

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*

宋超¹ 张皓¹ 陈旭羿¹ 杨浩淼¹ 梁伟波^{2**}

1 电子科技大学计算机科学与工程学院, 成都 611731

2 四川大学华西基础医学与法医学院, 成都 610041

摘要 针对网络与信息系统安全综合设计实验课程中存在的知识体系离散化、实践指导滞后性、能力评估片面化等教学痛点, 创新性提出三位一体的教学改革框架。通过构建知识图谱驱动的课程知识网络、AI 赋能的动态答疑支持体系以及代码智能评估反馈机制, 形成“结构化认知-个性化学习-精准化实践”的闭环教学模式。知识图谱实现安全领域核心概念的系统化关联, 智能答疑系统突破传统教学的时空限制, 代码评估平台建立量化能力评价标准。提升学生在安全机制设计、系统编程实现等维度的综合能力, 为工程实践类课程的智能化改革提供新范式。

关键字 知识图谱, 检索增强生成, 大语言模型

Teaching and Practice in Experiment Course of Network and Information System for Security Design Enhanced by Knowledge Graph

Chao Song¹ Hao Zhang¹ Xuyi Chen¹ Haomiao Yang¹ Weibo Liang^{2**}

1 School of Computer Science and Engineering, University of Electronic Science and Technology of China, 611731, China

2 West China School of Basic Medical Sciences & Forensic Medicine, Sichuan University, 610041, China

Abstract—To address the pedagogical pain points of fragmented knowledge, delayed practical guidance, and one-sided competency assessment in Experiment Course of Network and Information Systems for Security Design, this paper proposes an innovative, three-in-one teaching-reform framework. By building a knowledge-graph-driven course knowledge network, an AI-enabled dynamic question-answering system, and an intelligent code-evaluation feedback mechanism, a closed-loop model of “structured cognition–personalized learning–precise practice” is formed. The knowledge graph systematically interlinks core concepts in the security domain, the intelligent question-answering system breaks through the temporal and spatial limitations of traditional teaching, and the code-evaluation platform establishes quantitative standards for competency assessment. The reform enhances students’ comprehensive abilities in security-mechanism design and system-programming implementation, thereby offering a new paradigm for the intelligent transformation of engineering-practice courses.

Keywords—large language model, knowledge graph, retrieval-augmented generation

1 引言

随着信息技术的飞速发展, 网络安全已成为当今数字时代的关键议题。网络与信息系统的广泛应用, 使得其安全性直接关系到国家、企业以及个人的利益。在此背景下, 培养具备网络与信息系统安全设计能力

的专业人才显得尤为重要^{[1] [2] [3]}。《网络与信息系统安全综合设计实验》作为信息安全专业的实践型课程, 旨在通过项目驱动与实践教学相结合的方式^{[4] [5] [6]}, 培养学生在网络系统安全设计、密码学应用、漏洞分析与攻防实践等领域的综合能力。课程以在线考试系统开发为载体, 覆盖了网络安全协议、加密算法、身份认证、访问控制、数字签名和安全审计等多个技术模块, 为学生提供了理论与实践深度结合的学习平台。尽管课程已构建了完整的实验体系, 但在实际教学中仍然面临以下关键挑战: 一是知识碎片化问题, 在基础实验模块中, 各安全技术知识点相对独立, 学生难以形成系统化的知识网络。例如, 密钥协商实验与数字签名实验之间缺乏明确关联, 导致学生在综合应用

***基金资助:** 本文得到电子科技大学首批人工智能技术赋能本科教学教改项目(2024AIXM037); 电子科技大学2025年来华留学教研教改项目(JYJG2025013); 四川省高等教育人才培养质量和教学改革项目(JG2024-0001和JG2024-0939); 国家自然科学基金项目(62472070, 82241060和62020106013); 四川省科技计划项目(2024NSFSC0492)资助。

** 通讯作者: 梁伟波 liangweibo@scu.edu.cn

时出现概念混淆；二是实践能力培养的局限性，现有实验以功能实现为主，缺乏对代码质量、安全漏洞分析及攻防对抗能力的深度训练。学生在开发过程中容易忽略代码规范性与潜在安全风险，难以满足行业对网络安全人才的实战需求。三是教学交互的低效性，传统答疑方式难以及时响应学生在实验中遇到的个性化问题，且无法提供针对代码实现细节的精准指导。同时，实验评价以结果为导向，缺乏对学生学习过程的动态跟踪与反馈优化机制。

