

# 人工智能赋能信息安全技术课程教学改革研究<sup>\*</sup>

单棣斌<sup>1</sup> 王楠<sup>2\*\*</sup> 李冰<sup>3</sup> 祝宁<sup>1</sup>

1. 信息工程大学密码工程学院  
郑州 450001

2. 信息工程大学基础部  
郑州 450001

3. 陕西省军区  
西安 710061

**摘要** 针对信息安全技术课程面临的教学内容更新快、个性化学习需求迫切、全流程教学评估难等痛点,提出了“增强体系、个性学习、智能评估”三位一体的AI赋能教学模式。通过构建增强型教学内容体系实现教学内容迭代优化,运用AI助教支持个性化学习培养,建立多维多元评估机制支撑教学策略动态调整。实施结果表明,该模式使学生的知识点考核达标率增加7%,能力点考核达标率上升5%,学生满意度提高了4%,为解决信息安全类课程面临难题提供了可复制方案。

**关键字** AI赋能, 教学模式, 个性化学习, 智能教学评估

## Research on AI-Empowered Teaching Reform of Information Security Technology Courses

Shan Dibin<sup>1</sup> Wang Nan<sup>2\*\*</sup> Li Bing<sup>3</sup> Zhu Ning<sup>1</sup>

1. Institute of Cryptography Engineering  
Information Engineering University,  
Zhengzhou 450001, China;

2. Department of Basic Education  
Information Engineering University,  
Zhengzhou 450001, China;

3. Shaanxi Military Region  
Xi'an 710061, China  
376565149@qq.com

**Abstract**—Addressing challenges in information security technology courses—rapid content updates, urgent personalized learning demands, and difficulties in comprehensive teaching evaluation—this study proposes a tripartite AI-empowered teaching model: enhanced curriculum, personalized learning, and intelligent assessment. An augmented teaching content system enables iterative optimization, AI teaching assistants support tailored learning development, and a multidimensional evaluation mechanism facilitates dynamic teaching strategy adjustments. Implementation results indicate that this model increased student knowledge point assessment pass rates by 7%, ability point assessment pass rates by 5%, and student satisfaction by 4%, providing a replicable solution for addressing challenges in information security courses.

**Keywords**—AI-empowered, teaching model, personalized learning, intelligent teaching assessment

## 1 引言

在人工智能技术重塑全球生产生活方式的当下,教育领域正经历着从“经验驱动”向“智能驱动”的范式转型。联合国教科文组织2021年发布的《AI与教育:政策制定者指南》指出,人工智有望解决当今教育面临的部分重大挑战,革新教学实践,最终加快迈向可持续发展目标的进程;2025年发布的《人工智能与未来教育》中指出,AI赋能的教学模式需要重视个性化学习与高阶能力的培养。

我国对AI赋能教育的战略布局同样前瞻且系统。2017年国务院《新一代人工智能发展规划》首次明确“智能教育”为国家战略方向,提出构建智能化教学环境,推动教育模式变革;2023年教育部等六部门联合印发《生成式人工智能服务管理暂行办法》,为AI

在教育教学中的应用划定合规边界,鼓励创新应用与健康发展;2025年教育部正式启动“国家教育数字化战略行动2.0”,以集成化、智能化、国际化为战略方向,全面启动教育数字化发展新征程。在政策引领与技术驱动下,AI在教育领域的应用已取得显著成果,智能教学测评系统、个性化学习平台等得到广泛应用,并取得显著教学效果<sup>[1-2]</sup>。

信息安全技术作为信息安全专业的核心课程之一,其教学仍面临显著挑战,由于班额人数大、学习周期短、教学内容多且更新快等现实特点,课程在教学内容体系完善、学习能力培养、全过程教学评估等方面还需要进一步提升。如何将AI技术应用于课程教学模式改革,以有效解决上述问题,具有重要意义。

