网络安全虚拟云平台 HTTP 与 HTTPS 协议分析实验教学设计*

付小晶** 刘海波 李思照 刘泽超

哈尔滨工程大学计算机科学与技术学院，哈尔滨 150001

摘 要 距在产教融合背景下，本文以 HTTP 与 HTTPS 协议分析实验为例，设计了层次化、递进式的实验内容，满足信息安全专业个性化人才培养的迫切需求，依托网络安全虚拟云平台，并结合 BOPPPS 教学模型，构建了“双师协同”的实验教学模式，有效整合了校企双方的优质实验资源。设计了多平台、多维度的实验考核机制，实现了对学生实验成绩的校企联合评定及实践能力的综合评估。实践结果表明，该教学设计显著提升了学生在安全协议分析方面的专业技能以及网络安全实践与创新能力。

关键字 产教融合，网络安全实验，虚拟云平台，HTTPS 协议，Wireshark

Study and Analysis of Clustering Routing Protocol in Wireless Sensor Networks

fuxiaojing liuhaibo lisizhao liuzechao

College of Computer Science and Technology
Harbin Engineering University
Harbin 150001, China

Abstract—In the context of industry-education integration, this paper takes HTTP and HTTPS protocol analysis experiments as examples to design a hierarchical and progressive experimental framework. This approach addresses the growing demand for personalized talent development in information security education. Relying on the network security virtual cloud platform and combined with the BOPPPS teaching model, the experimental teaching mode of "dual-teacher collaboration" is constructed, which effectively integrates the high-quality experimental resources of both schools and enterprises. A multi-platform and multi-dimensional experimental assessment mechanism is designed to realize the joint evaluation of students' experimental achievements and the comprehensive evaluation of practical ability. Practical results show that the proposed teaching method significantly improves students' professional skills in security protocol analysis and network security practice and innovation ability

Keywords—Industry-education integration, network security experiment, virtual cloud platform, HTTPS protocol, Wireshark

1 引 言

我国网络空间安全正受到党和国家的高度重视，已上升到国家安全的战略高度[1]。实践能力是网络安全人才的核心竞争力。随着网络攻击手段不断翻新和技术快速迭代，对网络安全人才实践能力的培养提出了更高的要求。新形势下，信息安全专业人才应具备扎实的理工基础、较强的实践能力和创新能力。各高校积极探索产教融合背景下的网络安全课程教学改革[2,3]。企业技术专家与高校教师共同建设实验课程，能够将产业界的先进资源与宝贵实践经验融入课程改革和教学设计之中，从而有效增强学生的实践技能和未来就业的竞争力。运用云计算和虚拟化技术构建网络安全实验教学平台，不仅能显著降低教学成本、优化资源配置效率，还能突破时空限制，实现远程实验教学[4,5]。

《网络安全实验》是信息安全等专业必修的一门实验课。其传统教学模式常面临挑战：实验环境多为本地部署，所用软件与技术更新滞后，实验内容与业界实际有所脱节。部分网络安全实验因其可能对真实网络系统造成潜在风险，不宜直接在物理设备上开展。因此，教学往往以理论讲授为主，辅以少量课内验证性实验，导致实验平台匮乏、教学内容与形式较为单一等问题，难以满足应用型、创新型人才培养的时代需求[6]。针对这些问题，我院积极寻求与业界领先企业的合作，成功引入网络安全虚拟云平台，大力推进

* 基金资助：教育部产学合作协同育人项目（231007559075636），黑龙江省高等教育教学改革研究重点项目（SJGZB2024040），黑龙江省本科教育改革研究项目（SJGYB2024104）

** 通讯作者：付小晶 fuxiaojing@hrbeu.edu.cn。

网络安全实验课程的革新。借助教育部产学合作协同育人项目，校企双方共同研发了 30 余个高质量的实验项目，并编撰了配套实验教材，已交付清华大学出版社。这些实验项目广泛覆盖了网络监听、协议解析、网络扫描、渗透测试、防火墙配置、入侵检测等核心网络安全检测与防御技术，内容紧密追踪技术发展前沿，为学生构建了全方位的网络安全分析与防御实训体系。本文将以 HTTP 与 HTTPS 协议分析实验为例，详细阐述基于网络安全虚拟云平台的实验教学组织过程与成效考核方法。

