人工智能赋能的实验教学体系建设与实验案例设计*

张焘[1]** 唐湘云[2] 林怡静[3] 康嘉文[4] 孙庚[5]

1. 北京交通大学网络空间安全学院，北京 100044
2. 中央民族大学信息工程学院，北京 100081
3. 北京邮电大学信息与通信工程学院，北京 100876
4. 广东工业大学自动化学院，广州 510006
5. 吉林大学计算机科学与技术学院，长春 130012

摘 要 随着人工智能技术的快速发展，高校中的计算机课程亟需改革以适应新技术的发展。本文以云计算与大数据安全课程为例，探讨了人工智能技术与课程实验教学体系的深度融合。针对传统教学中实验内容与行业需求脱节、与AI技术融合不足等问题，本文构建了一个AI赋能的实验教学体系。该体系通过将机器学习等AI知识融入实验模块、构建支持GPU和机器学习框架的智能化实验环境，并采用“AI+教师”双导师制与“翻转课堂+项目驱动”的新型教学模式进行了改革。在此基础上，本文进行了实验案例研究，并通过问卷调查结果的方式调查了改革成效。结果显示，超过80%的学生认为该教学体系在培养专业技能和创新能力方面很有帮助。实践证明，该模式能显著提升学生的实践能力和创新意识，为人工智能时代培养高素质专业人才提供了有效途径。

关键字 云计算，人工智能，实验教学体系建设，实验设计

Building an AI-Empowered Experimental Teaching System and Designing Experimental Cases

Tao Zhang[1]** Xiangyun Tang[2] Yijing Lin[3] Jiawen Kang[4] Geng Sun[5]

1. School of Cyberspace Science and Technology, Beijing Jiaotong University, Beijing 100044, China
2. School of Information Engineering, Minzu University of China, Beijing 100081, China
3. School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
4. School of Automation, Guangdong University of Technology, Guangzhou 510006, China
5. College of Computer Science and Technology, Jilin University, Changchun 130012, China

Abstract—With the rapid development of artificial intelligence, computer curricula in higher education require timely reform to keep pace with emerging technologies. Using the Cloud Computing and Big Data Security course as a case, this study examines the deep integration of AI technologies into the experimental teaching system. Addressing issues such as the misalignment between traditional laboratory content and industry needs, as well as insufficient AI integration, we design an AI-enhanced instructional framework. The framework embeds machine-learning concepts into laboratory modules, provides an intelligent GPU-supported environment for ML frameworks, and implements a dual-mentorship model (“AI + instructor”) together with a “flipped classroom + project-driven” pedagogy. Experimental case studies and questionnaire data were used to evaluate the reform outcomes. Results indicate that over 80% of students perceived significant improvements in their professional skills and innovation capacity. The findings demonstrate that this model effectively strengthens students’ practical competence and creativity, offering a viable pathway for cultivating high-quality professionals in the AI era.

Keywords—Cloud Computing, Artificial Intelligence,Experimental Teaching System Development,Experimental Design

1 引 言

在数字化转型加速推进的人工智能时代背景下，教育领域正经历从“数字化”到“智能化”的跃迁。自《新一代人工智能发展规划》发布以来[1]，国家积极推进人工智能与教育的深度融合，旨在打造智能教育生态，提升人才培养质量。尤其是在云计算与大数

*基金资助：北京交通大学人才基金项目（2023XKRC050），国家自然科学基金青年基金（62402029），国家密码基金面上项目（2025NCSF02030），中国博士后科学基金特别资助（2024T170047），中国博士后科学基金面上项目（2024M750165），北京市自然科学基金丰台联合基金（L251041）

**通讯作者：张焘 taozh@bjtu.edu.cn

据安全等前沿交叉课程中，该类课程具有高度综合性、技术更新快、实操要求高的特点，对实验教学体系提出了更高要求，传统实验教学手段已难以适应技术发展与产业需求的变化[2]。而以机器学习、深度学习为代表的人工智能技术则为实验教学体系的建设提供了全新的解决方案，为教育模式创新和人才培养模式的变革带来了新的机遇和动力。

