

工程教育认证背景下AI赋能信息安全专业人才培养模式的创新与实践探索研究

丁海洋, 陈帅龙

北京印刷学院信息工程学院, 北京

收稿日期: 2026年9月6日; 录用日期: 2026年10月7日; 发布日期: 2026年10月14日

摘要

信息安全专业已完成课程资料和在线课程方面建设, 但与信息安全专业工程认证的培养目标仍有一定差距, 为提升人才培养质量, 本文在工程认证背景下针对AI赋能信息安全专业人才培养模式的创新与实践探索研究。使用已有在线学习数据训练生成学生学业分层模型, 对每个学生通过实时在线数据实现分类预测, 通过学习路径自动生成算法对每个学生实现个性化指导。本算法在专业课程中, 积极采用AI技术, 实现学生为中心、产出为导向、持续改进的OBE理念, 不断提升学生培养效果。实验验证, 本算法能实现学生学业分层模型训练, 对个体数据完成分类预测, 并根据学生情况完成个性化指导。

关键词

AI赋能, 人才培养模式, 学生学业分层模型, 分层预测

Innovation and Practice Exploration in AI-Enabled Talent Cultivation Models for Information Security under the Framework of Engineering Education Accreditation

Haiyang Ding, Shuailong Chen

College of Information Engineering, Beijing Institute of Graphic Communication, Beijing

Received: September 6, 2026; accepted: October 7, 2026; published: October 14, 2026

Abstract

Although the information security has completed the construction of course materials and online

文章引用: 丁海洋, 陈帅龙. 工程教育认证背景下 AI 赋能信息安全专业人才培养模式的创新与实践探索研究[J]. 教育进展, 2026, 16(10): 345-356. DOI: 10.12677/ae.2026.16102117

courses, a gap still remains between its current status and the cultivation objectives stipulated by engineering education accreditation. To enhance the quality of talent cultivation, this study proposes an innovative AI-empowered talent cultivation model for the information security program under the framework of engineering accreditation. Specifically, a student academic stratification model is trained using existing online learning data to perform real-time classification of each student based on their online learning records; a learning-path automatic generation algorithm is then employed to provide personalized guidance for individual students. By integrating AI technologies into specialized courses, the proposed model implements the student-centered, outcome-oriented, and continuous-improvement principles of Outcome-Based Education (OBE), thereby steadily improving the effectiveness of talent cultivation. Experimental results demonstrate that the proposed algorithm successfully accomplishes stratification model training, achieves accurate classification prediction on individual student data, and delivers personalized guidance tailored to each student's specific situation.

Keywords

AI-Empowered, Talent Cultivation Model, Student Academic Stratification Model, Stratification Prediction

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

网络空间安全已成为关乎百姓生命财产安全, 关系国家安全和社会稳定的重大战略问题[1]。2015年6月, 国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科, 并明确指出需加强“网络空间安全”的学科建设, 做好人才培养工作。

据《2024年网络安全产业人才发展报告》显示, 截至2024年6月, 我国已有626所高校开设网络空间安全专业¹。尽管开设网络空间安全的高校数量逐年攀升, 我国网络空间安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题, 与维护国家网络安全、建设网络强国的要求不相适应。信息安全本科专业承担着为国家网络空间安全培养人才的根本任务。

人工智能(Artificial Intelligence, 简称 AI)是新一次科技革命的主要推动力量。人工智能时代人才培养的挑战: 当代大学生普遍思想、视野较为开阔、人格独立和自我意识强、崇尚个性化, 但是深度思维缺失、过于自我中心化, 所以造成教师主导性弱化。人工智能带给高校思想政治教育的机遇: 自由支配时间的增多, 在线教学明显拓展教育空间; 网络环境便于实现对待每一位学生实现个性化教育[2]。

工程教育认证核心理念包括: 学生中心理念、产出导向理念(成果导向)、持续改进理念。工程教育认证背景下, 多个学校在计算机类专业中积极开展人才培养模式的改革和探索[3][4], 虽然取得一定成果, 但是没有结合学生的学情分析帮助改善人才培养模式, 文献[5]提出利用学情分析探索课堂教学质量改革的探索, 但并没有有效地利用 AI 技术赋能人才培养模式的创新与实践。

信息安全专业在人才培养方面取得一定建设成果, 但与信息安全专业工程认证的培养目标仍有一定差距, 为提升人才培养质量, 本文在工程认证背景下针对 AI 赋能信息安全专业人才培养模式的创新与实践探索研究。

¹<https://www.nisp.org.cn/NewsDetail/5175378.html>

2. 信息安全专业人才培养现有基础

为落实信息安全专业学生的能力培养, 信息安全专业已完成两方面建设:

(1) 建成多门课程的教学资料, 包括: 教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库;

(2) 各门课程已形成有效的在线课程资源, 在印苑 E 课堂上发布。

信息安全专业主要课程及其各类课程资料见表 1:

Table 1. Main courses and course materials of information security

表 1. 信息安全专业主要课程与课程资料表

序号	课程名称	学时	主讲教师	课程资料
1	数字图像处理	48	丁海洋	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
2	信息隐藏与数字水印	64	丁海洋	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
3	现代密码学	64	教师 1	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
4	程序设计基础	64	教师 2	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
5	网络舆情分析	48	教师 3	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
6	信息系统安全	32	教师 4	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
7	网络安全技术	64	教师 5	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库
8	数字逻辑	64	教师 6	教学大纲、教学日历、教案、教学 PPT、实验指导书、作业库、试题库

根据线上线下混合教学的需要, 信息安全专业各门主要课程已建成有效在线课程资源, 在北京印刷学院印苑 E 课堂上发布, 各门主要课程的在线课程网址见表 2:

Table 2. Online course URLs of main courses in information security

表 2. 信息安全专业主要课程在线课程网址

序号	课程名称	学时	主讲教师	在线课程网址
1	数字图像处理	48	丁海洋	https://mooc1.chaoxing.com/course/236314397.html
2	信息隐藏与数字水印	64	丁海洋	https://mooc1.chaoxing.com/course/232633770.html
3	现代密码学	64	教师 1	https://mooc1.chaoxing.com/course/232709136.html
4	程序设计基础	64	教师 2	https://mooc1.chaoxing.com/course/236276274.html
5	网络舆情分析	48	教师 3	https://mooc1.chaoxing.com/course/232828781.html
6	信息系统安全	32	教师 4	https://mooc1.chaoxing.com/course/232776880.html
7	网络安全技术	64	教师 5	https://mooc1.chaoxing.com/course/232735086.html
8	数字逻辑	64	教师 6	https://mooc1.chaoxing.com/course/236387113.html

所以, 信息安全专业主要课程的课程资料与在线课程建设情况见图 1:

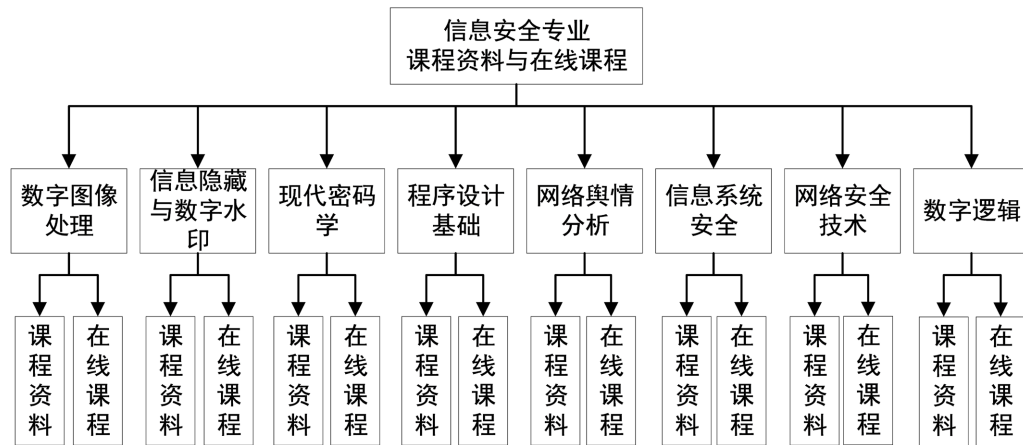


Figure 1. Course materials and online courses of information security

图 1. 信息安全专业课程资料与在线课程

虽然信息安全专业已完成课程资料和在线课程方面的建设, 但是信息安全专业目前开设的多门课程未能有效结合当前 AI 技术实现工程认证 OBE 理念, 与信息安全专业培养目标仍有一定差距, 在各部门专业课程中, 未能充分体现学生为中心、产出为导向、持续改进的 OBE 理念。

本文根据《工程教育认证标准(2024 版)》², 在工程认证背景下, 采用 AI 赋能信息安全专业人才培养模式的创新与实践探索研究, 在专业课程中, 积极采用 AI 技术, 实现学生为中心、产出为导向、持续改进的 OBE 理念, 不断提升学生培养效果。

3. 算法描述

本文在工程认证背景下针对 AI 赋能信息安全专业人才培养模式的创新与实践探索研究。算法流程见图 2, 主要流程包括:

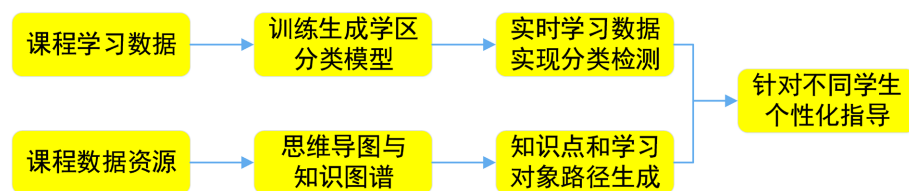


Figure 2. AI empowers the OBE algorithm in information security professional courses

图 2. AI 赋能信息安全专业课程 OBE 理念算法

(1) 使用已有在线学习数据训练生成学生学业分层模型。在线平台记录比较详细的学生用户行为轨迹, 采集各门课程已有在线学习数据, 对学情数据进行聚类, 对聚类后的在线学习数据, 输入到卷积神经网络进行训练, 得到训练后的模型文件, 用于后续实时学情数据的分类预测。