2 网络安全虚拟云平台实验流程

网络安全虚拟云平台聚焦网络安全领域的热点问题与前沿技术，通过理论与实践的紧密结合，为用户提供了一套综合性的实训课程体系。该平台预装了主流且必需的软件及开发工具，充分满足网络安全实验课程的教学需求。学生仅需通过标准网页浏览器即可便捷接入平台，利用平台提供的视频、音频及文档等多媒体教学资源，系统学习理论知识并掌握实际操作技能。平台内置了如 Wireshark 等专业网络安全分析软件，并针对 HTTP 与 HTTPS 协议提供了专门的学习模块及实战演练模块。减轻了实验教师在实验环境配置与维护方面的负担，使其能更专注于实验内容设计与实验教学指导。学生也因此能够更高效地完成实验任务，打破了传统实验在时间与空间上的局限，享受到一个在空间、时间及内容上均高度开放的个性化实验学习环境。将网络安全实验部署于云端，支持远程实验操作，学生无需在本地计算机安装复杂的实验软件，仅通过浏览器访问指定的网络安全虚拟云平台网址并完成登录认证即可开始实验。具体的实验流程如图 1 所示。

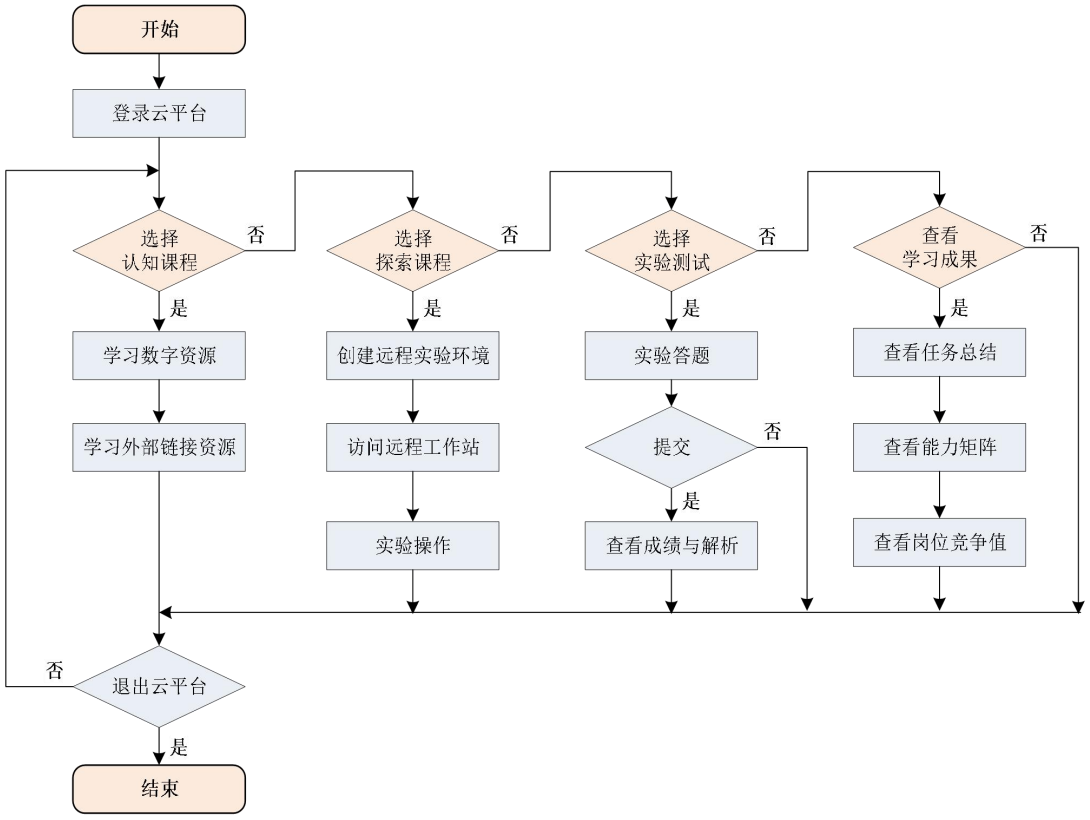

图 1 基于网络安全虚拟云平台的实验流程

在网络安全实训教程界面，学生首先进入“实验认知与探索任务”列表。选择相应的“认知课程”学习任务，例如“HTTP 与 HTTPS 协议基础”，完成前置的理论学习。然后选择“探索课程”实验任务，例如“HTTP 与 HTTPS 协议分析”，如图 2 所示。等待平台动态创建并初始化实验环境后，即可访问分配的任务工作站，进入远程桌面环境，开始具体的实验操作。平台还提供了在线实验测试功能，学生可以遵循引导式的答题流程逐步完成实验，通过实验测试的形式来可以检验实验结果的准确性、操作技能的熟练度以及综合实践分析能力。测试题目以实践操作验证为主，允许学生在答题过程中随时返回远程工作站进行必要的操作验证，然后选定答案。若遇到难题，可利用平台提供的“锦囊”功能获取提示，辅助完成作答。提交测试后，可以查看测试成绩和详尽的试题解析。实验操作与实验测试环节完成后，平台会自动生成一份全面的任务总结报告，如图 3 所示。

