

# 人工智能技术在大数据网络安全防御中的应用

仝彦荣

冀中能源集团有限责任公司 河北 邢台 054000

**摘要:** 人工智能技术作为各项技术中一种极具发展潜力的技术,其在大数据网络安全防御中的应用,对保护大数据的安全具有极其重要的现实意义。本文探讨了人工智能技术在大数据网络安全防御中的关键应用及其显著优势。通过深入分析模糊数据处理、学习推理能力、网络防御协助、智能防火墙、入侵检测、神经网络系统、数据挖掘与融合、垃圾邮件防御以及人工免疫技术等多个方面,揭示了人工智能如何有效提升大数据网络的安全性与防御能力,为构建更加稳固的网络安全体系提供了理论依据与实践指导。

**关键词:** 人工智能; 技术; 大数据网络; 安全防御; 应用

引言: 随着大数据时代的到来,网络安全问题日益凸显,成为制约信息技术发展的关键因素之一。传统的网络安全防御手段已难以满足日益复杂多变的网络威胁需求。在此背景下,人工智能技术的引入为大数据网络安全防御带来了革命性的变革。本文旨在全面阐述人工智能技术在大数据网络安全防御中的应用现状、优势及具体实践,以期对相关领域的研究与实践提供参考。

## 1 人工智能和网络安全防御概述

### 1.1 人工智能技术概述

人工智能科技和人们日常生活之间的关系非常密切,比如人们生活中常用的智能控制、智能搜索、指纹识别和机械视觉等就属人工智能科技领域范围。它是互联网知识和计算机技术为依据,针对人体大脑的建模,综合运用生理学、运动学和语言学等设计的相应软件,建立出人工智能系统,并显示出智能行为。

### 1.2 网络安全防御概述

近年来,电脑中毒事件和互联网信息被盗案件时有发生,导致了群众对安全持续重视,同时对安全防护的要求随之提高。通过采用不同技术手段和方法,可以对计算机网络实施防御保护,从而实现防止病毒对网络计算机产生危险和入侵的效果,这正是网络空间安全防护的意义。在现代信息安全时代背景下,安全防范主要涉及主动诱骗技术、入侵侦测技术和被动信息安全保护技术<sup>[1]</sup>。

## 2 人工智能技术在大数据网络安全防御中的应用优势

### 2.1 模糊数据的处理优势

在探讨大数据网络安全防御的语境下,人工智能技术的引入不仅革新了传统防御手段,更在模糊数据处理方面展现出了无可比拟的优势。模糊数据,作为大数据环境中不可避免的组成部分,往往蕴含了不确定性、非结构化等特性,给传统防御机制带来了巨大挑战。然

而,人工智能技术凭借其强大的学习和推理能力,能够有效地解析和处理这些模糊数据,精准识别潜在威胁,从而在源头上提升防御效果。具体而言,人工智能技术通过深度学习、模糊逻辑等算法,能够模拟人脑处理复杂信息的过程,对模糊数据进行高效整合与分析。这一过程不仅增强了系统对不确定性病毒的识别与拦截能力,还能够在保护用户隐私的前提下,实现数据价值的最大化利用。此外,人工智能技术的实时性和自适应性,使得它能够根据网络环境的动态变化,灵活调整防御策略,维护了网络安全的持久稳定性。但尤为重要的是,在大数据网络防御越来越广泛的大背景下,人工智能技术的运用也为建立更完善、智能的防范系统创造了机会。经过不断学习与改进,人工智能技术可以不断应对新的风险类型,从而有效应对个人信息泄露的安全风险,为客户的安全保驾护航。同时,由于人工智能技术在大数据处理与安全防范中的模糊处理功能,不仅提高了防范效率,更彰显了其在未来网络安全领域的广阔应用前景。

### 2.2 强大的学习推理能力

在过去,我们对大数据防范的理解仅局限于防范、管理和协调等层面,忽视在大数据网络防范中的认知与推演过程,使得在大数据网络防御中的功能与特色都无法被真正的充分发挥起来,由于这种在传统模式下的“治标不治本”的方法所具有的特殊性,给互联网信息系统的的天性增加了极大的变数,也为电脑木马、互联网病毒的肆虐带来了可乘之机。而人工智能技术在大数据防护中的运用不但突破了传统大数据网络防护的诸多局限,也提升了大数据网络防护的效率。此外,人工智能技术在大数据网络安全防范中的广泛运用,也推动了大数据网络防御技术和各产业间的有机融合,这也是人

