

人工智能技术在计算机网络安全管理中的运用策略

李文璇

广东华夏高级技工学校 广东 广州 510000

摘要: 随着计算机网络的飞速发展和信息技术的不断革新,网络安全日益成为人们日常生活和工作中不容忽视的问题。而人工智能技术的应用,为计算机网络安全管理提供了新的解决方案。基于此,本文简要介绍了人工智能技术在计算机网络安全管理中的作用,分析了其在安全管理中的具体应用,并提出了一些能够加强应用的有效措施,为促进网络安全的保障和发展提供了新的思路。

关键词: 人工智能技术; 计算机网络安全; 运用

引言

随着信息技术的快速发展和应用,互联网已经成为人们生活和工作中不可或缺的一部分。但随之而来的网络安全问题也日益凸显,网络攻击日益增多,其种类也越来越多。传统的网络安全技术已经无法满足安全防御的需求,因此人工智能技术应运而生。

1 人工智能技术在计算机网络安全管理中的作用

随着网络技术的飞速发展,计算机网络安全问题越来越引起人们的关注。网络攻击、数据泄露、黑客入侵等问题层出不穷,这对企业和个人的安全造成了巨大威胁。为了提高计算机网络安全,人工智能技术开始被广泛应用于网络安全管理中。第一,人工智能技术可以自动检测威胁,并采取相应的措施来防范这些威胁。使用人工智能技术可以更加准确地检测恶意软件、木马病毒、渗透等攻击,并在攻击发生之前,及时停止攻击。例如,通过深度学习算法,可以分析网络流量和日志记录,从而准确地检测出不寻常的网络活动,并发现对传输层协议的未经授权的访问尝试。第二,人工智能技术可以利用机器学习、深度学习等技术,学习网络数据的模式和规律,从而识别潜在的风险。在使用机器学习技术时,可以使用大量的样本数据,以帮助算法学习有关网络攻击的模式。通过这种方式,系统可以自动识别并在未来避免相似的攻击。第三,人工智能技术可以通过对历史数据的大规模分析和处理,预测未来的威胁和风险。通过对数据的分类、聚类和挖掘,可以发现网络上存在的安全漏洞。利用深度学习和语义分析技术,可以精准地推断最有可能的风险,并在系统中采取相应的措施。第四,人工智能技术可以为网络安全管理提供自适应的防御机制。例如,在网络流量管理中,人工智能技术可以根据实时流量的不同变化,自适应调整网络流量的优先级和量,以保持网络带宽的稳定和安全。第五,

人工智能技术可以帮助计算机网络系统实现自主修复,从而保护网络系统免受攻击和破坏。例如,在网络攻击发生后,系统可以自主启动自我修复程序,重构受损系统,并重新把系统恢复到安全的状态。

2 人工智能技术在计算机网络安全中的运用

2.1 智能识别垃圾信息和病毒

传统的防火墙技术通常基于规则和签名来检测和过滤潜在的威胁,但这种方法往往无法应对新型的、未知的攻击方式。而人工智能技术利用机器学习算法和深度学习模型,可以从大量的样本数据中学习和识别出垃圾信息和病毒的特征,具有更高的准确性和适应性。同时,人工智能技术还可以通过分析网络流量和日志数据来智能识别垃圾信息和病毒。传统的防火墙主要依赖于事先定义好的规则集合进行过滤,无法及时发现新型的攻击行为^[1]。而人工智能技术可以通过监控和分析网络流量和日志数据,利用机器学习算法构建模型,实时地识别出异常流量和可疑行为,并对其进行进一步的检测和阻止。此外,人工智能技术在计算机网络安全中的运用还包括了对恶意软件和病毒的自动化防御和应对。传统的防病毒软件通常依靠更新病毒库来检测和清除病毒,但这种方式在面对快速变化的恶意软件时效果有限。而人工智能技术可以通过学习和分析大量的样本数据,自动识别和分类不同类型的恶意软件,并采取相应的防御措施。最后,除了垃圾信息和病毒识别外,人工智能技术还可以用于异常检测、入侵检测以及安全事件响应等方面。例如,通过构建基于机器学习的异常检测模型,可以实时监测网络中的异常行为并发出警报;利用深度学习算法,可以识别并阻止未知的入侵行为;同时,通过自动化的安全事件响应系统,可以快速对网络安全事件做出反应并进行相应的处理。

