网络空间安全防御当中人工智能技术的应用

周琳唯
四川省双流棠湖中学，中国·四川 成都 610000

摘　要：随着科技的进步发展，人工智能技术作为一种先进的科技手段崭露头角。在网络空间安全领域，人工智能技术展现出巨大的应用潜力和发展前景，互联网的广泛普及虽然极大地为人们的生活提供便利条件，但也带来日益严重的网络安全隐患。为保护用户信息安全，人工智能技术被融入网络空间安全防御中，有效地侦测并应对网络中的信息安全风险，以此来提升网络信息的安全性。

关键词：网络空间；安全防御；人工智能技术

The Application of Artificial Intelligence Technology in Cyberspace Security Defense

Linwei Zhou
Sichuan Shuangliu Tanghu Middle School, Chengdu, Sichuan, 610000, China

Abstract: With the advancement of technology, artificial intelligence technology has emerged as an advanced technological means. In the field of cyberspace security, artificial intelligence technology has shown great application potential and development prospects. Although the widespread popularity of the Internet has greatly facilitated people's lives, it has also brought about increasingly serious network security risks. To protect user information security, artificial intelligence technology is integrated into network security defense, effectively detecting and responding to information security risks in the network, in order to enhance the security of network information.

Keywords: cyberspace; security defense; artificial intelligence technology

0 前言

在信息技术日新月异的今天，人们的日常生活已与网络紧密相连。但网络空间中的安全威胁层出不穷，网络攻击事件频发，严重威胁用户的信息安全，甚至带来财产损失或人身安全问题。为打造一个安全、便捷的网络环境，必须加强网络空间的安全防御能力。人工智能技术在这一领域的应用能有效识别和隔离各类网络威胁，为网络安全问题提供有力的技术支持。而从高中生的角度来说，能帮助他们更好地理解现代科技如何保障网络安全，还可以激发他们对科技和今后职业的兴趣和规划，并通过人工智能技术，也能更主动地应对网络安全挑战，确保网络空间的安全稳定。

1 人工智能技术的概述

1.1 安全态势的感知技术

众所周知，安全态势感知技术在计算机网络空间安全防护领域具有重要作用，该技术能准确对接 AI 专家知识库与相应的基础设施，实现对数据链路层和网络层的综合管控，确保网络环境的稳定性与安全性。在实施过程中，网络安全管理人员要对本地及分布式网络实施全方位监控，并深入观察操作环境中潜在的安全隐患，通过融合深度学习理念与人工智能技术的原理，尽可能打造出更智能化的安全环境监测功能。根据安全态势感知技术，能对网络空间的安全性能进行严苛的审核，同时有效约束用户的操作权限，以此来提升网络防御的响应速度。在应用该技术时，要对经典案例进行反复演练和对硬件设施进行定期安全检查，来增强系统的安全防护能力，还可以保障网络环境的持续稳定，为用户提供更信赖的网络服务。通过不断优化和升级安全态势感知技术，将更有信心应对日益严峻的网络安全挑战，捍卫网络世界的和平与安宁。

1.2 关联规则性挖掘技术

关联规则挖掘技术潜力与价值逐渐凸显，该技术针对不同的网络空间环境，能建立更周全、精细的安全防护系统，并赋予操作安全审计以动态灵活性。通过分析多源异构网络数据，准确捕捉其中潜藏的关联规则，为用户在网络中的安全航行提供保障。在实施过程中，关联规则挖掘技术需要从数据链路层和网络协议层两个方面入手，利用智能化的分类挖掘算法与非监督分析方法的融合，能定期从复杂的关联规则矩阵中提炼出重要信息，并在深度降维技术的辅助下，更深入地探索主成分结构的内涵与价值 [1]。

1.3 交互式网络分析技术

交互式网络分析技术以出色的集成能力，在网络安全领域大放异彩，该技术能实现对分布于不同网络节点的硬件设施的集中化监控与管理，并通过准确识别用户输入的指令，为他们提供丰富多样、高效实用的解决方案。在交互式网络分析技术的支持下，计算机网络的安全防线实现全面加固，系统也能即时评估交互操作的合规性与准确性，可以迅

速发现并应对网络环境中的安全隐患。这样不仅大幅度提升网络空间的整体安全水平，更为用户带来更稳定、流畅的网络体验。另外，交互式网络分析技术还能帮助用户对已训练完成的样本数据进行解读，通过对计算机网络架构模式进行全方位的安全审计，该技术进一步确保交互信息的保密性，能有力增强网络空间的抵御能力。而在这一过程中，既加深对网络空间安全状况的理解，更为建立坚不可摧的网络安全屏障贡献智慧与力量。