## 2 研究背景与现状

人工智能赋能高校课程教学改革是当前教育技术领域的热点话题,国内外多所高校及学者对此进行了广泛的研究与试点应用。

<sup>\*</sup> **基金资助:** 本文得到信息工程大学教育教学研究课题(JXYJ2025C047)支持

<sup>\*\*</sup> **通讯作者:** 王楠 duoduoxf@163.com

国外的研究重点之一是开发智能辅导系统<sup>[3]</sup>, 这些系统能够根据学生的学习行为和成绩自动调整教学内容和难度。例如, 美国多所大学开发了基于 AI 的自适应学习平台, 用于计算机类课程的教学。为了解决实验资源有限的问题, 国外研究者也在探索使用虚拟现实技术来创建模拟的实验室环境<sup>[4]</sup>, 让学生能够在安全的虚拟环境中进行实践操作。利用大数据分析技术<sup>[5]</sup>, 研究人员可以对学生的学习行为进行深入分析, 较为精准地把握每个学生的学习进度、知识掌握程度, 从而发现潜在的学习障碍, 并提供个性化的学习建议。个性化学习模式的构建成为了人工智能应用于教育的重要切入点。

智能评估体系的搭建也是国外高校积极探索的方向之一。国外研究机构<sup>[6]</sup>开发自动化的作业和考试评分系统, 这些系统能够快速准确地评估学生的作业质量, 更为全面的学习过程数据收集与分析, 使得对学生的评价不再局限于单一的考试成绩, 而是涵盖了课堂参与度、小组合作表现、在线学习互动情况等多维度的综合考量, 从而能够更加客观、全面且动态地反映学生的学习状况, 为教育教学决策提供了更为科学准确的依据。

国内的研究更多地集中在如何使用 AI 辅助教师进行教学活动<sup>[7]</sup>, 例如通过智能答疑系统帮助学生解答问题, 或者使用机器学习算法预测学生的学习成效。国内的许多高校<sup>[8]</sup>正在积极探索如何利用 AI 技术丰富和完善信息安全课程的教学资源, 包括在线课程、电子教材和互动式学习平台等<sup>[9]</sup>。基于学生的学习数据, 研究者开发个性化的学习路径推荐系统<sup>[10-11]</sup>, 旨在为每个学生提供最适合其水平和兴趣的学习方案。

然而, 信息安全技术作为信息安全专业的核心课程, 其教学仍面临显著挑战: 其一, 知识更新快, 许多新型安全技术迭代周期缩短至 6-12 个月, 学生对新型安全威胁及防护技术的学习存在滞后性; 其二, 班额规模大, 教师难以兼顾学生差异化需求, 个性化指导覆盖率不高; 其三, 教学评估面临新问题, 迫切需要对学生学习的全过程进行多维度、多阶段的客观评估, 并动态反馈学习建议与规划。在此背景下, 如何将 AI 技术与信息安全技术课程深度融合, 构建动态适配、精准赋能、高效评价的新型教学模式, 已成为破解信息安全人才培养困境的关键命题。

### 3 AI 赋能课程教学模式

课程组以优化教学内容、实施个性化学习、完善评估体系为核心, 依托知识图谱和 AI 助教技术, 构建了“增强体系—个性学习—智能评估”三位一体的教学模式。

#### 3.1 构建增强型教学内容体系

为优化教学内容、及时更新知识素材、帮助学生建立自己的信息安全技术知识体系, 课程组通过多类型课程资源库建设、教学内容智能优化和三类图谱构建等步骤, 构建了增强型教学内容体系, 如图 1 所示。

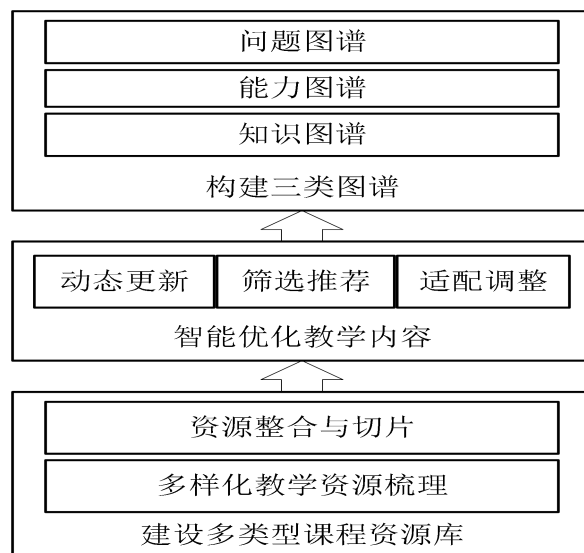


图 1 构建增强型教学内容体系

#### (1) 建设多类型课程资源库

##### ① 多样化资源梳理

一是基础资源, 整合教材、讲义、PPT、试卷库、作业库等传统教学材料, 形成结构化文档库。二是案例资源, 收集防御技术案例(如防火墙规则配置实验、入侵检测系统部署等)、安全防护项目案例(如企业级零信任架构实施案例、云安全防护策略案例)等, 强化学生动手能力。三是拓展资源, 引入信息安全方向国际顶尖会议论文、行业标准与框架、行业白皮书、技术博客等, 拓宽知识边界。

