ISSN:2661-3719(Print); 2661-3727(Online)

人工智能技术在网络空间安全防御的应用

王　君
西藏民族大学　咸阳市渭城区　712082

摘　要：运用人工智能技术实现网络空间安全防御，有助于提升网络信息安全水平。基于此，本文以网络安全防御和人工智能技术概述为出发点，比较分析了人工智能技术相较于传统网络安全防御技术的优势，探讨了关联规则挖掘技术、神经网络技术、智能防火墙技术在网络安全防御中的应用实践。在网络安全防御中，深化人工智能技术的应用推广，能够充分挖掘人工智能技术在信息安全防护方面的价值，有效抵御各类安全威胁，为网络空间安全提供保障。

关键词：人工智能技术；网络安全防御；应用

引言：

当前我国经济发展越来越迅速，相应的网络与计算机技术发展速度也在加快，推动了人工智能技术的发展，并使该技术在多个行业得到广泛应用，人们对其重视度越来越高。人工智能技术发展潜力较大，是一种新型技术，在网络安全防御中得到广泛应用，安全性较高，对降低安全事故发生率具有非常重要的作用。本文对数据网络安全防御中人工智能技术的应用进行了分析。

1　网络安全防御和人工智能技术概述

1.1 网络安全防御概述

网络安全防御主要是指运用各种技术和方式来保护和防御计算机网络，使其能够免受病毒和木马程序的威胁和入侵。网络安全防御的防御方式和技术比较多，一般采用监视和检测的方式进行防御，且防御的效果各不一致。目前网络安全防御应用较为广泛的技术为被动信息保障技术、入侵检测技术以及主动诱骗技术。随着网络空间应用的广泛深入，网络空间安全防御也对传统网络技术提出了新的要求，人工智能技术便是其中一个关键技术。

1.2 人工智能技术概述

人工智能是关于人造物的智能行为，而智能行为包括知觉、推理、学习、交流和在负责环境中的行为（Nilsson，1998年）。人工智能技术（Artificial Intelligence）是现代计算机科学技术领域的一种新型技术，伴随着现代科学技术水平的不断发展，它可以模拟人的思维活动来进行系统保护，当网络在使用期间受到外部威胁和攻击，便可以自主地实施系统防御保护。人工智能技术在进行实际应用时，需要多种学科进行相关协调和融合，从而使得其能够实现理论和技术的互相渗透和结合，以形成模仿人类大脑活动的智能技术。

2　人工智能技术在网络安全防御中的应用优势

2.1 模糊数据推理能力的优势

人工智能技术能够实现对模糊和非线性信息的模糊信息推理，使得其能够有效的辨别出信息的来源和类型，特别是在对未知病毒的检测防御中，人工智能技术的防御能力更强。在模糊信息处理中合理应用人工智能技术，可以对网络信息进行有效的网络安全防御，使得网络信息的安全性和确定性能够有效进行提高。

2.2 学习推理能力的优势

人工智能技术的应用，能够依托其强大的学习、推理等能力，弥补传统安全防御技术的不足，通过对网络安全体系及数据库的建立，实现对不同网络资源及攻击的有效识别和防御。因此，人工智能技术的学习、推理能力，能够有效提升网络空间安全防御能力，通过安全预防机制要素的不断生成，以弥补传统防御体系的不足。与此同时，面对庞大的数据库，人工智能技术的查询、推理分析等功能，能够及时发现有效信息，建立安全防御响应，进而更好地提高网络空间安全防御的实效性。

3　网络安全防御系统中的重要人工智能技术

3.1 关联规则挖掘技术

在海量复杂网络信息的传输、处理过程中，要采用给予规则的关联技术，对网络系统内设备运行、数据传输的情况进行综合分析，掌握网络安全隐患、报警事件，与现有日志数据之间存在的关联关系。这一过程中主要将网络安全攻击、报警事件产生后的序列模板，与安全

