第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

人工智能在网络安全威胁识别与防御中的应用

招吉润
泰山科技学院
DOI:10.12238/acair.v2i4.10284

[摘　要] 人工智能在计算机网络安全中展现显著效能,通过高级算法强化威胁识别与防御能力。在威胁识别方面,它精准检测恶意软件、监控异常流量、识别钓鱼攻击,有效预警潜在风险。防御层面,人工智能助力自动化渗透测试,提前暴露系统弱点；优化安全运营流程,提升响应速度；加强身份识别与认证机制,确保访问安全。这些应用共同构筑了更加智能、高效的网络安全防线。
[关键词] 人工智能；计算机网络安全；威胁识别与防御
中图分类号：Q143+.3　文献标识码：A

Application of artificial intelligence in network security threat identification and defense

Jirun Zhao
Taishan University of Science and Technology

[Abstract] Artificial intelligence has demonstrated remarkable effectiveness in computer network security, strengthening threat identification and defense capabilities through advanced algorithms. In terms of threat identification, it accurately detects malware, monitors abnormal traffic, identifies phishing attacks, and effectively alerts potential risks. At the defense level, artificial intelligence helps automate penetration testing to expose system weaknesses in advance; Optimize security operation processes to improve response speed; Strengthen the identity identification and authentication mechanism to ensure access security. Together, these applications build a more intelligent and efficient network security defense.
[Key words] artificial intelligence; Computer network security; Threat identification and defense

计算机网络安全是保障信息系统正常运行、保护数据完整性和机密性的重要基础。然而,随着网络环境的复杂化,传统的防御手段已难以满足日益增长的安全需求。人工智能以其强大的数据处理能力、学习能力和自适应能力,为网络安全领域带来了革命性的变化。

1 人工智能在威胁识别中的应用

1.1恶意软件检测

恶意软件,这一潜伏在数字世界中的隐形威胁,时刻威胁着网络安全与数据安全的稳定。作为网络安全领域的头号公敌,恶意软件以其多变的形态和狡猾的手段,不断挑战着传统的防御机制。然而,随着人工智能技术的飞速发展,尤其是机器学习和深度学习的崛起,恶意软件的检测与防御迎来了新的曙光。人工智能以其强大的数据处理和模式识别能力,为恶意软件检测提供了前所未有的解决方案。通过运用复杂的算法和模型,人工智能能够深入分析恶意软件的行为模式、代码结构以及网络活动轨迹,从而揭示其本质特征和潜在威胁。这些模型不仅能够对已知的恶意软件变种进行准确识别,更能在面对新型和变异恶意软件时,展现出卓越的适应性和学习能力。在深度学习技术的加持下,恶意软件检测模型的性能得到了显著提升。卷积神经网络(CNN)和循环神经网络(RNN)等先进模型,能够自动从海量数据中提取并学习复杂的特征表示,进而实现对恶意软件的精准分类和识别。CNN擅长于捕捉图像或二进制文件中的局部特征和纹理模式,这对于分析恶意软件的代码结构和行为模式至关重要；而RNN则擅长于处理序列数据,能够有效捕捉恶意软件在时间维度上的行为变化和网络活动轨迹,从而揭示其潜在的恶意意图。通过综合运用这些深度学习技术,恶意软件检测系统能够在极短的时间内对大量软件进行扫描和分析,迅速识别并隔离潜在的恶意威胁。这种高效且精准的检测能力,不仅极大地提高了网络安全防护的效率和水平,更为用户和企业提供了更加安全可靠的网络环境。

1.2异常流量检测

网络流量分析,作为网络安全领域的核心工具之一,其重要性不言而喻。在浩瀚的数据洪流中,网络流量承载着信息交流的使命,同时也潜藏着未知的安全威胁。为了有效应对这些威胁,人工智能技术的引入为网络流量分析注入了新的活力与智慧。通过深度挖掘网络流量的内在特征,人工智能能够构建起一套高

效且智能的异常流量检测机制。这一机制不仅依赖于对正常流量模式的深入理解,更在于对异常流量特征的敏锐捕捉。AI利用先进的异常检测和行为分析算法,对实时网络流量进行全方位、多角度的审视,从中筛选出与正常流量模式显著不符的流量样本。这些异常流量,可能是恶意软件的隐蔽传输、DDoS攻击的前兆、或是未经授权的访问尝试等,它们无一不构成对网络安全的潜在威胁。然而,在人工智能的助力下,这些威胁无所遁形。一旦异常流量被识别出来,AI将立即触发警报系统,通知安全团队采取相应的防御措施。这种自动化的威胁检测能力,极大地缩短了从威胁发现到响应的时间间隔,为安全团队争取了宝贵的应对时间。另外,人工智能还具备持续学习和优化的能力。通过不断分析新的网络流量数据和威胁案例,AI能够不断完善其检测模型和算法,提高异常流量检测的准确性和效率。这种自我进化的特性,使得人工智能在网络安全领域的应用更加广泛和深入。