##### ② 资源整合与切片

首先, 将教学资源按照标准化自动分类, 按基础理论、技术应用、前沿动态三级标签对资源进行梳理, 便于快速检索。

其次, 采用数据切片技术, 依托 AI 工作台, 利用自然语言处理模型对文本资源进行语义分割, 提取关键知识点(如多因素认证、安全基线配置、零信任架构等), 生成可独立调用的微内容单元, 并将其与相应的视频、音频、图片等教学资源片段进行自动关联。

#### (2) 智能优化教学内容

##### ① 内容动态更新

一方面, 利用 AI 技术对信息安全前沿发展进行追踪。例如, 通过 BERT 模型分析信息安全领域顶级期刊的论文摘要, 自动识别技术趋势, 如自适应安全架构、

AI 对抗样本防御、后量子密码学等，生成教学内容更新建议。另一方面，动态适配信息安全案例。主要是根据当前安全热点，自动匹配相关教学案例，如勒索软件攻击事件、防御 APT 攻击的日志分析等，从而增强课程时效性。

② 资源筛选推荐

一是优质教学资源筛选。依据教学资源属性标签，基于 AI 筛选算法，结合教师评分、学生使用频率、资源难度系数等指标，遴选出高价值教学内容和优质资源，如零信任架构实施指南、高评分实验视频等。二是优先级推送。根据学生学习阶段智能推荐资源，例如为新入门初级阶段的学生优先推荐网络安全防护基础类动画，如防火墙工作原理、Kerberos 原理动画解析等，为进阶学习阶段的学生推送高级持续防护安全实战项目，如流量分析实验、区块链安全实战项目等。

③ 内容适配调整

教学内容也要根据学情，进行动态的适配性调整。一是教学资源的难度匹配调整。通过聚类分析评估教学内容的难度分布，例如“安全基线配置”属于基础级，“威胁情报分析”属于进阶级，确保与学生的平均能力水平匹配。二是反馈驱动优化。首先收集学生课后评价，如知识点理解度、案例实用性评分等；然后利用情感分析技术提取改进意见，反向优化教学内容。

(3) 构建三类图谱

① 知识图谱

通过知识图谱建立课程的结构化知识体系。首先，知识抽取与关联。利用知识图谱工具，从课程资源库中抽取知识点，如哈希函数、数字签名、区块链、安全属性等，建立知识点之间的逻辑关系，如哈希函数→数字签名→区块链→安全属性。然后，可视化呈现知识点及其关联。通过交互式图谱界面，展示知识点层级结构，帮助学生建立系统化认知结构，展示从基础防护到高级防御的知识链路，如身份认证→访问控制→审计追踪等构成的知识链。

② 能力图谱

通过能力图谱精准对标技能需求。一是能力点定义，结合课程能力目标、教学内容要求，定义学生需掌握的能力点，如安全性分析、安全方案设计、多技术综合应用等。二是将能力点进行类别划分。比如按能力层级划分为基础能力、高阶能力，消息加密、消息认证、公钥证书应用等属于基础能力，而存储加密方案设计、Web 传输安全方案设计等则属于高阶能力。三是学习路径映射。将能力点与课程资源、实验任务关联，例如，公钥认证能力对应公钥分发、PKI、公钥

证书认证实验等内容；存储加密方案设计能力关联算法选择、算法实现、文件加密实验等内容。

③ 问题图谱

通过问题图谱预判与解决学习障碍。一方面，构建常见问题库。基于历史教学数据（如学生提问记录、作业错题集）归纳高频问题，如 Windows 操作系统中 DACL 与令牌的关系、MAC 为什么能够抗击木马攻击等。另一方面，智能诊断与干预。AI 助教通过问题图谱预判学生潜在困惑，主动推送解析视频或针对性问题练习，例如检测到学生在公钥基础设施章节停留时间过长时，自动触发辅助讲解有关 PKI 的问题。