(2) 对每个学生通过实时在线数据实现分类预测。在教学管理过程中, 将实时在线学习数据输入自适应图卷积神经网络, 实现节点的分类, 实现学生学业分层的分类预测, 对分类到重点关注学区的学生(即

²<https://meca.cmes.org/article?id=273>

表现落后或状态不稳定的学生)及时进行干预。

(3) 通过学习路径自动生成算法对每个学生实现个性化指导。采用信息安全专业主要课程的数据资源构建思维导图和知识图谱, 以知识图谱为基础研究知识点路径生成与学习对象路径生成算法: 根据不同学生情况和学习对象, 自动生成学习对象路径, 以满足学生个性化需求, 极大地提升学生的学习兴趣 and 效率。

下面选择《信息隐藏与数字水印》课程为例, 说明研究与实现流程。

3.1. 使用已有在线学习数据训练生成学生学业分层模型

采集近 5 年信息安全专业学生的在线学习数据, 采用下面的规则构建数据集, 并且进行学业分层划分:

- ① 选择《信息隐藏与数字水印》为主要课程提取在线学习数据。
- ② 每名学生针对每门课程采集的课程学习数据, 包括: 出勤统计、课堂练习完成情况、课后作业成绩、实验完成情况、考试成绩。
- ③ 补充每名学生的课程设计成绩。
- ④ 对学情数据进行聚类, 并且适当调整, 聚类为以下学业分层:
优秀分层: 学习成绩好, 动手能力强;
良好分层 1: 学习成绩好, 动手能力偏弱;
良好分层 2: 学习成绩偏弱, 动手能力强;
中等分层: 学习成绩一般, 动手能力一般;
重点关注分层: 学习成绩落后, 动手能力落后。
- ⑤ 将上述分类后的在线学习数据, 输入到神经网络进行训练, 得到训练后的模型文件, 用于后续研究。

3.2. 对每个学生通过实时在线数据实现分类预测

在教学管理过程中, 希望根据学生在线学习统计, 及时预测学生的分类, 并对重点关注学生进行干预:

- ① 在学期初或学期中, 对《信息隐藏与数字水印》课程, 提取新的学习数据;
- ② 将在线学习数据输入神经网络, 实现学生学区分层的分类预测;
- ③ 对分类到重点关注分层的学生(即表现落后或状态不稳定的学生)及时进行指导。

3.3. 通过学习路径自动生成算法对每个学生实现个性化指导

为实现重点学生的有效指导, 采用信息安全专业主要课程的数据资源构建思维导图和知识图谱, 以知识图谱为基础, 研究知识点路径生成与学习对象路径生成算法:

- ① 根据《信息隐藏与数字水印》课程的数据资料, 选取 8 个教学单元的教学资料, 构建思维导图见图 3;
- ② 结合课程中主要知识点构建课程的知识图谱, 见图 4;
- ③ 继续完善《信息隐藏与数字水印》的知识图谱, 以知识图谱为基础, 研究知识点路径生成与学习对象路径生成算法;
- ④ 根据不同学生情况和学习对象, 自动生成学习对象路径, 以满足学生个性化需求, 极大地提升学生的学习兴趣 and 效率。

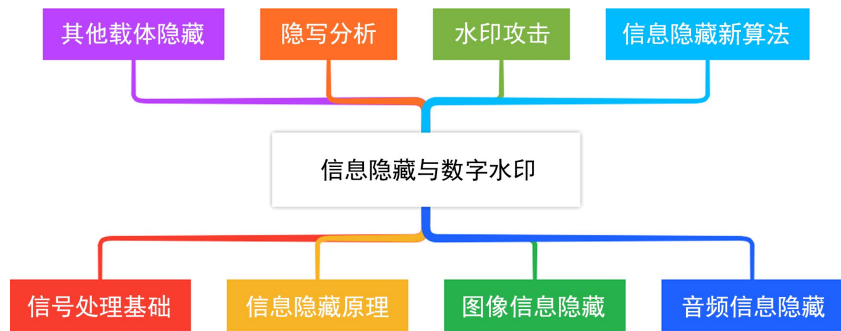


Figure 3. Mind map of the course “Information Hiding and Digital Watermarking”
图 3. 《信息隐藏与数字水印》课程的思维导图

