基于大模型的网络安全教学实验平台的构建*

谢海涛** 罗广昌 张吉昕 杜江毅

湖北工业大学计算机科学与人工智能学院，武汉 430068

摘 要 随着网络攻击技术的不断发展，网络安全教学需要更加贴近实战的教学环境。本文设计并实现了一个基于大模型的网络安全教学实验系统，通过自动化生成不同难度的正常与异常网络流量，结合大模型辅助分析和动态难度调整机制，构建了一个能提供实时反馈的流量判断答题环境。系统能够根据学员的实验表现（如准确率、完成率），通过内置的动态难度调整算法，实时适配实验内容的难度级别，从而为不同基础和能力水平的学习者提供个性化的学习路径和恰到好处的挑战。实验结果表明，该平台能有效模拟多样化的网络攻击场景，提供专业、及时的分析反馈，显著提升了网络安全教学的效果与效率，为创新网络安全实践教学模式提供了可行的技术方案。

关键字 网络安全教学，流量分析，异常检测， AI 大模型，自适应学习

Construction of Cybersecurity Teaching Experiment Platform Based on LLM*

Haitao Xie** Guangchang Luo Jixin Zhang Jiangyi Du

School of Computer Science and Artificial Intelligence
Hubei University of Technology
Wuhan 430068, China

Abstract—With the continuous advancement of cyberattack technologies, cybersecurity education requires teaching environments that closely resemble real-world scenarios. This study designs and implements a large model-based cybersecurity teaching experiment system. By automatically generating normal and abnormal network traffic of varying difficulty levels, combined with large model-assisted analysis and dynamic difficulty adjustment mechanisms, the system creates a real-time feedback-driven traffic analysis environment. Through built-in dynamic difficulty adjustment algorithms based on learners' performance metrics (e.g., accuracy rate and completion rate), the system dynamically adapts challenge levels to provide personalized learning paths and appropriate challenges for learners at different proficiency levels. Experimental results demonstrate that the platform effectively simulates diverse cyberattack scenarios, delivers professional analytical feedback, significantly enhances teaching effectiveness, and offers a viable technical solution for innovative cybersecurity practice education models.

Keywords—Cybersecurity Education, Traffic Analysis, Anomaly Detection, Large AI Models, Adaptive Learning

1 引 言

1.1 研究背景与意义

数字化时代的到来使得网络安全已成为国家安全、经济运行和社会稳定的基石。高级持续性威胁（APT）、勒索软件、大规模分布式拒绝服务（DDoS）攻击等复杂网络威胁层出不穷[1]，对关键信息基础设施和个人数据安全构成了严峻挑战。为了应对这些威胁，关键在于培养具备扎实理论功底和出色实战能力的网络安全专业人才。

当前的网络安全教育领域面临着“纸上谈兵”的困境。传统教学模式多以理论讲授和静态案例分析为主，学生很难获得处置真实网络攻击的体验[2]。尽管近年来虚拟化技术（如 VMware， VirtualBox）和专用网络实验平台的发展使得搭建模拟环境成为可能[4]，但它们在用于教学时仍存在诸多局限性：

(1)场景真实性不足：预置的攻击脚本和流量样本往往单一、固化，缺乏现实网络中流量行为的随机性和复杂性，难以模拟高级攻击手法[3]。

(2)缺乏智能导学能力：实验难度或主题通常是静态预设的，无法根据学生的实时表现进行动态调整，可能导致初学者挫败感强或高水平学生觉得挑战不足。

(3)评估与反馈滞后：实验结果的评估多依赖于教师事后手动批改，缺乏及时、自动化的专业反馈，学生学习闭环无法及时形成。

(4)教学评估分离：实验过程与知识传授、技能评

* **基金资助**：本文得到湖北工业大学教学研究项目（2025XZ12）、湖北省新工科实践教学建设项目（XGK03064）资助。

** 通讯作者：谢海涛 19991035@hbut.edu.cn 。

估环节相互孤立，未能形成一个有机的整体，不利于学习路线的构建[4]。

因此，构建一个能够自动生成高仿真网络流量、集成智能化分析引擎、并提供个性化自适应学习路径的网络安全教学实验平台，对于破解当前教学困境、提升人才培养质量具有极其重要的理论价值和现实意义。

