网络安全管理中人工智能技术的应用

黎西江

身份证：610103196303243698 陕西 西安市 710000

【摘　要】网络安全是当前数字化社会中的重要议题，而人工智能技术则为提升网络安全管理能力带来了新的机遇。本文以人工智能技术在网络安全管理中的应用为切入点，探讨了该技术对于网络安全的意义与潜在影响，分析了现阶段网络安全管理工作面临的挑战，并探讨了人工智能技术在网络安全中的具体应用，以期促进人工智能技术在网络安全管理中的广泛应用，为构建更安全的网络空间做出贡献。

【关键词】网络安全；管理；人工智能技术；应用

随着数字化时代的到来，互联网的普及和数据技术的快速发展，大数据的规模与价值不断攀升。然而，随之而来的是越来越多的安全威胁和网络攻击，给个人和组织的信息安全带来了巨大的挑战。为了应对这一挑战，人工智能技术逐渐应用于大数据网络安全管理领域，成为了预防和应对网络攻击的有力工具。基于人工智能的安全管理技术具有自动化、智能化和高效性等优势，能够有效提升网络安全的防御管理能力。

1 人工智能的概念

人工智能技术包括两部分，分别是人工与智能，人工技术是指技术运行过程中具有人的思维习惯，能够对人类的真实行为模仿并进行相关处理操作；智能技术是指与计算机和互联网等技术相关的现代化技术，能够促使计算机系统完成智能化运转。因此，人工智能技术就是通过计算机系统对人的思维行为进行模仿，基于编程技术和其他技术实现某种智能化需求的技术。现阶段，人工智能技术在社会发展中已经得到广泛应用，包括智能手机、智能机器人、智慧交通等，人工智能技术对社会发展具有十分重要的作用，因此其安全问题就成为了重点关注与研究的内容之一。

2 现阶段我国网络安全现状分析

2.1 网络安全工具的应用缺乏系统规定

在目前阶段，许多网络安全工具还没有形成一个统一的体系，而且还有一些工具在安全管理方面存在不足，因此，各种安全工具就像雨后春笋一样泛滥起来。很多安全工具在没有强大的技术支持的情况下，导致信息安全产生危险。

2.2 固有网络安全漏洞带来的危害

在网络安全系统刚开始发展的阶段以及发生问题的阶段，用户可以第一时间进入到系统中解决问题，这种做法虽然极大地提高系统的稳定性，也给不法分子窃取和破坏用户信息的可乘之机。

2.3 部分网络设备存在安全隐患

网络设备是构建计算机网络基础设施的重要组成部分，但也存在着一些安全隐患，可能会给网络安全带来威胁，常见的包括以下几种：第一，弱密码和默认口令：某些网络设备可能使用弱密码或默认口令，黑客可以通过破解这些密码或口令来获取设备的控制权。第二，恶意软件：黑客可以通过植入恶意软件，例如病毒、木马、蠕虫等，来窃取敏感信息或控制网络设备。

2.4 恶意攻击网络带来的隐患

恶意攻击网络可能会带来以下一些隐患：第一，数据泄露和盗窃：黑客可以通过恶意攻击获取网络中存储的敏感数据，例如个人信息、财务信息、商业机密等，并将其用于非法目的。第二，服务拒绝攻击：黑客可以通过向目标服务器发送大量无用的请求，导致服务器无法正常处理合法请求，从而影响正常的服务运行。第三，系统瘫痪：恶意攻击可以导致系统崩溃或停止运行，造成业务中断或数据损失。

3 网络安全防护中人工智能技术的应用优势

3.1 协作能力较强

伴随着互联网规模的不断扩大和愈加复杂的网络架构，网络安全防护工作的难度不断上升，单一管理者很难快速及时地处理大范围的网络风险，要借力系统性的协助处理才能达到最佳效果。同时，网络安全防护中若只采取简单化的防护模式和单一化的处理方式，很难取得理想的整体防护效果。对此，为加强网络安全防护，应尽量采取层次化的防御方式。引入人工智能技术，能使防御模态层次化和模块化，如此，有助于彼此之间展开高效协作，取得更理想的网络安全防护效果。在人工智能技术积极作用下，能形成较为完整的一个多层监测体系，从而实现网络安全的有效保障。

