人工智能技术在高校学生网络安全防护中的应用研究

闫宝多
北京邮电大学，北京 100876
DOI: 10.61369/TACS.2025100016

摘　　要： 随着数字化校园建设的持续深入，高校学生网络安全防护工作面临着前所未有的挑战，传统防护手段已难以应对复杂多变的网络安全威胁。人工智能技术拥有强大的数据处理以及自适应学习能力，这也为高校学生网络安全防护提供了全新的解决方案。鉴于此，文本将针对人工智能技术在高校学生网络安全防护中的应用展开分析，并提出一些策略，仅供各位同仁参考。

关 键 词： 人工智能；高校；学生网络安全；防护策略

Research on the Application of Artificial Intelligence Technology in the Network Security Protection of College Students

Yan Baoduo
Beijing University of Posts and Telecommunications, Beijing 100876

Abstract: With the continuous advancement of digital campus construction, the network security protection work for college students is facing unprecedented challenges, and traditional protection methods are no longer sufficient to cope with complex and ever-changing network security threats. Artificial intelligence (AI) technology, endowed with powerful data processing and adaptive learning capabilities, provides a brand-new solution for the network security protection of college students. In view of this, this paper analyzes the application of AI technology in the network security protection of college students and puts forward relevant strategies for reference only.

Keywords: artificial intelligence (AI); colleges and universities; college students' network security; protection strategies

一、人工智能技术在高校学生网络安全防护中的应用研究的意义

（一）有利于更好的应对高校网络安全威胁

在数字化时代，高校已成为网络信息的重要集散地，学生作为网络使用的活跃群体，他们的网络行为呈现出多样化、个性化和复杂化的特点。传统的网络安全防护手段主要依赖于静态规则和人工干预，对于一些新型、变异的网络威胁响应滞后，这样就很难实现全方位、实时性的防护[1]。人工智能技术能够通过对海量网络数据的实时分析和挖掘，帮助教师更为快速的识别潜在的安全威胁，还可使其提前预警并及时处置，这样可以有效弥补传统防护手段的不足，为高校学生构建更加坚固的网络安全防线。

（二）有利于推动数字化校园建设的重要支撑

数字化校园建设是高校教育现代化的重要标志，涵盖了教学、科研、管理、服务等各个领域，而网络安全是数字化校园建设的前提和保障。随着在线教学、智慧校园管理系统、科研数据共享平台等数字化应用的广泛普及，高校网络承载的数据量急剧增加，数据类型也更加复杂，对网络安全防护的要求越来越高。人工智能技术能够与数字化校园建设深度融合，通过对教学科研数据、学生行为数据、校园网络运行数据的智能分析，实现对网络安全风险的精准识别和动态防控，保障数字化校园应用的安全稳定运行[2]。同时，人工智能技术在网络安全防护中的应用，还能够推动高校网络安全技术的升级换代，提升高校信息化建设的整体水平。

（三）有利于提升学生网络安全素养的有效途径

高校是培养人才的重要阵地，提升学生的网络安全素养也是高校素质教育的重要内容。在传统的网络安全教育中，教师主要采用课堂讲授、专题讲座等方式，整体的形式较为单一，学生的参与度不高，这样会对教育效果产生很大影响。人工智能技术可以为学生网络安全教育提供新的载体和方法，可以让学生在模拟环境中体验网络攻击与防护的过程，这样可以大幅增强学生的实践能力[3]。此外，人工智能技术在网络安全防护中的实际应用也能够让学生直观感受网络安全的重要性，从而更为高效地激发学生学习网络安全知识的积极性和主动性，全面提升他们的网络安全素养。

二、当前高校学生网络安全防护存在的问题

（一）防护技术滞后，难以应对新型威胁

现阶段，很多高校的网络安全防护体系仍以传统的防火墙、防病毒软件等技术为主，这些技术主要基于已知的攻击特征和规则进行防护属于“被动防御”模式。随着人工智能技术的发展，

网络攻击手段也日益智能化、隐蔽化，比如，人工智能技术相关的恶意软件能够自动变异规避检测，钓鱼攻击能够结合目标用户的信息进行个性化定制，这些新型网络威胁往往没有固定的攻击特征，传统防护技术难以有效识别和拦截[4]。同时，高校网络边界逐渐模糊，学生通过移动设备、校外网络接入校园网络的场景越来越普遍，这样也会导致传统的边界防护技术难以覆盖所有接入终端和网络节点。