作者简介：王君，出生年月：1973.1，民族：汉，性别：女，籍贯：陕西，单位：中西藏民族大学，职位：无，职称：高级工程师，学历：硕士，邮编：712082，邮箱：575515320@qq.com，研究方向：计算机网络安全

事件发生的对应规则序列做出匹配，对正在传递的数据信息、数字签名进行验证，以此降低网络安全系统的非法控制情况。因而人工智能安全系统的规划设计部门，主要通过建立公共事件信息资源的采集接口，以及运用关联数据挖掘、专家评估等方式，从后台数据库的海量数据资源中，提取出与网络安全攻击、报警事件相关的代码数据，准确识别各种入侵风险，形成一套关联引擎的安全资源类目，将其存储在后台数据库之中。

3.2 神经网络技术

稳定的神经网络通常是基于多个简单处理元构建而成的，拥有良好的兼容性以及优异的学习能力，能够在极短的时间内完成各类信息的分布储存。在神经网络运用过程中能够符合各种信息处理的实际需求，完成相关知识的自动组织；另外，神经网络中涵盖的神经元计算一般是独立的，能够完成并行处理工作，现阶段已有的软件、硬件等都可以确保其发挥自身的价值和优势。将神经网络技术应用到计算机网络空间安全防御工作中，一般体现在对网络入侵的检测，这是由于神经网络技术能够精准识别出计算机网络中掺杂的无用信息、不良软件等，从而协助计算机网络信息的分析与处理。此外，agent决策算法是网络监测与管理中的重要手段，通过融入神经网络技术一方面可以有效强化网络监测效率与质量，另一方面也能够很好的防范各种小型监测误差的产生。在进行网络蠕虫病毒检测工作时，神经网络技术也能够很好的满足检测要求。与以往检测方式不同的是，神经网络技术拥有非常高的效率与准确性，同时还能够准确识别出各种蠕虫病毒。现阶段，计算机科学领域对神经网络技术的研究十分重视，并推动了有关领域的不断前进，将神经网络技术应用到网络空间安全防御中也逐渐增多，为促进网络空间安全防御能力的提升奠定基础。

3.3 智能防火墙技术

防火墙是计算机网络安全常用的防御手段，它可以对网络中的安全隐患进行识别和控制，从而对计算机设备起到很好的防护效果。传统的防火墙技术包括数据包过滤、网络地址转换（NAT）、协议状态检查以及VPN功能等，但这些防火墙的应用却没有达到预期的效果，难以全面有效抵御安全隐患。基于人工智能技术的智能防火墙拥有入侵检测功能，可应用于对外部入侵危险元素的智能化识别工作中，同时通过计算、统计与记忆数据内容对数据进行相关的分析和控制，实现对网络中海量数据的计算，发现网络中的特征值内容，对其进行相关的安全访问控制防御逸提高对危害信息的拦截能力。

4 结束语

综上所述，网络安全防御需要先进的技术作为支撑，人工智能技术作为一项新兴的技术，其学习能力和模糊数据处理能力，更适用于网络安全防御的发展，人工智能技术的应用，不但可以有效改善网络安全防御存在的问题，也能够提高网络安全管理的有效性和技术性，对于促进我国网络安全防御发展有着较大的有利之处。

参考文献：

[1]叶新英.基于大数据的计算机网络安全问题[J].郑州铁路职业技术学院学报，2019（4）：16-17+21.

[2]柏苗，万丽.基于大数据时代探索人工智能在计算机网络技术中的应用[J].中国新通信，2018（3）：89.

[3]任小成.基于大数据时代人工智能在计算机网络技术中的应用分析[J].中国战略新兴产业，2018（4）：17.

[4]温斯琴，王彪.基于神经网络的计算机网络安全评价仿真模型[J].现代电子技术，2017（3）：89-91.

[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.网络安全技术与应用，2021（2）：171-172.