针对上述问题，本文旨在通过以下创新举措提升教学效果：

(1) 构建知识图谱驱动的课程框架，通过将网络通信、加密算法、身份认证等知识点进行关联建模，形成可视化知识网络，帮助学生理解技术模块间的内在联系，强化系统思维能力。

(2) 引入 AI 赋能教学系统，开发智能答疑平台，采用基于本地部署大语言模型的检索增强生成 (Retrieval-Augmented Generation, 简称 RAG) 架构，实现对学生问题的精准解答与个性化学习路径推荐。

(3) 构建代码在线评估系统，提供实时代码质量分析与漏洞检测反馈，提升实践教学的深度与广度。

2 教改内容与设计

2.1 总体设计

本教改方案总体设计围绕《网络与信息系统安全综合设计实验》课程展开，旨在通过融合知识图谱、人工智能技术与智能评估平台，全方位提升教学质量与学生学习效果。方案包含构建知识图谱驱动的课程知识网络、基于本地部署大模型的智能答疑系统和代码智能评估平台三大核心模块。

通过构建课程知识图谱，将分散的知识点关联起来，形成可视化知识网络，帮助学生理解知识间的联系，构建系统知识体系，为教学与学习提供导航^{[7] [8] [9]}。同时，利用本地部署大语言模型构建智能答疑系统，结合 RAG 技术，实现精准答疑和个性化学习支持，满足学生在学习过程中的即时需求，提高学习效率^{[10] [11] [12]}。此外，还开发了基于 web 网页的代码智能评估平台，具备题库选择、代码填空和智能评分功能，为学生提供便捷的实验环境，实时评估代码质量，帮助提升编程能力^{[13] [14]}。这三方面相互配合，共同促进教学改革目标的实现，提高学生的综合实践能力和创新思维。