3.2 设计个性化学习模式

为促进学生主动学习、提升学生学习兴趣，课程组从 AI 助教构建、课堂 AI 互动设计、课后智能学伴三个方面入手，设计了基于 AI 助教的个性化学习模式，如图 2 所示。

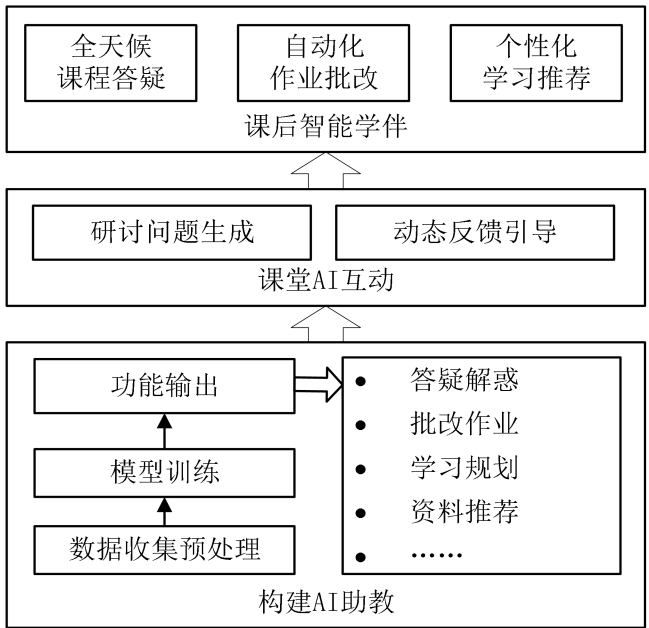


图 2 设计基于 AI 助教的个性化学习模式

(1) 构建 AI 助教

依托现有的在线教学平台和大语言模型，结合已建立的课程资源库，训练面向信息安全技术课程的 AI 助教。其主要过程包括：

首先，数据预处理，将之前建立的多类型课程资源库进行数据的清洗和预处理，以确保数据的质量和可用性。

其次，模型训练，基于预处理后的数据，使用机器学习算法训练 AI 助教模型。通过不断迭代和优化，提高模型的准确性和泛化能力。

最后，功能输出，训练完成的 AI 助教模型将具备多项功能，答疑解惑、批改作业、学习规划与资料推荐等，这些功能将极大地提升学生的学习效率和体验。

(2) 课堂 AI 互动

AI 驱动的课堂讨论设计主要包括研讨问题生成和动态反馈引导两方面。

实时问题生成通过场景模拟与思辨议题进行实施，例如：AI 模拟“某银行遭遇 DDoS 攻击”事件，要求学生基于流量日志分析防御策略。AI 提出“传统防火墙 vs. 云原生防火墙的优劣”，引导学生从成本、扩展性、防护效率等多个维度辩论。

动态反馈引导主要帮助学生在讨论时，提出新观点或者推送新数据案例，引导学生进一步发散思维、批判性思维。学生讨论“入侵检测系统误报率优化”时，AI 实时推送行业数据和学术论文观点，拓展讨论深度。学生在设计“信息传输安全方案”时，AI 推送“先加密后认证”、“先认证后加密”两种信息传输安全方案，引导学生通过对比这两种方案的优劣，给出不同应用场景下的最合适的选择，从而培养学生的批判性思维。

(3) 课后智能学伴

AI 助教为学生的全周期课程学习提供帮助与指导、作业批改和学习规划。

全天候课程答疑。学生可以随时向 AI 助教提问，AI 助教将基于知识图谱提供准确、及时的回答。训练基于 AI 智能体的课程助教，利用机器学习算法预测学生的学习难点，提前发现并解决潜在的学习障碍，及时给予辅导和支持。运用大语言模型，融合信息安全技术知识数据集，为批量学生提供个性化的课程答疑。

自动化作业批改。AI 助教可以自动批改学生的作业，给出评分和反馈意见，帮助学生及时发现并纠正错误。例如，自动分析学生提交的“防火墙规则作业”，自动标记作业中的错误，如“未设置端口”，并提供修复建议。