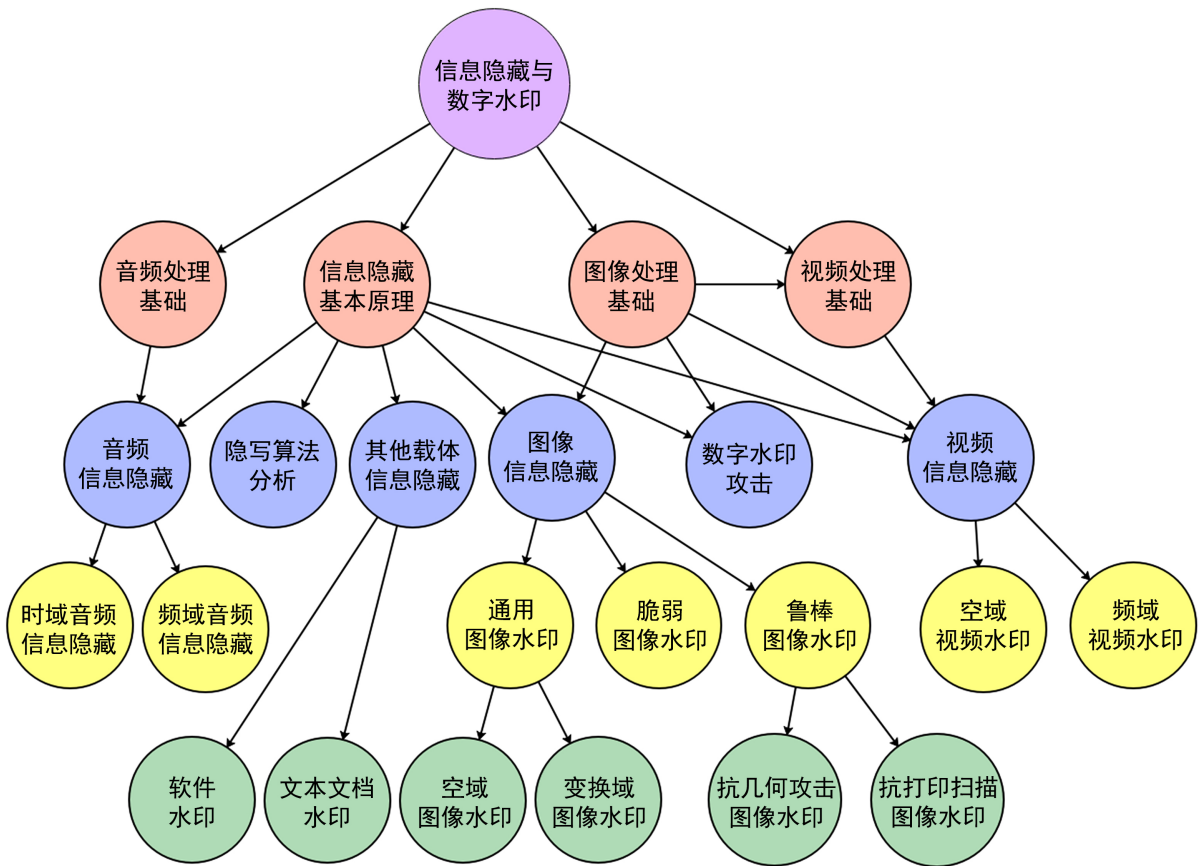


Figure 4. Knowledge graph of the course “Information Hiding and Digital Watermarking”
图 4. 《信息隐藏与数字水印》课程的知识图谱

4. 实验设计与结果分析

4.1. 实验条件与实验数据集说明

为验证本文提出的基于过程性评价学业预警方法在教学实践中的有效性,选取某高校本科生课程 5 个教学班为实验对象,采集了 127 名学生授课学期的完整课程学习数据。数据主要包括两类过程性评价指标:一是课后作业成绩,共 10 次,每次按 5 分制评分,反映学生理论学习能力的动态变化;二是实验完成情况,共 8 次,每次按 5 分制评分,反映学生动手实践能力的发展轨迹。

本实验的技术路线遵循“数据采集→学业分层→中途预测→精准干预”的闭环流程。为满足学期中途预警的实际需求,实验模拟了不同教学进度下数据完整度不同的情形:随着作业次数与实验次数的逐步增加,可用的过程性数据逐步丰富,模型据此不断更新对学生期末成绩的预测,从而为教师提供随时推进、动态调整的学业预警。

4.2. 学业分层分类训练

4.2.1. 学业分层划分标准

教学改革的核心在于因材施教,而因材施教的前提是对学生群体的科学分层。本文依据学生期末综合成绩,将学生划分为三类具有明确教学含义的学区,如表 3 所示:

Table 3. Classification criteria for three types of academic stratification
表 3. 三类学业分层划分标准

学区	综合成绩范围	教学含义	教学定位
优秀分层	85 分及以上	学业表现优异	拔尖培养
中等分层	60~85 分	学业水平中等,有提升空间	稳步提升
重点关注分层	60 分以下	存在不及格风险,需重点帮扶	重点帮扶对象

4.2.2. 分类模型的构建

学生学业分层模型的训练采用“回归预测 + 分数线映射”的方式:首先训练一个回归模型,利用学生的作业成绩与实验成绩预测其期末综合成绩,随后依据表 3 的分数线将预测成绩映射至对应的分层。这一方式相较于直接多分类具有两方面的优势:其一,回归模型保留了 5 分制评分的完整信息粒度,避免了强制离散化造成的信息损失;其二,模型不仅输出分层标签,还能输出具体的预测分数,使教师能够了解学生距离分层边界的真实距离,从而实施更具针对性的指导。