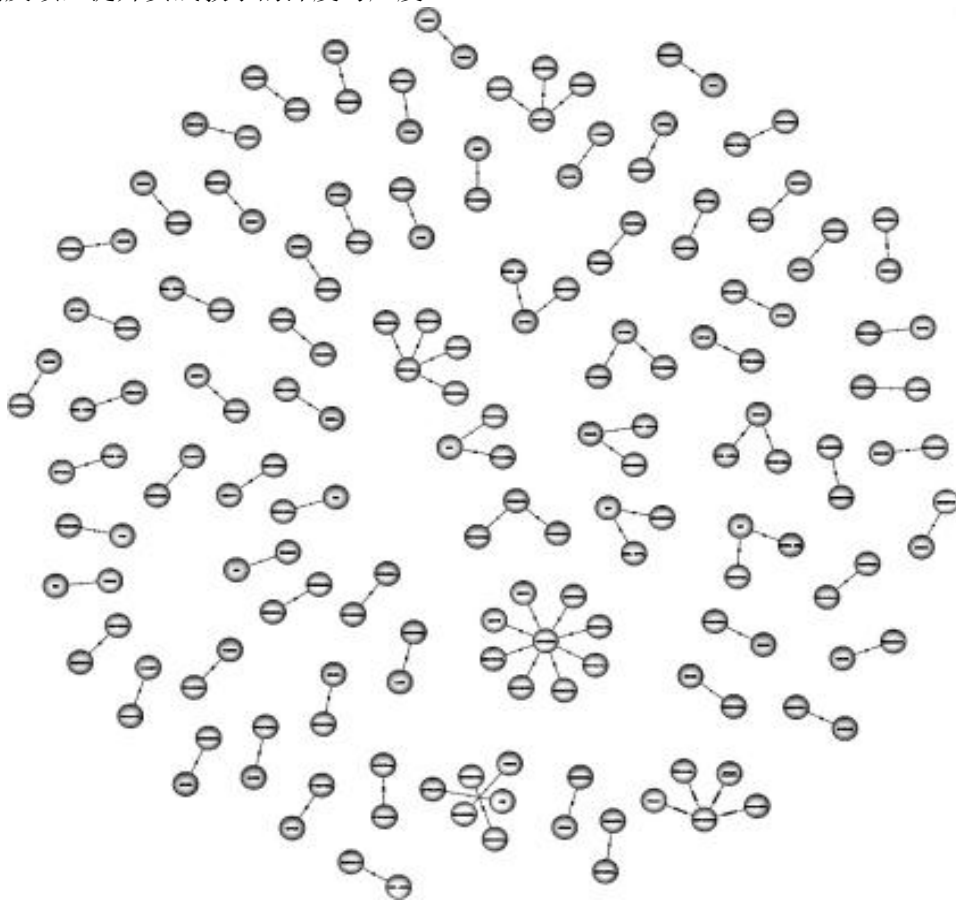


图 1 《网络与信息系统安全综合设计实验》课程知识图谱

2.2 知识图谱驱动的课程知识网络

以《网络与信息系统安全综合设计实验》课程的教学内容为基础，提取各实验模块中的关键知识点，如网络通信原理、数据库操作、密钥协商算法、加密技术、身份认证机制、访问控制原理、数字签名原理、安全审计等，将这些知识点作为图谱的实体(entity)节点。同时，分析知识点之间的关联关系(relation)，如密钥协商为加密算法提供密钥、加密算法用于保障网络通信安全、身份认证与访问控制相结合实现用户权限管理等，以边的形式连接相关节点，构建起完整的课程知识图谱，如图1所示。

通过知识图谱的可视化技术，将复杂的知识点网络以直观的图形方式呈现给学生。学生可以清晰地看到各知识点之间的层次结构、依赖关系和相互联系，从而更好地理解课程的整体框架和知识体系。例如，学生在学习密钥协商实验时，可以通过知识图谱看到

其与后续加密算法实验的紧密关联，了解到密钥协商是实现安全加密通信的前提步骤。

在教学过程中，教师可以依据知识图谱进行课程讲授，按照知识网络的逻辑顺序展开教学内容，使教学更加系统连贯。同时，知识图谱也可以作为学生的学习导航工具，学生可以根据自己的学习进度和知识掌握情况，在图谱中找到相应的知识点进行深入学习，自主探索知识之间的关联，构建个性化的学习路径。

2.3 基于本地部署大模型的 RAG 智能答疑系统

选用大语言模型(LLMs)如DeepSeek-R1-70B、Qwen2.5-32B等，在本地服务器上进行部署，确保数据安全和隐私保护，同时降低对外部网络的依赖，提高系统的稳定性和响应速度，为课程提供强大的语言理解和生成能力支持。

请解释下安全审计实验中的do_log函数功能

✎ ○ ○

Q GNAG-local-local-qwen2.5:32b

do_log 函数在安全审计实验中用于插入日志消息到数据库。具体来说，该函数接收一个指向包含日志信息的结构体指针和一个数据库对象作为参数，并执行将日志消息插入数据库的操作。

以下是 **do_log** 函数的具体实现：

```

cpp
1 bool do_log(char *pdata, CDATABASE &db)
2 {
3     SLOG *plog = (SLOG *)pdata; // 将输入数据转换为日志结构体指针
4     CSQL sql;
5     CString strsql;
6     bool rtnflg;
7     // 构造插入日志的SQL语句
8     strsql.Format("INSERT INTO LOG (logtime,msgtype,username,msg) values ('%s','%d','%s','%s')",
9                 plog->time, plog->msgtype, plog->username, plog->msg);
10    // 将构造好的SQL语句添加到SQL对象中
11    sql.AppendSQL((LPTSTR)(LPCSTR)(strsql));
12    // 执行SQL事务，将日志信息插入数据库，并返回操作结果
13    rtnflg = db.ExecSqlTransaction(sql);
14    return rtnflg;
15 }

```

该函数的主要功能是通过构造并执行一个INSERT SQL语句来实现日志消息的存储。它确保了所有重要的系统活动都被记录下来，这对于安全审计至关重要，因为这些日志可以用于检测安全事件、[↓](#)自安全漏洞和遵守合规要求。

输入消息 ↓ ↻

图2 课程问题答疑中对关键函数解析的展示

结合课程知识图谱和相关教学资料，构建检索增强生成(RAG)系统。当学生提出问题时，系统首先通过检索模块在知识图谱和资料库中快速定位与问题相

关的知识点和信息，然后利用大语言模型的生成能力，基于检索到的结果为学生生成准确、详细且符合课程语境的解答，实现智能答疑功能。

智能答疑系统能够实时回答学生在学习过程中遇到的各种问题，无论是关于理论概念、实验操作还是代码实现等方面。图 2 所示系统回答课程实验的关键函数问题，讲解了安全审计实验中函数 do_log 并对代码添加了注释说明。除了提供直接的答案外，系统还可以根据学生的问题和学习历史，分析学生的学习薄弱点，为学生提供个性化的学习建议和拓展学习资源，帮助学生有针对性地加强学习，提高学习效果。