2 课程内容与特点

云计算是一种计算模型，通过虚拟化技术将海量计算资源进行整合，为各种终端用户和应用系统提供计算、存储和信息服务，并且具备自我管理计算资源的能力。云计算与大数据安全课程主要聚焦云计算环境与大数据隐私保护技术，主要教学内容有：

（1）云计算篇：云计算的一般性概念、原理和相关机制，包括云计算定义与特征、产生与发展、体系架构、云计算数据中心、虚拟化与容器技术、云存储、云计算系统、云计算安全、云计算节能技术；

（2）大数据篇：大数据的相关概念、关键技术和典型应用，包括大数据基本概念、生命周期、数据思维与大数据价值、大数据采集、大数据处理、大数据应用、大数据隐私保护；

（3）平台篇：云计算与大数据的相关平台，包括商用云计算平台、云操作系统 OpenStack、云仿真平台 CloudSim、分布式大数据处理平台 Hadoop、分布式内存计算平台 Spark 等的来源背景、版本演变、体系架构、核心组件以及安装与部署流程。

云计算与大数据安全课程体系庞杂，具有显著的跨学科融合、实践性强、内容抽象且更新迭代快的特点。当前，云计算技术正呈现蓬勃发展的态势，我国高等教育领域积极响应这一趋势，众多高等院校为适应产业对专业技术人才的需求，纷纷将云计算课程纳入教学体系。部分走在前列的高校院系已经根据自身实际情况开展了形式多样的教学创新实践，并在不断的探索与实践中发现问题，解决问题。

3 当前教学体系现状

针对现有云计算与大数据安全课程的培养目标和教学大纲，许多高校提出了具有针对性的教学改革与探索方案。武汉大学计算机学院针对云计算平台与技术课程实施中存在的问题，提出相应的改革思路和探索实践[3]，在课程建设过程中，坚持课程核心内容不变的原则，并采取比较灵活的策略与行业内头部企业合作，充实实验案例和实验资源。重庆工商大学人工智能学院通过提供线上课程资源，采用互动教学以及设置新的课程体系去解决《云计算》课程教学中存在的不足之处[4]。福州大学数据科学与大数据技术专业结合自身实际情况[5]，从合理构建师资队伍、建立专业实践教学平台、引入优质课程体系和科学合理的人才培养方案等方面进行分析和探讨，研究新工科背景下具有特色的数据科学与大数据技术专业建设方案。华南理工大学基于产业实际需求重构云计算课程体系，采用模块化教学设计，并创新性地运用沙箱技术平台实施实验教学实践[6]。天津大学结合云计算课程的特点，将“产学合作”作为云计算教学的破局之路，建成了云计算课程的“原理-应用-实验”课程体系[7]。中国石油大学计算机科学与技术学院以“亚马逊 AWS-中国石油大学云创学院”为合作基础开展云计算技术与应用课程建设[8]，在新工科与新基建背景下，探索了一条云计算人才培养的产学研合作之道。长江大学提出了基于实例项目驱动的教学内容设计方案，通过引入丰富的项目案例并利用基于互联网的在线实践平台，从课堂教学有效过渡到双创项目的设计与实现，从而优化大数据与云计算技术课程的教学效果[9]。

尽管上述高校的教学改革实践在课程教学优化方面取得了一定成效，但在当前人工智能技术迅猛发展的新形势下，其教学体系仍存在一些问题：

（1）目前国内高校开设的云计算课程多以理论课程为主，这些内容涉及的知识抽象庞杂且枯燥乏味，课程内容往往停留在对云计算基础概念的简单复述和传统大数据安全原理的机械讲解上，教学方式以填鸭式的知识灌输为主，缺乏生动形象的案例解析和互动讨论，这种枯燥乏味的教学方式导致课堂气氛沉闷，学生参与度低。

（2）在实践教学环节，问题同样突出。多数院校的实验设置过于简单化、程序化，往往只停留在"照着实验说明手册点鼠标"的层面。并且高校中的实验任务内容也多年未更新[10]，还在使用早已过时的技术方案，与行业实际需求严重脱节。这种低层次的实验设计完全无法模拟真实业务场景中的复杂安全挑战，对于培养学生的实际问题解决能力的作用更是微乎其微。