2 人工智能技术在计算机网络防御的应用优势

2.1 认知与推演技能

人工智能技术在网络安全领域的应用已成为一道坚固的防线，能强化防御层级并确保网络环境的整体安全。但网络技术的发展也带来新的挑战，网络安全形势日趋复杂和严峻。层出不穷的网络安全问题，既种类繁多且变化迅速，这让依赖专家知识和固定应对规则的传统防御手段响应迟缓。与此同时，专业安全人才的短缺更加剧这一困境，让有效应对当前及未来安全威胁变得越发困难。在该背景下，人工智能技术的介入为网络安全防御注入新的生机与活力，其出色的识别与高效处理能力，能进一步提升防御的实时性和准确性。与传统技术相比，人工智能展现出更卓越的学习和推理能力，并通过对大量数据的深度分析，自我优化和进化，从而作出更精准的决策和预测，还有助于实现数据资源与重要信息的有效整合，更高网络安全防御的智能化和自动化水平。因此，在网络安全防御的实践中，应积极利用人工智能技术，不断探索其更深层次的应用，以此来提升防御效率，建立更坚实、全面的网络安全防护体系。

2.2 模糊信息处理能力

网络环境的错综复杂带来数据信息的多样化和异构性，对传统网络安全技术构成不小的挑战。特别是那些非结构化、非线性的数据，它们如同难解的谜团，常常让传统技术束手无策，在网络安全的防御体系中留下不小的隐患。但人工智能技术的出现，为该难题提供有效的解决方案，利用关联分析、深度学习等技术手段，人工智能能对这些模糊信息进行高效处理，这如同拥有洞察先机的能力，能提前感知网络中潜在的安全威胁，实现防患于未然，提升网络对模糊数据的处理能力 [2]。

2.3 高效稳定的算力

在计算机网络防御的战场中，算力能及时应对各种网络安全隐患的关键。而在这方面，人工智能技术展现出令人瞩目的实力，其算力之强大，主要体现在对大量数据的从容应对及对非线性数据的处理，通过模拟人类的学习与思维方式，人工智能能不断完善自身的知识架构，形成无与伦比的计算能力。在 CPU 和 GPU 等硬件技术的助力下，人工智能的计算能力更是实现提升。当前，能轻松应对大量的网络信息，为技术人员减轻沉重的负担，在网络安全防御的实践中，人工智能技术全天候地进行数据分析、整合与检测工作，为技术人员提供有力的后盾。通过其强大的数据处理能力，技术人员能对各个模块进行分类解析，更高效地检测和应对各种网络安全隐患。

3 网络空间安全防御当中人工智能技术的应用

3.1 智慧防火墙技术的运用

防火墙是现代计算机网络安全的基础，担当着捍卫网络空间安全的重任，能迅速侦测并遏制网络中潜在的风险，为计算机设备提供稳定的防护。但当面对错综复杂且不断演变的网络威胁时，传统的防火墙技术常显疲态，而正是在这样的背景下，人工智能防火墙技术的应用，凭借卓越的数据挖掘与风险评估能力，能进一步分析网络中的各类安全隐患，并在威胁触及计算机系统之前就将其拦截。这种预防性的安全策略，能成功遏制恶意攻击的发生，更在本质上弥补传统防火墙在防御方面的不足 [3]。

另外，该技术对安全访问控制策略进行优化，确保只有授权用户才能触及敏感资源，并显著提升网络系统的整体安防水平。而对于高中生来说，更应该理解这项技术，了解人工智能在网络安全领域中的优势和可能，通过领悟人工智能防火墙的运作制度和应用场景，来提升自身的网络安全素养，更为将来投身科技行业、研发更先进的网络安全技术奠定坚实的基础。

3.2 反垃圾邮件的安全策略

根据人工智能技术的强大功能，能更高效地实施网络空间中的垃圾邮件防御手段，保障网络环境的稳定与安全运行。在当前网络生态中，垃圾邮件泛滥成灾，这些邮件不仅会扰乱系统的正常运作秩序，更对网络安全构成一定挑战，尤其是众多垃圾邮件暗藏木马程序与病毒，一旦这些恶意邮件渗透到网络空间且没能得到及时应对，便会引发整个网络的恶意攻击事件。为提升网络空间的安全防御层级，对垃圾邮件进行准确识别与分析显得尤为重要，人工智能技术在该领域中发挥着重要作用，能提高对垃圾邮件的识别准确度，并有效遏制这些邮件的扩散，阻断其进入网络空间的途径。

从网络防御的战略角度出发，应该建立一套完善的反垃圾邮件系统。该系统将建立坚实的防线，抵御垃圾邮件与恶意软件的侵袭，来全面提升网络空间的整体安全防护水平。除此之外，人工智能技术还能提供分析已经识别垃圾邮件的能力，通过对邮件的分析与系统整合，编纂出内容详细的防护报告，为今后防范垃圾邮件的工作提供有力的数据支持，让防御策略更准确、高效。这种以数据为驱动的防御模式，既优化垃圾邮件的处理流程，更彰显人工智能技术在网络安全领域的潜力与价值。从高中生的角度来说，应理解并掌握这些技术原理，有助于他们在学习与工作中更好地保护个人隐私与信息安全，同时也为职业发展铺设坚实的基础。

