Engineering Technology and Development, 工程技术与发展 (17)2022,4
ISSN:2661-3506 (Online) 2661-3492(Print)

人工智能技术在大数据网络安全防御中的运用

江志晃
广东培正学院　广东省　广州市　510830

摘　要：现今，伴随着我国科学技术水平的不断提高，计算机网络技术越来越复杂，其广泛应用于人们的社会生产和日常生活中，因此，在当今的大数据时代，网络安全的重要性日益凸显。然而，在保护消费者网络数据的安全性方面仍存在着一些问题。人工智能作为一种新兴技术，具有重要的防御作用，在实践中，通过应用人工智能技术维护大型数据网络的安全，可以提高大型数据网络的安全性与稳定性，帮助人们在日常生活中高效地进行信息的处理，确保计算机网络的安全运行。因此，本文主要对大数据网络安全防御中人工智能技术的运用进行分析。
关键词：人工智能技术；大数据；网络安全防御；运用

The application of artificial intelligence technology in big data network security defense

Jiang Zhihuang
Guangdong Peizheng College, Guangzhou City, Guangdong Province 510830

Abstract: Nowadays, with the continuous improvement of China's science and technology level, computer network technology is more and more complex, and it is widely used in people's social production and daily life, therefore, in today's big data era, the importance of network security is increasingly prominent. However, there remain some issues in protecting the security of consumer network data. Artificial intelligence as an emerging technology, has an important defensive role, in practice, the application of artificial intelligence technology to maintain the security of large data network, can improve the security and stability of large data network, help people efficiently for information processing in daily life, to ensure the safe operation of the computer network. Therefore, this paper mainly analyzes the application of artificial intelligence technology in big data network security defense.
Keywords: Artificial intelligence technology; Big data; Network security defense; Application

大数据时代的来临，在给人们的工作生活带来便利的同时也带来了安全隐患，甚至会给企业带来严重的经济损失。因此，为了最大程度提高网络安全系数，相关部门在大数据网络防御中运用了人工智能技术，以满足实际的工作和生活需求。

1 关于人工智能和网络安全防御概述

1.1 人工智能技术

当前，人工智能技术作为我国科学发展的新型产物，其类型较多，其中较为常见为智能识别、智能搜索、智能控制等。人工智能技术在运用的过程中主要是结合网络信息或者设备存储的信息，根据其信息指令展开运用，它主要通过模仿人类大脑的结构，这样则可以为人们提供所需的信息内容。在实际运用人工智能的过程中，该技术所产生的效果尤为明显，从其运用人工智能技术的系统中可以发现系统为人们呈现的内容更加人性化，但人工智能技术在运用的过程仍存在一定的问题，所以，我国仍需不断研究人工智能技术，对人工智能技术的运用进行相对的调节和优化，让人工智能技术可以运用到各个领域中并发挥独特的价[1]。

1.2 大数据网络安全防御

计算机病毒的侵入、个人信息的窃取，增强了人们对网络使用的安全性意识， 也对大数据网络安全防御提出了更高的要求，而利用人工智能技术进行大数据网络安全防御，既可以实现对计算机的保护，还能提高个人信息的安全性，这也是人工智能技术在大数据网络安全防御应用的根本目的。从目前的情况来看，防火墙技术、入侵检测技术、垃圾邮件自动检测技术、神经网络系统、人工免疫技术以及专家系统等都是大数据网络安全防御的构成要素。

2 人工智能技术在大数据网络安全防御的运用优势

2.1 良好处理模糊数据能力。在大数据网络安全防御中，人工智能技术应用广泛，且发掘能力越来越强，在防御大数据网络安全过程中，处理模糊数据能力非常高，可更好地实现其应用价值。在网络安全防御工作中，模糊数据处理

能力可提升网络系统安全性，准确处理不确定性问题。开放性是网络主要特点之一， 能够实现快速传播数据信息，在管理网络安全中具有必要性，应用人工智能技术可提升处理数据能力，特别是在处理不确定信息方面作用明显[2]。

2.2 学习推理能力较强。人工智能技术主要模仿人类的大脑，但其中的内容却需要不断的更新，因为人的大脑是灵活多变，思维在不断发展，而人工智能技术只能通过在系统中输入的信息为人们提供服务，所以，人工智能技术在运用过程中要不断改进，尤其是安全防御能力的改进，相关的研究人员需要让其技术可以具备较强得自身学习能力，这样在遇到问题时则可以及时应对，并且在自动更新的过程中也能再次对知识进行整合，让系统更加优化。学习推理能力的增加会让人工智能技术可以实现网络防御协助能力的提升，在一定范围内实现对自身运行安全维护，这也就指出人工智能技术的优势[3]。