（二）数据安全管理薄弱，隐私泄露风险突出

现阶段，高校在教学、科研和管理过程中积累了大量的学生数据，主要包括学生的个人基本信息、消费记录以及健康信息等，这些数据蕴含着极高的价值，这也使其成为了网络攻击者的重点目标。当钱，很多高校在学生数据安全管理方面存在诸多问题，比如，一些高校缺乏专门的安全数据存储平台，学生数据通常会分散存储在各个部门的服务器中，同时，这些存储设备的安全防护措施不足，这样会导致其很容易遭受攻击[5]。不仅如此，一些学校的数据访问权限混乱，他们并没有建立一个严格的权限管理机制，不同部门、不同人员的访问权限划分不清晰，这样就存在一定的越权访问和数据滥用的风险，不仅如此，一些学生缺乏数据安全意识，他们会在网络上泄露个人信息，这样也会进一步增加隐私泄露的风险。

（三）安全预警能力不足，应急响应效率低下

网络安全防护的关键在于“早发现、早预警、早处置”，但是，当前多数高校的网络安全预警能力严重不足。实际上，高校对于网络中产生的海量日志数据、流量数据等缺乏有效的分析手段，相关的管理人员也很难从海量数据中挖掘出潜在的安全威胁，他们往往在安全事件发生后才能察觉，这样会导致其错失了最佳的处置时机。同时，高校也缺乏一个更为完善的安全预警机制，他们并没有建立一个更为科学的风险评估指标体系，这样会导致其无法对网络安全风险进行量化评估和分级预警，管理人员也对网络安全态势的掌握不够全面和准确[6]。在应急响应方面，多数高校虽然制定了网络安全应急预案，但相应的预案缺乏针对性和可操作性，同时，学校的相关人员也缺乏定期的应急演练，在发生重大网络安全事件时管理人员往往不知所措，这样也会导致安全事件造成的损失扩大。

三、人工智能技术在高校学生网络安全防护中的应用策略

（一）构建智能防护体系，提升主动防御能力

为提升人工智能技术在高校学生网络安全防护中的应用效果，我们可以尝试利用人工智能技术构建智能化的网络安全防护体系，这样可以有效实现从“被动防御”向“主动防御”的转变。为此，我们可以尝试采用智能防火墙技术，通过机器学习算法对网络流量进行实时分析，识别正常流量与异常流量的特征，这样能够有效拦截新型的网络攻击。和传统防火墙相比，智能防火墙能够根据网络环境的变化自适应更新防护策略，这对提高对未知攻击的识别率有极大促进作用[7]。此外，我们还可部署智能入侵检测与防御系统，利用深度学习算法对网络中的入侵行为进行建模，通过对网络数据包、日志数据的实时监测和分析，可以让相关工作人员更为快速的发现潜在的入侵行为并自动采取阻断、隔离等防御措施。同时，这一系统还能够通过不断学习新的入侵模式，提升自身的防护能力。不仅如此，我们还可尝试引入智能防病毒软件，这一软件可以基于人工智能技术对恶意软件的行为特征进行分析，即使恶意软件经过变异也能够通过其行为模式识别出来，从而更为有效的实现对恶意软件的精准检测和清除。

（二）强化智能数据管理，保障学生隐私安全

为保证人工智能技术在高校学生网络安全防护中的应用效果，我们应进一步强化对数据的管理，我们可以尝试借助人工智能技术加强对学生数据的全生命周期管理，这样可以更为有效的防范数据泄露风险。在实践方面，我们可以尝试构建一个智能数据存储平台，通过区块链、加密技术等对学生数据进行安全存储，同时，我们还可利用人工智能技术对存储设备的运行状态进行实时监测，这样可以更为及时的发现并修复存储系统中的安全漏洞。通过智能分类算法，我们可以实现对学生数据进行分类分级管理，对一些敏感数据，我们可以通过采取加密存储、访问控制等方式对数据展开更加严格的防护措施。我们还可建立一个智能权限管理系统，基于角色的访问控制模型，结合人工智能技术对用户的身份信息、行为特征进行分析，这样可以自动为不同部门、不同人员分配合理的访问权限[8]。同时，这一系统能够实时监测用户的访问行为，在发现越权访问、异常访问等情况时可以自动触发预警并阻断访问。为提升人工智能技术在高校学生网络安全防护中的应用效果，我们可以尝试引入智能数据传输安全技术，在学生数据传输过程中采用人工智能驱动的加密算法对相关数据进行加密处理，同时利用智能认证技术对传输双方的身份进行验证，这样可以有效确保数据传输的安全性和完整性。