图 2 HTTP 与 HTTPS 协议分析实验首页面

图 3 网络安全虚拟云平台实验测试成绩与任务总结

3 层次化实验内容

为满足不同认知水平和能力层次学生的个性化学习需求，按照由浅入深、循序渐进的原则，设计了三个层次的实验内容，具体如表 1 所示。

（1）基础实验

主要目标是使学生熟练掌握使用 Wireshark 软件查询和分析 HTTP 与 HTTPS 协议数据包的基本方法。通过分析平台预置的 HTTP&HTTPSAnalysis.pcapng 流量捕获文件，学生应能识别并初步分析：HTTP 与 HTTPS 服务器的默认端口号、GET 方法和 POST 方法的 HTTP 请求数据包、包含用户凭证的登录请求、登录成功的

响应数据包、HTTPS 加密数据包的基本特征、SSL/TLS 握手过程中的密码套件协商信息，以及 HTTP 与 HTTPS 协议的整体流量统计信息等。

（2）进阶实验

在基础实验之上，对 HTTP&HTTPSAnalysis.pcapng 文件进行更深层次的分析。使用 Wireshark 的过滤功能精确筛选出 HTTPS 数据包，并按数据包编号顺序，分析 TCP 三次握手建立连接过程中的各个数据包的详细信息，包括服务器与客户端的 IP 地址和端口号等。SSL/TLS 协议是构成 HTTPS 安全性的核心。客户端与服务器之间通过四次握手完成身份验证和会话密钥的确立。按照表 2 所列要求，完成对 SSL/TLS 协议握手全过程的详细分析。

表 1　层次化实验内容

实验目的	实验类别	实验内容	实验难度	实验性质
具备利用 Wireshark 软件分析网络协议数据包的基本能力	基础实验	分析 HTTP 与 HTTPS 协议的数据包结构和关键统计信息	容易	必做
具备分析 HTTPS 工作机制和数据加密传输的能力	进阶实验	分析 TCP 协议的三次握手过程和 TLS/SSL 协议的四次握手过程	一般	必做
具备初步的安全协议设计与深入分析能力	拓展实验	完善 HttpsWeb 应用实例，利用 Wireshark 进行 HTTPS 抓包与详细分析	困难	选做

表 2　SSL/TLS 协议实验内容与要求

协议阶段	分析要求
第一次握手	列出客户端发送的 Client Hello 消息数据包编号，识别其中声明的 SSL/TLS 协议版本、客户端生成的随机数 random_C、客户端支持的密码套件列表
第二次握手	列出服务器回应的 Server Hello 消息对应的数据包编号，分析服务器选择使用的 SSL/TLS 协议版本、确定的密码套件、压缩算法（如有）、服务器生成的随机数 random_S、服务器下发的数字证书、密钥交换信息以及握手结束标志等
第三次握手	列出客户端发送的相关报文数据包编号，分析客户端的数字证书（双向认证时）、客户端密钥交换参数、加密通信算法改变通知、加密握手消息和客户端握手结束通知等
第四次握手	列出服务器发送的相关报文数据包编号，分析服务器发送的加密通信算法改变通知、加密握手消息和服务器握手结束通知和所有握手数据包数据摘要等

（3）拓展实验

主要目标是提升学生综合运用 Wireshark 进行实时数据包捕获与 HTTPS 协议深度分析的能力。在云平台启动预置的 HttpsWeb 应用实例，在浏览器中访问 Web 页面，执行文件上传等操作，利用 Wireshark 软件实时捕获浏览器与服务器之间的所有网络通信报文，并将捕获结果保存为 PCAP 文件。然后，利用 Wireshark 软件打开此 PCAP 文件，对 HTTPS 协议的数据包格式和工作过程进行详尽分析。