3.2 具有处理模糊信息的能力

个人用户在通过互联网从事信息管理工作过程中，

极易遭遇不明源头病毒入侵的危险，如未及时对不明源头病毒开展监测和研究，做出正确诊断，必然会危害网络通信安全性。人工智能技术可对不明源病毒做出相应的模糊信息推理，使其更有效地识别出信息来源和类别，以便对此类信息做出正确的处置，从而有效防止信息泄漏。

3.3 拦截垃圾邮件

人工智能技术可以利用自然语言处理、图像识别等方法，对邮件内容进行语义分析和图像识别，判断邮件是否为垃圾邮件或恶意邮件。同时，人工智能技术可以根据用户的反馈和行为，动态调整邮件过滤规则和策略，提高拦截垃圾邮件的准确率和灵敏度。

4 人工智能技术在网络安全管理中的应用

4.1 网络安全中的常规应用量化风险

量化风险是一种将风险转化为可量化的数值或范围的方法，它可以应用于不同的领域和场景，如金融、保险、工程、项目管理等。在网络安全领域，量化风险是指利用数学模型和统计方法对网络系统中存在的各种威胁、漏洞、影响和损失进行定量或定性的评估和预测，从而为网络管理者提供有效的决策支持。随着网络技术的发展和应用的广泛，网络安全风险也日益增加和复杂化，传统的基于经验或规则的风险管理方法已经难以满足实际需求。因此，人工智能技术作为一种强大的数据处理和分析工具，可以为量化风险提供更高效和精准的解决方案。人工智能技术可以通过机器学习、深度学习、自然语言处理等方法，对海量的网络数据进行智能化的采集、清洗、整合、挖掘和建模，从而发现潜在的风险因素和规律，生成可视化的风险报告和预警信息，帮助网络管理者及时发现和应对网络安全风险。总之，量化风险是一种将风险可视化和可控制的方法，它可以为网络安全管理提供科学的依据和指导。人工智能技术是量化风险的重要支撑和推动力，它可以提高网络数据的利用效率和价值，增强网络安全风险的识别和预防能力。

4.2 防护文件网络攻击

文件网络攻击是指利用恶意文件或代码对目标系统或用户进行破坏或窃取信息的行为，它是一种常见的网络攻击手段，如病毒、木马、勒索软件等。人工智能技术可以通过图像识别、语音识别、文本分析等方法，对文件内容进行检测和识别，判断其是否含有恶意代码或隐藏信息，从而实现文件的分类和过滤。文件网络攻击的危害很大，它们可以破坏系统功能、窃取用户数据、篡改用户行为、散播恶意信息等，给用户带来严重的经济损失和信誉损害。传统的防御方法，如杀毒软件、防火墙、沙箱等，往往依赖于已知的恶意特征或行为模式，难以应对新型的、变异的、隐蔽的文件网络攻击。人工智能技术可以提高文件网络攻击的防御能力，利用机器学习、深度学习等算法，从海量的正常文件和恶意文件中学习特征和规律，构建智能的检测模型，实现对未知的、复杂的、多样的文件网络攻击的有效识别。

4.3 强化网络防火墙

在网络防火墙与人工智能技术相结合后，即可为企业和其他机构的网络提供更为强大、全面的防护，有效降低机密数据外泄的几率，提升企业和各类机构网络系统运行的安全性。在利用人工智能技术提升网络防火墙防护性能的过程中，人工智能技术可借助网络边界建设更为完善的通讯系统，并且可及时阻隔外部网络中的不稳定因素，减少外来用户在内部网络违规操作的几率。此外，将人工智能技术与网络防火墙结合后，还可利用其及时发现内部网络的安全风险，让技术人员尽早对安全风险进行处理，加强了对重要信息的保护力度。

4.4 快速检测入侵操作

在当前的网络环境中，数据传输量及频率均在快速增加。如不做好网络安全防范工作，让不法分子肆意攻击数据传输渠道，企业和各类机构的重要数据将在传输过程中泄漏。因此，需利用人工智能技术快速检测不法分子的入侵操作，确保重要数据不外泄，以及保证用户接收到完全、真实的数据。目前，支付宝和微信均有大量用户，如不法分子利用其漏洞修改信息，让用户接收到错误信息，即会让用户承受经济损失。

