

人工智能对网络安全的威胁与应对

张旭

海南师范大学 海南海口 571127

摘要: 近几年来,网络空间安全问题层出不穷,给国家、社会、经济带来了全方位的威胁。人工智能一方面推动着人类社会的发展,另一方面也给网络空间安全带来了深刻的变革。在新时期发展进程中,既要加大科技的创新与研究,又要深入剖析网络应用的安全性,以确保网络的安全性和稳定性。本文针对人工智能环境下对网络安全的威胁进行了研究,并提出了相应的对策。

关键词: 人工智能;网络安全;威胁;应对措施

引言

随着人工智能技术的迅速发展及普及,网络安全面临着新的威胁与挑战。随着人工智能技术的发展,攻击者可以更加精确和自动化地进行攻击,同时也为攻击者提供了一种新的手段来应对不断发展的威胁。为此,开展基于人工智能的网络安全威胁分析与对策研究具有重要意义,本文以此为基础,研究人工智能环境下的安全威胁与应对策略。

1. 人工智能技术的优势

1.1 网络防御能力较强

将人工智能应用于信息化网络,可进一步提升网络的安全性。面对日新月异的网络环境,随着互联网的发展,人类在充分地享受着互联网所提供的无尽的空间和速度,也不可避免地遇到了由网络所引起的各种问题。所以,利用人工智能技术,可以很好地解决目前信息化网络中存在的安全问题。首先,结合人工智能技术,构建良好的监督系统,用于复杂的网络环境。在此基础上,通过构建多层防护体系,提升网络的安全性,推进网络安全防御体系的构建,同时,人工智能能够对网络中传播的有害数据进行实时截获与过滤,实现对网络环境的净化,为广大网民提供优质的信息。所以,利用人工智能技术建立的网络防御体系,能够有效地保障网络的安全。

1.2 信息化使用成本较低

首先,信息化数据处理。需要大量的数据作为基础,这就需要保证整个网络系统的安全。与传统网络信息处理方式相比,其总体功能和严重性都较低,在某种程度上占用了有效的数据资源,导致信息化网络工作的效率下降,已不

能适应目前的网络环境。为提升网络安全防御能力,减少构建网络安全防护体系的代价,节约企业的经济利益,融合人工智能技术能够去除许多滞后的算法,达到精确计算的目的,对信息化网络中的数据进行有效保障,对网络数据进行优化,进而提升网络信息运行的安全性。在网络环境下,人工智能也能够对程序问题进行有效地防御。能有效地规避传统信息化模式的计算错误,并能有效地规避在信息化系统中进行软、硬件系统的研发与现代化所带来的成本问题,从而为企业带来更大的经济效益,并提升信息化工作的效率。

1.3 可以处理模糊的数据信息

在信息化建设今天,信息化数据应用正逐步渗透到人们的工作、生活中。在对模糊信息进行处理时,传统的信息处理方法不能有效地进行模糊信息的提取和筛选,从而降低了数据的使用效率。这就导致企业在实际工作中出现了各种不良后果。网络信息使用者在处理这些模糊信息时,往往会遇到一些难题,如处理不当,就有可能造成经济上的损失。同时,还存在着错失有效的数据,给提高网络的安全性和可靠性带来了新的挑战。但是,通过人工智能技术的融合,能够有效地防范和规避模糊数据带来的不利影响。在对数据进行统计、筛选时,采用人工智能技术能够有效地改善数据处理的精度。根据已知的数据,进行更明确的计算,并将无用的数据去除。从而有效地提高了对信息数据的处理能力。利用人工智能技术,可以合理地处理信息网络运行中产生的某些未知问题,从而保证网络工作的高效性,同时也为企业的工作人员提供了快速有效的解决方案。