1.2 本文主要工作及贡献

针对上述问题，本文设计实现了基于大语言模型的网络安全教学（流量判断答题）实验系统。本文的主要工作有：

（1）设计了多层次、可配置的网络流量生成算法：通过精细建模不同难度的正常用户行为和多种网络攻击（如端口扫描、多种洪水攻击、HTTP 攻击等），生成贴近实战的混合流量数据包，为实验提供高质量的数据基础。

（2）构建了集成特征提取与智能分析的评估框架：CICFlowMeter[6]特征提取工具，将原始流量数据转化为包含 80 多个维度的结构化特征向量；并创新性地引入 DeepSeek 大型语言模型，对特征进行深度推理与判定，模拟网络安全专家进行分析决策的过程。

（3）实现了一种基于表现的自适应难度调整机制[7-8]：根据学员答题的正确率（RR）和完成率（CR）动态加权计算能力得分，并据此自动调节后续实验任务的难度级别（简单、中等、困难），帮助用户实现个性化学习。

（4）形成了“实验-评估-反馈”的完整教学闭环[9]：平台提供了从流量生成、特征提取、智能问答、结果评判到难度调整的全流程自动化功能，为学生提供了即时、专业、结构化的反馈，极大地提升了学习效率和沉浸感。

（5）进行了充分的实验验证与案例分析：通过让实验者（本文作者）亲身完成不同难度的实验任务，收集了翔实的性能数据，并对典型判断案例进行了深入剖析，验证了系统的有效性，同时也指出了当前局限性和未来优化方向。

2 教学能力框架设计

2.1 四维能力培养框架内涵

构建"基础认知-技能实践-综合应用-创新研究"四维递进式能力培养框架[10-11]：

(1) 基础认知层：掌握网络安全基础理论、协议原理、攻击类型定义等知识

(2) 技能实践层：熟练使用流量分析工具、掌握常见攻击检测方法、具备基础异常判断能力

(3) 综合应用层：能够在复杂流量环境中识别混合攻击、结合多维度特征进行综合研判

(4) 创新研究层：探索新型攻击检测方法、优化分析算法、提出防御策略创新思路

2.2 能力指标分级体系

表 1 四维能力培养指标分级表

能力维度	初级（L1）	中级（L2）	高级（L3）
知识掌握	了解常见 5 种攻击类型原理	掌握 10 种以上攻击特征与检测方法	熟悉各类高级持续性威胁技术细节
实践技能	能准确识别简单单一攻击	能在混合流量中检测常见攻击	能识别隐蔽性强的高级攻击手法
分析能力	能基于单一特征作出判断	能综合多维度特征进行分析	能结合上下文推理复杂攻击链
创新能力	能复现已知攻击检测方法	能优化现有检测规则	能提出新型攻击检测思路

3 系统架构设计

3.1 总体架构

平台采用前后端分离+微服务架构设计，分为五层，如图 1 所示.