HttpsWeb 应用实例模拟实现 TLS/SSL 协议的四次握手过程，包括服务器与浏览器之间传输的数据和会话密钥的计算方法，以及如何运用协商好的会话密钥对上传文件进行加密，并在网页前端直观显示明文与密文的对比。利用 Wireshark 软件分析抓取的数据包只能分析服务器与客户端的加密数据传输，难以展示双方内部计算会话密钥和数据加解密的具体过程。HttpsWeb 应用实例的引入能够弥补这一不足，使学生更完整、更深入地理解 HTTPS 协议实现细节与过程。HttpsWeb 应用实例是一个 Java 开发的基本框架，鼓励学有余力的学生对其功能进行扩展和二次开发，然后将其重新部署到网络安全虚拟云平台上，用于进行更复杂应用场景下的 HTTPS 协议数据包捕获与深度协议分析。

4　实验教学组织与考核评价

4.1　“双师协同”个性化实验教学模式

要实现产教融合，关键在教育者，教育者包括高校的教师，企业的技术人员和管理人员[7]。将企业人员引入融入到实验课程的开发与教学环节，是提升实验教学质量与实效性的关键途径。网络安全实验课程依托网络安全虚拟云平台、智慧实验室、智慧树平台以及学校统一的实验运行与管理平台，构建了一个多方联动的教学支持体系。在此基础上，形成了高校教师和企业教师共同参与教学的“双师协同”网络安全实验教学模式，如图 4 所示。网络安全虚拟云平台与其他平台相辅相成，实现慕课学习、实验测试、直播教学、成绩综合评定和实践创新能力评价等核心功能。

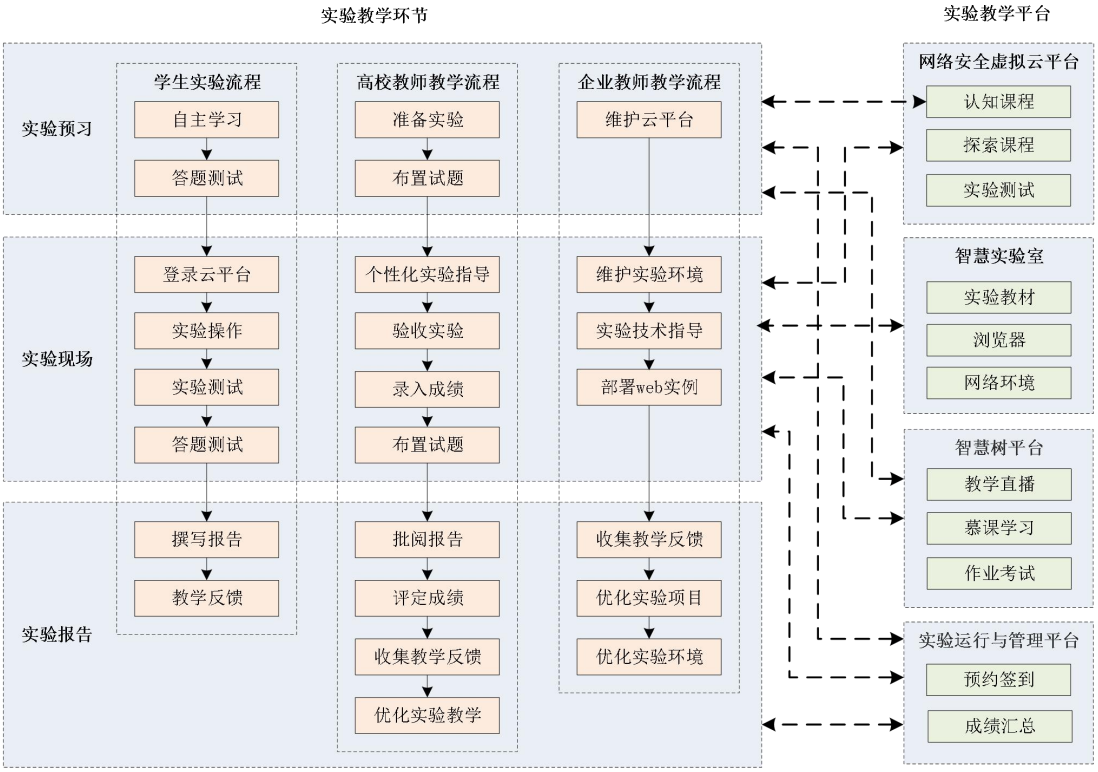

图 4　基于网络安全虚拟云平台的“双师协同”网络安全实验教学模式

BOPPPS（Bridge-in，Objective/Outcome，Preassessment，Participatorylearning，Post-assessment，Summary）教学模型[8]在各类学校教学中广泛应用，包含六个环节：导入（Bridge-in）、学习目标（Objective/Outcome）、参与式学习（Participatorylearning）、后测（Post-assessment），总结（Summary）。网络安全实验课程划分为：实验预习、实验现场和实验报告三个主要阶段。依照 BOPPPS 教学模型，为每个阶段设定了明确的教学目标和相应的教学活动。

