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

大数据时代人工智能（AI）在计算机网络技术中应用分析

张　翼

中国航空工业集团公司 洛阳电光设备研究所　河南洛阳　471000

摘　要：本文旨在深入探讨大数据时代中人工智能在计算机网络技术中的应用。通过概述大数据和人工智能的基本概念及其相互关系，强调在网络技术中应用的优势，如提高效率、增强安全性、优化资源管理。在具体应用策略方面，探讨了构建智能防火墙、优化数据信息管理、生成智能入侵检测以及计算机内部业务模块配置处理等关键策略。本文旨在为读者提供对大数据和人工智能在网络领域的全面理解，强调其在提升网络性能和安全性方面的潜在价值。

关键词：大数据时代；人工智能；计算机；网络技术

引言

随着科技的迅速发展，大数据时代为计算机网络技术带来了新的挑战与机遇。在这一背景下，人工智能（AI）也得到了迅速崛起，2019 年，37% 的组织在工作场所使用人工智能。2015 年至 2019 年间，在商业中使用 AI 的企业数量增长了 270%。因此，人工智能成为推动网络领域革新的关键动力。大数据和人工智能的融合为网络提供了巨大的优势，不仅在提高效率、优化资源管理方面具备潜在能力，更在加强网络安全性、实现智能服务等方面展现出前所未有的潜力。本文将深入探讨大数据时代中人工智能在计算机网络技术中的应用，旨在为读者呈现这一科技融合的新局面。

1. 大数据和人工智能的概述

大数据的概念涵盖了数据的多样性、速度、规模和价值。在大数据时代，能够采集和存储以前无法想象的数据量，包括社交媒体信息、传感器数据、交易记录等。这些数据的快速增长为未来网络提供了丰富的信息资源。同时，人工智能作为处理这些庞大数据的利器，通过智能算法和模型使得能够从这些海量数据中提取有意义的信息 [1]。

人工智能则是以计算机程序的使用模拟人类认知过程实现智能化。机器学习、深度学习等技术使计算机能够从经验中学习，逐渐提高其在问题解决和决策制定上的准确性。以生成对抗网络（GANs）为例，其就是代表性的深度学习模型类型，其能够实现数据的生成与处理，其训练过程主要包括生成器训练、判别器训练。在计算机网络中，人工智能的应用不仅体现在数据处理上，更体现在网络管理、安全防护等方面，提升了网络的自适应性和智能化水平。

2. 大数据时代人工智能在计算机网络技术中的应用优势

2.1 提高网络效率和性能

在大数据时代，网络面临着越来越复杂和庞大的数据流量，传统的网络管理和优化手段已经显得力不从心。而人工智能技术的引入为网络效率提升提供了新的途径。通过大数据分析，智能算法能够更好地理解网络中的数据流，识别出关键节点和瓶颈，并通过自适应的方式对网络进行调整和优化。

2.2 强化网络安全

网络安全一直是计算机网络技术中的重要问题。在 2022 年 9 月，国内的一种“黑客”以木马病毒对超过 2000 台计算机进行非法控制，并入侵了 40 多个国内的金融机构内网数据库，实现交易指令以及内幕信息的非法获取，后进行股票的交易，非法获得了 183.57 万元人民币。大数据时代的人工智能为网络安全性提供了新的解决方案。智能防火墙的建立通过实时监测庞大的网络流量，能够准确地识别并阻止潜在的威胁，提高了网络的抗攻击能力，保障了网络的安全性。

2.3 优化资源管理

大数据时代，网络不仅仅面临着庞大的数据流量，还有着各种各样的业务需求。通过人工智能的资源管理系统，网络可以更加智能地分配和管理资源，确保每个业务模块都能够得到足够的支持。通过大数据分析，网络管理者可以更好地了解各个业务模块的运行状况，预测未来的资源需求，实现资源的合理分配和利用 [2]。

3. 大数据时代人工智能在计算机网络技术中的应用策略

3.1 构建智能防火墙

智能防火墙具备自适应学习能力，通过大数据分析实现实时威胁检测。同时智能防火墙则能够通过机器学习不断优化自身的规则，适应网络威胁的动态变化，大幅提高了防护的灵活性。