2.2 构建网络安全威胁态势感知体系

近几年来,网络安全问题层出不穷,攻击手段和方式不断翻新,企业和个人安全面临的威胁和风险越来越大。面对复杂的网络威胁,如何全面地了解网络安全态势,及时发现和防范各种网络攻击行为,成为了网络安全管理工作中的一项重要任务。而人工智能技术具有智能化、自主学习和自我优化等特点,能够处理大量数据信息,并且能够识别隐藏在大量数据中的模式和规律,从而更好地实现对网络安全威胁态势的感知。在构建网络安全威胁态势感知体系中,人工智能技术具有以下应用方向:(1)通过深度学习和机器学习技术,可以对流量数据进行分析,密切监视网络容易受到攻击的部位,并及时发现和防范各种攻击行为。(2)通过使用机器学习技术,可以自动保护网络安全,及时分析、响应和处置攻击事件。例如,当发现恶意软件时,可以自动将恶意软件识别为高风险事件,并自动启动防御机制,运用人工智能技术对事件进行充分的分析,从而快速确定攻击行为的真实性,并将正确的响应策略,自动反馈到网络安全管理中心^[2]。(3)利用人工智能技术,可以对大量数据进行分析和挖掘,并筛选出可能对网络造成潜在威胁的因素,实现智能化的预测和风险评估。例如,可以利用机器学习和数据挖掘技术,对恶意软件进行深入分析,并筛选出最有可能对某种类型网络造成实际威胁的恶意软件,从而评估网络的风险,并提供相应的建议。

2.3 机器学习提升网络安全防护的智能化和自动化

第一,机器学习和深度学习在网络安全防护中的智能化应用可以大大提升系统的防护能力。传统的基于规则的方法往往需要手动更新规则,而且无法有效应对未知的攻击方式。相比之下,机器学习可以自动学习并适应新的威胁,从而更加灵活和高效地应对网络攻击。第二,深度学习作为机器学习的一种主要技术手段,可以通过构建深层神经网络来挖掘数据中的复杂模式和特征。此外,深度学习模型在网络安全领域的应用还包括入侵检测、威胁情报分析、恶意代码检测等。通过深度学习,系统可以从海量的网络流量和日志数据中提取出有价值的信息,并准确地判断是否存在潜在风险。第三,机器学习和深度学习的智能化和自动化应用可以提高网络安全防护的效率和准确性。传统的网络安全防护往往需要依赖专业人员进行手动分析和决策,这不仅耗时且容易出错。而机器学习和深度学习可以通过算法自动处理和分析大量的数据,从中找到隐含的规律和模式,并根据预先定义的策略做出相应的响应。这种智能化和自动化的防护方式不仅能够及时发现和应对攻击,还能够减轻人力负担,提高整体的安全性能。

2.4 在Agent技术中的应用

Agent技术是一种人工智能代理技术,它可以通过模拟人类智能行为、获取信息和加工数据,实现对信息的智能处理和管理,从而使计算机系统具有智能化和自动化的特点。在实际应用中,Agent技术被广泛地应用于各个领域,例如,企业管理、信息检索、安全监控等等。具体来说,Agent技术在数据库中的应用主要包括以下几个方面:首先,在数据库管理中,Agent技术可以实现自动化的数据管理,包括数据备份、数据恢复、数据转储等操作^[3]。同时,Agent技术还可以自动识别数据文件的格式和类型,从而提高了数据整理的效率和准确性。其次,对于大型数据库系统,Agent技术可以实现高效、准确的查询和检索。它可以帮助用户准确地定位并检索出所需数据,避免不必要的查询时间和工作量,同时还可以提高系统的响应速度和数据检索的准确度。最后,数据库的安全问题一直是企业和组织管理中的重要问题之一。Agent技术可以实现数据库的安全管理,并通过监测用户操作和记录数据修改日志等方式,提高数据库的安全性和可靠性。同时,它还可以自动识别和排查潜在的安全隐患,以及提高数据库的安全性和防护能力。

3 对人工智能技术在计算机网络应用提出建议

3.1 提高人工智能技术的智能化程度

想要人工智能技术更好的应用于计算机网络技术领域,必须要提高人工智能技术的智能化程度。只有人工智能技术足够智能,才能更好的体现发挥自身的优势,才能更好的应用与发展。第一,要提高人工智能技术的智能化程度,需要加强对底层算法和模型的研究与改进。目前,深度学习是人工智能领域最为热门和有效的技术之一,但其仍然存在许多限制和挑战。因此,研究者们需不断探索新的算法和模型,以提高智能化程度。第二,数据是人工智能的基础,而且越多越好。因此,研究者们需要收集更多的高质量、多样化的数据,并进行有效的数据预处理和特征选择。通过使用更多的数据,并借助数据清洗和特征提取等方法,可以提高人工智能系统的泛化能力和准确性。第三,要提高人工智能技术的智能化程度,还需要注重模型的解释性和可解释性。尽管深度学习在图像识别、自然语言处理等领域取得了重大突破,但其黑盒特性使得难以理解其决策过程。因此,研究者们需要致力于开发能够解释和理解模型决策的方法和技术,从而提高人工智能系统的可信度和可接受性。第四,为了提高人工智能技术的智能化程度,需要加强与其他学科的交叉融合,人工智能是一个涵盖多个学科的综合领域,包括数学、计算机科学、