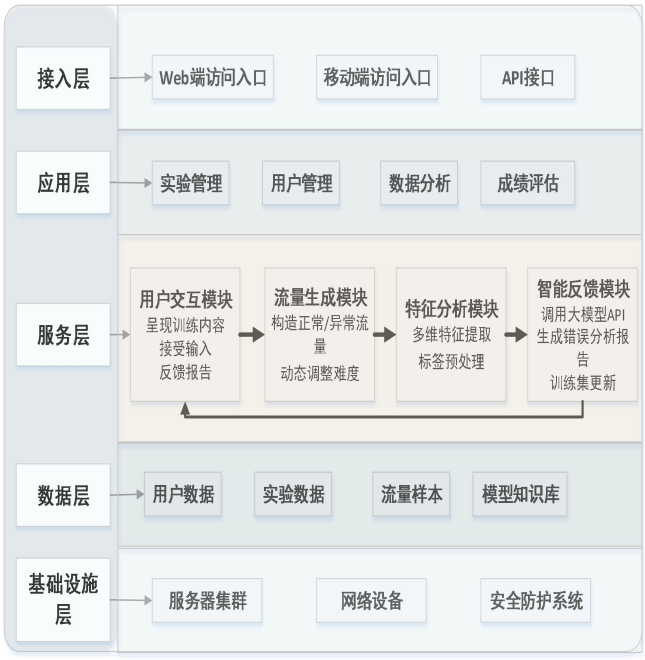

图 1 平台总体架构图

(1) 接入层：提供 Web 端、客户端、API 三种访问方式，支持多终端适配。

(2) 应用层：包含实验管理、用户管理、数据分析、反馈评价四大业务模块。

(3) 服务层：提供流量生成、特征提取、大模型分析、难度调整四大核心服务。

(4) 数据层：存储用户数据、实验数据、流量样本、模型知识库四类数据资源。

(5) 基础设施层：支持本地服务器、云平台、边缘节点多环境部署。

系统核心服务层包含：用户交互模块、流量生成模块、特征分析模块和智能反馈模块，通过串联各个模块形成完整闭环，提供了及时的训练反馈并提供更个性化的训练内容。

3.2 核心模块设计

（1）流量生成模块

主要实现三种难度级别的流量生成（初始化默认中等难度），包括异常流量和正常流量两种生成器：

① 异常流量生成器：

- 攻击类型多样性：简单难度仅包含最常见的扫描和洪水攻击，困难难度则扩展到包括应用层慢速攻击在内的多种复杂攻击（共 7 种）。

- 攻击强度与隐蔽性：包发送间隔从简单的 0.01s 缩短到 0.0001s，模拟高速洪水攻击。源 IP 地址的范围从私有地址段 192.168.0.0/16 扩展到庞大的公网地址段 1.0.0.0/8，并引入随机目标 IP，增加了攻击检测的难度。

- 攻击混合策略：每种难度下，不同攻击类型的出现概率经过精心设计。例如，在中等难度下，SYN Flood 这种更常见的攻击权重设置为 0.4 高于 DNS 放大攻击 0.1。

表 2 展示了具体难度下的各种攻击流量分布情况，攻击类型随难度递增，权重配置符合实际情况。

② 正常流量生成器：

生成背景流量旨在模拟真实网络中的合法用户行为，使异常流量隐藏其中，更贴近实战场景。其难度体现在(见表 2)。

- 协议复杂性：从简单的Web和DNS流量（easy）扩展到包含SSH、FTP等更多协议（hard）。

- 行为真实性：在困难模式下，使用更真实的端口号范围（49152-65535）、模拟完整的TCP三次握手过程、并构建简单的HTTP请求载荷，而非仅仅生成孤立的SYN包。

表 2 攻击类型分布

难度	攻击类型
easy	port_scan:0.5,syn_flood:0.5
medium	port_scan:0.3,udp_flood:0.4,syn_flood:0.2,dns_amplification:0.1
hard	port_scan:0.2,udp_flood:0.2,syn_flood:0.1,icmp_flood:0.1,dns_amplification:0.2,http_attack:0.1,slowloris:0.1

生成逻辑与异常流量类似，但侧重于建立完整的协议交互。例如，生成 HTTP 流量时，会依次构造 SYN、SYN-ACK、ACK 握手包，紧接着构造携带 HTTP GET 请求的 PSH+ACK 包。具体分布情况如表 3 所示。

表 3 协议类型分布

难度	协议类型
easy	http:0.5,dns:0.3,https:0.2
medium	http:0.4,dns:0.3,https:0.3
hard	http:0.3,dns:0.2,https:0.3,ssh:0.1,ftp:0.1

（2）特征分析模块

集成CICFlowMeter进行流量特征提取生成包含80余个特征的CSV文件。关键信息如表4所示.