以一家国际性金融机构为例，该机构的网络面临着持续不断的网络攻击和威胁，包括恶意软件、网络钓鱼和零日漏洞利用等。这家金融机构在构建智能防火墙时，通过大数据分析建立了庞大的网络数据集。这包括历史网络流量、用户行为、异常事件记录等。通过对这些数据的深入挖掘，智能防火墙能够了解正常的网络模式，并识别异常活动，从而建立起对潜在威胁的有效感知，其功能如下图所示。同时，采用机器学习算法，智能防火墙对大量数据进行训练，以了解各种攻击的模式和特征。例如，通过分析以往的网络攻击事件，智能防火墙可以学习到特定的攻击签名、恶意软件的行为模式等。这使得防火墙能够不断提升自身的识别能力，更好地适应新型的威胁。

智能防火墙功能图

在实际运行中，智能防火墙采用实时监测机制，对网络流量进行持续监控。当智能防火墙检测到异常模式或符合先前学到的攻击特征时，它能够立即做出反应，将受感染的设备或用户隔离，阻止潜在的攻击扩散。为了应对零日漏洞攻击，智能防火墙还采用了行为分析技术。通过分析用户和设备的行为模式，防火墙能够检测到尚未被公开披露的漏洞利用。例如，如果某个用户在短时间内尝试多次访问系统中的不同部分，智能防火墙就可能将其行为标记为可疑，并立即采取措施进行阻止。

3.2 优化数据信息管理

引入人工智能的数据信息管理系统，能够通过学习算法识别数据的关键特征，自动进行分类和标签化，从而使得数据更具有组织性和可搜索性 [3]。同时，人工智能在优化数据信息管理中扮演了重要角色，实现了数据质量的自动监测和修复。通过应用人工智能技术，网络系统可以自动检测并纠正数据质量问题，提升数据的准确性和可靠性。

以一国内电商公司为例，该电商公司面对庞大的用户交易数据和商品信息。为了更好地理解这些数据并提高数据质量，公司引入人工智能技术进行数据质量监测。通过建立智能算法，系统能够自动识别数据中的异常值、冗余信息和缺失项。例如，当系统检测到某一批次商品的销售数据异常，可能是由于数据输入错误或者系统故障导致的，智能系统能够自动标记这些异常数据并提示数据管理员进行修复。这样的智能数据质量监测机制有效地减少了因为低质量数据而导致的业务错误和决策偏差。

同时，人工智能在优化数据信息管理中的应用还包括对数据的智能分类和标签化。在这家电商公司的情景中，大量的商品信息需要进行分类，以便于用户搜索和推荐系统的精准运作。通过机器学习算法，系统能够根据商品的属性、销售数据等信息，智能地对商品进行分类并为其打上相应的标签。例如，系统能够自动识别一款商品属于哪一类别、适合哪一类用户，并为该商品添加相应的标签，从而提高了商品分类的准确性和智能性。

在实际运行中，这个电商公司通过人工智能的数据信息管理系统，为用户提供了更加智能和个性化的购物体验。当用户在网站上搜索商品时，系统能够根据其以往的购物历史、浏览行为等数据智能地推荐相关商品，提高了商品推荐的精准性，从而提升了用户的满意度。

3.3 生成智能入侵检测

生成智能入侵检测通过人工智能技术实现了对网络行为的更加精准的分析和识别。借助入侵检测系统能够通过机器学习算法学习网络的正常行为模式，从而更加准确地识别出异常和潜在的入侵行为 [4]。

异常入侵检测可以采用以下算法实现：

每个系统或行为均能够以各类属性进行度量，通过对当前系统、用户行为和正常要求进行对比，就能够实现攻击或者非法行为的识别。设 $x_1,x_2,\cdots\cdots$，xn, 代表 n 个数量测量属性，若测量属性的值越大，则说明系统异常程度就会越高，异常程度的计算公式如下。

$$f(X) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = \sum_{i=1}^{n} a_ix_i^2$$