2. 网络安全防御概述

网络安全防御就是将一系列的技术与管理手段运用于网络环境中,以防止信息系统与数据受到威胁或破坏的行为。随着互联网的普及与信息技术的迅速发展,网络安全防御变得越来越重要。但是,在网络安全防御方面还存在着诸多难点。首先,由于网络威胁种类繁多且不断演化,因此很难遵循防御战略。黑客一直在利用新技术和方法突破已有的防御。其次,由于网络环境复杂,海量的数据,使得真正的威胁与异常行为难以被发现。另外,由于企业自身的资源限制,也很难将其用于建立健全的安全防御系统。但是,由于网络中存在的信息泄漏以及恶意攻击等问题,会给用户带来重大的数据安全隐患,甚至造成巨大的经济损失。在这种情况下,如何有效地抵御网络安全威胁,是保障信息安全、保障网络空间稳定的关键。高效的网络安全防御机制,既能保护核心信息资源、防范非法存取与数据遗失,又能增强抵御网络攻击的能力,减少网络安全风险。完善的信息安全防御系统,是保障网络空间稳定的重要保障。如图1,网络安全威胁。



如图1,网络安全威胁

3. 人工智能背景下的网络安全威胁

3.1 拒绝服务攻击威胁

随着人工智能技术的广泛应用,对网络安全提出了更高的要求。其中DDoS攻击是威胁之一。DDoS攻击是指将高速率的信息传输到某一具体对象的系统中,以阻止该系统的正常运行。现代黑客经常利用“僵尸网络”实施DDoS攻击,botnet是一系列能够利用自动软件发动袭击的受控电脑。随着人工智能的发展,DDoS攻击越来越受到攻击者的重视。比如,攻击者可以通过机器学习算法发现并利用目标系统中的弱点,从而对攻击策略进行优化,从而最大化网络带宽。

另外,攻击者还可以利用人工智能的自适应攻击方法,通过对被攻击对象的反应,自动地调节攻击的强度、频率。这类攻击不但难以侦测与防御,而且会造成更严重的网络破坏。

3.2 智能网络恶意代码威胁

随着人工智能技术的发展,智能网络中的恶意代码所面临的威胁越来越大,也越来越复杂。传统的网络安全防御技术以规则检测与分析为基础,而现代智能网络中的恶意代码通常表现出智能、自适应等特征,能够主动地改变自己的行为以规避或规避安全防护体系。同时,通过引入智能算法、机器学习等方法,进一步提升攻击效率,并利用现有的规则检测方法对其进行检测。

4. 人工智能背景下的网络安全防御关键技术

4.1 智能包过滤防火墙技术

智能包过滤防火墙是一种与人工智能相融合的新方法,能够在网络层,依据存取控制表ACL,对数据包进行智能化的大数据分析、优先级选择以及多函数筛选。实现了预先确定的内部网络与外部网络之间的通信访问限制。智能包过滤防火墙(IntelligentPackageFilter)通过检测数据流中的报文的来源、目标地址、所使用的端口数目、协议状态等,根据不同的信息类型,自动判断数据的排序与合并方式,判断数据包能否通过。智能包过滤防火墙在过滤过程中,除了对数据包进行过滤、转发之外,还负责将报警信息及时地发送到监测终端;配置程序主要是对过滤器主机自身的配置及筛选规则进行进一步的修改与改进。在此基础上,通过智能包过滤防火墙技术,实现了对过滤次数的智能调整。

4.2 智能化社会工程学攻击技术

智能化社会工程学攻击技术就是利用神经网络、专家系统等技术对垃圾邮件、钓鱼式攻击、电脑蠕虫传播等进行智能化的识别与管理,保障用户的隐私。基于NLG的网络钓鱼是一种常用的攻击手段。攻击者利用专家系统、深度学习等方法,对文本进行深度挖掘,自动识别出所关注的话题,并自动生成能够让用户即时做出反应的文字内容。是一种用于与社交网站和电子邮件为主要攻击目标的传输媒介网络钓鱼攻击方式。

4.3 智能化反恶意代码攻击技术

随着人工智能的发展,对恶意代码的抵抗力也极大增强。随着恶意代码带来的新威胁与挑战,反病毒引擎需要持续升级,以增强抵御恶意代码的能力。防病毒引擎对攻击的

鲁棒性越来越强，基于深度学习的抗恶意代码攻击技术在这一领域具有重要的应用前景。比如，腾讯开发就利用了基于深度神经网络的 TRPAI 技术，从而达到了发现并消灭恶意程序的目的。相对于机器学习，基于深度学习理论智能化反恶意代码攻击技术能够实现机器学习的自动化的目标。通过对已发现的恶意代码进行动态添加和去除，极大地提升了相关恶意代码的搜索效率。