3.3 安防设施的规划与安装

通过周密的部署与合理配置的安全防御措施，可以促成人工智能系统与网络空间安全防御制度之间的无缝衔接，

保障各项安全策略能顺利高效地执行。在如今错综复杂、同源异构的计算机网络环境下，传统的安全防护手段时常很难全方位地抵御各类潜在的网络威胁，这无疑对等保制度的有效落地构成一定挑战。因此，需要引入更先进的安全防御措施，来加固网络空间的安全堡垒。

例如，通过引入网络防火墙、病毒防火墙等高效的安全防护工具，不仅能大幅度提升网络系统的整体防御能力，还能更好地符合网络空间实时共享的特性，为数据信息的采集、交换与共享提供更牢靠的安全保障。而这些先进防御措施的合理运用，有助于建立更坚实的网络安全屏障，还为广大用户营造一个更安心、稳定的网络操作氛围。但单纯依赖安全防御措施的部署与配置并不足以确保网络环境的绝对安全，作为网络空间的重要参与者，高中生这类网络用户应进一步提升对计算机网络操作环境的安全检查意识，确保在网络活动中的每一个环节都能严格遵守安全规范。只有这样，才能在网络空间安全领域建立坚不可摧的防线。

3.4 打造网络安全平台框架

通过进一步建立和完善人工智能网络安全平台架构，可以实现人工智能技术与网络空间安全防御体系的深度融合。该架构将显著提升网络管理人员的工作效能，让他们能更准确地执行各项安全管理任务。同时，该架构还具备分析不同网络环境潜在风险的能力，从而为企业提供更全面的安全防护。

另外，该平台的高灵活性也让其能轻松适配各种高级别的安全防护标准，有效应对不断变化的网络安全威胁。在具体实施阶段，将注重人工智能系统与专家知识库的高精度对接，不断优化 AI 网安平台的各项功能，并提升其性能表现。与此同时，还将注重提升网络安全态势的感知层次，确保 AI 系统的判断与辅助决策能力达到高度协同，通过打造数据标准一致的 AI 网安平台，能有效挖掘并修复本地网络空间安全防御体系中的漏洞，实现对网络空间中各类安全威胁与隐患的迅速识别与有效处置。

3.5 在样本训练过程的应用

在人工智能技术的广泛应用中，对于安全防御系统的建设具有积极的作用，特别是在安全势态感知与预测功能的实现方面，该功能结合历史数据和网络实时状态，对未来网络安全趋势进行准确预测，并为防御策略的制定提供重要依据，保障网络空间的整体安全。针对该理念，AI 技术贯穿于安全防御系统建设的多个重要环节，如样本训练、参数优化算法设计以及系统仿真测试等。

例如，样本训练环节，主要通过大量的历史数据对安全系统进行深度训练，让系统能进一步理解并掌握基本的安全防护规则，从而在复杂多变的网络环境中游刃有余。具体来说，向系统展示各种病毒样本、恶意代码等安全威胁，并利用 AI 技术出色的学习能力，让系统能逐渐建立起针对这些威胁的有效防御体系，这样在实际应用中，系统才能展现出强大的基础防御实力。而在实施阶段，工作人员要根据 AI 技术的学习特性，合理确定训练样本的规模，在通常情况下，利用 BIC 准则建立 ARMA 模型，通过这一模型精确计算出所需的训练样本量。在此基础上，根据这一计算结果，工作人员策划并制作出各类训练样本，确保系统能得到全面且高效的训练，从而不断提升其抵御安全威胁的能力。

4 结语

综上所述，在人工智能技术的推动下，网络安全防御系统在设计理念和应用实践方面都取得一定进展，该系统凭借全面的功能、出色的通用性，以及对用户体验的充分考量，在计算机系统安全防护领域大放异彩，并赢得用户的信赖。今后为不断增强系统的可维护性和扩展性，希望软件开发人员能不断精进技艺，以更精湛的编程技艺和高效的代码实现，为系统注入更多创新且实用的功能，经过长时间的努力，推动网络安全防御系统向着更健康、更可持续的方向发展，提升其应用价值，拓展其广阔的应用前景。

参考文献：

[1] 白杨,周益民.人工智能技术在网络空间安全学科建设中的应用探究[J].中国教育学刊,2024(2):I0037.

[2] 贾焰,方滨兴,李爱平,等.基于人工智能的网络空间安全防御战略研究[J].中国工程科学,2021,23(3):98-105.

[3] 廖文佳.人工智能在网络空间安全领域的应用探究[J].信息记录材料,2024,25(7):71-73.