人工智能和大数据技术在计算机网络安全防御中的应用探析

牛帅帅

山东机场信息科技有限公司，山东 济南 250100

摘　　要： 伴随先进科学技术发展，计算机网络环境日趋复杂化，对网络安全防御手段提出了更高的要求。在计算机领域，人工智能和大数据是先进的科学技术，具备高效、自动、快速处理网络数据的能力，如何发挥两种技术的优势，提高网络安全防御水平，保证用网环境的可靠性、安全性和稳定性，成为计算机人员关注的重要问题。本文简介人工智能与大数据技术，从自动学习和推理、处理模糊数据、协助网络处理入手，阐述人工智能和大数据在网络安全防御中的优势，结合非法网络攻击行为、网络入侵技术、用户安全意识，分析计算机网络安全现状，围绕网络防火墙、安全防御系统、安全预警、入侵检测、智能控制，探讨人工智能和大数据技术在计算机网络安全防御中的应用。

关 键 词： 人工智能；大数据技术；计算机；网络安全防御；应用

Application of Artificial Intelligence and Big Data Technology in Computer Network Security Defense

Niu Shuaishuai

Shandong Airport Information Technology Co., LTD. Jinan, Shandong 250100

Abstract: With the development of advanced science and technology, the computer network environment is increasingly complex, and higher requirements for network security defense means. In the field of computer, artificial intelligence and big data is advanced science and technology, has the ability of efficient, automatic, fast processing network data, how to play the advantages of two technologies, improve the level of network security defense, ensure the reliability, security and stability of network environment, become an important problem of computer personnel. Artificial intelligence and big data technology, from automatic learning and reasoning, processing fuzzy data, assist network processing, expounds the advantages of artificial intelligence and big data in network security defense, combined with illegal network attacks, network intrusion technology, user security consciousness, analysis of computer network security situation, around network firewall, security defense system, security warning, intrusion detection, intelligent control, discusses the application of artificial intelligence and big data technology in computer network security defense.

Keywords: artificial intelligence; big data technology; computer; network security defense; apply

引言

在互联网技术高速发展时代下，计算机网络风险层出不穷，各个行业对网络安全防御的要求不断提高。计算机网络系统的开放性极强，各类人群都可通过互联网，检索和搜集所需信息，在无形中面临着较大的安全风险。对此，相关工作人员有必要科学地运用先进技术手段，更新网络安全防御和管理体系，让计算机系统能够自动、持续地防范病毒入侵和非法攻击，提高应对非法入侵行为的能力，降低网络安全风险。

一、人工智能与大数据技术概述

（一）人工智能技术

人工智能指的是计算机仿照人的思维方式，建立工作模型，完成特定工作内容。社会生活和生产领域存在诸多高危工种，工作人员面临高危作业风险，而人工智能恰好能够通过模拟人的思维方式，处理信息、传递信息和指令，替代工作人员，执行一些高危工作任务，既能够提高工作效率，又能保证工作人员的生命安全[1]。与传统技术相比，人工智能具备较强推理能力和学习能力，可自动提取底层数据，建构数据库，且具有较强稳定性，支

持自动升级和动态输出数据，在各个领域展现出良好应用前景。

（二）大数据技术

伴随计算机网络的广泛使用，人们生活、工作与计算机网络的联系日益紧密，网络中信息量呈现爆发式增长[2]。面对网络中大规模、复杂化、海量化的数据，大数据技术具备整合各个领域信息的能力，在特定软件和设备的支持下，快速采集、分析和处理数据，以可视化的方式呈现出来。从数据分析角度的角度看，大数据技术主要包含数据安全与隐私保护、数据可视化、数据处理与分析、数据存储与管理、数据采集等。

二、人工智能和大数据技术在网络安全防御中的优势

（一）具备自动学习和推理能力

人工智能技术具备自动学习和推理能力，在融合大数据技术的基础上，在网络环境治理中具有突出作用[3]。在网络安全管理和保障领域，传统方式存在一定滞后性和局限性，未能涉及防御手段的自动学习和推理，很难有效清除多方面的风险，防御效果不理想[4]。而通过运用人工智能技术，工作人员能够突破既定网络安全防御手段的限制，将人工智能融入网络安全防御的总体设计中，发挥其在学习和推理作用，保证网络安全防御体系的先进性，提高系统的信息处理能力和网络安全防御水平。

