基于人工智能的高校网络安全防护体系构建研究

杨梦希
(无锡商业职业技术学院,江苏无锡　214000)

[摘　要]随着教育信息化进程的持续推进,学校的管理工作、教学工作、科研工作由原来的传统模式向数字化模式转型,这种深度融合使得高校对信息化的依赖程度不断攀升。为智慧校园的发展提供安全、稳定、高效的网络保障,是当前高校信息化工作的重点。人工智能技术的诞生,为构建高校网络安全防护体系开拓了新思路、新方法。本研究报告旨在探讨基于人工智能的高校网络安全防护体系的构建,通过对高校网络安全现状的分析,结合人工智能技术的特点和优势,提出了一套基于人工智能的高校网络安全防护体系框架设计。

[关键词]人工智能;网络安全;防护体系
[中图分类号] TP393.08; TP18; G647　[文献标识码] A　[文章编号]2096-711X(2026)02-0157-03
doi:10.3969/j.issn.2096-711X.2026.02.051　[本刊网址] http://www.hbxb.net

引言

随着高校智慧校园建设持续深入开展,网络已经成为推动高校教学、科研、管理等各项工作有序运转的核心支撑力量。然而,与之相随的是网络安全问题愈发严峻,黑客攻击频发、恶意软件感染蔓延、数据泄露事件时有发生,这些问题严重阻碍了高校工作的平稳开展,师生的个人信息安全也遭受着严峻挑战。传统的网络安全防护手段已经难以满足当前高校网络安全的需求,因此,引入人工智能技术构建一套有效的高校网络安全防护体系,保障高校网络安全,具有重要的现实意义。

一、研究目的和意义

本研究报告的目的是探讨基于人工智能的高校网络安全防护体系的构建,为高校网络安全防护提供新的思路和方法。具体来说,本研究报告的意义主要体现在以下几个方面:

(一)提高高校网络安全防护水平

通过引入人工智能技术,构建更加智能化的高校网络安全防护体系,能够提高高校网络安全防护的准确性、及时性和有效性,降低网络安全风险。

(二)保障高校教学、科研和管理的正常进行

高校网络是教学、科研和管理的重要基础设施,一旦出现网络安全问题,高校的正常运行将受到严重影响。构建有效的网络安全防护体系,才能保障高校教学、科研与管理等工作顺利开展。

(三)保护师生个人信息安全

高校网络存储海量师生信息,涵盖学生学籍、教师科研成果等。网络安全事故易引发信息泄露,严重损害师生利益。构建高校网络安全防护体系是守护师生信息安全的关键。

二、高校网络安全工作现状

通过前期团队对江苏几所高校进行实地调研中发现,目前的网络安全工作存在着以下几个问题:

(一)用户群体大,行为难控制

高校师生数量庞大,网络用户基数大,导致管理对象众多且复杂度显著提升。师生群体知识水平高、技术能力强,对新技术、新应用探索意愿强烈,频繁尝试各类网络服务与工具,在学术研究与创新中深度使用网络资源的同时,也可能引发网络安全风险。

(二)终端多样化,风险难评估

随着智慧校园的建设,高校网络逐步形成了有线无线一体化,网络终端不断增多,种类也越来越多样化。不同终端的操作系统、应用程序以及使用习惯等存在巨大差异。这些因素相互交织,因而出现风险难评估、预警告警难、追踪定位难等问题,使得准确评估整个校园网络面临的风险变得极为复杂。

(三)信息资产基数大,难管理

高校信息化资产规模庞大且层级多元,就校级层面部署的业务系统就有数百之多,同时各二级单位也大多自建独立网站。资产管理工作中也存在资产全生命周期数据动态掌握不足、安全风险评估支撑数据匮乏、责任主体信息管理碎片化等信息缺口,导致资产管理困难且安全风险难以评估。

(四)安全域管理粗放,难防护

多数高校已意识到安全域划分的重要性,并进行了一定程度的划分。然而,这种划分相对粗放,划分时较少从风险评估和业务流程角度进行细致分析,没有充分考虑到各区域内不同业务系统、应用的具体安全需求差异。当前高校在域间访问控制层面管理比较粗放。一旦外网被突破,内网情况便会完全暴露。