表 4 关键特征提取

关键特征	特征列名
时间特征	Flow Duration
包数量	Total Fwd Packets,Total Bwd Packets
标志位	SYN Flag Count,ACK Flag Count,FIN Flag Count, RST Flag Count,PSH Flag Count,URG Flag Count
包大小	Fwd Packet Length Mean,Bwd Packet Length Max
流量速率	Fwd Packets/Flow Duration

（3）智能评估模块

① 特征预处理与结构化：将CICFlowMeter输出的CSV文件的一行即一条流的特征转换成一个结构化的数据字典或一段描述性文本。这包括元数据（难度、分析时间）、基础流信息（五元组、持续时间）、包

统计（总包数、前向包数、后向包数）、流量大小（字节数）、标志位统计（TCP）、时间特征、吞吐量（秒）和行为指标等。同时，会计算一些衍生指标，如特征完整性评分、标志位异常分数、突发性指数等，为模型提供更多推理线索。

② 提示词工程：这是成功调用大模型的关键。首先规定分析维度：明确要求模型从连接行为、流量模式、时间特征、包特征、吞吐量和行为模式六个专业维度进行思考。其次严格约束输出格式：要求模型必须输出格式良好的XML片段并对每个字段的内容和长度做了严格限制。这种结构化输出极大地方便了后续程序化解析与展示。

③ API调用与响应解析：将组合好的提示词（系统指令+结构化特征数据）通过DeepSeek API发送给大模型。收到模型的文本响应后，使用XML解析器提取出各个字段的内容，并封装成一个完整的反馈对象，最终呈现给用户。

4 关键技术实现

4.1 多难度流量生成算法

表 5 难度参数对比

参数	简单难度	中等难度	困难难度
攻击类型	2 种	4 种	7 种
包间隔	0.01s	0.001s	0.0001s
源 IP 范围	192.168.0.0/16	172.16.0.0/12	1.0.0.0/8
目标 IP	固定	固定	随机
攻击比例	固定	固定	动态调整

实现三种难度级别的流量生成，关键参数对比如表 5 所示。

4.2 动态难度调整机制

依据用户得分划分难度（默认中等难度，50 以下调整为简单，80 以上调整为困难）

简化的导师模型 simplified_tutor_model(基于正确率 RR 和完成率 CR 的难度调整算法,权重可根据需要调整)[8]。构造核心函数 adjust_difficulty(rr,cr)，其接收两个参数：rr 正确率和 cr 完成率，根据手动分配权重计算加权得分（满分 100），动态难度调整算法伪代码如下：

```
    def adjust_difficulty(current_level, rr, cr, history_scores)
    参数说明:current_level: 当前难度级别 (1=简单, 2=中等, 3=困难); rr: 本轮正确率 (0-1); cr: 本轮完成率 (0-1); history_scores: 最近5轮得分历史
    返回: 调整后的难度级别
    #计算当前加权得分,正确率权重0.6,完成率权重0.4
    current_score = 0.6 * rr * 100 + 0.4 * cr * 100
    # 计算历史平滑得分，最近轮次权重更高
    weights = [0.1, 0.15, 0.2, 0.25, 0.3]
    if len(history_scores) < 5:
    padded = [current_score] * (5 - len(history_scores)) + history_scores
    smoothed_score = sum(w * s for w, s in zip(weights, padded))
    else:
    smoothed_score = sum(w * s for w, s in zip(weights, history_scores[-5:]))
    # 难度调整规则
    if smoothed_score >= 80 and current_level < 3:
    new_level = current_level + 1
    elif smoothed_score <= 50and current_level > 1:
    new_level = current_level - 1
    else:
    new_level = current_level
    # 更新历史得分
    history_scores.append(current_score)
    if len(history_scores) > 10:
    history_scores.pop(0)
    return new_level, history_scores
```

