基于人工智能的高校网络安全防护体系构建研究

江丹
河北工程大学，河北 邯郸 056038

DOI: 10.61369/TACS.2026090019

摘　　要： 数字化教育转型背景下，高校智慧校园建设持续深化，教学科研、学生管理、校园服务等各项工作全面依托网络信息化系统开展，校园网络数据体量、用户规模、业务场景持续扩张，随之而来的网络安全风险也呈现复杂化、多元化、隐蔽化特征。为破解传统防护体系的局限性，以人工智能技术为核心支撑，结合高校网络运行特点与安全风险特征，从技术、管理、运维、保障四个维度解决难题，筑牢校园网络安全屏障，为智慧校园安全稳定运行、师生信息数据安全、高校数字化教育高质量发展提供坚实支撑。

关 键 词： 人工智能；高校网络；网络安全；防护体系；智慧校园

Research on the Construction of University Network Security Protection System Based on Artificial Intelligence

Jiang Dan
Hebei University of Engineering, Handan, Hebei 056038

Abstract: Against the background of digital education transformation, the construction of smart campuses in universities has been continuously deepened. Teaching and research, student management, campus services and other daily work are fully dependent on network information systems. The continuous expansion of campus network data volume, user scale and business scenarios has led to increasingly complex, diversified and concealed network security risks. To break through the limitations of traditional protection systems, this paper takes artificial intelligence technology as the core support, combines the operational characteristics and security risk attributes of university networks, and solves practical problems from four dimensions: technology, management, operation and maintenance, and guarantee. The research aims to consolidate the campus network security barrier and provide solid support for the safe and stable operation of smart campuses, the security of teachers' and students' information data, and the high-quality development of digital education in universities.

Keywords: artificial intelligence; university network; network security; protection system; smart campus

一、人工智能及网络安全防护体系概述

人工智能是用计算机技术模拟人的智能思维和行为的一种技术集合，包含了机器学习、深度学习、自然语言处理、智能算法分析等核心技术，具有自主学习、动态分析、精准识别、快速运算等核心优势，可以对大量的数据进行自动化整理、筛选、研判，克服了人工处理效率低、精确度差的缺点[1]。相比传统的手工排查、静态设备防护方式，人工智能网络安全技术具有主动的、动态的、实时的、精准的特点，可以做到24小时不间断地进行监测，大大降低了人工维护的成本，减少了由于误报、漏报造成的隐患，从而大大提高网络安全防护的智能化程度。目前，人工智能技术已经被广泛应用到政企网络防护、互联网安全治理等各个领域当中，将它引入到高校网络安全防护当中，是解决校园网络安全治理难题、适应智慧校园发展的一种必然选择。

高校网络安全防护体系是依托各种软硬件设备、管理制度、运维机制所构建起来的综合性安全保障系统，涵盖校园网络终端、数据、业务、设备、用户行为等各个方面，目的就是防止网络攻击、杜绝数据泄露、规避网络风险、保证校园网络的稳定运行。高校校园网络不同于社会企业、政务网络，在网络安全防护层面需要注意以下几点：一是开放性好，面向全体师生开放，接入终端包括电脑、手机、智能教学设备等各种设备，接入场景分散；二是数据类型多样，科研涉密数据、师生个人隐私数据、校园政务数据等各类数据都有涉及，防护等级不同；三是用户网络安全意识参差不齐，师生网络操作不规范、随意点击不明链接、弱密码使用等行为较为普遍，人为安全风险较高[2-3]。这使得既定防护体系达不到全场景、全流程、全时段的安全防护要求，需要依靠人工智能技术来完成体系的升级重构，创建起全方位、立体化、智能化的校园网络安全防护体系。