（1）实验预习阶段

通过智慧树直播或者线下课堂讲解，明确实验目标、实验任务和实验原理。完成 BOPPPS 模型中的“导入”和“学习目标”环节。借助智慧树平台的在线测验功能和云平台“认知课程”学习模块，了解学生对相关知识点的掌握情况，实现“前测”目标。

（2）实验现场阶段

采用多样化的教学策略和方法，积极引导学生动手完成预设的实验任务。通过云平台内置的实验测试功能、教师的实验验收，以及智慧树平台的在线测验等等多种方式，检验学生的实验操作成果，评估实验目标的达成度，完成 BOPPPS 模型中的“参与式学习”和“后测”环节。具体可实施的教学方法包括：

① 课外自主探索与课堂指导深化相结合

学生可以在实验室，利用网络安全虚拟云平台完成实验，由实验教师根据学生的个体能力差异和实验进展情况，启发引导学生由易到难、循序渐进地完成各项实验任务，并对实验结果进行现场验收；课外时间，学生可以利用自己的笔记本电脑登录云平台继续进行实验的探索与深化，充分实现学生的自主学习。

② 个性化实验指导与专业技术支持相结合

在实验室现场操作过程中，高校教师主要负责提供实验答疑和阶段性的实验考核，根据每个学生的特点给予个性化的实验指导，激发学生的创新思维，使其高质量完成实验。企业教师侧重于提供更具针对性的实验技术支持，例如特定软件的高级操作技巧、远程服务器访问故障排查等方面的答疑，并协助学生在网络安全虚拟云平台中成功部署和调试 HttpsWeb 应用实例等拓展性内容。

（3）实验报告阶段

学生独立撰写实验报告，反馈实验意见与建议。实验教师批阅报告，并完成成绩评定。高校教师与企业教师根据学生的反馈信息，持续优化实验项目和实验环境，推动实验课程的迭代改进与教学改革的深化，完成 BOPPPS 模型中的“总结”环节，并形成教学闭环。

该教学模式充分整合并发挥了高校教师和企业教师的优势，为学生提供了灵活的实验项目、个性化的实验指导和高效稳定的实验环境，从而有效地提升了

学生的网络安全实践能力和创新素养。

4.2 多平台联动的多维度实验考核与评价体系

实验课程采用多平台、多维度、过程化考核方法，构建了一个融合学校与企业双重视角的学生实验成效考核与综合能力评价体系。实验课程成绩评价指标与细则如表 3 所示。

表 3 多平台评价指标与细则

实验阶段	学习平台	学习形式	主要评价指标	评价成绩占比
实验预习	智慧树平台	实验慕课	数字化资源学习进度	10%
	虚拟云平台	认知课程学习	数字化资源学习进度	
	智慧树平台	实验答题	答题分数	10%
实验现场	虚拟云平台	实验操作	熟练程度与实验质量	50%
		实验测试	测试分数	
	课堂教学	实验验收	回答问题难度和正确性	
	智慧树平台	实验答题	答题分数	10%
实验报告	课堂教学	撰写指导	实验数据分析正确性与全面性	20%

网络安全虚拟云平台记录了每个学生的知识、技能、能力和任务完成度，统计学生的实验完成情况。并且展示了每个学生的“技能矩阵”和“攻击矩阵”，学生每完成一个实验项目，其相关的技能点和攻防能力评估值便会相应累积。这些技能和能力的评估维度均参照当前网络安全行业各主流岗位的具体任职要求进行设定，确保了评估标准的行业对标性。平台可以通过相应的算法对学生的岗位胜任力进行量化计算和预测。学生查阅这些数据后，可以直观地认识到自身能力与目标岗位需求之间的匹配度，从而进行针对性的学习和提升。通过这种方式，学生完成实验后，不仅能获得该课程的学业成绩，更能得到一份实践能力评价报告，清晰了解自己在网络安全领域的实践水平和行业竞争力。