（二）具备处理模糊数据的能力

在网络安全防御领域，凭借处理模糊数据的能力，人工智能与大数据技术展现出强大的应用优势。在计算机网络安全体系中，通过运用人工智能与大数据技术，工作人员能够升级网络安全防御体系，提升系统问题处理能力，及时发现和响应不确定性问题[5]。尤其是在复杂的网络环境中，大量数据信息在应用的同时快速传播，信息内容体现出了不确定性，给网络安全管理工作带来新挑战。而通过发挥人工智能与大数据技术优势，工作人员能够提高系统分析、甄别和处理信息效率，高效地处理网络中的模糊数据。

（三）具备协助网络处理能力

在复杂的网络安全环境中，人工智能与大数据技术是工作人员开展网络安全防御工作的助手，对充分整合和运用各项防御手段，抵御网络安全风险具有重要意义[6]。在网络安全防御工作中，通过运用人工智能与大数据技术，工作人员能够兼顾各个层次管理任务，协调实现上层、中层与下层管理功能，完善网络安全管理和防御体系，实现网络安全防御目标。

三、计算机网络安全现状

（一）非法网络攻击行为不断增多

在网络环境下，连接互联网的设备类型不断增多，除了 PC 端，为快捷地获取和传递信息，人们开始运用移动终端设备连接网络，再加上网络运行模式和架构的变化，计算机网络系统面临的安全风险越来越复杂，随之诞生了各类病毒和木马程序[7]。对于不同系统终端和执行程序，黑客利用各终端交互和连接的漏洞，开展非法网络攻击，甚至诞生了持续变异和传染的病毒，使计算机网络安全防御难度增加。

（二）网络入侵技术水平日益提高

在数字化转型过程中，各个行业利用先进技术、设备，优化生产经营模式，在享受网络带来便利的同时，也存在一些安全隐患[8]。部分人未能树立网络安全意识，过于看重经济利益，出现了盲目地使用或盗用他人信息现象[9]。同时，计算机和大数据类人才不断增多，对网络攻击手段和入侵技术的研究越来越深入，涌现出隐蔽性、传染性和破坏性更强的病毒，甚至有不法分子利用垃圾邮件，传播病毒。

（三）网络用户安全防护意识不强

部分网络用户尚未认识到网络安全防护的重要性。部分用户未能接受系统的教育和训练，对计算机网络安全专业知识和技术了解不够深入，学习网络防御技术的主动性不足，甚至不了解计算机网络安全防御的概念和构成[10]。同时，部分用户对网络安全规范缺乏了解，不了解正确操作与违法操作的界限，在用网过程中容易忽视安全提示，产生违法违规行为。

四、人工智能和大数据技术在计算机网络安全防御系统中的应用

（一）应用于网络防火墙模块

在计算机网络安全防御中，防火墙技术得到广泛应用，广受普通用户与企业用户的欢迎，为工作网络、家庭网络安全提供屏障。由于防火墙手段的应用范围较为广泛，部分用户忽视了网络安全防御体系的漏洞和不足，误认为防火墙能解决任何安全问题，抵御所有安全风险，导致网络中出现大量安全问题[11]。在设计计算机网络安全防御体系时，为提高防范水平，设计者可运用人工智能与大数据技术，改进防火墙防护手段[12]。在具体实施阶段，设计者可建立双层防火墙，第一层防火墙为常规防火墙，主要通过设置访问权限，避免外部用户入侵内网。第二层防火墙是基于子系统的防火墙，设计者可利用人工智能技术，了解内部用户的网络访问行为，限制内网用户的违规行为，避免病毒有可乘之机。在此基础上，工作人员可借助人工智能与大数据辅助功能，构建外部与内部双重防护机制，搜集和监测不良访问行为，提高整个系统的安全防范质量。

（二）应用于安全防御系统

移动端与 PC 端是网络攻击的主要来源，黑客的攻击范围具有不确定性，且部分病毒在计算机系统的潜伏时间较长[13]。对此，在构建网络安全防御体系时，为完善系统的防御功能，设计者应从实际情况出发，充分考虑网络安全防御需求，构建具有主动防御功能的安全防护系统，实现网络攻击和病毒的防范目标。在具体设计环节，设计者可应用人工智能与大数据技术，结合计算机网络安全系统实际情况，从六个维度优化防护安全防御功能。一是管理系统配置功能；二是管理系统中用户行为的功能；三是管理系统的安全策略功能；四是实时监控网络状态的功能；五是生成和存储网络运行日志；六是生成网络运营报表。在人工智能处