个性化学习规划。根据学生的学习进度和兴趣偏好，AI 助教可以为学生进行学习能力画像，提供个性化的学习规划和资料推荐服务。应用智能学习平台，根据学生的测试成绩、学习历史和个人偏好，推送个性化学习资料和练习题，提供定制化的学习路径和资源推荐。例如，针对正在复习授权管理技术的学生，智能生成访问控制策略、PMI、单点登录等核心知识点的复习计划。

3.3 建立智能化教学评估机制

为全过程评估学习效果、动态调整教学策略、持

续保持学生的学习主动性，课程组建立了多维度评估模型、多元化评估场景和动态学情分析与反馈相结合的智能化学教评估机制，如图 3 所示。



图 3 建立智能化教学评估机制

(1) 多维度评估模型

构建多维度的教学评估模型，集成多维度数据收集工具，数据收集涵盖过程性评价和终结性评价，全面评估学生的学习表现。

过程性评价占 40%，主要包括课堂互动参与度、实验表现、阶段性测试、综合性作业等，其中，课堂互动参与度负责通过 AI 分析研讨发言质量；实验表现负责记录学生在实验中的操作日志及成绩；阶段性测试负责每单元安全防护知识测验；综合性作业负责典型场景的信息安全方案设计，如某单位的内网安全防护方案设计，评估方案合规性、技术可行性等。

结果性评价占 60%，通过闭卷考试、实验考核等方式，由试题库自动组卷，覆盖信息安全技术体系的各个知识点、能力点，综合考核学生的学习效果。

(2) 多元化评估场景

通过课前诊断进行智能预评估。在每个知识单元开课前的预习作业中，学生通过 AI 预评估系统完成知识水平测试，系统基于知识图谱分析其知识储备，生成个人知识雷达图。

通过课中反馈进行实时动态评估。对学生实验课中的操作过程实施监控，AI 系统实时分析学生操作，如 VPN 网关配置耗时、防火墙规则设置步骤等。通过可视化看板展示班级操作进度与典型错误，例如 80% 学生未使用标志位参数配置防火墙包过滤规则等。

通过课后拓展进行长期学习过程评估。依托 AI 平台对学习轨迹实施追踪,通过学习管理平台采集学生的学习过程数据,如实验报告完成率、实验操作时间、在线测试答题时间、线上测试正确率、安全方案设计成果等,构建课程学习成长曲线以评估能力提升趋势。

(3) 动态学情分析与反馈

通过教学过程评估数据进行学情分析。应用数据分析和可视化技术,生成详细的学习报告,帮助教师了解班级整体和个体学生的学习状况。一方面,对教学班级整体学习情况进行分析。例如,利用热力图展示学习过程中的常见错误,比如在安全基线配置实验中,80%学生未禁用 Telnet 服务;利用曲线图展示各个知识单元的平均学习投入时间,比如在公钥认证部分学习过程中,学生学习投入时间较多,说明该知识单元学习难度较大,需要进一步增加教学辅导时间。另一方面对每个学生进行个体学习情况诊断报告,通过雷达图呈现学生能力维度,例如“访问控制策略设计能力”强,“日志分析能力”弱等。

依据学情分析结果动态调整教学实施策略。例如,学情分析发现,学生普遍在“公钥认证方案”作业中失分,在课外辅导中增加“基于证书的认证方案设计”作业案例分析内容。针对“防御体系设计”能力薄弱,引入 AI 模拟单位网络仿真环境,指导学生在虚拟环境中部署网络安全设备,设计并实现多层防护方案。

4 教学改革效果

通过上述“增强体系一个性学习一智能评估”三位一体的教学模式的实施,信息安全技术课程在内容更新迭代、个性化学习培养、全流程动态反馈等方面取得了明显的成效,知识点考核达标率增加 7%,能力点考核达标率上升 5%,学生满意度提高了 4%,详见表 1。

通过构建增强型教学内容体系,知识体系完整性得到了提升,构建了包含 600+节点的信息安全知识图谱,知识点关联度提升 35%。知识更新效率显著提升,教学案例更新周期从季度缩短至周级,确保教学内容与技术发展同步;学生可快速定位三类图谱的薄弱环节,按需获取适配资源,查漏补缺,避免盲目学习。