人工智能技术在大数据网络安全防范运用中,其具备了良好的机器学习推理功能的关键原因所在。

### 2.3 网络防御的协助优势

在大数据安全网络防御的广阔舞台上,人工智能技术的融入不仅是对传统防御手段的革新,更是对防御体系整体效能的全面提升。面对网络环境的日益开放与快速变化,人工智能技术的应用复杂性与系统性日益凸显,这要求我们在实践中不断探索与优化。当前,我国网络环境规模持续扩张,数据流量呈爆炸式增长,这无疑给大数据安全网络防御带来了前所未有的挑战。为有效应对这一局面,加强各防御系统之间的协同合作显得尤为重要。通过构建智能化、一体化的防御体系,实现不同防御模块之间的信息共享与策略联动,能够显著提升防御的响应速度与精准度,有效抵御来自各方的网络攻击。同时,提升大数据安全网络防御的管理能力也是关键一环。这包括建立健全的管理机制、优化资源配置、加强人员培训等方面。通过引入先进的人工智能管理工具,实现防御过程的自动化与智能化,减轻人工负担,提高管理效率。此外,加强网络安全意识教育,提升全员参与网络防御的积极性,也是构建坚固防御体系不可或缺的一环<sup>[2]</sup>。

### 2.4 具有比较强的学习推理能力

传统意义上,人们只觉得网络安全的保护措施重点在于进行防范与管理双方的相互配合,而没有对相关技术的掌握与运用能力加以重视,这确实可以改善用户的网络安全防护问题,但却没有从根本上对网络安全进行维护。由于上述防治手段的限制,也将会使得网络信息处理具有很大的不确定性。不过,当使用人工智能技术手段时,完全能够克服这些问题,真正意义上完成了网络安全防御和理论知识的有机融合,使网络安全防护技术拥有了基本的认知与推理工具。另外,由于互联网网民的规模呈现相当大的增长,这就会导致大规模的处理信息,提高了互联网防御的困难系数。人工智能技术一旦实现了知识推理功能后,将可以大大提高数据资料的处理质量,对于保障当前的互联网环境安全性有着很大意义。

## 3 人工智能系统在网络安全防御中的应用分析

### 3.1 智能防火墙技术

防火墙在整体互联网防护中具有非常关键的作用,良好的防火墙技术可以让互联网屏蔽掉各种安全隐患,从而达到良好的计算机设备与终端的防护作用,一般的网络防护终端尽管设置更高的防火墙,但其防护性能仍不理想。人工智能防火墙产品,将改变中国传统防火墙

在安全防护上的困境,它会依照人工智能系统来智能的对网络系统中存在的各类安全隐患进行统计与分类,从而做出更有效、精准的信息拦截措施,而在应对非法入侵的过程中,人工智能防火墙技术还会实现自我更新与修补,从而避免了网络安全中的明显缺陷,从而达到了安全防护效率的提高。

### 3.2 入侵检测技术

入侵检测技术已成为信息安全中的重要防线,其重要性在电子商务和移动支付服务(如微信支付、支付宝支付)广泛应用的今天,尤其突出。这种便利的服务手段极大地推动了经济社会发展和生活方式,但同时也对网络安全保护提出了更多需求。入侵侦测技术通过实时检测网络流量、系统日志和异常行为模式,可以精确辨识和预防可能的非法入侵、信息盗取、非法浏览等网络安全风险,有效保证了客户的信息安全和个人隐私。另外,由于大数据分析技术的蓬勃发展,以及互联网信息量的爆炸性增加,入侵检测技术仍需要继续改进,以应对错综复杂的互联网环境。而新型的入侵检测技术融合机器学习、人工智能等前沿技术,可以自动识别海量信息,并智能识别未知的危险,实现从被动防御到主动防御的转变,显著提升网络和大数据安全防御的精准度与效率,为构建更加安全、可信的网络空间奠定坚实基础。

### 3.3 神经网络系统

神经网络系统,作为现代网络安全防御体系的核心组件,其强大功能远不止于简单的信息收集与处理。这一系统犹如智能大脑的延伸,在网络空间的浩瀚数据中穿梭,不仅高效收集各类信息,还具备敏锐的监测能力,能实时捕捉网络流量的微妙变化,对潜在威胁进行深度剖析。其内置的计算引擎,如同精密的计算器,快速处理海量数据,提取关键特征,为决策提供坚实支撑。更重要的是,神经网络系统凭借其卓越的识别分析能力,能够精准辨别入侵因素,无论是已知的病毒攻击,还是复杂多变的零日漏洞利用,都能迅速响应,有效预防。这一特性,正是人工智能技术在网络安全领域的深度应用与体现。通过将人工智能技术融入神经网络建设,系统能够不断学习进化,自我优化识别模型,提升对未知威胁的预测与防御能力,从而构建起更加坚固、智能的网络安全防线<sup>[3]</sup>。