为使模型能够在“数据尚不完整”的真实教学情境下完成预测,训练过程模拟了作业与实验进度独立滑动的各种情形——即学生在不同作业完成次数(1~10 次)与不同实验完成次数(1~8 次)的各种组合状态下,模型均需能够依据当前可见的部分成绩预测其期末综合成绩。这一训练方式赋予了模型处理学期中途任意数据完整度的能力。

4.3. 学业分层预测

4.3.1. 预测精度

在全部过程性数据(10 次作业与 8 次实验)均可获得的情况下,模型对期末综合成绩的预测平均误差为 8.24 分,拟合优度 R^2 为 0.445,三类分层的分类准确率达到 71.2%。这意味着基于过程性评价数据,能够对学生的期末学业表现进行较为可靠的预估,为教学干预提供客观依据。

4.3.2. 作业与实验成绩的独立贡献

图 5 以热力图的形式展示了作业完成次数与实验完成次数各自独立变化时,预测误差的变化规律。图中可以直观地看到两个重要特征:

- (1) 随着作业与实验完成次数的增加,预测误差整体呈下降趋势,即两个维度的过程性数据均对预测精度做出贡献。当仅完成 1 次作业与 1 次实验时,预测误差约 10.3 分;而当作业与实验全部完成后,误差降至约 7.8 分。

(2) 作业成绩对预测精度的贡献略高于实验成绩。沿作业维度(固定实验次数、增加作业次数), 预测误差约下降 2 分; 沿实验维度(固定作业次数、增加实验次数), 预测误差约下降 1 至 1.5 分。这一差异源于作业次数(10 次)多于实验次数(8 次), 且作业成绩能够更频繁、更及时地反映学生日常的学习状态。

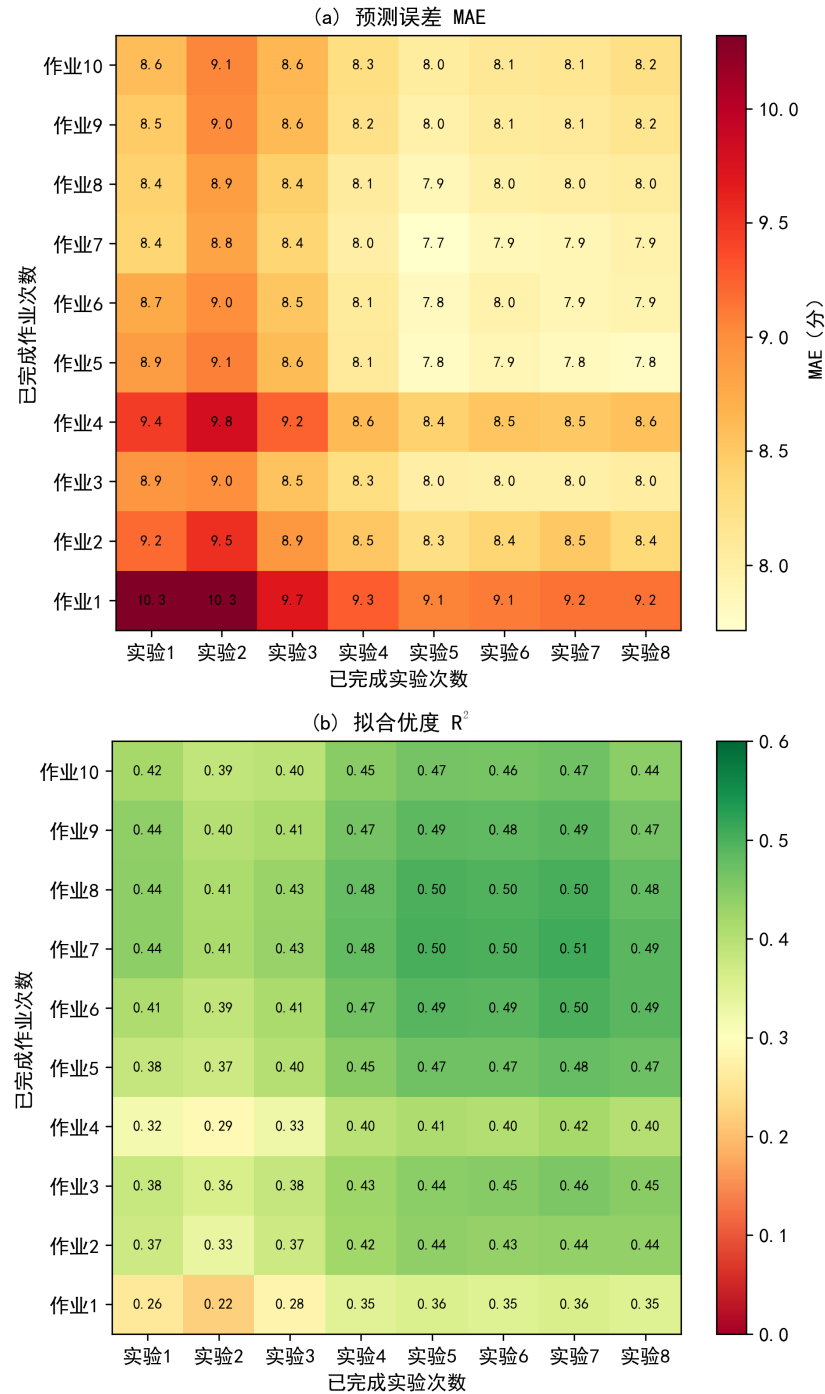


Figure 5. Influence of independently varying homework and laboratory completion progress on prediction accuracy. (a) The prediction error (MAE, in points); (b) the goodness of fit (R^2)