表1 异常流量检测数据示例

指标	描述/数值
总流量	100GB
正常流量占比	99% (99GB)
异常流量占比	1% (1GB)
AI前异常流量检测准确率	70%
AI后异常流量检测准确率	95% 以上
威胁响应时间(AI前)	数小时至更长
威胁响应时间(AI后)	几分钟至秒级
算法模型优化周期	每月一次
安全事件减少率	50% 至 80%
成本效益分析(每年)	AI系统投资的数倍至数十倍节省

1.3钓鱼攻击识别

钓鱼攻击,作为网络安全领域中的一种常见且狡猾的威胁手段,常常利用人性的弱点和社会工程学技巧,诱导用户点击恶意链接或下载恶意附件,进而窃取敏感信息或执行恶意操作。为了有效抵御这一威胁,人工智能技术的运用显得尤为关键。自然语言处理(NLP),作为人工智能的一个重要分支,为钓鱼邮件的识别提供了强大的技术支持。通过深入分析邮件内容的文本信息,NLP技术能够识别出钓鱼邮件中常见的异常词汇、语法结构和表述方式。这些异常特征往往与正常邮件存在显著差异,如拼写错误、语法不通、紧急或威胁性的语气等,都是钓鱼邮件的典型标志[1]。AI利用NLP算法对这些特征进行精准识别,能够迅速筛选出可疑的钓鱼邮件,为后续的防御措施提供有力支持。除了对邮件内容的分析外,人工智能还具备学习用户行为模式的能力。通过持续监测用户在日常工作中处理邮件的行为习惯,如打开邮件的时间、阅读时长、点击链接的频率等,AI能够建立起用户的正常行为轮廓。一旦用户的邮件处理行为出现异常,如短时间内大量打开或点击来自未知发件人的邮件,AI便能立即察觉到这种变化,并判断其可能受到了钓鱼攻击的影响。基于这种对用户行为的深入理解,人工智能能够实施更加精准的防御策略。当识别出潜在的钓鱼攻击时,AI可以自动触发警报系统,提醒用户注意邮件的安全性;还可以采取进一步措施,如暂时隔离可疑邮件、限制邮件中的链接和附件的访问权限等,以防止恶意代码的执行和信息的泄露。

2 人工智能在防御措施中的应用

2.1自动化渗透测试

自动化渗透测试,作为现代网络安全领域的一项重要技术革新,正逐步成为保障系统安全性的关键手段。这一过程巧妙地融合了人工智能(AI)的智慧与自动化技术的效率,模拟出黑客可能采取的多种攻击路径和策略,从而对目标系统进行全面而深入的安全评估。在自动化渗透测试中,AI技术发挥着核心作用。通过训练机器学习算法,系统能够智能地分析目标系统的结构、配置及运行状况,自动生成并执行一系列复杂的攻击脚本和测试用例。这些测试不仅覆盖了常见的安全漏洞和弱点,还能探索未知的、潜在的威胁面,从而确保测试的全面性和深入性。与传统的手动渗透测试相比,自动化渗透测试展现出了显著的优势。首先,在效率方面,自动化测试能够大幅度缩短测试周期,减少人工干预,使安全评估工作更加高效快捷[2]。其次,在精准度上,AI驱动的测试工具能够基于大数据分析和模式识别技术,更准确地定位系统中的安全漏洞,减少误报和漏报的情况。此外,自动化渗透测试还能提供详细的测试报告和修复建议,帮助系统管理员快速响应并修复发现的问题,从而有效提升系统的整体安全性。随着技术的不断进步和应用的深入推广,自动化渗透测试将在网络安全领域发挥越来越重要的作用。它不仅能够为企业和组织提供更加可靠的安全保障,还能促进网络安全技术的创新和发展,为构建更加安全、可信的网络环境贡献力量。