通过探索个性化学习模式,学习路径得到优化,AI 助教为不同层次学生提供差异化学习方案,学习主动性得到提升。常规型实验完成率到达 100%以上,技术应用型方案设计作业优良率从 25%提升至 37%,创新型实践作业优秀率从 10%提升至 19%,多数作品推选参加信息安全竞赛、密码技术竞赛等。

通过实施智能化教学评估机制,智能教学平台全

面刻画学生学习全过程,平均每个知识单元向学生推送自学资源 3.7 项、学习预警 0.3 项,平均每个单元向教师反馈教学调整策略建议 0.6 次,客观呈现了学生学习效果,动态反馈学生学习不足,并且激发了学生持续性、长期的学习热情。

表 1 教学改革实施数据统计表

指标	改革前	改革后	变化率
知识点数量	570	632	11%
知识点联系数量	271	368	35%
教学案例更新数量	25.7个/学年	22.1个/周	-
常规型实验完成率	91%	100%	9%
技术应用型实验优良率	25%	37%	12%
综合创新型实验优秀率	10%	19%	9%
自学资源推送数量	教师人工推荐	3.7项/单元/人	-
学习预警数量	教师人工提醒	0.3项/单元/人	-
教学实施计划微调数量	教师自己确定	0.6次/单元	-
知识点考核达标率	74%	81%	7%
能力点考核达标率	71%	76%	5%
学生满意度	91%	95%	4%

5 结束语

人工智能与教育的深度融合,正以不可逆转的态势重塑全球教育生态。从知识图谱构建到生成式 AI 普及,从虚拟仿真到多模态评估,AI 技术已从辅助工具升级为教育系统的智能中枢。本课程改革将 AI 技术应用于教学全流程,对提升课堂教学质量发挥了重要作用。在内容层面,通过动态知识图谱与多源资源库建设,实现了教学内容与技术革新的动态同步;在学习层面,依托 AI 助教与多模态交互设计,构建了诊断、适配与提升相结合的个性化学习模式;在评估层面,借助多维度模型与动态学情分析,形成了过程可溯、能力可测的智能评价机制。但是 AI 在赋能教学的同时,也带来了学习过程过度依赖 AI、算法不透明影响评估公平等问题,需要我们在后续教学改革中进行深入探索与研究。

参考文献

[1] 周延泉,蒋思,张玥,等.人工智能背景下的自然语言处理研究生课程群建设模式研究[J].计算机技术与教育学报,2024,12(03):6-10.

[2] 覃希,陈燕,姚怡,等.“教评双驱”教学实验平台赋能人工智能通识教育路径探索[J].计算机技术与教育学报,2025,13 (01):119-124.

[3] 景玉慧,赵思宇,张晓晴,等.国外生成式人工智能赋能教学:路径与启示——基于 LDA 主题建模和内容分析的文本挖掘[J].现代教育技术,2025,35(06):14-23.

- [4] 郑庆华.人工智能赋能 STEM 教育创新发展: 认识与实践[J].中国高教研究,2025,(01):1-7.
- [5] 王志君,管武,罗汉青,等.AI 赋能微处理器设计课程改革与实践[J].计算机教育,2025,(06):152-157.
- [6] 胡小勇,张雅慧,李艺凡,等.科学教育的政策研究: 国际动向与本土启示[J].中国电化教育,2025, (02):42-50.
- [7] 贾隆嘉.智能技术赋能教育评价改革: 实际需求、现实挑战与实践路向[J].中国现代教育装备,2025, (15) :152-154.
- [8] 李雪,范青刚,王忠,等.AI 赋能的程序设计类课程项目化教学模式探索[J].计算机教育,2025,(05):33-38.
- [9] 王晓燕,黄岚,王岩,等.人工智能赋能大数据实验课程改革与实践[J].计算机教育,2025,(07):91-97.
- [10] 雷晓锋,董景凡,盛昱豪,等.面向大学生思政教育的生成式人工智能使用情况调查研究[J].计算机技术与教育学报,2024,12(03):11-16.
- [11] 邓攀.人工智能课程中数学基础的教学体系探讨[J].计算机技术与教育学报, 2024,12(04):26-33.