图 5. 作业与实验进度独立滑动对预测精度的影响。(a) 预测误差(MAE, 单位: 分), (b) 拟合优度(R^2)

4.3.3. 预测的收敛过程

图6展示了预测值随过程性数据积累逐步逼近真实成绩的收敛过程。左图固定实验已全部完成、观察作业次数增加时预测值的变化；右图固定作业已全部完成、观察实验次数增加时预测值的变化。可以清楚地看到，随着数据的逐步积累，预测值逐渐向真实成绩(虚线)靠拢，体现了“过程性数据越充分、预测越准确”的基本规律。

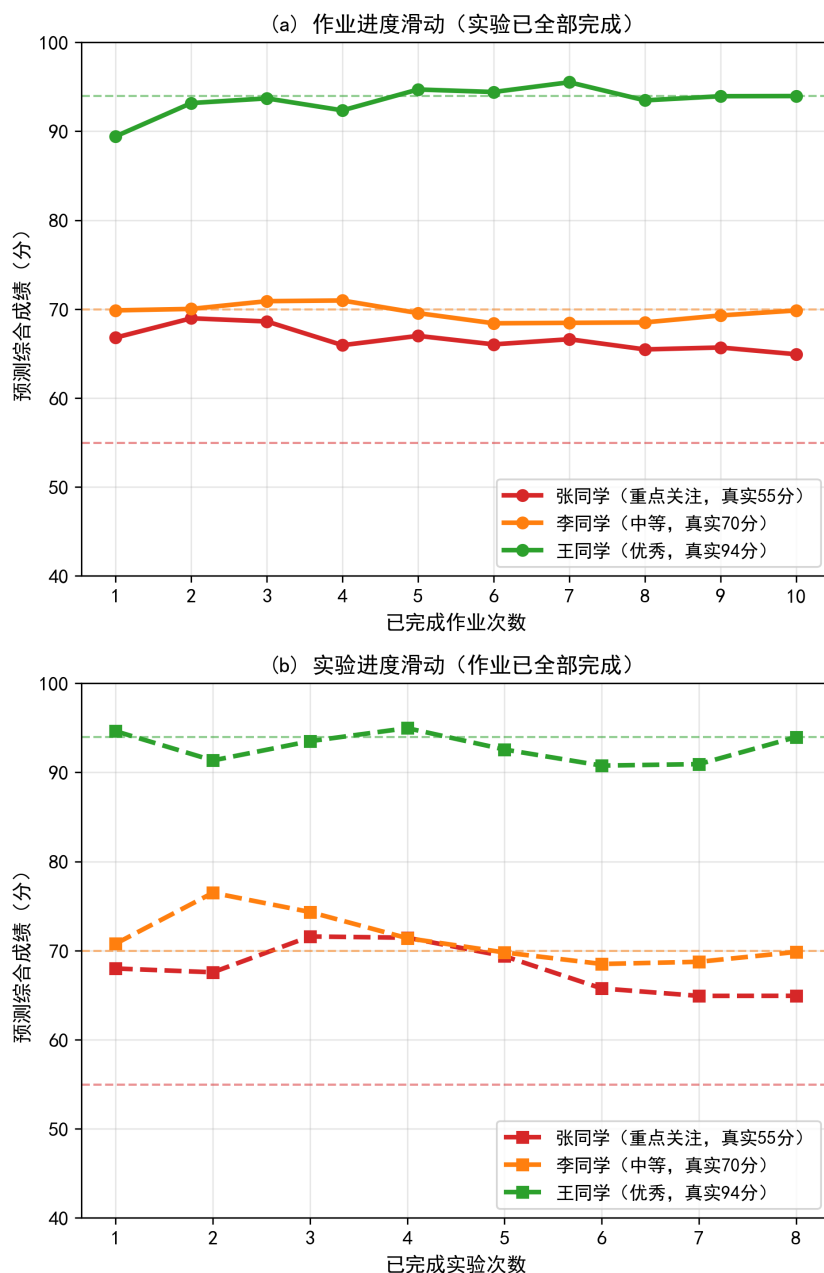


Figure 6. Convergence of predicted scores as process-based data accumulate. Panel (a) varies the homework progress (with all laboratory reports completed); panel (b) varies the laboratory progress (with all homework assignments completed). The dashed lines denote the actual comprehensive scores

