第 1 卷◆第 2 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

# 人工智能技术在网络空间安全防御中的应用

刘胜西
河南经贸职业学院 计算机工程学院
DOI:10.12238/acair.v1i2.6444

[摘　要] 随着互联网的普及和网络威胁的不断演变,网络空间安全已成为人们关注的焦点。传统的网络安全工具和方法往往难以应对复杂和多样化的网络攻击。人工智能技术的快速发展为网络空间安全提供新的方法。人工智能技术通过模拟人类智能行为和决策过程,实现智能化的网络安全防御,更好地发现和应对威胁。本文探讨人工智能技术在网络空间安全中的各种应用,包括威胁检测、入侵防御、威胁情报分析和漏洞管理等领域。
[关键词] 人工智能技术；网络空间；安全防御；应用
中图分类号：TP18　文献标识码：A

## Application of Artificial Intelligence Technology in Cyberspace Security Defense

Shengxi Liu
College of Computer Engineering, Henan Institute of Economy and Trade
[Abstract] With the popularization of the Internet and the continuous evolution of cyber threats, cyberspace security has become the focus of people's attention. Traditional cybersecurity tools and methods often struggle to cope with complex and diverse cyberattacks. The rapid development of AI technology provides a new approach to cyberspace security. Artificial intelligence technology simulates human intelligent behavior and decision-making processes to achieve intelligent cyber security defenses and better detect and respond to threats. This article explores the various applications of AI technology in cybersecurity, including threat detection, intrusion prevention, threat intelligence analysis, and vulnerability management.
[Key words] artificial intelligence technology; cyberspace; security defense; application

## 引言

在当今数字化时代,网络攻击不仅在数量上呈不断增长的趋势,而且攻击方式也变得越来越复杂和隐匿。传统的网络安全方法和工具往往难以应对这一挑战,因此,人工智能技术的崭露头角成为网络空间安全防御的新方向。人工智能的发展使得计算机系统能够模拟人类智能,从而更好地识别和应对各种威胁,提高网络的安全性。本文将探讨人工智能技术在网络空间安全防御中的应用,以及其对网络安全的潜在影响。

## 1 网络空间安全防御体系中存在的问题

### 1.1访问权限问题

首先,弱密码和密码重复使用是访问权限问题的主要根源。用户经常使用容易猜测或破解的密码,导致攻击者更容易入侵系统或账户。其次,多因素认证,虽然提供了额外的安全性层次,但钓鱼攻击欺骗用户提供多因素认证的信息,绕过安全措施。最后,企业组织内部复杂的层次结构和多个系统,导致权限管理的混乱,从而增加潜在的风险。所以应加强密码策略和访问权限管理。用户应创建强密码,并使用密码管理工具来生成和保存密码。企业应实施强制性密码策略,明确密码复杂性要求和密码更改周期。采用多因素认证,同时应加强对社会工程和钓鱼攻击的防护。此外,建立自动化的权限管理系统,以更好地管理和维护用户权限,减少管理难度[1]。

### 1.2隐私安全问题

首先,隐私安全问题涉及到未经授权访问个人信息和财务数据,导致大规模的数据泄露事件,对用户的隐私和财产构成威胁。其次,随着物联网设备的广泛使用,越来越多的个人数据被收集和存储,导致数据被滥用或不当使用。最后,某些不法机构滥用网络监控权力,侵犯公民的隐私权,引发合法性和伦理问题。

数据加密和访问控制是保护个人信息和财务数据的关键,企业应实施强制性数据加密和访问控制策略,以确保只有授权人员能访问敏感数据。同时,应明确规定数据收集和使用的限制,以保护用户的权益。对于物联网设备,制造商应强制内置隐私和安全控制,以防止滥用用户数据。最后,监管机构应强化对于不法机构的监控[2]。

1.3存储管理问题

首先,大规模数据的存储和管理需要大量的基础设施,而基础设施可能成为攻击目标。数据中心和云存储服务提供商需要采取物理和网络层面的安全措施,以保护存储的数据。其次,数据备份不充分会导致数据的永久丢失。组织应定期备份数据,并测试灾难恢复计划以确保其有效性。最后,数据在多个利益方之间的传输和存储可能引发争端。针对存储管理等问题,企业应对数据的存储位置和归属权问题进行法律和合同的明确定义,以解决潜在的争议。

综合来看,网络空间安全防御体系面临的问题涉及访问权限、隐私安全和存储管理等多个方面。解决以上问题需要综合的方法,包括教育和培训用户,加强密码策略和权限管理,实施数据加密和访问控制,加强隐私政策和法规,强化数据备份和灾难恢复计划,以及明确数据存储和归属权,更好地保护用户的隐私和数据安全。