2.2安全运营优化

安全运营,作为维护网络空间安全稳定的重要基石,其效率与准确性直接关系到企业的业务连续性和数据安全性。在这个背景下,人工智能(AI)技术的引入为安全运营带来了革命性的变革,极大地优化了安全运营流程,提升了整体防护能力。首先,AI以其强大的数据处理和分析能力,为安全分析人员提供了前所未有的支持。面对海量且复杂的安全数据,AI能够迅速捕捉关键信息,识别异常行为模式,从而快速发现潜在的安全事件。这一自动化过程不仅极大地减轻了分析人员的工作负担,还显著缩短了安全事件的响应时间,使得企业能够更早地介入并控制事态发展。进一步地,AI还能够自动完成安全事件的分析和初步

响应工作。通过深度学习、模式识别等先进技术,AI能够对安全事件进行深度剖析,提取出有价值的情报信息,如攻击来源、攻击手法、影响范围等。同时,AI还能根据预设的响应策略,自动执行一系列防御措施,如阻断攻击路径、隔离受感染设备、启动应急响应流程等,有效遏制安全事件的扩散和恶化。除了直接参与安全事件的处置外,AI还能够在安全知识库的建设和维护中发挥重要作用。通过建立和维护一个全面的安全知识库,AI能够整合来自各个渠道的安全漏洞信息、攻击手法和防御策略,形成一套完整的安全知识体系。这一知识库不仅为安全分析人员提供了及时、准确的参考信息,还能够帮助他们更好地理解当前的安全态势,制定更加有效的安全策略。

表2 人工智能安全运营的效率和准确性数据

指标/数据项	描述/数值
AI前异常流量检测准确率	7%
AI后异常流量检测准确率	90% 以上
安全事件响应时间缩短	从数小时缩短至几分钟至秒级
自动化分析与初步响应率	80% 以上
安全知识库更新频率	高频更新(取决于新威胁出现速度和AI学习能力)

2.3身份识别与认证

身份识别与认证,作为网络安全防护体系中的第一道防线,其重要性不言而喻。在数字化时代,随着网络空间的日益开放和互联,确保用户身份的真实性和合法性成为了维护网络安全、保护个人隐私的关键环节。而人工智能技术的引入,则为身份识别与认证领域带来了革命性的变革,极大地提升了认证的精确度和安全性。人工智能技术通过融合多种先进的生物识别和行为分析技术,为用户身份认证提供了更为丰富和可靠的验证手段[3]。其中,人脸识别技术以其非接触、高精度的特点,成为了身份认证领域的佼佼者。通过深度学习算法对人脸特征进行精准提取和比对,AI能够在极短的时间内完成用户身份的验证,有效防止了冒名顶替等欺诈行为的发生。例如,苹果公司的Face ID技术,就是基于人脸识别原理开发的一项创新应用,它不仅提高了手机解锁的便捷性,还显著增强了设备的安全性。除了人脸识别外,声纹识别也是AI在身份认证中的一项重要应用。每个人的声音都是独一无二的生物特征,声纹识别技术正是利用这一特性来验证用户身份。通过采集用户的语音样本,并对其进行特征提取和比对,AI能够准确识别出用户的声纹信息,从而实现高效的身份认证。这种技术不仅适用于手机、电脑等智能终端设备,还广泛应用于金融、政务等需要高安全性认证的场景。另外,行为分析技术也是AI在身份认证中不可或缺的一环。通过分析用户在使用设备或访问系统时的行为习惯、操作模式等信息,AI能够构建出用户的行为轮廓,并实时监测用户的操作行为。一旦发现异常行为,如异常登录地点、异常操作时间等,AI将立即触发警报,并采取相应的防御措施,从而有效防止身份盗用和欺诈行为的发生。

3 结语

人工智能在计算机网络安全中发挥着核心作用,从威胁识别到防御措施,均展现出其无可替代的价值。通过精准识别恶意软件、异常流量及钓鱼攻击,AI有效遏制了安全威胁的蔓延。同时,自动化渗透测试、安全运营优化及身份识别与认证等防御措施,进一步巩固了网络安全防线。未来,随着AI技术的不断进步,计算机网络安全将更加稳固可靠。

[参考文献]

[1]吴越,唐志辉.人工智能技术在网络安全防御中的应用[J].集成电路应用,2023,40(08):264-265.

[2]邓玉,宋良,孙剑.基于人工智能技术的计算机网络安全防御系统设计[J].无线互联科技,2023,20(14):147-149.

[3]李凤鸣.基于大数据及人工智能技术的计算机网络安全防御系统[J].电子技术与软件工程,2022,(17):1-4.

作者简介：

招吉润(2002--),男,汉族,山东省青岛市人,本科在读,研究方向：计算机网络安全、人工智能。