2.4 代码智能评估平台

开发基于 web 网页的实验操作页面，将实验中的代码填空题目以及相关的上下文信息清晰地展示给学生。学生可以在浏览器中直接进行代码填空操作，无需安装额外的软件，方便学生随时随地进行实验学习，

提高学习的灵活性和便捷性。

平台建设丰富的代码题库，涵盖课程中的各个实验模块和知识点，学生先进入实验题库选择界面。每个题目都包含完整的代码上下文以及需要填空的部分，学生根据题目要求填写代码后，可以点击提交按钮，系统自动接收学生提交的代码。

学生提交代码后，平台调用预先集成的代码评估接口，利用智能评分算法对填空的代码进行自动评分，如图 3 所示。评分过程中，系统会检查代码的语法正确性、逻辑完整性、与预期结果的符合度等多个方面，并根据评分标准给出相应的分数。同时，系统还会为学生提供详细的错误反馈和改进建议，帮助学生了解自己代码中的问题所在，促进学生编程能力的提升。



图 3 代码智能评估系统中的代码评分区域界面展示

3 评测与讨论

3.1 系统级量化评测

为客观评估本次教改核心模块的建设质量，我们开展了可重复、可量化的技术基准实验，结果如下。

- (1) 知识图谱建设质量

如表 1 所示,以课程大纲列出的 80 个核心概念为黄金标准,我们构建的知识图谱实体已覆盖 68 个,实体覆盖率为 85%。

表 1 知识图谱建设质量评估表

指标	分数(百分比)
实体覆盖率	85%
关系准确率	93%

在知识图谱的关系层面,随机抽取了 100 条“实体-关系-实体”三元组,由大语言模型“豆包”进行独立判断,其中 93 条被判为语义正确,关系准确率达 93%。

(2) AI 答疑系统性能

表 2 AI 答疑对比评分

RAG	BertScore		
	Precision	Recall	F1 score
GraphRAG	71.09	72.57	71.74
LightRAG	72.14	66.98	69.31
GNAG(本研究)	73.03	73.74	73.28

我们在自建 100 条 FAQ 测试数据集上,将本文研究提出的 AI 答疑系统 GNAG 与两种主流基于知识图谱检索的 RAG 基线(GraphRAG^[15]和 LightRAG^[16])进行了横向对比,统一采用 BertScore 作为评价指标,结果如表 2 所示。

可以看出,本文的 AI 答疑系统 GNAG 在 Precision、Recall、F1 score 三项指标上均取得最高值,验证了课程知识图谱与本地大模型融合方案的有效性。

3.2 教改成果讨论

通过构建知识图谱驱动的课程知识网络、引入基于本地部署大模型的智能答疑系统以及开发代码智能评估平台,本教改方案在提升《网络与信息系统安全综合设计实验》课程教学效果方面取得了进展性成果。知识图谱的构建有效解决了传统教学中知识碎片化的问题,将各个实验模块中的关键知识点紧密关联起来,形成了一个有机的知识整体。这不仅帮助学生更好地理解了网络与信息系统安全领域的复杂概念和技术,还培养了他们的系统思维能力,使学生能够从整体上把握课程的知识架构,为解决实际问题时的综合应用奠定了坚实基础。

基于本地部署大模型的智能答疑系统为学生提供了便捷、高效的学习支持渠道。通过本地部署的大语言模型和检索增强生成技术,学生在学习过程中遇到的问题能够得到及时、准确的解答。这种智能化的答疑方式不仅提高了学生的学习效率,还增强了他们自主学习的信心和积极性,使学生在主动探索知识的过程中不断深化对课程内容的理解和掌握。

代码智能评估平台的引入在很大程度上优化了实践教学环节。该平台基于 web 网页的题库选择、代码填空和智能评分功能,为学生提供了丰富多样的编程练习机会,并且能够实时评估学生的代码质量,及时反馈问题所在。这有助于学生在实践中不断提高编程能力和对安全机制算法的运用能力,同时也减轻了教师的批改负担,使教师能够将更多精力投入到教学内容的优化和学生能力的培养上。