(五)纵深防御能力差,难响应

高校网络安全防护存在三重短板:一是过度依赖防火墙、入侵检测系统等边界设备,内部深度防护不足,攻击者突破边界后易渗透核心资源;二是区域安全策略执行不一致,易被攻击者利用差异绕过防护,削弱纵深防御效果;三是安全事件检测滞后、研判偏差、预案缺失及响应能力不足,导致无法快速有效处置。

三、高校网络安全防护设计需求

(一)全面的风险评估需求

高校网络环境时刻处于动态变化中,新应用上线、新设备接入、用户行为模式更迭等情况不断出现。鉴于此,必须对网络安全风险开展持续评估工作,从而及时洞察潜在安全威胁。评估范围需全面覆盖网络基础设施、数据资源、应用系统以及用户行为等各个层面,通过综合分析识别可能存在的风险点,为制定精准有效的防护策略筑牢根基。

收稿日期:2025-6-6
基金项目:本文系中国高校产学研创新基金项目"网络安全课程思政示范项目的探索和实践"(项目编号:2022HS006)成果。
作者简介:杨梦希(1981—),女,江苏无锡人,实验师,硕士,研究方向:计算机信息管理、网络安全管理。

(二)实时风险监测需求

实时监测网络活动的能力,涵盖网络流量、设备状态、用户行为及应用系统运行状况等。借助实时监测,能迅速捕捉异常,第一时间察觉安全隐患。

(三)多层次的防护架构需求

要构建坚实有力的防护屏障,制定严苛的访问控制规则。针对进出校园网络的流量,展开全面筛选与过滤工作,坚决阻挡外部恶意流量的入侵,同时杜绝校内敏感数据在未获授权的情况下流出。此外,精准划分不同区域、不同用户群体的网络访问权限,保证唯有经过授权的用户,才能够访问特定的网络资源。

(四)强大的数据安全需求

为契合数据保密性要求,针对学生个人信息、教师科研成果这类敏感信息,运用先进加密算法加密处理。如此一来,即便数据在传输时遭窃取,或是存储设备失窃,未经授权者也无法解读数据内容。同时,搭建数据完整性校验机制,定期校验数据,确保存储与传输过程中数据未被非法篡改。一旦察觉数据完整性受损,可即刻启动修复机制,让数据恢复至原始准确状态。

借助人工智能技术,搭建起一套集可发现、可预警、可联动、可溯源、可视化于一体的高校网络安全防护体系。使高校能够更全面、有效地应对网络安全威胁,保障校园网络的安全稳定运行,为高校的教学、科研、管理等各项工作提供有力支持。

四、高校网络安全运营防护体系整体框架设计

高校智能网络安全运营防护体系的整体架构,依托"统筹规划、立体防护、资产清晰、预测精准、主动防御、高效处置"的核心思路搭建。着重打造兼具前瞻性、兼容性与实效性的校园智能网络安全管理平台,通过整合组织架构、管理机制与技术支撑三大维度,构建覆盖全生命周期的智能防护体系。

高校网络安全运营防护体系建设遵循关键信息基础设施等级保护测评标准,开展网络资产普查、分类梳理及登记备案工作,实现资产状态动态监控。通过智能分析引擎自动识别安全隐患,建立攻击行为预警模型,构建多层级主动防御体系。同时配套完善的应急响应机制,确保网络威胁的快速发现、智能分析与协同处置。该体系通过整合管理流程与技术工具,实现资产底数透明化、风险防控精准化、应急响应流程化,全面提升校园网络安全运营能力,筑牢数字化校园安全防线。

五、基于人工智能的高校网络安全防护体系框架设计

依托人工智能构建的高校网络安全防护体系框架,运用分层架构模式,重点包含数据采集层、数据处理层、智能分析层、决策与响应层以及管理与监控层这五大层级。各层级紧密配合、相互协作,全方位守护高校网络安全,共同致力于实现对高校网络安全的高效、精准防护。