（3）在人工智能技术迅猛发展的时代背景下，云计算与大数据安全课程与 AI 技术的融合程度明显不足。当前的课程体系架构仍延续着传统的知识分类框架，对机器学习、深度学习等前沿人工智能技术内容鲜有涉及，并且将云计算、大数据与人工智能视为平行发展的技术领域，而未能建立起有机融合的知识体系。这种割裂的课程设计导致学生难以形成对智能云计算安全生态的整体认知。

这些问题制约了人才培养的质量和效果，特别是在人工智能技术快速迭代的背景下，课程内容与 AI 技术的融合严重不足，导致学生难以构建系统性知识框架，无法有效掌握 AI 前沿技术的发展趋势。更无法满足人工智能时代对于高素质综合型人才的要求。

4 实验教学体系建设

针对上述存在的问题，本文主要从如图 1 所示的几个方面来构建 AI 赋能的实验教学体系：

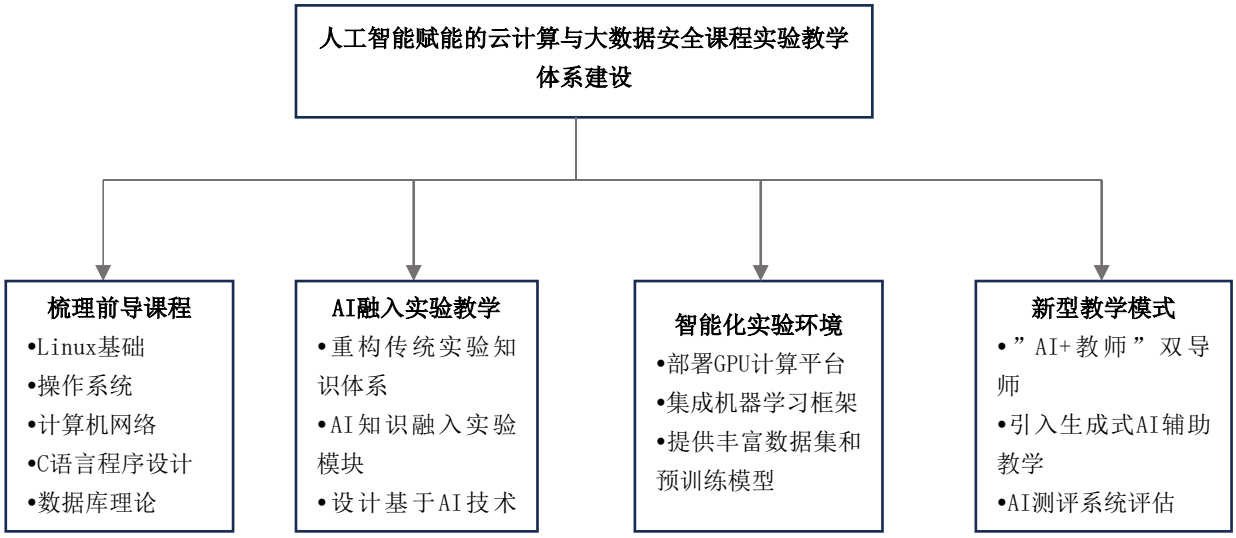

图 1 实验教学体系框架

（1）梳理相关前导课程。首先，云计算平台搭建与运维涉及操作系统尤其是 Linux 操作系统知识，重点包括用户权限管理、文件系统安全配置、进程调度机制以及 Shell 脚本编程等核心内容。其次是涉及网络通信原理的计算机网络技术，学生需要掌握 TCP/IP 协议栈、网络安全协议（SSL/TLS）以及防火墙配置等网络基础知识。云计算系统的开发与优化需要扎实的 C 语言编程能力，这部分基础技术包括内存管理机制、多线程编程技术、网络套接字编程以及系统级 API 调用等核心内容。此外，数据库原理与数据管理技术也是重要的前置知识，特别是关系型数据库安全机制和 NoSQL 数据库的访问控制等内容。因此，云计算与大数据安全的前导课程应包括 Linux 基础、操作系统原理、计算机网络、C 语言程序设计以及数据库理论等。

