and inadequate personalized instruction—failing to meet the need for “practical” and “innovative” talent. The rapid advancement of artificial intelligence (AI) technology offers a novel approach to addressing these challenges. Its strengths in intelligent resource generation, personalized learning, and virtual simulation experiments can be integrated with the practical and real-time demands of teaching. Based on the current state of information security education, this paper proposes AI-driven solutions to these challenges, providing insights for advancing information security teaching reform.
Keywords: Artificial Intelligence; Information Security; Higher Education

1 引言

1.1 研究背景

目前，网络攻击呈现出“智能化”“复杂化”“产业化”等特征，从定向攻击的病毒到长期潜伏的 APT 攻击，从 AI 自动生成恶意代码到量子计算对传统密码体系的威胁，“攻防对抗”已经到达“技术竞速”阶段。《2024 年网络安全产业人才发展报告》的数据显示，2024 年网络安全人才的需求总量已经超过 150 万，但是高校每年培养的相关人才不足 3 万人。

高校是人才培养的主阵地，但如今的信息安全专业教学面临双重压力：一方面，技术更新快，使用的教材与案例难以跟进；另一方面，教学模式以“理论讲授+简单实验”为主，学生缺少真实攻防场景下的实践。在此背景下，探索技术赋能教学的新方式成为必然。

1.2 AI 赋能的核心逻辑

AI 技术的原理是“数据驱动的智能决策”，与信息安全专业在教学中融合具有天然合理性。从教学目标看，教学中需培养学生的攻防能力，而 AI 可模拟真实的黑客攻击，构建真实的实践环境；从教学过程看，信息安全知识体系比较复杂，学生基础差异大，AI 可通过学习分析技术实现因材施教；从教学资源看，信息安全领域的漏洞库、攻击案例等数据比较分散，AI 可通过自然语言处理（NLP）、知识图谱技术实现资源的整合与动态更新[1]。

因此，AI 赋能并不是一味的“技术叠加”，而是通过重构教学资源、优化教学过程、创新评价方式，推动信息安全教学从“被动传授”向“主动实践”、从“统一教学”向“因材施教”转型。

2 信息安全专业课程教学现状与痛点

2.1 教学内容：滞后于技术迭代，理论与实践割裂

目前，在信息安全专业课程中，教材中的大多数的案例都是 SQL 注入、DDOS 攻击等传统的网络攻击方式，对于 AI 自动生成钓鱼邮件、智能入侵绕过等的新型攻击手段涉及较少。与此同时，在授课中实践环节与行业脱节：高校实验课依赖固定实验箱或虚拟平台，实验内容比较固定，学生按

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

照固定步骤操作即可，缺乏自主设计防御策略和应对真实环境攻击的能力。

2.2 教学模式：“单向灌输”为主，个性化指导缺失

由于班级人数比较多，现有的教学模式以“教师讲授+PPT 展示”为主，学生是被动学习。在实操过程中，教师课上同时指导多名学生，难以关注个体化差异。基础薄弱的学生可能因为实验过于复杂而放弃实践，而能力较强的学生会因为实验内容太简单，导致实践能力没有获得过多的提升。

此外，学生在学习过程中缺乏动态反馈。目前，学生完成实验后以提交实验报告让教师批改为主，由于学生过多，通常教师人工批改周期较长，导致对学生知识掌握情况反馈滞后且针对性不足。

2.3 实践资源：场景单一，缺乏真实对抗环境

信息安全的核心是“攻防对抗”，但目前高校难以模拟真实的实践场景：一方面，“攻防对抗”环境涉及不同厂商的多个设备并且实现的业务系统复杂；另一方面，案例要涉及真实环境下漏洞被利用细节，现有的公开资源有限，并且更新速度慢。一些高校尝试与企业合作引入搭建好的攻防平台（如奇安信的“攻防演练系统”），在该平台中，实验环境和实验步骤已经全部给出，包括攻击路径、防御策略等，学生只需按实验步骤操作，难以培养实战能力。

3 人工智能赋能信息安全课程教学的应用场景

3.1 智能教学资源建设：动态生成与精准匹配

AI 技术可以解决传统教学资源“静态化”“滞后性”的问题，通过数据整合智能生成构建出“动态资源库”，具体包括三个维度：

（1）智能案例库构建

AI 能够通过 NLP 与知识图谱技术，自动爬取、清洗、整合多个平台的信息安全数据，并且能够按照“攻击类型”“漏洞等级”“影响范围”等方面构建出知识图谱。例如，当新漏洞出现时，AI 能够在 24 小时内提取漏洞原理、利用的资源、攻击手段、防御方案等关键信息，生成包含原理图解、攻击演示视频、防御实验步骤的教学案例，并能够将此案例与知识点关联[2]。