(一)数据采集层

通过部署网络探针、日志收集器等设备,对高校网络全域数据实施标准化采集:在校园网出口、核心交换机等关键节点布置探针抓取全流量数据;在服务器、终端设备安装轻量化采集代理,实时获取系统日志、设备运行状态数据、用户行为数据等,为后续的数据分析和防护决策提供充足的数据基础。

(二)数据处理层

数据处理层包含三个核心部分:首先,对原始数据进行清洗,通过系统性过滤冗余信息、异常值和错误数据,确保数据的准确性、完整性与一致性,提升数据质量;其次,对数据进行归一化处理,构建一个能够进行比较的标准化数据体系,为后续分析提供规范的数据基础;最后,通过深度解析清洗归一化后的数据,提取网络流量和用户行为等反映安全状态的核心特征要素,形成用于构建人工智能模型的关键特征向量。

(三)智能分析层

在网络安全分析中,需根据多样化需求选择适配的人工智能算法:监督学习适用于有标记数据场景,无监督学习针对无标记数据,而深度学习在处理复杂网络数据、捕捉序列特征方面优势显著。模型构建时,融合提取的网络流量与用户行为特征,通过长期监测统计建立正常流量基线模型。

(四)决策与响应层

决策响应层基于智能分析层输出的威胁类型、严重程度等结果,为安全响应提供决策依据。针对不同威胁等级与类型,系统可自动执行分级响应措施:对低风险威胁发送警报通知管理员;对中高风险威胁实施攻击源阻断、受感染设备隔离修复等操作,确保校园网安全运行。

(五)管理与监控层

管理监控层包含两大核心模块:管理层负责制定网络安全策略与决策,通过分析威胁检测层数据精准掌握安全态势,制定适配措施并定期评估防护效能,持续优化防护策略以应对动态威胁;监控层则将复杂安全数据转化为可视化界面,通过图形、图表等形式展示攻击类型分布、风险区域等关键信息,辅助管理人员理解威胁本质,为科学决策与优化安全资源配置提供直观依据。

六、应用实施

(一)构建实施

无锡商业职业技术学院以人工智能技术为核心驱动力,全面构建高校智慧化网络安全防护体系。通过系统性布局,建立起整合网络基础层、技术平台层、数据资源层、应用服务层及管理规范层的多层次防护框架,同步打造智能化运维中枢,实现安全威胁的自动化识别与响应。重点围绕"安全运营、合规管理、风险监测、数据治理、审计追踪"五大核心维度,深化全域网络安全能力建设,形成覆盖策略制定、标准执行、威胁处置、审计评估的全链条管理机制。通过构建高校网络安全防护体系平台,实现了安全策略的动态优化、合规流程的集约管理以及安全事件的闭环处置,显著提升了校园网络安全防御的智能化水平和协同响应效率。

1. 异构数据治理应用,消灭数据孤岛,整合安全要素

采用高效的数据采集技术,汇聚主机、安全设备、第三方系统及流量日志等安全数据。采集后,对这些安全数据进行归一化处理,并以可视化形式直观展现,以此提升对自身数据的认知,更易发现其中潜藏的安全问题,并构建分级存储架构实现数据统一管理与长期留存。

2. 集中安全要素管控,提升安全运营效率

安全服务平台作为核心枢纽,对已部署的边界防护、安全审计等设备进行统一管控。它向下对接安全基础资源,实现资源优化配置与高效利用;向上为安全管理中心及实体安全层提供全面优质服务,协助安全管理中心制定策略、评估风险等,构建起上下贯通、协同运作的安全保障体系。

3. 建设高级威胁溯源能力,提升安全事件调查取证

平台通过智能安全分析中枢,显著增强了对安全事件的溯源和调查能力。基于时间轴可视化、多维度数据标注等技术,对安全事件的发展进程与影响范围进行回溯。通过深度挖掘事件间的因果关系,还原完整攻击过程。

4. 建设安全编排与自动响应及时,提升安全运营能力

持续安全运营的核心目标是为信息化建设提供高效、专业的安全服务支撑。该体系以“主动防御—智能响应—持续进化”为核心理念。依托专业化安全运营团队,推动安全能力的动态演进。通过“监测预警—数据分析—威胁溯源—应急响应—信息共享”的全闭环管理流程,构建覆盖网络安全事件全生命周期的处置体系,有效提升安全防护与态势感知能力,实现安全运营价值的最大化。