### 3.4 数据挖掘与融合

人工智能技术在大数据网络安全防御领域的深度应用,不仅限于数据的简单收集与存储,更在于其强大的数据挖掘与融合能力。这一过程如同在浩瀚的数据海洋中淘金,通过复杂的算法模型,自动筛选出有价值的信

息片段,并进行深度分析与整合,从而揭示出隐藏的数据关联与趋势,为安全决策提供有力支持。在数据挖掘的基础上,人工智能技术还能实现数据的智能分类与标签化,使得海量数据变得有序可循,便于后续的安全分析与处理。同时,结合先进的计算机传感器技术,人工智能系统能够突破传统检测手段的局限,实现更广泛、更深入的入侵检测,即便是面对复杂多变的网络攻击,也能迅速响应,精准定位威胁源头,有效遏制病毒扩散,确保网络环境的安全与稳定。此外,人工智能技术的持续学习与进化能力,使其能够不断适应新的安全挑战,优化防御策略,为大数据网络安全防御体系注入源源不断的活力与智慧。

### 3.5 垃圾邮件网络安全防御

在维护网络安全的征途上,垃圾邮件如同一颗隐藏的定时炸弹,不仅侵扰用户的日常通信,还可能携带恶意软件,对整个网络系统的稳定性和安全性构成严重威胁。因此,构建一套高效、智能的垃圾邮件防御体系至关重要。人工智能技术在此领域展现出了卓越的能力,它通过深度学习和自然语言处理等技术,精准识别邮件内容中的特征模式,有效区分有用信息与垃圾信息。这一过程不仅涉及对邮件标题、正文、发件人信誉度等多维度信息的综合分析,还能实时学习最新的垃圾邮件特征,快速适应不断演变的攻击手段。更重要的是,人工智能系统能够自动化生成详尽的报告文件,为网络安全管理员提供直观的威胁情报,包括垃圾邮件的来源、类型、危害程度等关键信息,有助于快速响应并采取相应的防御措施。这种智能化的决策支持,极大地提升了网络防御的效率和准确性,为构建安全、健康的网络环境奠定了坚实基础。

### 3.6 人工免疫技术

人工智能技术在大数据防范中的广泛应用,与之相伴的人工免疫技术也获得了快速的普及。人工免疫科技是在大数据安全防御的模式下产生并开发出来的一项智能科技,它能够模拟人脑处理事务的方法,解决传统

计算机的数据安全不足的问题,保障了计算机的安全运作,并实现了对病毒的迅速截获与处理。人工免疫方法主要由否定选择、基因库和克隆三个阶段所构成。其中,基因库说的是能够有效阻挡病毒的攻击;克隆指的是针对病毒的入侵性,给整个系统再克隆一种同样的病毒,从而对病毒进行更深层次的研究,并为用户创造安全的大数据环境。人工智能技术在大数据防护方面的运用能够提高计算机的网速,使其能够一直处在高速运转的状态中,进行数据资料的高速传输,并为用户创造安全的大数据环境。人工智能技术在大数据防护方面的运用能够提高计算机的网速,使其能够一直处在高速运转的状态中,进行数据资料的高速传输<sup>[4]</sup>。

### 结束语

人工智能技术的引入,为大数据网络安全防御带来了前所未有的变革与提升。通过模糊数据的精准处理、强大的学习推理能力、网络防御的协同优化以及具体应用场景如智能防火墙、入侵检测、数据挖掘与融合、垃圾邮件防御和人工免疫技术的不断创新,我们见证了AI在构建更加稳固、智能的网络安全防线中的核心价值。未来,随着技术的不断进步和融合,人工智能将在大数据网络安全领域发挥更加重要的作用,为信息社会的健康发展保驾护航。

### 参考文献

- [1]赵学栋.人工智能技术在大数据网络安全防御中的应用研究[J].计算机产品与流通,2020(05):153-153.
- [2]杨斌.人工智能技术在大数据网络安全防御中的应用[J].计算机产品与流通,2019,000(003):142-142.
- [3]胡文娟.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),2018,416(22):155-156.
- [4]吴彦坤.大数据网络安全防御中人工智能的创新应用思考[J].产业科技创新,2019,32(32):106-108.
- [5]鲍豫鸿.基于大数据时代计算机网络技术中人工智能的应用解析[J].粘接,2020,319(09):108-111.