4.3 大模型辅助分析

选取CICFlowMeter生成的CSV文件中关键特征进行预处理，形成的关键指标具体如表 6 所示。

提示词构造：

请从以下维度进行专业威胁评估：

① 连接行为分析（端口扫描、异常握手模式、连接状态异常）

② 流量模式识别（DDoS洪水、UDP洪水、ICMP洪水、DNS放大攻击）

③ 时间特征分析（慢速攻击、脉冲攻击、定时洪水）

④ 数据包特征检测（畸形包、碎片化攻击、协议违规）

⑤ 吞吐量异常（带宽滥用、资源耗尽攻击）

⑥ 行为模式匹配（僵尸网络、C2通信、数据渗出）

请严格按以下XML格式响应：

```
<verdict>malicious/normal/suspicious</verdict>
<confidence>0.0-1.0</confidence>
<evidence>具体攻击类型和技术说明（不超过40字）</evidence>
<technique>MITRE ATT&CK技术编号（如T1048、T1498等）</technique>
<rationale>简要分析理由，突出关键异常特征（不超过60字）</rationale>
<severity>low/medium/high/critical</severity>
"""
```

增设衍生指标计算函数如下：

特征完整性评估：_calculate_feature_completeness()用于计算关键特征完整性评分

标志位异常检测：_calculate_flag_anomaly_score()用于SYN扫描、异常重置检测

时间异常识别：_detect_timing_anomalies()用于极短连接、慢速攻击检测

流量突发性分析：_calculate_burstiness()用于流量突发模式识别

协议类型划分：_get_protocol_specific_insights()用于协议类型关联分析

表 6 结构化预处理特征

预处理特征	关键特征名
元数据信息	difficulty_level,analysis_timestamp,feature_completeness
基础信息	protocol,src_ip,src_port,dst_ip,dst_port,flow_duration_seconds,connection_state
包统计信息	total_packets,forward_packets,backward_packets,packet_ratio,packet_rate
流量大小分析	total_forward_bytes,total_backward_bytes,forward_avg_size,backward_max_size,size_ratio,packet_size_std
标志位分析	SYN_count,ACK_count,FIN_count,RST_count,PSH_count,URG_count,flag_anomaly_score
时间特征分析	flow_duration,forward_iat_total,backward_iat_total,iat_std,timing_anomaly_indicator
吞吐量指标	forward_bytes_per_second,backward_bytes_per_second,total_throughput
行为异常指标	avg_packet_size,small_packet_ratio,burstiness_index,protocol_specific_anomalies

5 实验设计与评估

5.1 实验环境

实验硬件配置:

CPU：AMD Ryzen 7 5800H with Radeon Graphics

内存（RAM）：16GB DDR4 3200MHz

GPU：NVIDIA GeForce RTX 3060 Laptop GPU

操作系统：Windows 11 专业版，版本号 23H2，操作系统版本 22631.5909

5.2 实验对象与内容

作者分别尝试 3 种难度的题组，总计 50*3=150 道题。

5.3 实验结果

不同难度下的表现如表 7 所示。

5.4 案例分析

示例流量基本信息：

连接: 8.8.8.8:53 → 192.168.234.242:43993
协议: UDP
时长: -100000.000000s
包数: 前向=1 后向=1
流量: 前向=0.1KB 后向=0.0KB
包大小: 前向平均=56.0字节 后向最大=29.0字节
判断：malicious
结果：错误 (实际: normal)
Deepseek api返回结果：
异常 DNS 响应，负持续时间和零吞吐量表明流量伪造或时间戳篡改

结论: SUSPICIOUS (置信度: 75%)
严重程度: MEDIUM
MITRE ATT&CK: T1048
分析理由: UDP 53 端口响应异常大小比 1.93，负流持续时间-100000 秒，零吞吐量，疑似伪造 DNS 流量