理模型与大数据技术的支持下，设计者能够扩展和完善系统的安全防御功能，满足计算机在应用中的实际需要。

（三）应用于安全预警模块

在计算机网络安全防御中，由于各软件程序实现条件和开发语言存在差异，大数据应用中心主要通过多个软件，以集成形式实现数据分析功能，在使用过程中出现了多个接口，计算机网络容易因接口差异，产生安全漏洞[14]。所以，在计算机网络安全防御体系中，设计者应运用人工智能与大数据技术，如智能事件分析处理技术、高性能协议分析技术、行为技术，引进高精准度传感器，建立安全预警模块，主要包含漏洞、行为和攻击趋势预警，提高原始事件分析精准度。基于漏洞预警信息，实时地检测和定位系统漏洞，为漏洞修复提供依据；基于行为和攻击趋势预警信息，诊断网络环境中的异常状态或数据信息，判断是否在安全范围。

（四）应用于智能控制模块

在计算机网络安全防御领域，设计者可应用人工智能与大数据技术，引入智能处理知识库，建立智能控制模块，实现防火墙、交换机与路由器的联动智能控制，高效地分析和挖掘各种安全问题，避免网内数据被窃取[15]。借助人工智能的自主学习能力，设计者可针对木马和病毒，建立安全防御模型，使系统自动更新知识库，有效拦截互联网攻击。借助大数据技术，智能控制模块能够针对入侵事件，生成处理预案，解决同类型网络安全问题。

五、结束语

综上所述，面对多样化的非法网络攻击和入侵手段，传统网络安全防御体系已经难以满足时代要求。因此，计算机工作人员应紧跟科学技术发展趋势，结合大中国需求，将人工智能和大数据技术应用在安全防御总体设计中，建立起更智能的网络安全防御系统，使系统具备自我更新、自主学习、自我修复功能，实现计算机入侵事件的快速响应、自动处理和智能解决，全面提高计算机网络防御能力，为各个行业发展提供安全、稳定、优质的网络环境。

参考文献

[1] 陆华. 基于人工智能与大数据的计算机网络安全防御系统研究［J］. 信息与电脑（理论版），2024,36(03):47-49.

[2] 孙瑜. 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分析［J］. 网络安全和信息化，2024,(02):143-145.

[3] 刘王宁. 大数据及人工智能技术的计算机网络安全防御系统［J］. 网络安全技术与应用，2023,(10):67-69.

[4] 贾珺. 人工智能技术在大数据网络安全防御中的运用研究［J］. 天津职业院校联合学报，2023,25(09):31-35+54.

[5] 项建德. 基于大数据的计算机网络安全防御系统建构分析［J］. 信息记录材料，2023,24(09):53-55.

[6] 李晓. 人工智能技术在计算机网络防御中的应用研究［J］. 信息与电脑（理论版），2023,35(16):212-214.

[7] 徐楚原. 大数据及人工智能技术的计算机网络安全防御系统设计分析［J］. 数字技术与应用，2023,41(07):216-218.

[8] 邓玉，宋良，孙剑. 基于人工智能技术的计算机网络安全防御系统设计［J］. 无线互联科技，2023,20(14):147-149.

[9] 李凤鸣. 基于大数据及人工智能技术的计算机网络安全防御系统［J］. 电子技术与软件工程，2022,(17):1-4.

[10] 宋午阳，张尼. 基于大数据及人工智能技术的网络安全防御系统设计策略［J］. 网络安全技术与应用，2022,(07):56-57.

[11] 耿杨. 人工智能技术在大数据网络安全防御机制中的应用研究［J］. 数据，2022,(01):48-50.

[12] 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.

[13] 曹琰. 人工智能技术在大数据网络安全防御中的运用［J］. 郑州铁路职业技术学院学报，2020,32(04):37-38+58.

[14] 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.

[15] 张健. 人工智能技术在大数据网络安全防御中的应用［J］. 信息与电脑（理论版），2020,32(16):136-137.