

# 大数据网络安全防御中人工智能技术的运用分析

吴楚洲

(广东省外语艺术职业学院, 广东 广州 510640)

**摘要:** 随着大数据技术的不断发展, 网络安全防御体系也不断改革。由于大数据环境下, 网络攻击手段不断演变, 因此人们也在不断探索融入新的技术, 打造新的网络安全防御体系。人工智能技术与大数据的融合是目前网络安全防御体系建设所依赖的重要技术能力, 具有更强大的数据处理能力和模式识别能力, 提供新的网络安全维护方案。本文对大数据网络安全防御中人工智能技术的运用展开分析, 分别讨论了大数据与网络安全的概念、大数据网络安全防御中人工智能技术的主要优势和具体应用, 希望能够为新时期网络安全防御体系建设提供有价值的参考。

**关键词:** 大数据; 网络安全; 人工智能; 防御策略

在信息化时代, 数据量呈爆炸性增长, 为各行各业发展带来了新的机遇和挑战。在网络安全领域, 数据量的激增和网络系统的升级使得网络安全防御工作越来越复杂。网络安全防御体系只有不断升级才能应对快速变化的网络威胁。人工智能技术具有强大的学习能力和数据处理能力, 为网络安全防御建设提供了新的视角和工具, 其应用于网络安全防御体系建设中, 能够通过其强大的学习和识别能力识别潜在的安全威胁, 还可以自动调整防御策略以抵抗潜在的威胁。下文对大数据网络安全防御中人工智能技术的运用展开分析。

## 一、大数据与网络安全概述

### (一) 大数据定义与特点

大数据指数据的规模、处理速度、多样性和复杂性方面远超传统数据的一种数据集合, 大数据技术是指对海量数据进行记录、存储、分析和应用的数字技术。大数据具有数据体量巨大、处理速度快、数据种类繁多、价值密度低但潜在价值高、复杂性高、可扩展性强等特点。

### (二) 人工智能技术

人工智能依托于计算机技术和互联网, 参照人脑活动的规律模拟人类的思想, 其应用的技术原理较为多样化, 包含生物学、语言学、运动学等多方面的内容, 呈现出人性化、智能化的特点。人工智能是信息技术深度发展的产物, 其应用范围较广泛, 具有广阔的发展前景。当前, 人工智能在安全管理、信息检索、控制系统等领域都有一定程度的应用。

### (三) 网络安全的基本概念

网络安全包括确保数据保密性、完整性和可用性; 高效开展身份验证、授权控制; 保障数据传输的加密性; 高效开展入侵检测与防御识别安全威胁; 风险评估确定保护优先级。网络安全防御体系是指通过一系列措施保护网络、数据和设备免受未经授权的访问、攻击或破坏, 确保网络信息的安全性和业务的连续性, 维护网络环境的稳定性和信任度, 保障信息的安全性和业务的连续性。

### (四) 大数据对网络安全的影响

大数据从多维度影响网络安全, 它所带来庞大的数据资源为网络安全带来了新的威胁, 使得数据泄露、用户身份检测、数据存储、数据处理等难度增大, 网络安全体系建设需要更先进的技术和策略。依托于大数据技术, 网络安全领域逐步探索应用人工智能技术和机器学习识别潜在威胁并自动抵御外部入侵。

## 二、大数据网络安全防御中人工智能技术的主要优势

利用人工智能技术, 网络安全防御体系发展出了威胁自动化识别、系统持续学习与自动更新能力, 增强了新攻击模式的适应能力, 提高了大数据处理能力, 为应对大数据背景下不断升级的

网络威胁提供了较为坚实的保障。在大数据网络安全防御体系中应用人工智能技术提升了对外部攻击的响应速度, 使得安全防护体系更为主动和智能。

### (一) 自动化的威胁识别能力

人工智能技术依托于复杂的算法对访问行为进行分析, 进而识别非法访问和异常模式, 有效提高了威胁检测的速度和准确性。相较于传统的依托于签名的检测方法, 人工智能技术并不依托于特定签名, 而是基于机器学习做出分析和检测, 将非法访问识别, 拦截未知攻击和变种恶意软件。此外, 基于人工智能技术自动化的响应机制保障了系统在检测到威胁时自动开启拦截行为, 隔离恶意流量、更新防火墙规则, 自动化处理使得系统运行效率更高、响应速度更快。上述优势让人工智能技术成为网络安全防御体系中不可缺少的重要支撑性技术, 为网络安全提供了坚实的保障。