表 7 不同难度实验测试结果

难度级别	准确率	完成率	得分
简单	87.8%	98%	90.9
中等	79.5%	88%	82.0
困难	68.5%	70%	67.0

分析：

此案例凸显了数据生成和特征提取过程中的一个陷阱。极端异常的特征值（如巨大的负持续时间）在真实网络中几乎不存在，它通常源于流量生成器或抓包工具的时间戳设置错误。学员和模型都被这个极其明显的“异常”指标所误导。然而，模型给出了 suspicious 而非 malicious 的谨慎判断,并指出了“流量伪造”的可能性，这体现了其推理能力。这对教学而言是一个绝佳的案例，它教导学生：网络安全分析不能孤立地依赖一两个特征，必须综合考虑特征的合理性和现实性。需要检查数据来源的可靠性。

5.5 学员能力变化对比分析

（1）AI 认知/实践/创新思维前后测试数据

选取湖北工业大学计算机学院 2022 级信息安全专业 30 名本科生作为实验对象，进行为期 8 周的平台

教学实验，前后测试数据如表 8.

其中，认知思维测试：涵盖大模型原理、网络安全知识、攻击类型识别等客观题；实践操作测试：包含 10 道不同难度流量分析实操题，统计准确率与完成时间；创新思维测试：通过开放式问题考察新型攻击检测思路的创新性与可行性.

表 8 学员 AI 能力提升测试结果

测评维度	实验前平均得分	实验后平均得分	提升幅度	显著性 P 值
AI 认知思维	58.2±12.3	82.5±9.7	41.8%	<0.001
实践操作能力	47.6±15.2	78.3±11.4	64.5%	<0.001
创新思维能力	52.3±13.7	73.6±10.8	40.7%	<0.001
综合问题解决能力	49.8±14.5	76.4±12.1	53.4%	<0.001

（2）学员准确率/完成率前后对比实验数据

选取 30 名学员进行为期 8 周的对照实验，其中实验组 15 人使用本平台学习，对照组 15 人使用传统教学模式，前后测试结果如表 9 所示。

表 9 学员实验能力对比实验结果表

指标	实验组	对照组	提升差异
使用前			
准确率	52.3%	51.8%	无显著差异
完成率	63.5%	62.7%	无显著差异
完成时间	12.8 分钟/题	13.2 分钟/题	无显著差异
使用 8 周后			
准确率	79.4%	62.1%	高 17.3%
完成率	88.2%	70.5%	高 17.7%
完成时间	6.3 分钟/题	10.1 分钟/题	快 37.6%
提升幅度			
准确率提升	27.1%	10.3%	提升 2.6 倍
完成率提升	24.7%	7.8%	提升 3.2 倍
效率提升	50.8%	23.5%	提升 2.2 倍

通过测试结果说明，不同能力层级学员提升情况：

(1) 基础薄弱学员（初始准确率<40%）：平均准确率提升 35.2%

(2) 中等水平学员（初始准确率 40%-70%）：平均准确率提升 26.8%

(3) 高水平学员（初始准确率>70%）：平均准确率提升 18.5%

6 系统优化与改进

尽管当前平台实现了核心功能并取得了初步验证，但仍有多方面的优化和扩展空间。

(1) 流量生成细节：对各种数据包的构造进行除结构外的细节补充，如增加载荷；优化时间戳生成逻辑，避免乱序问题。

(2) 流量生成速度：采用 IP 池预生成，预先生成大量 IP 地址并存入内存池，避免在循环中频繁调用 generate_ip()函数带来的开销。

(3) 性能比较：传统方法的异常检测来源于专家学者的知识和经验以及威胁情报，基于预定义规则和签名，AI 大模型驱动的异常检测则通过深度学习、异常检测算法，基于大规模的训练数据并且可以自动迭代训练；可以通过图表等方式进行对比。

7 教学改革成果分析

基于大模型的网络安全教学实验分析系统，集成动态流量生成、精细化特征提取和大型语言模型分析等功能模块，有效地解决了传统网络安全教学中存在的场景真实性低、缺乏个性化指导、反馈滞后等痛点。本次教学改革在提升网络安全类课程实践方面取得如下进展性成果：

(1) 通过动态流量生成，构建了实战化的数据环境。设计的多难度流量生成算法能够模拟从基础扫描到复杂应用层攻击的多种威胁，为学生提供了贴近真实网络的高质量数据环境，培养学生在实际网络场景中分析和解决问题的能力。