认知科学等。通过与其他领域的合作和交流,可以借鉴其他学科的理论和方法,提供新的思路和创新,推动人工智能技术的发展。

3.2 鼓励以政府与企业为主对人工智能技术应用

随着信息技术的不断发展,人工智能技术已经成为当前科技领域的前沿技术之一,它不仅为传统行业的升级改造提供了新的解决方式,也为未来的科技发展奠定了基础。而鼓励政府和企业将人工智能技术应用于计算网络,是当前产业升级和数字化转型的重要举措。一方面,政府与企业应共同推进计算网络领域的人工智能技术应用。政府可以制定相应的政策和法规,为人工智能技术的发展提供支持和保障。这些政策可以包括减少人工智能技术研发过程中的审批程序,提供税收优惠政策,并提供相关的贷款和资金支持,以促进企业在人工智能技术领域的创新和应用^[4]。此外,政府还可以建立开放的数据共享平台,为企业提供更多的数据资源,以便他们能够更好地开发和应用人工智能技术。另一方面,政府和企业需要加强对人才的培训和科技应用。在人工智能技术领域,拥有具备相关专业知识和技能的人才至关重要。政府可以通过设立教育基金、提供奖学金等方式,鼓励学生选择与人工智能相关的学科,并且提供高质量的教育和培训资源。同时,政府还应与企业合作,共同开展人才培养计划,为企业提供专业的技能培训,以满足市场对人工智能人才的需求。

3.3 建立相应的治理和监管机制

为了确保人工智能技术在计算机网络应用中得到合理和负责任的使用,建立相应的治理和监管机制至关重要。这些机制的目标是保护公众利益、维护数据隐私和确保技术的安全性。首先,政府应该制定明确的政策和法规来规范人工智能系统的使用。这些法规应该明确人工智能系统的使用范围和限制,以保护人们的权益和避免滥用。例如,法规可以包括对敏感个人信息的处理和保护的規定,以及对不当行为的处罚措施。其次,为了有效监督和评估人工智能系统的使用情况,建议设立

独立的监管机构。该机构应由专业人士组成,负责审核和批准人工智能系统的应用,并监督其运行过程中是否存在违规行为。同时,人工智能技术的发展具有全球性的影响力,因此建议各国之间加强合作,分享经验和最佳实践。这将有助于建立更一致和有效的治理和监管框架,避免不同国家之间的冲突和差异。最后,人工智能系统的开发者和供应商应该接受审查和认证,以确保他们的技术符合标准和规范。审查和认证过程应包括对算法、数据集以及系统运行的测试和验证,这样可以降低人工智能系统出现安全漏洞或错误的风险。此外,在治理和监管机制中,人工智能系统的使用应该是透明的,用户需要了解何时和如何使用这些系统。因此,相关机构应要求人工智能系统提供透明度报告,解释其决策过程,并确保没有歧视性、不公平或潜在的偏见。

结语

综上所述,计算机网络安全管理是现代化社会的重要保障之一,而人工智能技术的应用则在该领域中提供了新的解决方案。通过人工智能技术的应用能够实现数据驱动的安全决策、自适应防御和实时威胁情报等策略,提高网络安全管理的效率和灵活性。未来,需要进一步研究和发 展人工智能在网络安全管理中的应用,并探索更加有效的策略和解决方案,以应对日益复杂的网络安全挑战。

参考文献

- [1]张清舒.基于云计算的大数据安全隐私保护的研究[J].电子技术与软件工程,2020,(21):255-256.
- [2]王大萌.计算机应用中的网络安全防范对策[J].电子技术与软件工程,2020,(17):247-248.
- [3]陈志涛.大数据时代人工智能在计算机网络技术中的应用——评《计算机网络》[J].现代雷达,2021,43(07):107.
- [4]徐天奕,单炜航.大数据背景下人工智能在计算机网络技术中的应用[J].计算机与网络,2021,47(12):39.