（2）自适应题库生成

传统课程的题库需要教师手动出题，效率较低。AI 能够将知识点与学生现有的能力相结合自动生成题库，通过分析课程大纲内容结合学生能力动态生成不同难度的题目。例如，针对密码学中“RSA 算法”知识点，基础题可考查“RSA 算法原理”，应用题可要求“用代码实现简易 RSA 加密”，创新题则可设计“基于 RSA 的密钥协商协议优化”，并通过学生答题情况动态调整题目难度，如某题错误率超 70%则降低难度，错误率低于 20%则增加难度。

3.2 个性化学习路径：数据驱动的精准引导

AI 可通过对学生进行学习分析、路径规划、动态调整三个环节，为学生提供个性化学习方案，实现因材施教：

（1）学习状态精准画像

基于教育数据挖掘（EDM）技术，AI 能够实时获取学生的学习数据，包括课堂互动数据（如提问次数、答题正确率）、实验操作数据（如实验操作时长、防御策略尝试次数）、资源访问数据（如题库练习记录）等，通过聚类算法（如 K-Means）获取学生知识掌握情况。例如，学生在“入侵检测”实验中多次因“特征库更新不及时”导致漏报，AI 可判定他对“动态特征提取”知识点内容掌握不牢固。

（2）个性化学习路径推荐

AI 可为学生生成“一对一学习路径”：对基础薄弱的学生，优先推荐“理论微课+基础实验”；对能力较强的学生，推荐“进阶案例+创新任务”。

（3）实时学习干预

AI 可对学生的异常行为进行识别，及时干预学习过程：当学生在实验中出现多次实验失败，AI 可自动推送错误原因及正确的案例；当学生学习进度滞后，AI 可发送“学习提醒”并降低后续任务难度。

3.3 虚拟仿真实验：构建真实攻防场景

AI 可突破传统实验平台的“固定化”的限制，实现“真场景、真对抗、真反馈”：

（1）智能攻防演练平台

基于强化学习（RL）技术，AI 可模拟“攻击者”与“防御者”，构建开放式演练场景。例如，在“网络攻防”实训中，AI 模拟“黑客”，根据学生的防御策略（如防火墙规则、入侵检测配置）动态调整攻击手段—若学生仅部署“端口封禁”进行防御，AI 会尝试“端口扫描绕过”（如使用碎片化扫描）；若学生启用“异常流量检测”，AI 会转变为“低频率攻击”（如发送攻击包速度降低），迫使学生动态优化防御方案。同时，AI 还实时监控学生操作，当学生因操作不当导致系统崩溃时，会触发“紧急修复引导”，避免实验中断。

（2）漏洞挖掘虚拟环境

在“漏洞挖掘”课程中，存在真实漏洞样本少的问题，AI 能够自动生成“漏洞环境”：通过代码生成技术（如 CodeLlama）生成含有“逻辑漏洞”“内存漏洞”的环境，并隐藏漏洞特征。学生完成漏洞挖掘实验后，AI 能够自动分析学生实验过程并生成“能力评估报告”。

3.4 智能教学评价：高效精准的能力评估

AI 能够突破传统“人工主观化”的局限，实现“全维度、动态化、精准化”的评价：

（1）实验过程性评价

传统评价主要依赖实验报告，难以反映学生操作能力。AI 能够根据学生实验中的操作进行行为分析，实现过程性评价[3]。比如：在“网络攻防”实训中，AI 记录学生的每一步操作过程（如“漏洞扫描工具选择”“防御策略调整”等），并能够从效率、准确性、创新性三个维度对学生进行评分。其中“效率”关注完成实验的时长，“准确性”关注实验操

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

作过程是否正确，“创新性”关注是否使用传统方法。例如，某学生使用自己编写的脚本替代现有的扫描工具完成漏洞检测，AI 会在“创新性”维度给予额外加分。

（2）综合能力可视化评价

AI 能够通过多维度数据生成能力雷达图：结合理论测试成绩、实验操作评分、创新任务完成度等数据，直观展示学生在“理论基础”“实战能力”“创新思维”“协作能力”等维度的表现。教师可基于学生雷达图因材施教，调整教学重点（如针对“实战能力弱”的学生增加演练次数），学生也能够明确自身短板，加强训练。