## 2 人工智能技术在网络空间安全防御中的应用和技术类型

2.1安全态势感知技术

首先,安全态势感知技术结合深度学习和人工智能技术。通过深度学习算法,分析网络流量、日志文件和系统活动数据,识别异常行为和潜在威胁。同时,其还利用人工智能专家知识库,以提供实时的决策支持和应对策略,使系统能够快速检测和应对各种网络威胁。其次,安全态势感知技术的应用领域非常广泛。首,例如,在企业网络中,应用安全态势感知技术,能及时发现并应对潜在的威胁,减少数据泄露和系统漏洞的风险,而个人用户能应用安全态势感知技术保护个人隐私和财务信息,防止个人信息被黑客盗取。最后,安全态势感知技术能够提高网络空间的安全防御敏感度。通过实时监控和深度分析网络活动,快速发现新的威胁和漏洞,确保网络环境的安全和稳定。此外,安全态势感知技术能限制用户操作权限,防止内部威胁。通过审计和检测用户行为,及时发现员工的不当行为,减少企业的内部风险[3]。

2.2关联规则挖掘技术

关联规则挖掘技术是一项在多源异构计算机网络中数据挖掘的重要技术,其目的是识别和提取隐藏的关联规则信息,以增强网络操作的安全性和稳定性。这项技术结合人工智能分类挖掘算法和非监督分析方法,以及关联规则矩阵中的关键信息定期提取,用于发现网络空间安全防御体系中的功能缺陷问题。首先,关联规则挖掘技术的基本原理是通过分析多源异构计算机网络中的数据,发现数据之间的关联规则。数据包括网络流量数据、日志数据、系统活动数据等,挖掘的目标是识别不同数据之间的关联。其次,关联规则挖掘技术的应用领域非常广泛,例如,在网络入侵检测和网络安全监控中,通过挖掘网络数据中的关联规则,及时发现潜在的攻击和异常行为,从而提高网络安全性；在威胁情报分析领域具有重要作用。通过分析不同来源的威胁情报数据,揭示攻击者的行为模式和目标,帮助程序员及时制定有效的应对策略。另外,关联规则挖掘技术能优化网络性能,提高网络的稳定性和效率。最后,关联规则挖掘技术有助于发现网络空间安全防御体系中的功能缺陷问题。通过挖掘数据之间的关联规则,揭示系统中的弱点和漏洞,帮助程序员及时修复和增强网络的安全性。此外,其能加强网络操作的安全性和稳定性,保障网络的安全[4]。

2.3大数据分析技术

大数据分析技术将大数据分析与网络安全相结合的强大工具,用于对多源异构网络进行深度分析,并将分析结果用于辅助用户决策。大数据分析技术在网络安全领域具有广泛的应用,其整合多种线性和非线性分析要素,确保数据分析的安全性,同时深入处理和分析多维度数据。首先,大数据分析技术的核心原理是利用大数据技术来处理和分析来自多源异构网络的海量数据,包括网络流量、日志、事件记录以及其他相关信息。通过数据清洗和预处理,消除数据中的噪声和冗余信息,提高数据质量。接着采用数据挖掘和机器学习算法,从数据中发现隐藏的模式、趋势和异常,再将分析结果以可视化的方式呈现,以帮助程序员更好地理解网络安全状况。其次,大数据分析技术在网络入侵检测和威胁情报分析、网络性能优化领域、恶意软件检测和预测等方面发挥重要作用。最后,大数据分析技术整合多种线性和非线性分析要素,包括传统的网络流量分析、日志分析、行为分析,帮助系统更全面地了解用户的网络活动,增加发现威胁和异常的可能性。此外,确保数据分析结果的安全性,通过加密和权限控制等手段,保护敏感数据免受未经授权的访问[5]。

2.4交互式网络分析技术

交互式网络分析技术允许用户与系统进行交互操作,帮助监管不同网络空间部署的硬件设施,以快速发现问题和安全漏洞,从而提高安全防御能力。首先,交互式网络分析技术的核心原理是通过用户与系统的互动,实时监测网络的状态和性能。用户使用合适的权限进行网络控制和管理操作,从而能够快速发现潜在的问题和安全漏洞。其次,交互式网络分析技术在网络入侵检测和事件响应、网络性能监控和优化、网络安全培训和模拟演练中得到应用,能帮助网络专业人员提高应对网络威胁的能力。最后,交互式网络分析技术的重要性在于其能够提高网络的安全防御能力。通过实时交互操作,用户能够迅速发现和解决网络中的问题,从而降低潜在威胁的影响。此外,通过用户的口令和授权进行交互操作,从而保护系统,免受未经授权的访问[6]。