2.3 计算的成本比较低。传统的网络安全防御系统在运用的过程中十分容易受到自身因素的限制，在处理大量信息时会出现故障无法正常运行，并且也无法满足是计算机处理信息量，这样则会导致计算机出现超负荷的现象。而通过优化的网络安全防御系统，在运用的过程中则有效的解决了传统网络安全防御系统的问题，人工智能技术的优化实现了该系统对资源的整合，并且提升了计算能力，这样就可以为计算机节省空间，也能降低计算成本，在抵御外界干扰的过程中为人们创造优质的服务。因此，我国各个行业在发展的过程中，应加强对人工智能技术优化的关注，要合理的运用人工智能技术，在保障网络信息安全运用安全的基础上，使用人工智能技术创造经济效益，进而在我国科学技术的引领下，更好的发展。

3 防御大数据网络安全现状分析

在一定程度上，互联网技术的发展会加快人工智能技术的发展速度，能够更大程度保证大数据网络安全防御能力。但是在发展网络安全过程中也存在不足之处，研究数据显示，我国网络安全事故发生率较高，严重威胁了网络用户利益，降低了网络使用安全性。多项研究表明，人为因素是诱发网络安全主要因素，数据泄露是较为严重的网络安全问题。应用人工智能技术能够很好地避免网络安全问题，对提升网络安全防御能力具有非常重要作用，人工智能技术的引入，可帮助完善网络安全体系建立。

4 关于大数据网络安全防御中人工智能技术运用探究

4.1 网络防火墙技术

在对人工智能技术进行改进的过程中，相关的专业人员将其网络防火墙技术融合在人工智能技术中，与传统的网络防护墙技术的区别时，该技术既具有相应的硬件和软件设备，与此同时，网络内部和外部也构建一层安全保护屏障，这样则可以有效的提升人工智能技术在运用时的安全性，计算机网络可以安全的运行保障人工智能技术的正常运转。此外，经过创新的人工智能网络防火墙技术也可以结合周围网络，构建一个安全可靠的网络通信系统，进而对外部网络进行相应的隔离，抵御外界网络的入侵。而人们在使用人工智能技术时，该系统可以直接防止外界用户的直接访问，该技术的出现有效的提升了网络环境使用的安全性。 并且也增强了计算机网络技术抵御病毒的性能，让计算机可以处于稳定的状态运行，这对于我国企业而言具有良好的影响，企业可以合理规范的运用人工智能防火墙技术，维护企业内部的私密信息[4]。

4.2 垃圾邮件自动检测技术

在人们日常使用邮箱的过程中，垃圾邮件地出现在给其带来困扰的同时，也给大数据网络安全防御带来了巨大的挑战。邮件作为人们工作中的一个重要的沟通渠道，如果在发送过程中出现漏洞，容易引起邮件被不法分子利用的安全事故。

而垃圾邮件自动检测技术的应用，可以为邮箱的正常使用提供安全保障。垃圾邮件自动检测技术指的是利用智能化的邮件识别系统，实现对垃圾邮件的检测，合理避免垃圾邮件中携带的不良信息入侵计算机内部系统。

4.3 人工神经网络技术

人工神经网络技术是人工智能技术的典型代表，近年来已广泛应用于网络安全防御工作中。神经网络具有较高的容错能力与学习能力，不仅可满足许多信息处理的具体要求，还能实现对多种类型信息的并行处理、高效存储[5]。在网络安全防御领域，人工神经网络技术的应用主要集中在网络入侵检测方面。计算机用户在上网时往往会遭受垃圾信息、恶意软件的干扰与攻击，人工神经网络技术可充分发挥处理元的作用，对各类垃圾信息以及违法软件进行检测并作拦截处理，让计算机免受侵害。在网络安全防御管理中，网络监测需要用到 agent 决策算法，人工神经网络的运用不仅能让agent决策算法更加精准无误，而且极大提高了网络监测的效果[6]。在对病毒进行检测时，人工神经网络可对新型蠕虫技术进行安全监测，这是传统检测技术无法办到的。

4.4 人工智能系统中的专家系统

人工智能系统中的专家系统是最重要的防御方式之一，其发展较为完善。专家系统的应用可以为整个网络安全防御工作提供基本的理论经验和优质的实践经验，还可以指导网络防御系统对各项信息进行准确的辨识和判断，从而全面提升整个网络安全防御系统的稳定性。

结束语

综上所述，人工智能作为一种新型的先进网络技术，具有重要的信息处理能力，能够有效拦截和处理网络中的有害

信息，保障大型数据网络的安全。并为保护大数据网络安全方面的具体应用深入研究人工智能，以提高计算机网络运行安全和信息处理的效率的目的。

参考文献

[1]李泽宇.人工智能技术在网络安全防御中的应用探析[J].信息通信，2018（11）：136-139.

[2]廖宇翔.人工智能技术在网络安全防御中的应用[J].信息技术与信息化，2021（6）:182-184.

[3]吴京京.人工智能技术在网络安全防御中的应用探析[J].计算机与网络，2017,43(14):60-61

[4]崔英敏.大数据时代人工智能在计算机网络技术中的应用策略研究[J].电子商务，2020(05):24-25.

[5]焦少波，沈浩，陈鑫.探索网络空间安全防御当中人工智能技术的应用[J].网络安全技术与应用,2021(2):171-173.

[6]王逸鹤，黄亦.面向网络安全防御防护的大数据平台架构研究[J].信息安全研究，2021,7(1):75-80.