（三）搭建智能预警平台，提高应急响应效率

在人工智能技术在高校学生网络安全防护中的应用实践中，我们可以利用人工智能技术搭建一个网络安全智能预警平台，这样可以实现对网络安全风险的精准预警和快速处置。为此，我们可以尝试建立一个智能数据分析中心，这样可以更为高效的整合校园网络中的日志数据、设备数据等多源数据，而后通过大数据分析和机器学习算法对这些数据展开更深入挖掘，识别其中的网络安全风险的特征和规律，构建一个更为合理、科学的风险评估模型。此外，我们还可开发一个智能预警推送系统，根据风险等级和预警信息的类型自动将预警信息推送给相关的管理人员和学生[9]。对于那些高风险预警信息，系统能够通过短信、电话等多种方式实时推送，这样可以确保管理人员能够及时收到并采取处置措施。对于针对学生的预警信息，系统能够直接推送给相关学生并提醒他们注意防范。我们还应构建一个智能应急响应系统，基于人工智能技术对网络安全事件进行智能分析，这样可以更好的判断事件的类型、规模和影响范围，而后可以自动生成一个应急处置方案。

（四）建立智能协同机制，明确责任分工

在人工智能技术在高校学生网络安全防护中的应用活动中，

我们可以利用人工智能技术建立多部门协同、内外联动的网络安全防护机制，进一步明确各主体的责任分工。为保证实践工作的效果，我们可以打造一个智能协同管理平台，积极整合教务处、学生处等多个部门的网络安全相关数据，而后以此为基础建立一个信息共享机制，这样可以更为高效的实现各部门之间的信息实时传递和交流。通过智能协同管理平台，各部门能够及时了解网络安全态势，协同开展防护工作。在人工智能技术在高校学生网络安全防护中的应用工作中，我们要进一步明确各部门的职责分工，通过智能协同管理平台对各部门的网络安全工作进行量化考核和监督，这样可以确保各部门切实履行防护职责。信息中心主要负责网络安全技术防护、智能平台建设和维护，学生处则负责学生网络安全教育、异常行为干预和安全事件善后处理，保卫处主要负责网络安全事件的调查处理和与公安机关的联动配合[10]。不仅如此，我们还需加强与外部机构的合作，学校可以结合实际情况与网络安全企业、公安机关等建立智能联动机制，而后可以通过数据共享、技术合作等方式提升网络安全防护水平。例如，学校可以与网络安全企业合作开展网络安全技术研发和漏洞挖掘，与公安机关共享网络安全预警信息，共同打击网络犯罪行为。

参考文献

[1] 王志翔 . 基于人工智能的网络安全研究 [J]. 中国宽带 ,2024,20(12):43-45.

[2] 曾羽 . 基于人工智能的网络安全渗透测试系统研究 [J]. 电子元器件与信息技术 ,2024,8(12):175-177+181.

[3] 高洁 . 基于人工智能的网络安全防护策略研究 [J]. 信息与电脑 ,2024,36(23):98-100.

[4] 蔡俊 . 人工智能背景下公共图书馆网络安全防护的挑战与对策研究 [J]. 无线互联科技 ,2024,21(22):125-128.

[5] 魏敏 . 基于人工智能的计算机网络信息安全防护模式研究 [J]. 信息记录材料 ,2024,25(11):130-132.

[6] 姚仕聪 . 人工智能在移动通信网络安全防护中的应用 [J]. 中国新通信 ,2024,26(20):13-15+19.

[7] 孙鹏 . 基于人工智能的计算机网络安全防护技术研究与实践 [J]. 中国高新科技 ,2024,(19):28-30.

[8] 胡丰 , 马月姣 , 陈川 . 人工智能技术在大数据网络安全防御中的研究探索 [C]// 中国水力发电工程学会梯级调度控制专业委员会 . 中国水力发电工程学会梯级调度控制专业委员会 2024 年年会论文集 . 华能澜沧江水电股份有限公司集控中心 ; ,2024:179-182.

[9] 王俊岭 . 网络安全防护迎来新需求 [N]. 人民日报海外版 ,2024-08-07(011).

[10] 袁超 . 基于人工智能技术的高校智能网络安全防护系统设计 [J]. 网络安全和信息化 ,2024,(08):53-55.