## 3 人工智能技术在网络空间安全防御中的应用

3.1构建人工智能网络安全平台架构

首先,整合人工智能技术,包括机器学习、深度学习和自然语言处理,构建人工智能网安平台架构是应对不断演进的网络威胁和提高网络空间安全性的关键。其次,人工智能网安平台架构的核心原理是利用大数据分析和机器学习算法,对网络流量、日志数据和其他网络信息进行实时监测和分析。通过构建数据分析模型,快速识别异常行为、潜在威胁和漏洞。分析模型能自

动学习和适应新的威胁,从而提高网络安全性。此外,应用自然语言处理技术用于分析文本数据,例如恶意软件分析报告和威胁情报,帮助网络管理员更好地理解威胁环境。人工智能网安平台架构的应用非常广泛,其在网络入侵检测和威胁情报分析中发挥重要作用。通过分析大规模数据,平台能自动发现网络中的异常行为、恶意软件和潜在攻击；在恶意软件检测和防护中,平台能自动识别和隔离恶意软件,帮助保护终端设备和数据[7]。总之,构建人工智能网络安全平台能提升网络安全的安全性。

3.2安全防御设施的部署和配置

随着网络威胁不断演进和增加,应采取适当的安全措施,设置防火墙,能过滤网络流量、识别潜在威胁和保护内部网络不受外部攻击。防火墙的配置需要考虑流量规则、访问控制策略和日志记录,以确保网络操作的安全性。例如,病毒防火墙能检测和阻止恶意软件、病毒和恶意脚本的传播。部署和配置病毒防火墙时,程序员需要定期更新病毒定义库,并设置实时监测和自动隔离功能,以迅速应对病毒威胁。此外,应当配置邮件过滤器来检测和阻止恶意附件和链接。除了防火墙和病毒防火墙,采用网络入侵检测系统(IDS)和网络入侵防御系统。IDS可以监测网络流量和系统活动,检测潜在的入侵行为,而IPS则可以主动阻止恶意活动。另一安全设施是虚拟专用网络(VPN),其能加密数据传输,保护敏感信息不受窃听和拦截。最后,应定期备份和存储设施,保障数据安全。总之,部署和配置安全防御设施,如防火墙、病毒防火墙、IDS、IPS、VPN以及备份和存储设施。配置设施时,程序员需要考虑合适的规则、策略和算法,以确保网络操作的安全性和稳定性。

3.3非线性网络的安全强化模式

首先,非线性网络的安全强化模式旨在通过全程监督和分类判断操作来解决网络空间中的安全隐患问题。与传统线性网络安全方法不同,非线性网络的安全强化模式使用非线性算法和技术,以适应网络威胁的多样性和复杂性,基于机器学习、深度学习、自然语言处理等领域的非线性算法,通过实时分析网络流量、日志数据和其他结构化和非结构化数据,快速识别和应对威胁。非线性算法能够更好地捕捉网络威胁的复杂性和多样性,因为其能处理非线性关系、多维度数据和大规模复杂性,包括各种深度学习技术,如卷积神经网络(CNN)、循环神经网络(RNN)和自动编码器,以及自然语言处理技术,用于分析文本数据。程序员通过综合运用非线性算法,实现全程监督和分类判断操作,从而提高网络安全。最后,非线性网络的安全强化模式在网络安全领域的应用前景广阔,其能用于网络入侵检测和威胁情报分析,以提高网络的实时威胁感知和快速应对能力,进行恶意软件检测和分析,识别潜在的风险和安全隐患。

## 4 结束语

人工智能技术在网络空间安全中的应用为网络安全领域带来新的希望。针对威胁检测、入侵防御、威胁情报分析、漏洞管理和访问权限控制等多个领域,通过机器学习、深度学习和自然语言处理等技术,人工智能能够更好地分析和理解网络数据,自动发现威胁、恶意行为和漏洞,为网络管理员和安全专家提供强大的工具,以更好地保护网络中的数据和信息安全。

## [参考文献]

[1]贾晓东,张冰.网络空间安全智能主动防御关键技术的思考与实践[J].科技创新与应用,2020,(32):152-153.

[2]温丽丽,王彦沣,赵静,等.云计算环境下网络安全空间的搭建探究[J].信息与电脑(理论版),2020,32(20):175-177.

[3]敖道恒.人工智能技术在网络空间安全的应用[J].电子技术与软件工程,2020,(15):254-255.

[4]杨林,陈实.网络空间动态防御技术[J].保密科学技术,2020,(06):4-8.

[5]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):151.

[6]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.

[7]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.

## 作者简介：

刘胜西(1994--),男,汉族,河南郑州人,硕士,助教,研究方向：人工智能、情感计算。