4.3 实验效果

网络安全虚拟云平台后台日志记录了“配置 HTTPS 服务器”和“成功捕获 HTTPS 握手包”两个关键任务的完成时间。与传统未使用云平台的实验效率对比如图 5 所示。2024 级学生使用虚拟云平台后，完成核心实验任务的平均时间缩短约 35.6%，任务成功率也从 72%提升至 95%。这一成效主要得益于云平台提供的一键部署和快速重置功能，大幅减少了环境配置错误所耗费的时间，使学生能够更专注于协议分析本身，从而显著提高了实验效率与完成质量。

在未增加实验学时的前提下，信息安全专业学生通过该平台完成的实验项目数量增加了 50%。借助企业资源的有效融入，师生从繁琐的本地环境搭建与维护中彻底解放，将更多时间投入创新性实验内容的设计与实践，推动创新性实验项目占比达到 75%。实验内容紧密结合当前网络安全领域的技术趋势和实际应用，有效提升了学生的参与积极性与主动性。选做拓展性实验的学生比例从 10%大幅提高至 55%，切实锻炼和提升了学生的网络安全实践核心能力。

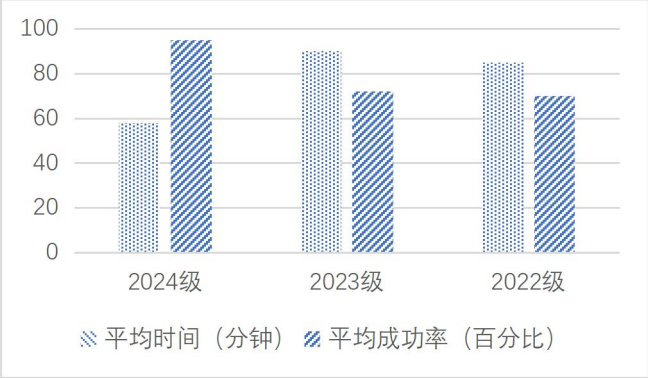

图 5 采用虚拟云平台前后实验效率对比

目前，该网络安全虚拟云平台已覆盖天津大学、长沙理工大学等 20 余所高校，服务学生用户 2000 余人，并于 2025 年在北京大学计算机网络实验暑期课程中成功支持约 45 人开展网络安全实验。基于网络安全虚拟云平台的网络安全实验应用规模持续扩大，将在网络安全课程教学与网络空间安全专业建设中发挥日益重要的作用。

5 结束语

在产教融合背景下，高校教师与企业教师充分考虑当前网络安全领域的发展趋势与人才需求，以网络安全虚拟云平台为核心，构建了一个生动、高效的实验教学环境。根据网络安全的体系结构，科学合理地设计了层次化实验内容，选取了业界最具代表性的分析工具与核心技术。通过基础实验、进阶实验和拓展实验的锻炼，不仅满足了网络安全实验教学大纲的要求，还为学生提供了深入探索网络安全知识的机会。基于网络安全虚拟云平台的“双师协同”实验教学模

式为网络安全实验课程提供了便捷高效的环境，有力推动了网络安全学科建设，并为国家培养高素质网络安全专业人才做出了积极贡献。

参 考 文 献

[1] 肖凌,陈凯,付才,等.网络空间安全综合实践分级通关实验平台建设[J].实验室研究与探索,2021,40(10): 236-243,284

[2] 姚晔,张玉蓉,邱洪君.虚拟专用网络加密技术实验教学改革探索[J].实验室研究与探索,2023,42(04):227-231

[3] 李向军,刘伯成,张坚林,等.数字化转型背景下实战型网络安全人才培养探索与实践[J].计算机技术与教育学报，2024, 12 (2):77-82

[4] 刘勇.基于云计算和虚拟化的网络安全实验教学平台建设研究[J].对外经贸,2024,(07):89-92.

[5] 谭畔,袁慧.云计算在图书馆数据管理中的应用研究[J].中国管理信息化,2021(5):179-180

[6] 彭玉兰,代琪怡,李佳芮,等.基于GNS3+Wireshark的网络协议分析实验教学改革[J].现代信息科技,2022,6(18):185-187,191

[7] 丁国富,马术文,孟祥印,等.面向产业的开放式云产教模式探索[J].高等工程教育研究,2023,(01):55-61

[8] 曹丹平,印兴耀．加拿大 BOPPPS 教学模式及其对高等教育改革的启示[J]．实验室研究与探索,2016,35(2):196-200