(2) 通过动态难度调整机制，构建了个性化的学习路径。能够根据学生的实时表现自适应地调整实验难度，实现了因材施教，保证了学习过程的挑战性和可持续性。

(3) 通过基于大模型的智能评估分析，构建了智能化的专家辅导。学生在学习过程中遇到的问题，系统提供即时、专业、可解释的分析报告，极大地提升了教学效率和效果。

本次教学改革构建了从实验生成、主动学习、智能评估到自适应调整的完整教学闭环，有效解决了传统网络安全教学中"重理论轻实践、重知识轻能力"的痛点，实现了个性化、自适应的实践教学模式，相关教学模式已在湖北工业大学信息安全专业教学中得到

实践和应用，实验结果显示，本次教学改革在提升教学和人才培养质量方面效果明显。

8 结束语

综上所述，本次教学改革通过集成动态流量生成、精细化特征提取和大型语言模型分析，构建基于大语言模型的智能化网络安全教学实验系统，有效提升了网络安全类课程实践教学质量。动态流量生成，构建了实战化的数据环境，动态难度调整机制，构建了个性化的学习路径，基于大模型的智能评估分析，构建了智能化的专家辅导，形成了实验生成、主动学习、智能评估到自适应调整的完整教学闭环，未来，我们讲持续优化系统各模块功能，进一步提升实践教学效果，为信息安全专业人才培养提供有力支撑。

参 考 文 献

[1] 包象琳,徐晓峰,刘涛,章平. 新工科背景下信息安全课程教学创新实践[J]. 计算机技术与教育学报, 2025（13）:82-86.

[2] 宋超，张皓，陈旭羿，杨浩淼，梁伟波. 知识图谱增强网络与信息系统安全综合设计实验课程教学[J]. 计算机技术与教育学报，2026，14(1):49-54

[3] 朱辰，孙斌，金心宇，魏兵. 网络空间安全攻防实验教学与实训平台的构建[J]. 实验室研究与探索，2021，40（6）：265-267

[4] 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

[5] 许博，王秀磊，邢长友，张国敏. 基于NFV的网络空间安全专业课程实验考核方法改革[J]. 计算机技术与教育学报, 2025. 13(3）：58-61

[6] Basheer Husham Ali, Nasri Sulaiman, S.A.R. Al-Haddad, Rodziah Atan, Siti Lailatul Mohd Hassan:DDoS Detection Using Active and Idle Features of Revised CICFlowMeter and Statistical Approaches. 2022 4th International Conference on Advanced Science and Engineering (ICOASE). [Online]https://ieeexplore.ieee.org/xpl/conhome/10075549/proceeding

[7] Nataliia Barchenko,Andrii Tolbatov,Tetiana Lavryk,Volodymyr Tolbatov,Victor Obodiak,Valerii Yakovliev,Yurii Motorin &Yevhen Artamonov:An approach to the formation of adaptive learning paths for students of cybersecurity in e-learning system.2nd International Conference on Conflict Management in Global Information Networks.November 30,2022.

[8] Jan Vykopal,Pavel Seda,Valdemar Svábensky,and Pavel Cˇeleda:Smart Environment for Adaptive Learning of Cybersecurity Skills.IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES,VOL.16,NO.3,JUNE 2023.[Online].Available:https://ieeexplore.ieee.org/abstract/document/9926178

[9] 苏婷，蒋琳，汪花梅，杨扬. 基于“学练训赛”一体的网络安全人才培养探索与实践[J]. 计算机技术与教育学报，2025，13(4):107-111

[10] 昌燕,苟智坚,周益民,白杨,叶晓鸣. 网络空间安全领域高层次人才培养路径探讨[J]. 计算机技术与教育学报, 2025（13）:103-107

[11] 单棣斌,，王楠，李冰，祝宁. 人工智能赋能信息安全技术课程教学改革研究[J]. 计算机技术与教育学报，2025，13(5):99-104