4 AI 赋能信息安全课程教学的实施路径

4.1 构建 AI 赋能的教学平台体系

AI 能够整合“资源库、学习分析、虚拟实验、评价系统”四大模块，打造一体化的教学平台：

底层架构：采用“云-边-端”的架构，在云端存储海量数据（案例库、题库、漏洞样本）[4]，在边缘端部署 AI 推理模型（如攻击模拟模型、学习分析模型），在终端供学生通过 PC、平板访问。

核心功能：实现基于学习画像的“资源智能推送”、基于能力水平的“实验动态生成”、基于操作数据的“评价实时反馈”的闭环。

协同机制：与企业平台对接，确保资源实时更新；与高校现有教务系统或 MOOC 平台打通，实现数据互通。

4.2 重构课程体系与教学内容

将 AI 技术与信息安全专业知识深度融合，实现 AI 技术驱动专业知识的授课过程：

基础层：增设“AI 与信息安全”交叉课程，增强学生对 AI 对现有信息安全技术的影响。

实践层：增加实验课程比例，增设“AI 攻防演练”“智能漏洞挖掘”等实验模块，并在实验课时增加无固定步骤，需要学生设计方案的开放式实验。

创新层：引导学生基于 AI 技术解决实际问题。如“用大语言模型优化安全日志分析”，鼓励学生参与 AI 安全竞赛。

同时，还需要建立“动态更新”机制：每学期联合企业专家、AI 技术团队修订课程内容，确保至少有 30%的案例实验场景是近 6 个月内的新技术和新漏洞。

4.3 加强师资队伍与校企协同

AI 赋能教学还需“技术+教学”两方面的支撑，通过“内培外引”的方法强化校内师资，通过“校企协同”的方法弥补资源短板：

（1）师资能力提升

通过开展 AI 教学工具的培训，定期组织教师学习 AI 平台操作、AI 教学方法。

组建“跨学科教学团队”：通过联合人工智能教研室教师、企业技术专家成立团队，共同设计课程标准。比如：人工智能教研室教师负责智能平台技术的实现，信息安全教师负责教学内容，企业专家提供真实案例。

（2）校企协同机制

校企共建“AI 安全教学实验室”：企业提供攻防平台部署和 AI 模型优化等技术支持，高校提供场地与学生资源，共同开发“企业真实场景复刻实验”[5]。

在人才培养上，推行“双导师制”：企业工程师与高校教师共同指导学生，企业导师负责实战技能教学，高校导师负责理论与创新指导，并联合开展“AI 安全科研项目”。

5 结论与展望

AI 技术为信息安全专业课程教学提供了“动态化、个性化、实战化”的改革路径，能够通过智能资源建设解决资源滞后问题，通过个性化学习突破“统一教学”的局限，通过虚拟仿真实验弥补“实战场景缺失”的短板，最终实现校内人才培养与行业需求的精准对接。然而，AI 赋能并非“技术万能”，其落地需要高校、企业协同推进。但无论技术如何迭代，“以学生为中心”的核心逻辑不会改变，使用 AI 的目的就是让每个学生成长为“懂技术、能实战、有担当”的信息安全人才，为数字经济安全发展筑牢人才防线。

[参考文献]

[1]胡泽,杨宏宇.基于新型对分课堂的人工智能入门课程建设——以信息安全专业为例[J].教育教学论坛,2024(28):138-143.

[2]刘红梅.人工智能赋能职业教育课程改革路径与实践探索[J].时代汽车,2025(22):43-45.

[3]王晶.高职院校信息安全技术应用专业课程体系探究与实践[J].家电维修,2024(6):40-42.

[4]李翠丽,何钰枫,王建夏.基于云平台的物联网信息安全实验课程建设与教学模式探索[J].中国现代教育装备,2025(17):31-34.

[5]李焱,孙国坤.人工智能赋能下高职“双师型”教师团队协同共融成长模式构建与实践研究[J].时代汽车,2025(21):26-28.

作者简介：

杨蒙蒙（1997.04-），女，汉族，河南周口人，硕士研究生，助教，研究方向为信息安全、图像识别。

赵丽梅（1969.04-），女，汉族，吉林四平人，本科，教授，研究方向为软件开发、自动控制。

基金项目：

绵阳职业技术学院·基于深度学习的实时车牌检测与识别(项目编号：MZ24YB05)；绵阳市社会科学研究基地·四川幼儿教育与发展研究中心资助项目（项目编号：SCYJ2024ZC10）。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.