图6. 预测值随过程性数据积累的收敛过程。(a) 作业进度滑动(实验已全部完成); (b) 实验进度滑动(作业已全部完成)。虚线为真实综合成绩

图 7 从整体层面进一步对比了不同进度下的预测准确度。左图为学期早期(仅完成 3 次作业与 2 次实验)的预测散点分布, 右图为学期末(完成全部 10 次作业与 8 次实验)的预测散点分布。从早期到完整, 预测误差从 10.3 分降至 7.9 分, R^2 从 0.46 提升至 0.65, 散点分布明显向对角线(完美预测线)收拢, 直观地体现了预测精度的整体提升。

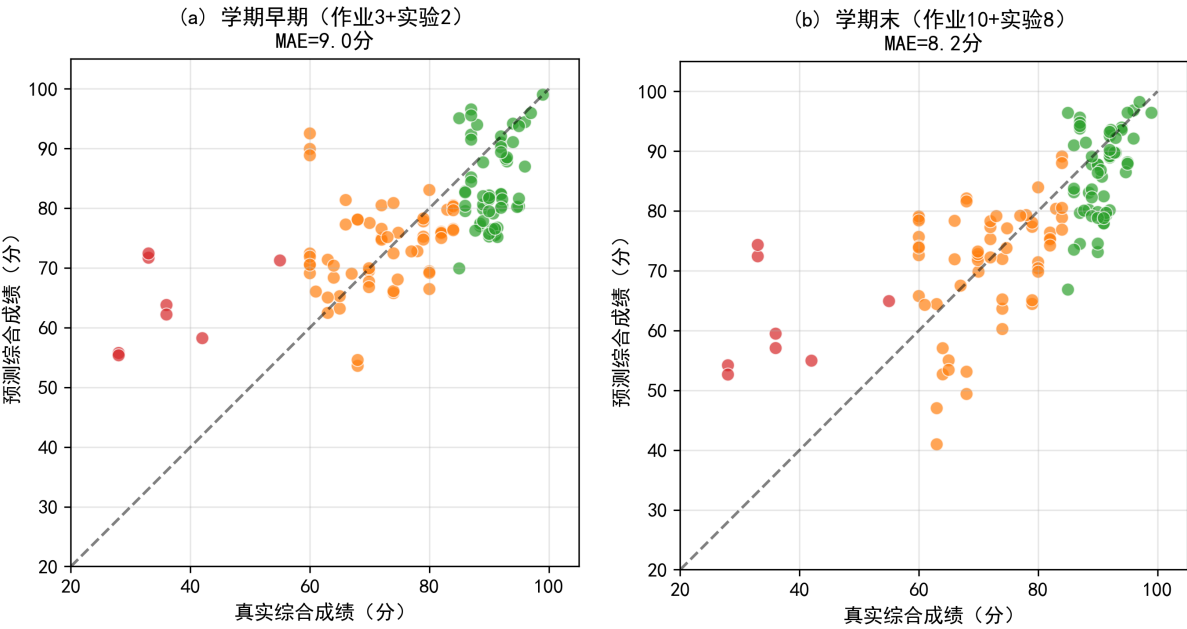


Figure 7. Scatter comparison between predicted and actual scores. (a) shows the early semester (homework 3 + laboratory 2); (b) shows the end of the semester (homework 10 + laboratory 8)

图 7. 预测值与真实值散点对比。(a) 学期早期(作业 3 + 实验 2); (b) 学期末(作业 10 + 实验 8)

4.4. 个性化指导

4.4.1. 分层导向的差异化教学策略

学业分层分类的最终落脚点是为学生不同提供差异化的教学支持。针对三类分层学生的不同特点, 本文设计了对应的个性化指导方案, 如表 4 所示。方案遵循“因材施教”原则, 对重点关注学区实施高强度的一对一帮扶, 对中等学区注重过程督促与巩固提升, 对优秀学区则提供进阶挑战。

Table 4. Differentiated teaching strategies for each layer

表 4. 各分层差异化教学策略

学区	个性化指导策略	干预强度
重点关注分层	每周一对一辅导不少于 2 次、布置基础强化练习、家校联合制定帮扶计划、优先安排实验补做	高
中等分层	小组互助学习、定期检查作业完成质量、提供课后答疑辅导	中
优秀分层	保持当前学习状态、推荐进阶课程或科研项目、选拔担任学习小组组长	低

4.4.2. 预警精度与干预时机的匹配

预警系统的价值在于“不漏报任何需要帮扶的学生”。本实验中, 重点关注学区的查全率达到 43.3%, 即系统能够在全部真实需要帮扶的学生中识别出近四成。结合图 6、图 7 揭示的收敛规律, 个性化指导的

启动时机可以进一步精细化：在学期早期(如完成 3 次作业后)，系统即可依据部分过程性数据对重点关注学生做出初步筛查，此时启动一对一帮扶能够覆盖最早暴露学业风险的学生群体；随着作业与实验的陆续提交，教师可根据系统更新的预测结果动态调整帮扶名单。

在实际教学中，教师收到重点关注分层学生名单后，可依据表 2 的策略开展针对性帮扶；系统每周依据新增的过程性数据更新一次预测，教师据此动态调整帮扶对象，实现了“数据驱动、动态调整”的精准教学闭环。