（2）将 AI 技术深度嵌入实验教学环节。重构传统的实验知识体系，将机器学习算法、深度学习模型等 AI 核心技术与云计算安全、大数据隐私保护等专业内容有机融合。具体而言，在异常流量检测、入侵行为分析、数据脱敏处理等实验模块中，设计基于 AI 技术的解决方案，使学生掌握如何运用智能算法解决实际安全问题。建立系统化的教学实施路径实现算法原理与工程实践的平衡，既要让学生理解模型背后的数学原理，又要培养其调参优化、结果分析的实践能力。

（3）构建支持 AI 技术应用的智能化实验环境。包括部署具备 GPU 加速能力的计算平台、集成主流的机器学习框架和工具链、提供丰富的安全数据集和预训练模型，支持从基础算法到复杂系统的多层次实验需求。此外，实验平台还应具备实验过程记录、结果可视化、智能反馈等功能，通过 AI 驱动的分析系统，学生可以即时获得实验结果的深度解析和改进建议，为教学提供数据支撑。

（4）发展适应 AI 技术特点的新型教学模式。采用"AI+教师"双导师制教学机制，利用智能教学系统实现个性化学习[11]路径推荐，基于学生的学习行为数据动态调整实验难度和内容。引入生成式 AI 辅助教学，通过大语言模型构建虚拟实验助手，为学生提供 7×24 小时的智能答疑和代码调试支持。在教学过程中，采用"翻转课堂[12]+项目驱动"的混合式教学方法，课前通过微课视频讲解核心概念，课中聚焦实际项目开发，课后利用 AI 测评系统进行学习效果评估。同时，建立多元化的考核评价体系，不仅考察实验结果的技术指标，更注重评估学生在问题分析、算法选择、模型优化等环节的创新思维和工程能力。

5 实验案例设计

5.1 基于机器学习的云计算环境异常流量检测

（1）实验目标

本实验旨在通过机器学习技术实现云计算环境下的异常流量检测，帮助学生了解云计算平台环境下常见的安全威胁与异常流量。首先，学生需要掌握 OpenStack 等主流云计算平台的搭建与基础运维技能，包括虚拟机的创建、网络配置等核心操作。其次，实验重点培养学生对云环境网络流量的采集与分析能力，要求熟练使用 Wireshark、tcpdump 等工具捕获流量数据，并能对原始数据进行预处理和特征提取。在机器学习应用方面，学生将通过实践完整掌握从数据标注、特征工程到模型训练与评估的全流程，最终具

备在小规模云环境中部署异常检测模型的工程实践能力。通过本实验，学生不仅能够理解异常流量检测的技术原理，更能培养解决实际安全问题的综合能力。

（2）实验理论讲解

本实验的理论基础涵盖云计算平台架构、网络流量分析技术和机器学习算法三个关键领域。云计算平台部分重点介绍 OpenStack 的核心组件及其网络架构，帮助学生理解云环境下的流量传输特点。网络流量分析技术主要讲解 TCP/IP 协议栈的组成、常见网络攻击特征以及流量采集工具的使用原理。在机器学习方面，系统讲解机器学习在异常检测中的应用，包括特征工程的方法、随机森林等分类算法的原理，以及准确率、召回率、F1 值等评估指标的计算方式和实际意义。

（3）实验内容与步骤

本实验采用教师指定技术路线的指导性实验模式。具体课时安排和各环节考核标准可参见表 1 和表 2。

① 搭建实验环境

学生在本地计算机上安装并配置好 Ubuntu Server 操作系统（使用虚拟机 VMware），确保能够联网访问。随后，在 Ubuntu 环境中部署 DevStack 来搭建一个小型的 OpenStack 测试环境。若设备资源有限，也可以连接教师事先部署好的共享 OpenStack 实验环境。此外，需要在系统中安装 Python3 及其常用库（包括 numpy、pandas、scikit-learn、matplotlib），并安装网络流量采集分析工具，Wireshark 和 tcpdump，对实验过程中生成的网络流量进行采集和分析。

② 数据采集

在环境搭建完成后，学生在 OpenStack 云主机内使用 tcpdump 或 Wireshark 工具实时抓取正常网络行为产生的流量数据，并保存为 pcap 文件。为了模拟异常攻击流量，学生使用 hping3 工具模拟 DoS 攻击发起简单的攻击行为，再次采集对应的异常流量数据。同样将异常流量保存为单独的 pcap 文件。最后，通过 tshark 工具将所有 pcap 数据转存为结构化的 CSV 文件，方便后续的数据处理和建模使用。