在上式中，ai 代表属性 i 权重。

在大数据时代，网络流量巨大而复杂，传统入侵检测难以应对。而生成智能入侵检测通过实时监控庞大的网络数据流，能够及时发现异常模式和可能的网络入侵。例如，当系统检测到网络流量中出现异常的数据包传输模式或频繁的非法访问行为时，可以迅速发出警报并采取相应措施，使得网络能够在攻击发生之初即刻做出反应。

通过大数据集的训练，模型能够学习网络正常的行为模式，包括用户的登录模式、设备的通信模式等。例如，员工在工作日的特定时间段登录公司内部系统，而设备在正常情况下会与特定的服务器通信。通过对这些正常行为的学习，深度学习模型能够形成对正常网络活动的基准认知。

同时，建立一个大规模的入侵行为数据库，通过与实际攻击事件的关联，深度学习模型能够逐步学习到不同类型的入侵行为，不断完善其对恶意活动的识别能力。例如，当有新的攻击模式出现时，系统会将相应的数据特征加入数据库，并通过模型的在线学习，使系统能够更早地识别出类似的未知入侵行为。系统实时监控网络流量，将实时的数据与模型学到的行为模式进行比对。当模型发现某一网络行为与已知的入侵特征相匹配时，系统会立即发出警报，并采取相应的阻断或隔离措施。例如，如果系统检测到某用户在短时间内多次尝试访问系统中的敏感信息，模型可能识别出这种行为模式与先前学到的入侵行为相符，触发警报并阻止该用户的访问。

3.4 计算机内部业务模块配置处理

通过人工智能优化计算机内部业务模块配置处理，可以实现对系统性能的智能调优。系统可以根据不同时间段的业务需求，动态调整 CPU、内存等资源的分配，以保证系统在高峰时期能够高效运行，而在低谷时期实现资源的节约。

以一家云服务提供商为例，云服务提供商面临着来自不同客户的各种业务需求，包括计算密集型的科学计算、存储密集型的大数据分析等。在过去，该公司采用静态的业务模块配置，往往导致资源浪费和性能不足。通过引入人工智能技术，他们建立了一个智能化的业务模块配置系统。系统通过大数据分析积累了大量历史业务数据，包括不同业务类型的峰值负载、用户行为模式等。通过这些数据，系统利用机器学习算法能够更准确地预测未来的业务需求。例如，对于某个特定业务，系统可以分析历史数据，了解在不同时间段和日期的负载峰值，从而在峰值时分配更多的计算资源，而在低谷时减少资源分配，实现对计算资源的智能动态调配。

在实际运行中，当系统检测到某一业务类型的负载开始上升时，人工智能系统可以通过实时监控业务流量，迅速做出反应。例如，如果系统预测到一个大规模的数据分析任务即将开始，系统会自动调整相关业务模块的配置，为该任务分配更多的计算和存储资源，确保任务能够在最短的时间内完成。这种实时响应的能力使得系统能够更好地适应不同业务场景下的需求，提高了服务的稳定性和可靠性。

4. 结论

本文深入研究了大数据时代中人工智能在计算机网络技术中的应用。通过构建智能防火墙、优化数据信息管理、生成智能入侵检测以及计算机内部业务模块配置处理等策略，揭示了大数据与人工智能相互融合的潜在优势。这不仅提升了网络性能、优化了资源利用，更强化了网络安全性。未来，期待这些技术的不断演进，为计算机网络领域带来更为创新和可持续的发展，推动数字时代网络技术走向新的高峰。

参考文献

[1] 张江 . 大数据时代人工智能在计算机网络技术中的应用 [J]. 黑龙江科学 ,2022,13(22):103–105.

[2] 傅金睿 , 王雪芬 . 大数据时代人工智能在计算机网络技术中的应用 [J]. 无线互联科技 ,2022,19(15):16–18.

[3] 王成志 . 基于大数据背景下人工智能在计算机网络技术中的应用 [J]. 软件 ,2022,43(7):110–112.

[4] 王宝龙 . 大数据时代人工智能在计算机网络技术中的运用探讨 [J]. 中国新通信 ,2022,24(18):104–106.