4.5 过滤垃圾邮件

现阶段，许多个人用户以及机构用户都会接收到垃圾邮件。某些垃圾邮件只是存在广告信息，无法对用户产生严重危害。而某些垃圾邮件则存在着病毒，一旦用户打开，病毒就将对用户的计算机设备造成破坏，影响用户的网络使用体验。一些垃圾邮件会诱导用户输入个人信息，如用户输入自身的真实信息，经济方面就将遭受严重损失。为避免垃圾邮件对财产安全的不良影响，进一步保障个人用户或机构用户的财产安全，需利用人工智能技术建设反垃圾邮件系统，对邮箱进行实时监测，并分析其接收到的邮件，然后结合邮件信息形成相应的报告。若存在危害性较大的垃圾邮件，反垃圾邮件系统即会发出特别警示。

4.6 强化用户认证与访问控制

强化用户认证与访问控制是使用人工智能技术加强网络安全防御体系的重要策略。传统的用户名和密码认证方式易受到攻击和破解，因此采用生物特征识别、行为分析、多因素认证等人工智能技术可以提高用户身份验证的准确性和安全性。此外，在访问控制方面，基于机器学习的模型可以对用户行为进行实时监测和分析，根据行为模式和风险评估来自动调整访问权限，并及时阻止异常活动和未授权访问。

4.7 高效查杀木马病毒

随着各类网络安全防御技术不断加强，通过网络获取利益的不法分子也在深入研究网络攻击技术，开发新型的木马病毒。若个人用户、机构用户不应用人工智能技术，未提升计算机设备的网络防御登记，就将遭受新型木马病毒的影响。人工智能技术中的神经网络具有较强的执行能力、计算能力、存储能力，以及较为出色的容错性，可快速、准确识别网络环境中的各种信息。因此，将神经网络和网络防御系统相融合，可明显增强智能检测技术的识别能力，加快其识别病毒的速度，降低网络防御系统决策的失误概率。当前某些新型木马病毒的隐蔽性极强，传统病毒识别技术无法快速识别，如未及时识别出木马病毒，也就无法进行查杀，从而让木马病毒破坏计算机设备、盗取计算机设备中的信息，使木马病毒的制作者谋取到大量经济利益。

4.8 网络资源调度和智能网络管理

网络资源调度是计算机网络中的一个重要问题，涉及网络中带宽、存储、计算等资源的分配和管理，以提高网络的性能和可靠性。网络资源调度在大规模分布式系统中具有重要的意义。在这样的系统中，资源的分配和管理需要考虑到多个因素，如负载均衡、故障容错和用户体验等。利用人工智能技术，可以实现更加智能的网络资源调度。其中，机器学习算法是常用的技术之一。通过对网络中的流量进行学习和预测，可以实现对网络带宽资源的动态调整，以保证网络中的各项服务都能够得到优先的资源保障。

5 结束语

综上所述，随着科技的蓬勃发展，互联网在现代化建设中的功能越来越明显，而网络安全问题日益突出。在现代化社会背景下，人工智能和物联网应用技术已经成为推动社会发展和经济建设水平的关键性因素之一，在多个领域中得到广泛应用。人工智能和物联网应用技术提高社会科技水平的同时，也存在一定的网络安全问题，需要人们重点关注研究，不断加强网络安全管理技术，从而为人工智能和物联网应用技术应用提供良好的环境保障。

【参考文献】

[1]郭健.人工智能和物联网应用的网络安全管理方法[J].网络安全技术与应用，2021（12）：171-172.

[2]姚克.基于人工智能和物联网应用的网络安全管理[J].计算机产品与流通，2020（04）：155-156

[3]吴志雄.基于人工智能和物联网应用的网络安全管理[J].中国信息化，2019（09）：164-165.

[4]刘准.计算机网络安全管理中人工智能技术的运用分析[J].电脑知识与技术：学术版, 2020, 16(30):2.