4 结束语

综上所述,本次教改方案通过构建知识图谱驱动的课程知识网络、引入大模型和知识图谱融合的智能答疑系统以及开发代码智能评估平台,有效提升了《网络与信息系统安全综合设计实验》课程的教学质量。知识图谱帮助学生建立了系统化的知识体系,智能答疑系统提供了高效的学习支持,代码智能评估平台强化了学生的实践能力。未来,持续优化教改方案各模块,有望进一步提升课程教学效果,为信息安全专业人才培养提供有力支撑。

致谢

特此感谢鲁力老师、汪小芬老师以及胡瑞林、周乐川、任政三位同学对本教改研究的贡献。鲁力老师和汪小芬老师为教改方案设计提建设性意见,保障教改与教学目标契合。胡瑞林协助完成课程知识图谱的构建与智能答疑系统测试,周乐川负责代码评估平台题库整理与测试,任政承担教学辅助与系统联调工作。老师和同学们共同为教改系统落地提供实践支撑,感谢各位的支持,助力本课程教改探索顺利推进。

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. DOI:10.12427/jcte2325-0208.20250515
- [2] 蒋远宏. 信息时代高校网络安全教育策略[J]. 安全与环境学报,2023,23(9):3381-3382.
- [3] 王宇. 师生网络安全素养教育指南[J]. 中国教育网络,2022(4):16-18. DOI:10.3969/j.issn.1672-9781.2022.04.013.
- [4] 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. DOI:10.12427/jcte2325-0208.20250519
- [5] 杨健晟,杨兴,张梅,等. 基于小任务大挑战的项目进阶教学

- 模式探讨[J]. 高教学刊,2025,11(11):120-123. DOI:10.19980/j.CN23-1593/G4.2025.11.029.
- [6] 龙勇. 基于项目教学法的计算机教学方法及网络安全研究[J]. 应用化工,2024,53(4):后插4. DOI:10.3969/j.issn.1671-3206.2024.04.054.
- [7] 尚凤军. 知识图谱驱动的计算机网络数智化课程建设探索. 计算机技术与教育学报,2024(12):71-77. DOI:10.12427/jcte2325-0208.20241212
- [8] 周东岱,董晓晓,顾恒年. 教育领域知识图谱研究新趋向:学科教学图谱[J]. 电化教育研究,2024,45(2):91-97,120. DOI:10.13811/j.cnki.eer.2024.02.013.
- [9] 姚屏,张佩美,何日恒,等. 基于知识图谱的双轨协同个性化教学模式研究[J]. 广东技术师范大学学报,2024,45(6):55-62. DOI:10.3969/j.issn.1672-402X.2024.06.009.
- [10] 陆楚龙,蔡国永,肖微,等. 基于大语言模型的课程教学答疑系统设计[J]. 计算机科学与技术,2024,14(5):165-171. DOI:10.12677/csa.2024.145125.
- [11] 张欢,郑晨,赵艳,等. 在线学习场景下大语言模型辅助教学评测[J]. 现代教育技术,2024,34(11):15-26. DOI:10.3969/j.issn.1009-8097.2024.11.002.
- [12] 蒲晓蓉,任亚洲,杨阳,汤志伟. AI大模型驱动高校人才培养改革. 计算机技术与教育学报,2024(12):101-105. DOI:10.12427/jcte2325-0208.20241217
- [13] 张定峰. 程序设计实验教学智能化评测及监控系统的研究与实现[J]. 电脑迷,2014(5):59-59.
- [14] 乌达巴拉,寇婕婷. "文心一言"在计算机编程课程中的应用效果研究[J]. 电脑知识与技术,2024,20(26):7-9.
- [15] D. Edge, H. Trinh, N. Cheng, J. Bradley, A. Chao, A. Mody, S. Truitt, and J. Larson, From local to global: A graph RAG approach to queryfocused summarization, CoRR, vol. abs/2404.16130, 2024.
- [16] Z. Guo, L. Xia, Y. Yu, T. Ao, and C. Huang, LightRAG: Simple and fast retrieval-augmented generation, CoRR, vol. abs/2410.05779, 2024.