### (二) 持续学习与适应新攻击模式的能力

因为人工智能技术能够持续学习进而可以有效适应新攻击模式。基于人工智能技术, 网络安全防御体系持续性地在数据和攻击中学习, 进而优化算法, 将各类新的攻击行为和恶意软件拦截在外。依托于人工智能技术的自适应学习机制使得系统能够预测攻击行为的变化, 并提前调整防御策略, 提高对高级持续性威胁 (APT) 和零日攻击的防御能力。同时, 伴随着数据的积累和模型的优化, 基于人工智能技术的网络安全防御体系将累积更多威胁情报, 进而增强识别和应对复杂攻击模式的精准性和效率。人工智能技术所具备的持续优化性能保证了网络安全防御体系可以随着网络威胁的发展而发展, 使得长期的安全防护得以实现, 让网络安全防御工作动态化、智能化和前瞻化。

### (三) 高效的大数据处理能力

人工智能技术结合大数据技术强大的数据处理能力, 让网络安全防御得到了革命性的改革。依托于大数据处理能力, 人工智能系统快速识别出复杂的攻击和异常行为并展开分析和处理, 达到高精度、自动化威胁检测和处理。这种强大的数据处理能力使得网络安全防御体系从被动防御向主动识别转变, 使得系统得以及时响应各种复杂的网络攻击。网络安全防御体系所拥有的强大的数据处理和分析能力有效保障了网络环境的稳定性和安全性。

## 三、人工智能技术在网络安全中的应用分析

### (一) 入侵检测系统

基于大数据技术和人工智能技术打造的入侵检测系统 (IDS) 可实现对网络流量的实时监控, 它通过机器学习和深度学习算法对网络流量展开实时监控和分析, 学习网络行为模式, 并建立行为模型。当系统检测到与行为模型存在显著差异的行为模式或与已知攻击模式匹配的流量, 系统会发出警报。基于机器学习生成的自适应能力保证了网络安全防御系统能够持续更新数据和建立

模型,进而有效识别网络攻击。这也是新时期大数据网络安全防御体系中人工智能技术应用的典型代表。

#### (二) 恶意软件识别

基于人工智能技术,系统搭建起机器学习模型,通过复杂算法对软件行为展开分析,进而实现对恶意软件行为的早期识别和防御。这种机器学习模型首先对大量恶意软件样本展开训练,学习其基本行为特征和模式,之后学习模型才能对系统中出现的各类恶意软件和零日威胁展开识别。因为机器学习模型具备持续学习能力,因此其可以不断更新样本以适应新的恶意软件操作者的新攻击策略。除了搭建机器学习模型进行恶意软件识别外,依托于人工智能技术网络安全防御系统还能够对网络流量和用户行为展开分析,进而识别出潜在的恶意软件传播渠道并调整策略进行防御。在检测到恶意软件后,基于人工智能技术,系统还可以自动对恶意软件进行隔离和防御,以防止其进一步传染。这种智能化的恶意软件识别技术,显著提高了网络安全防护的效率和准确性。

#### (三) 钓鱼攻击识别

基于人工智能技术,系统还可以有效识别钓鱼邮件和网站,防止用户上当受骗。这主要是通过自然语言处理技术(NLP)和机器学习算法对诸如电子邮件、网站链接、文件等展开分析,识别出其钓鱼企图。机器学习模型针对钓鱼邮件展开训练,分析其典型特征,之后对系统中可疑的发件人地址、语法错误、不寻常的链接以及试图诱导用户泄露敏感信息的语言模式进行识别,将钓鱼行为识别出来并加以标记和隔离,防止用户点击或下载。面对钓鱼模式,人工智能技术的机器学习模型也可以持续更新以识别新的钓鱼模式和技巧。这种智能化的钓鱼攻击识别可以大大降低用户上当受骗的几率。

#### (四) 垃圾检测技术

网络空间管理是网络安全的重要保证。网络空间管理一方面拦截垃圾信息,另一方面维护网络秩序。在网络空间管理工作中引入人工智能技术,可以自动化检测垃圾邮件,对垃圾邮件进行安全隔离。智能化反垃圾邮件系统能够实现24小时全天候自动化检测,让检测实时化、动态化,为网络安全防护工作提供技术保障。针对一些顽固垃圾信息,人工智能技术能够对信息技术进行跟踪检测,高效解决垃圾信息,彻底屏蔽信息。