5. 形成全局态势感知,辅助可视化安全决策

运用大数据技术全面掌握网络中的各类数据安全要素信息后,整合攻击路径、威胁来源、资产状态等关键维度,运用交互式图表动态呈现全局安全态势。依托数据驾驶舱式交互界面,实现威胁溯源追踪、风险态势评估与防护策略优化的一体化决策支持,有效提升安全事件响应效率与风险管控精准度。

(二)实施成效

1. 检测准确率提高

通过引入基于人工智能的网络安全防护体系,我校的网络安全检测准确率得到了显著提高。入侵检测系统和恶意软件检测系统可以自动识别出各种类型的网络攻击和恶意软件,有效保护了学校的网络安全。

2. 响应速度加快

人工智能系统通过智能分析引擎,可以对网络流量数据和系统运行参数实施动态监控,及时发现安全威胁,主动启用对应的防护措施。这使得我校对网络安全事件的响应速度大大加快,减少了网络安全事件对学校的影响。

3. 管理成本降低

基于人工智能的网络安全防护体系可以自动完成大部分的网络安全监测和防护工作,减少了对人力的依赖,因而我校的网络安全管理成本得到了降低。

4. 师生满意度提高

通过加强网络安全防护,我校的网络安全状况得到了明显改善,师生的个人信息安全得到了更好的保障,师生对学校的网络安全管理工作满意度获得提高。

七、结论与展望

(一)研究成果总结

本研究围绕基于人工智能的高校网络安全防护体系构建展开深入探讨,取得以下成果:证实了人工智能技术在高校网络安全防护体系建设中的关键作用和实施必要性;分析了高校网络安全现状,包括面临的挑战与风险以及防护的不足之处;创新性地构建了人工智能驱动的校园网络安全防护体系,并通过实证评估验证了该体系在实际应用中的有效性与可操作性。

(二)未来发展展望

人工智能技术的演进将持续驱动高校网络安全防护体系向智能化方向迭代。未来,人工智能技术将在安全策略自适应生成、威胁行为智能研判等核心防护环节展现更大价值。建议高校同步推进人工智能安全技术创新与学科交叉融合,着力构建“人工智能技术+网络安全”人才培养体系,为智能时代校园网络安全建设提供人才保障与技术储备。

参考文献:

[1]陈跃辉. 高校零信任网络安全体系建设实践与探讨[J]. 网络安全和信息化,2023(9):41-44.

[2]刘鹏飞,王铁柱,韩佳乐,等. 高校网络安全发展实践与研究[J]. 网络安全技术与应用,2022(3):86-87.

[3]高薇,许浩,宁玉文,等. 基于安全态势感知平台的高校网络 SOC 研究——以第四军医大学为例[J]. 计算机技术与发展,2018,28(1):150-154.

[4]郑阳,杜大运. 高职院校网络安全防护体系建设研究——以济南职业学院为例[J]. 济南职业学院学报,2023(4):15-19.

[5]陈敏锋. 高校网络安全运营防护体系研究[J]. 无锡商业职业技术学院学报,2022,22(6):108-112.

[6]姜海,董升来. 基于人工智能的电视台网络安全监测与预警系统构建[J]. 广播电视网络,2024,31(8):62-64.

[7]殷媛. 引入偏移量递阶控制的主动防护网络入侵防御方法的研究[J]. 中国宽带,2024,20(10):124-126.

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

YANG Meng-xi
(Wuxi Vocational Institute of Commerce, Wuxi Jiangsu 214000, China)

Abstract: With the ongoing digital transformation in education, universities are shifting from traditional to digital modes of administration, teaching and research. This deep integration has significantly increased reliance on digital infrastructure, making secure, stable, and efficient network systems a priority for smart campus development. AI technologies provide innovative approaches to cybersecurity. This study explores the construction of AI-driven campus cybersecurity systems by analyzing current challenges, leveraging AI's technical strengths, and proposing a framework for intelligent threat detection, adaptive response, and automated management in higher education networks.

Key words: artificial intelligence; network security; protective system　　(责任编辑:桂杉杉)