③ 数据预处理与特征提取

学生使用 Python 脚本对 CSV 格式的流量数据进行清洗与特征提取。首先筛选出有效的数据字段，包括源 IP、目的 IP、源端口、目的端口、协议类型、数据包大小、时间戳等。然后提取统计特征（包括数据包发送速率、连接持续时间等）。接着进行数据标注，数据标注是本步骤的关键：将正常流量标记为“0”，异常流量标记为“1”，以便进行有监督学习。在特征工程完成后，应用标准化处理对特征进行归一化。

④ 模型训练与测试

将数据集划分训练集与测试集、构建随机森林分类器，进行训练。训练完成后，使用测试集评估模型效果，输出混淆矩阵、准确率、召回率、F1 值等指标，绘制 ROC 曲线直观展示分类性能。

⑤ 实验报告撰写

将以上实验过程进行总结，撰写最终的实验报告。

（4）实验内容与步骤

表 1　实验 1 课时安排

实验内容	课时安排
环境准备与搭建	1课时
网络流量采集	3课时
数据处理与特征提取	3课时
模型构建与训练	3课时
模型部署与实时检测	3课时
实验总结与报告撰写	3课时
总计	**16课时**

（5）实验考核与评分

表 2　实验 1 考核要求

考核项	成绩占比
成功采集并标注数据	20%
成功完成模型训练与测试	30%
模型的准确率达到设定阈值	30%
实验报告内容完整，分析到位	20%

5.2　基于 GAN 的大数据脱敏与隐私保护

（1）实验目标

本实验旨在通过生成对抗网络（GAN）技术实现大数据环境下的隐私保护与数据脱敏，培养学生在大数据安全管理方面的实践能力。学生首先需要理解大数据隐私保护的基本概念和主要技术挑战，包括数据脱敏的必要性和常见实现方法。在此基础上，重点掌握生成对抗网络的核心原理及其在隐私保护领域的创新

应用方式，特别是如何通过 GAN 模型生成既保留原始数据统计特征又能有效保护隐私的合成数据。实验要求学生能够独立完成从环境搭建、模型构建到训练优化的完整流程，并掌握数据效用评估的关键指标和方法，包括统计特征保持度、机器学习任务性能等。

（2）实验理论讲解

本实验的理论基础涵盖大数据隐私保护与数据脱敏、生成对抗网络和隐私评估三个重要领域。大数据隐私保护部分系统介绍数据脱敏的技术原理和常见方法，包括泛化、扰动、合成等不同技术路线的优缺点比较。生成对抗网络方面详细讲解 GAN 的基本架构和工作原理，重点分析生成器和判别器的对抗训练过程，以及如何通过这种机制学习原始数据的潜在分布。在隐私评估环节，深入探讨数据效用和隐私保护这对矛盾指标的平衡问题，包括定量评估方法如统计距离计算、机器学习任务性能比较，以及定性评估方法如可视化分析和攻击模拟。

（3）实验内容与步骤

本实验采用开放式探究模式，鼓励学生自主选择技术方案，教师主要提供辅助性指导，不限定具体实现细节。具体课时安排和各环节考核标准可参见表 3 和表 4。

① 搭建基本的深度学习实验环境。

② 下载开源大数据样本集作为实验基础数据。

③ 构建并训练一个简单的 GAN 模型，基于原始数据生成隐私数据。

④ 对比原始数据和生成数据的统计特征，评估脱敏效果与数据效用。

⑤ 模拟简单的重识别攻击，评估隐私保护强度。

⑥ 撰写实验报告，分析 GAN 脱敏方法的优势与不足。

（4）实验内容与步骤

表 3 实验 2 课时安排

实验内容	课时安排
实验环境搭建与数据准备	2课时
构建生成对抗网络模型	4课时
生成隐私保护数据	4课时
隐私保护与数据效用评估	4课时
实验总结与报告撰写	2课时
总计	**16课时**