5. 基于人工智能的网络威胁应对策略

随着人工智能技术的迅猛发展，网络威胁日趋复杂化，基于人工智能技术发展更加智能化的信息安全防御对策显得尤为重要，既能节约人力、降低各类成本，又能有效应对网络安全威胁。

5.1 建立完善的安全机制

要实现信息系统的安全防护，既要依靠技术措施，又要有完善的安全机制。这包括制订详尽的网络安全政策，网络行为准则，并进行有效的安全培训。一是有关部门应加大立法力度，尽快建立健全与网络安全有关的法律法规，使之成为一种有效的防御手段。另外，有关部门也要按照国家有关法规，制订自立的网络安全政策与标准，明晰各自的责任与义务。这种关联组织可以更有效地监视网络的行为，避免因政策漏洞被内部员工或外界的攻击者所破坏。同时，各有关组织也要制定严密的安全检查制度，以保证各合作伙伴及供应链各成员都能符合相应的安全规定。而安全培训则是提升员工的安全意识与技巧的重要步骤。有关组织可利用人工智能技术量身定做个性化培训课程，并依其责任与知识程度，设定不同层次的培训课程。

5.2 建立智能化的威胁检测系统和自动化防御机制

构建智能化的威胁检测系统，是提升信息安全工作效率与精度的有效途径。安全工作者需要采集海量的互联网数据，采用机器学习和数据挖掘技术对数据进行了分析和建模，通过对网络数据的规律及异常行为的分析，可以有效地发现可能存在的威胁或攻击。建立实时检测系统，对网络流量进行不间断地监测，并对系统的运行情况进行监控，并给出相应的报警提示。利用机器学习、人工智能等方法，对网络中的异常行为及攻击方式进行自动识别，并给出预警。建立自动化防御机制，以对威胁及攻击作出反应。比如，机器学习算法与自动化工具能够自动拦截恶意通信、隔离被感染的系统、修补弱点与漏洞。运用人工智能算法与辅助决策系

统，对威胁与攻击进行智能决策，实现对威胁与攻击的优化。比如，在系统中，可以根据系统的威胁等级，对系统进行相应的保护，并对系统进行相应的资源配置，从而达到降低系统的安全风险的目的。建立不断学习与改善、不断更新与改善威胁检测与防御系统。在此基础上，引入机器学习、反馈等技术，对系统进行自主学习，并对其进行优化。

5.3 加强多领域合作与信息共享

在许多领域，应加强合作与信息共享，以增强网络安全。在政府、行业协会、企业之间建立跨行业合作机制。通过信息共享、资源共享、经验共享等方式，增强共同应对网络安全威胁的能力。要加强国际合作与信息共享，以应对跨国网络的安全威胁。透过培训，宣传及教育，提升使用者的网络安全意识，并降低网络安全脆弱性。因此，必须加强多领域合作与信息共享，才能更好地保障网络安全。只有通过共同努力，才能有效地解决网络安全问题，保障网络与信息的安全。

6. 结束语

综上所述，随着人工智能技术的飞速发展，科技发展对网络安全提出了新的要求：网络安全问题日趋严重，而人工智能对网络安全防御起到了至关重要的作用。本文介绍了人工智能技术给保障网络安全带来的威胁与挑战，并提出了相应的对策，同时，从实际的角度出发，综合运用各种方法，建立具有较高可操作性和可执行性强的安全防护系统。在网络安全防御中利用人工智能技术与人力资源相结合，可提升网络安全防御效能。同时，也要密切注意科技的发展动向，对网络安全防御进行持续的优化，持续提升网络空间的安全性。

参考文献

- [1] 王德. 威胁网络安全的因素及防范对策研究 [J]. 网络安全技术与应用, 2021, (12): 162-163.
- [2] 宋佩阳. 计算机网络安全威胁因素与防范策略 [J]. 网络安全技术与应用, 2021, (11): 162-163.
- [3] 莫媛淇, 陈智慧. 信息通信网络安全威胁与漏洞分析 [J]. 电子元器件与信息技术, 2021, 5(07): 247-248+250.
- [4] 方滨兴, 时金桥, 王忠儒, 余伟强. 人工智能赋能网络攻击的安全威胁及应对策略 [J]. 中国工程科学, 2021, 23(03): 60-66.