4.5. 实验数据统计与分析

表 5 汇总了本实验的核心量化指标。

Table 5. Summary of key experimental metrics
表 5. 核心实验指标汇总

评价维度	指标	数值	教学含义
预测精度	平均预测误差(MAE)	8.24 分	预测偏差约 8 分，可用于粗粒度预警
拟合优度	R^2	0.445	过程性数据可解释约 45%的期末成绩变化
分类准确率	三类分层准确率	71.2%	约七成学生被正确归类
预警能力	重点关注查全率	43.3%	可识别约四成需帮扶学生
早期预测	作业 3 + 实验 2 时 MAE	10.3 分	学期早期即可启动预警
收敛效果	完整数据时 MAE	7.9 分	数据越充分、预测越准确

综合上述数据，本文方法在学业预警改革中展现出以下三方面的优点：

- (1) 预警时效的前移。传统教学评价往往需等到期中、期末才能获得可靠的学业反馈，而本文方法在学期早期(完成 3 次作业后)即可依据过程性数据启动预警，将干预时机前移数周，实现了从“事后补救”到“早期预防”的转变。
- (2) 评价维度的多元。本文方法充分利用了作业成绩与实验成绩两个维度的过程性数据，并通过实验证实了两者对预测期末成绩的独立贡献。这种“理论学习 + 动手实践”的二维评价模式，相较于传统的“唯分数论”，能够更全面地刻画学生的学业状态，为差异化教学提供依据。
- (3) 干预策略的可落地。学业分层分类与对应的个性化指导方案直接对接，教师依据系统输出的学区标签和预测分数，即可实施有针对性的帮扶，无需额外的技术门槛。这种“数据驱动、直接可用”的特性，为过程性评价支撑精准教学改革提供了可复制、可推广的实践范式。

4.6. 基线模型对比

为验证本文方法相较其他模型的性能优势，在相同数据集与相同划分下，将本文方法与随机森林、LightGBM 两种代表性机器学习模型进行了对比，结果如表 6 所示。

对比结果表明：在预测误差(MAE)上，三个模型差异很小(8.13~8.66 分)，本文采用的模型在拟合优度($R^2 = 0.463$)上优于随机森林(0.292)和 LightGBM (0.387)。实验结果表明，在 127 名学生的中小规模数据上，本文的算法足以反映过程性成绩与期末成绩之间的关系，复杂模型并未带来额外的预测增益，反而因参数过多而存在过拟合风险。因此，本文模型，既保证预测精度，又具备模型简单、计算高效、系数可解释等优势，便于在教学实践中推广应用。

Table 6. Model performance comparison
表 6. 模型性能对比

模型	MAE (分)	R ²	查全率(<60 分)	查全率(<70 分)
本文方法	8.22	0.463	0.333	0.525
随机森林	8.66	0.292	0.367	0.483
LightGBM	8.13	0.387	0.333	0.361

4.7. 算法实施效果对比

本算法应用于某高校《信息隐藏与数字水印》课程 2023 级学生教学过程中, 2023 级学生的平均成绩得到明显提升, 2023 级本课程平均成绩达到 76.3, 而未实施本算法的 2022 级学生本课程平均成绩为 70.6, 可见本算法通过学生的分类与个性化指导, 有效提升学生学习效果。

5. 结论

为提升信息安全专业人才培养质量, 本文在工程认证背景下针对 AI 赋能信息安全专业人才培养模式的创新与实践探索研究。使用已有在线学习数据训练生成学生学业分层模型, 对每个学生通过实时在线数据实现分类预测, 通过学习路径自动生成算法对每个学生实现个性化指导。实验验证, 本算法能实现学业分层模型训练, 对个体数据完成分层预测, 并根据学生情况完成个性化指导。

本算法中在预测的准确率方面仍然有一定提升空间, 可以通过丰富实验数据和改进实验模型来进一步提升。

基金项目

北京市高等教育学会项目(MS2023204); 2026 年北京印刷学院本科教学改革创新项目(工程认证背景下 AI 赋能信息安全专业人才培养模式的创新与实践探索研究)。

参考文献

[1] 冯登国. 准确把握网络空间安全技术发展的新特征全力助推国家安全体系和能力现代化[J]. 中国科学院院刊, 2022, 37(11): 1539-1542.

[2] 刘明龙. 人工智能背景下高校智慧思政建设研究[D]: [博士学位论文]. 西安: 陕西师范大学, 2021.

[3] 李海涛, 陈红梅. 工程教育专业认证背景下计算机专业人才培养模式探索——以商丘师范学院为例[J]. 商丘职业技术学院学报, 2026, 25(3): 63-66.

[4] 王崇霞, 赵晓丽. 工程教育认证背景下网络工程专业教学改革与实施[J]. 现代职业教育, 2026(9): 121-124.

[5] 王怡丹. 高校智慧教室环境下的学情分析系统设计研究[D]: [硕士学位论文]. 西安: 西北大学, 2020.