（5）实验考核与评分

表 4 实验 2 考核要求

考核项	成绩占比
成功搭建GAN并生成脱敏数据	30%
脱敏数据统计特性与原始数据对比分析合理	20%
隐私保护效果与数据效用评估完整，分析有逻辑	30%
实验报告规范，思考与总结到位	20%

6 教学改革成效

本文所提出的教学体系核心目的在于解决传统实验教学中内容陈旧、形式单一、与前沿 AI 技术脱节的问题。我们期望通过将 AI 技术深度融入实验设计、构建智能化实验环境、并采用“AI+教师”的新型教学模式，打破传统教学的局限性，最终目标是显著提升学生的工程实践能力、数据驱动的安全分析能力以及在 AI 时代的创新意识，培养能够解决复杂实际问题的高素质专业人才。

为精确评估这一教学改革体系的实际成效，教学团队在课程结束后对学生进行了匿名的问卷调查。该问卷旨在从学生的视角评估 AI 赋能教学体系关键组成部分的效果。问卷采用三级评定方式（“很有帮助”、“没有帮助”、“效果更差”），问卷内容如下：

（1）您认为将机器学习/深度学习技术（如实验 1 中的随机森林）融入云计算与大数据安全实验，对您理解和掌握复杂安全威胁（如异常流量检测）的帮助程度是？（A. 很有帮助； B. 没有帮助； C. 效果更差）

（2）智能化实验环境（包括 GPU 平台、预置的机器学习框架、AI 虚拟助手）对您在实验中分析和解决问题效率的提升是？（A. 很有帮助； B. 没有帮助； C. 效果更差）

（3）相较于传统的实验指导模式，“AI+教师”双导师制以及项目驱动的教学模式（如实验 2 中的开放式探究）对您自主探究能力和工程实践能力的提升是？（A. 很有帮助； B. 没有帮助； C. 效果更差）

（4）总体而言，本课程构建的“AI 赋能实验教学体系”在培养您的创新思维和解决实际安全问题能力方面，相比传统教学？（A. 很有帮助； B. 没有帮助； C. 效果更差）。

问卷调查的具体结果可见图 2。在本次教学改革课程班级的 26 名学生中，超过 80%的学生都对本课程的课堂学习效果产生了正面的评价。学生的反馈证实

了新的教学模式有效提升了他们的实践动手能力和数据驱动的安全分析能力，并通过开放式探究实验激发了自主创新思维。同时，智能化实验平台与 AI 助教显著提高了学习效率和课程参与度，表明该教学模式在培养学生专业技能和创新能力方面具有实质性的帮助。