#### (五) 安全态势感知

当前在网络安全态势感知领域,人工智能技术必不可少。基于人工智能技术,系统可以实现对网络安全数据的分析和关联。首先,系统通过利用机器学习和深度学习算法对网络浏览数据、网络流量、用户行为、系统日志等展开分析,建立基本模式,对与基本模式存在显著偏差的模式进行标注,从而提供全面的网络安全态势感知。此类网络安全态势感知让用户得以实时了解网络系统中的用户活动,对系统的安全性进行评估。依托于人工智能技术,系统跨不同数据源对数据关联分析,让分散的信息整合起来,使用户得以纵览全局,全面分析系统的安全性和可靠性。这包括识别潜在的攻击向量、评估系统脆弱性以及监测可疑行为。

总而言之,基于人工智能技术的网络安全防御系统通过数据分析和智能关联搭建起网络安全态势感知能力,有力保障了网络系统的安全性和稳定性,是保护网络安全的关键技术之一。

### 四、人工智能技术在网络安全防御中的挑战

从本文的分析可以看出,人工智能技术在网络安全防御中有非常多的优势,但也面临着一些挑战。

#### (一) 数据采集和隐私保护

尽管人工智能技术应用于网络安全防御体系显现出强大的数

据处理和威胁识别能力,但同时也带来了数据采集和隐私保护方面的挑战。因为人工智能技术的机器学习、神经网络建设等需要大量数据展开训练,如果此环节数据训练的管理不规范,就可能导致隐私泄露和数据滥用问题。因此,如何确保人工智能技术性数据的合法采集、存储和使用,保护用户隐私权益,是人工智能技术在网络安全领域应用需要面对和解决的重要问题。这要求相关企业和机构在技术开发和应用过程中,严格遵守数据保护法规,采取有效措施确保用户数据安全,同时加强对人工智能系统的监管和伦理审查,以实现技术进步与隐私保护的平衡。

#### (二) 智能化深度挖掘的威胁

人工智能技术在网络安全防御中,可通过强大的数据分析、关联、预测能力为网络安全防御提供保障,但其强大的数据处理能力也带来了新的威胁。这种技术能够对用户数据进行细致的关联分析,深度挖掘出用户可能不愿意公开的敏感信息,侵犯个人隐私和数据安全。随着大数据分析技术的不断进步,进行精准生产和个性化服务成为各行各业改革的重要目标,但由此带来的对用户数据的持续追踪和分析增加了用户隐私泄露的风险。一旦这些隐私数据被用于不当或非法目的,如虚假政治宣传或商业恶性竞争,会严重干扰个人生活、社会和谐。因此,如何在利用人工智能进行网络安全防御的同时,防止其智能化深度挖掘带来的潜在风险,是当前亟须解决的挑战。

#### (三) 数据质量和偏见问题

数据的好坏直接关系到人工智能系统的精准度与可靠性,当数据有误差或不全面时,人工智能模型就会自动识别出错误的模式,从而造成虚假结果或漏报。带有偏差的数据会使模型对特定的用户或群体做出不公正的评价,从而影响到网络安全防护的效果,同时也会带来一些法律、道德等方面的问题。如何保证高质量、高公平的数据是促进人工智能技术在网络安全中广泛应用的关键。这就要求在数据采集、净化、模型训练等环节建立一套严密的数据管理与审计机制,以降低偏差,提升数据的代表性与准确度。此外,为了保证其在网络安全防护中的公平与高效性,还需定期对其进行评价与修正。

### 五、结束语

人工智能技术由于具备强大的数据分析和学习能力而被用于网络安全防御领域,这是大数据时代背景下网络系统更新升级的必然要求,也将为网络系统的发展产生深远的影响。本文通过对人工智能技术在网络安全防御中的优势与挑战的深入探讨,揭示了其在入侵检测系统、恶意软件识别和钓鱼攻击识别等方面的巨大应用潜力。同时,人工智能技术带来的隐私保护、信息深度挖掘、数据质量和算法偏见等问题也不容忽视。展望未来,我们需要在技术创新与伦理法规之间找到平衡点,加强跨领域合作,推动人工智能技术的健康发展。

#### 参考文献:

- [1] 赵薇. 大数据时代人工智能在高校校园网络安全技术中的运用[J]. 软件, 2024, 45(01): 158-160.
- [2] 马雯阳, 倪瑞. AI技术应用于网络安全防御的途径探索[J]. 数字通信世界, 2023(05): 63-65.
- [3] 张超, 郑茗泽. 大数据网络安全防御中人工智能技术的运用[J]. 中国新通信, 2021, 23(07): 121-122.
- [4] 熊涛. 人工智能技术在网络安全防御中的应用[J]. 电脑编程技巧与维护, 2020(11): 110-111+126.
- [5] 柴项羽. 基于大数据及人工智能技术的计算机网络安全防御系统设计[J]. 网络安全技术与应用, 2020(09): 52-53.