二、基于人工智能的高校网络安全防护体系构建策略

（一）搭建人工智能智能监测预警技术体系，实现风险主动预判

技术架构升级是高校智能化网络安全防护体系建立的基础，

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

需要依靠人工智能技术创建起全方位、动态化的网络安全智能监测预警系统，从根本上克服传统被动防御的不足。高校要整合校园全网网络运行数据、终端访问数据、业务操作数据、流量传输数据，创建基于机器学习的校园网络大数据分析平台，用深度学习算法不断收集、整理校园网络正常运行状态下各项数据特征，创建标准的校园网络运行基线模型。那么，系统可以利用该基线模型实时比较全网动态数据，准确找出异常流量、异常终端接入、违规访问、高频数据传输等风险行为，对传统设备不能识别出的隐性攻击、变异病毒、APT 渗透攻击做出精准的发现，从源头上提高风险识别的能力。采用人工智能关联分析技术，把零散的安全日志、告警信息加以整合研判，避开单个数据的误报状况，准确判定风险等级，把网络安全风险分成一般预警、中级隐患、高危漏洞这三个层次，依照不同的风险等级制订相应的预警措施。采用弹窗提醒、后台告警、短信通知等手段，第一时间把风险信息告诉运维人员，说明风险所在、风险类型、影响范围，实现网络风险“早发现、早预警、早处置”[4]。另外还要依靠人工智能自主学习的能力，系统可以及时更新网络攻击特征库，不断吸收新的网络威胁数据，动态改进识别算法，适应网络攻击手段的更新换代，全面加强校园网络风险的提前预判和前置防控能力，筑牢技术防护的第一道防线，夯实高校网络安全防护体系的坚实基础。

（二）构建智能化安全运维管控机制，提升风险处置效率

高效的运维管控机制是保证网络安全防护体系落地运行的重要环节，针对高校传统网络运维人工依赖度高、处置效率低、流程不规范的问题，需要依靠人工智能技术搭建起自动化、智能化、标准化的安全运维体系。首先创建人工智能自动化处置平台，对校园网络常见的弱密码登录、违规外网访问、恶意流量攻击、终端病毒入侵等低、中风险问题创建智能处置规则，实现风险自动拦截、漏洞自动修复、异常终端自动隔离，无需人工干预即可完成基本的风险处理工作，大大缩短了风险处置时间，解决了人工运维响应迟缓的问题。其次，对高危网络攻击、大规模网络异常、核心数据泄露等复杂风险进行人工智能系统风险溯源、数据分析、影响研判，产生最佳的处置方案，辅助运维人员及时应对应急处理[5]。利用人工智能大数据统计分析功能，对校园网络每天、每周、每月发生的安全事件、风险类型、漏洞分布、违规行为等进行汇总统计，形成可视化的安全运维报告，准确找出校园网络的防护盲区，为运维工作改进提供数据支持。最后，建立智能化运维台账管理机制，用人工智能自动记录各种安全事件的处置过程、处置结果、整改情况，实现网络安全运维全过程可追溯、可监管、可复盘，不断规范校园网络安全运维流程，全面提升高校网络安全应急处置和常态化运维管控水平，切实提升高校网络安全防护水平，值得我们深入探索与实践。

（三）完善校园智能数据安全防护体系，筑牢核心数据屏障

数据安全是高校网络安全的核心内容，校园科研数据、师生隐私数据、校园政务数据的安全防护直接影响到高校的核心利益和师生的合法权益，需要依靠人工智能技术建立全过程、分层化的数据安全防护体系。首先实行人工智能数据分级分类管理，利用自然语言处理、智能识别算法对校园全网数据展开自动梳理、分类标注，依照数据的涉密等级、重要程度，把数据分成公开数据、内部数据、涉密科研数据、核心隐私数据这四个类别，对各个等级的数据执行不一样的防护权限、访问规则、传输管控措施，从而达成精准化的分级防护。其次，创建起人工智能数据动态监测防护系统，就核心数据访问、下载、传输、拷贝、共享等各个环节的行为展开不间断地检测，准确地找出越权访问、批量下载、违规外传、恶意拷贝这些异常数据行为，立刻拦截掉数据泄露的风险，并且对违规行为开展溯源记录。利用人工智能加密技术对高校核心涉密科研数据、师生身份证、学籍、联系方式等隐私数据实施动态加密，用自适应加密算法，依照数据使用场合自行调节加密等级，既保证数据的使用便利性又保持安全性。此外，采用人工智能数据备份和恢复技术，对校园核心数据进行常态化的增量备份，定期检测备份数据的完整性，针对网络攻击、系统故障造成的数据丢失、数据损坏等事件，实现快速智能恢复，最大限度地减少由于数据安全事故造成的损失，全方位地筑牢高校校园核心数据的安全防线[6-8]。