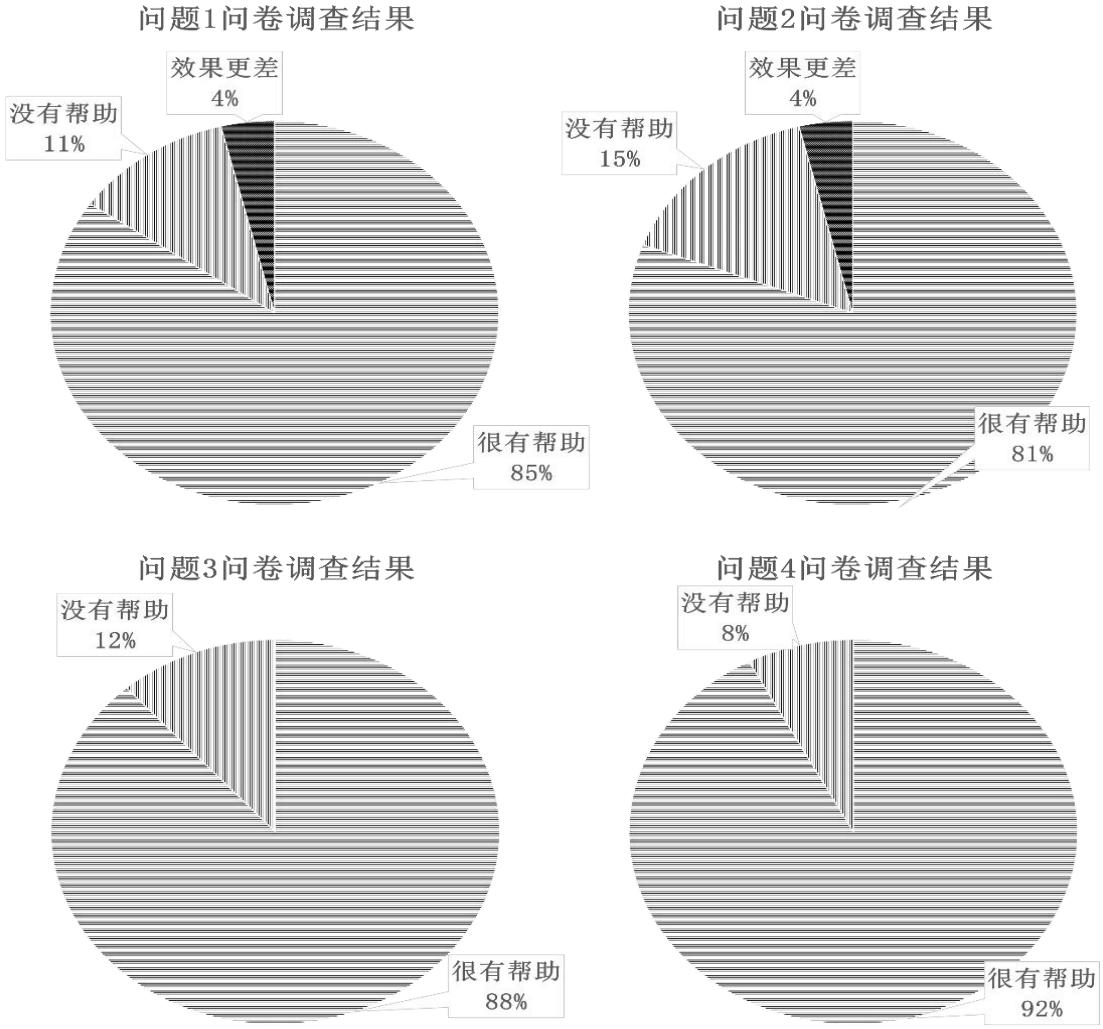

图 2 问卷调查结果

参 考 文 献

[1] 顾小清, 李世瑾, 李睿. 人工智能创新应用的国际视野——美国NSF人工智能研究所的前瞻进展与未来教育展望[J]. 中国远程教育, 2021, (12):1-9+76.

[2] 彭文娟,李清勇,周围,等. 高铁智能运维虚拟仿真实验设计与应用[J]. 计算机技术与教育学报, 2022, 10(5): 49-56.

[3] 刘浩文,李兵,桂浩,等. 云计算平台与技术课程改革探索与实践[J]. 软件导刊, 2023, 22(6): 20-24.

[4] 金鑫,刘波. 《云计算》课程的教学改革研究[J]. 创新教育研究, 2022, 10(12): 3016-3020

[5] 郭文忠,张浩,董晨. "新工科"背景下数据科学与大数据技术专业建设探索与实践——以福州大学为例[J]. 电脑知识与技术：学术版, 2020, 16(25):3.

[6] 邓芳,叶文,卢向群,等. 新工科背景下融合OBE 的《数据库系统原理》实验环节教学改革与实践[J]. 计算机技术与教育学报, 2021, 8(2): 54-58.

[7] 赵来平,黎杰,单小洋,等. 新工科背景下产学合作的云计算课程教学改革[J]. 高等工程教育研究, 2022, 70(6):111-115.

[8] 王勃,李华昱,董玉坤,等. 云计算课程教学模式探索与实践[J]. 高教学刊, 2021, 7(28): 122-125.

[9] 叶青,刘长华. 新工科背景下的《大数据与云计算技术》课程建设研究[J]. 湖北经济学院学报：人文社会科学版, 2020, 17(11):3.

[10] 刘凯,闫文君,凌青,等. 基于线下线上混合式信息技术课程综合实验设计[J]. 计算机技术与教育学报, 2023, 11(5): 69-73.

[11] 曾志宏. 基于云计算与大数据的高校个性化教学[J].长春大学学报, 2018, 28(2):102-105.

[12] 黄厚财,郑伟俊. 基于SPOC 的翻转课堂教学设计与实践[J], 计算机技术与教育学报, 2021, 9(2): 65-68