（四）建立智能化安全管理与教育保障体系，规避人为风险

人为操作不规范、网络安全意识缺乏是造成高校网络安全风险的主要原因，大部分校园网络安全事件都是由于师生违规操作、轻信网络诈骗、随意接入陌生网络等造成的，所以需要依靠人工智能技术建立全方位的安全管理及安全教育保障体系，从源头上杜绝人为安全风险。在安全管理上，创建校园用户智能行为管控平台，利用人工智能算法分析师生日常网络使用行为习惯，创建用户行为信用模型，对长期合规使用网络的用户简化权限审核流程，对存在频繁违规访问、高危操作、异常上网行为的用户实施智能提醒、权限限制、行为预警，达成用户网络行为的动态化、智能化管控。借助人工智能智能审核技术，对校园官网、校园论坛、师生社交平台上的网络内容实施实时筛查，自动找出不良信息、谣言信息、违规言论并予以拦截删除，防止校园网络舆论安全风险[9-10]。在安全教育上，创建人工智能个性化安全教育平台，依靠大数据剖析各个用户群体的网络操作漏洞和风险短处，对教职工、学生、运维人员等各类人群展开有针对性的网络安全知识、案例警示、操作规范培训内容推送工作，冲破传统统一化、形式化的安全教育模式。同时利用人工智能智能答题、模拟攻防、风险场景演练等方式提高安全教育的趣味性和实效性，使师生迅速掌握网络安全防护知识和技能，规范网络操作行为，全面提高全校师生网络安全素养，从人为上筑牢校园网络安全防护基础，构建起技术防护、智能管控、全员教育三位一体的全方位防护体系。

三、结论

如今。智慧校园高速建设、网络威胁持续迭代，传统被动式、人工化、静态化的网络安全防护体系已无法适配高校网络安全治理的发展需求，将人工智能技术融入高校网络安全防护体系建设，是提升校园网络安全防护能力、保障高校数字化建设稳步

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

推进的必然趋势。结合当前高校校园网络的运行特征与安全防护短板，从智能监测预警、智能运维管控、数据安全防护、安全管理教育四个核心维度，构建全方位、立体化的智能化高校网络安全防护体系，形成了技术赋能、机制保障、全员参与的一体化防护格局，值得我们深入探索与实践。

参考文献

[1] 朱清莹 . 基于人工智能的高校网络安全防护系统设计与应用 [J]. 网络安全和信息化 ,2025,(12):120-122.

[2] 陈倩倩 . 人工智能技术在高校学生网络安全防护中的应用研究 [J]. 通讯世界 ,2025,32(10):52-54.

[3] 邓国胜 . 基于新一代智能通信技术的网络安全防护体系研究 [J]. 江苏通信 ,2025,41(2):93-95+107.

[4] 穆雷霆 , 乐翔 . 基于 AI 大模型技术构建安全业务融合的工业控制系统安全可信防护体系 [J]. 自动化博览 ,2025,42(1):48-52.

[5] 张建娇 . 高校数据中心网络安全入侵防护体系构建 [J]. 网络安全和信息化 ,2024,(8):126-128.

[6] 谭小伟 . 基于人工智能的网络威胁情报分析与网络信息安全防护体系研究 [J]. 信息记录材料 ,2023,24(12):59-61.

[7] 李静 , 单晴晴 . 基于大数据和人工智能技术的网络安全防护体系功能需求分析 [J]. 信息与电脑 (理论版),2023,35(7):225-227.

[8] 赵艳花 , 陈阳 . 大数据及人工智能背景下的网络安全防御系统设计研究 [J]. 信息记录材料 ,2022,23(10):176-178.

[9] 宋钊 , 孙骞 . 人工智能背景下全球关键信息基础设施安全挑战与对策 [J]. 信息安全与通信保密 ,2022,(6):94-101.

[10] 罗秀春 , 陈睿智 . 人工智能在网络流量分析中的研究与应用 [J]. 通信技术 ,2022,55(2):258-264.

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License