 DOI: https://doi.org/10.12345/bdai.v5i6.18991

Network Security Management Methods for Artificial Intelligence and Internet of Things Applications

Yuechao Hui

Suzhou Gaobo Vocational College, Suzhou, Jiangsu, 215163, China

Abstract

In the context of the rapid development of information technology, the application technology of artificial intelligence (AI) and the Internet of Things (IoT) has been widely used in People's Daily life. Artificial intelligence and Internet of Things application technology are modern technologies based on the Internet system. The corresponding network security plays a very important role in the development of enterprises and social stability. Therefore, on the basis of clarifying the application of artificial intelligence and the Internet of Things, the hidden dangers of network security in the technology application at the present stage, which can further analyze the security management strategy of artificial intelligence and the Internet of Things, in order to provide necessary reference for follow-up research.

Keywords

AI; Internet of Things application; network security management

人工智能和物联网应用的网络安全管理方法

惠越超

苏州高博职业学院，中国·江苏 苏州 215163

摘　要

在信息技术快速发展的背景下，人工智能（AI）与物联网（IoT）应用技术在人们的日常生活中得到了广泛的应用。人工智能与物联网应用技术是基于互联网系统进行的现代化技术，对应的网络安全性对企业的发展以及社会的稳定都有着非常重要的作用。为此，在明确人工智能与物联网应用的基础上，对现阶段技术应用中存在的网络安全隐患展开探究分析，能够更加深入的分析人工智能与物联网应用安全管理策略，以期为后续研究提供必要的参考借鉴。

关键词

人工智能；物联网应用；网络安全管理

1 引言

在数字化转型的浪潮中，人工智能与物联网已成为推动社会进步的关键力量，AI 通过深度学习、机器学习等技术赋能物联网设备，使其能够自主决策、优化运行，实现万物互联的智能世界。但这一愿景的实现离不开坚实的安全保障。物联网设备的海量性、异构性、远程访问等特点，加之 AI 算法的潜在漏洞，使得网络攻击面急剧扩大，数据泄露、服务中断、恶意控制等风险显著增加。因此，构建一套适用于 AI 与 IoT 应用的网络安全管理方法，对于保障国家安全、企业利益和个人隐私具有重要意义。

2 人工智能与物联网应用概述

2.1 人工智能概述

人工智能（Artificial Intelligence，简称 AI）是指通过计算机程序或机器来模拟、实现人类智能的技术和方法。其核心在于使计算机具备感知、理解、判断、推理、学习、识别、生成、交互等类人智能的能力，从而能够执行各种任务，甚至在某些方面超越人类的智能表现 [1]。人工智能技术的核心算法包括机器学习和深度学习，这些算法通过大量数据和训练，使计算机能够自动发现数据中的规律，并进行模式识别、分类、预测等操作，逐渐渗透并成熟应用到当今的各个行业当中。人工智能的发展历程大致可以划分为五个阶段：从 1943 年—20 世纪 60 年代为起步发展期，20 世纪 70 年代为反思发展期，80 年代为应用发展期，20 世纪 90 年代—2010 年为平稳发展期，2011 年至今为蓬勃发展期。人工智能的应用领域广泛，如智能家居、智能制造、金融科技、智能医疗、智能安防以及智能交通等诸多领域，对推动社会的发展起到了至关重要的作用。

2.2 物联网应用概述

物联网（Internet of Things，简称 IoT）是指通过信息传感设备，如射频识别（RFID）、红外感应器、全球定位

【作者简介】惠越超（1985–），男，中国江苏苏州人，硕士，讲师，从事移动通信、物联网技术研究。

系统、激光扫描器等，按约定的协议，将任何物体与网络相连接，实现物体间的信息交换和通信，以达到智能化识别、定位、跟踪、监管等功能的一种网络 [2]。物联网的核心在于实现“万物互联”，即将物理世界与数字世界紧密融合，通过智能化手段提升生产、生活的效率和便利性，如图 1 所示。物联网应用涉及多项关键技术，主要包括传感器技术、通信技术、云计算技术、大数据技术以及边缘计算技术等多个关键性技术。因此，物联网技术也被广泛应用于智慧城市、健康医疗、智能家居、工业制造、农业生产等多个领域，而随着科技的不断进步和应用场景的不断拓展，物联网的未来发展会为人们的生活和工作带来更多便利和智能化体验。

图 1 物联网“万物互联”理念图

3 人工智能与物联网应用中的网络安全隐患

3.1 相关操作人员能力不足

在人工智能与物联网技术的广泛应用中，一项不容忽视的问题是部分操作者未能严格遵守网络安全管理规范。在这些操作者中，有些操作者受限于自身的认知水平和教育背景，对于网络安全的复杂性认识不足，尤其是针对病毒攻击与防火墙系统的重要性缺乏应有的警觉。这种忽视不仅降低了个人或企业网络系统的安全防护级别，更使其在面对多样化的网络威胁时显得尤为脆弱。因此，提升操作者的网络安全意识，加强相关培训，确保每位参与者都能充分认识到网络安全的重要性，并熟练掌握防御技能，已成为保障人工智能与物联网技术健康发展的重要环节。

3.2 网络安全管理机制设计不严谨

网络技术研发人员在构建系统时，往往面临网络安全管理机制设计不够周全的挑战。这种不足可能源于对潜在威胁的预见性不足或是对安全措施的重视程度不够。而部分系统操作者在使用过程中，因对系统性能的过度信赖，可能放松警惕，不经意间成为病毒入侵的门户 [3]。一旦系统遭受病毒侵袭，由于网络安全管理机制的缺陷，往往难以及时有效地抵御，导致系统性能受损，甚至用户信息数据的安全受到严重威胁。因此，强化网络安全管理机制的设计与实施，提升操作者的安全意识与操作规范，是保障网络安全、维护信息数据安全的必要之举。

3.3 数据库系统安全受到影响

在大数据浪潮的推动下，数据库系统安全成为了人工智能与物联网应用技术的坚实后盾，但其面临的挑战亦不容忽视。随着技术的飞速发展，公共数据库系统频繁被人工智能与物联网应用所依赖，进行数据存储与处理。然而，若数据库系统的安全管理体系未能紧跟时代步伐，其更新速度迟缓或效果欠佳，将直接削弱对新型安全威胁的防御能力。特别是在木马病毒等恶意软件不断迭代更新的背景下，这种滞后性可能使人工智能与物联网应用面临前所未有的网络安全风险，难以确保数据的安全性与完整性，进而影响技术的稳定应用与发展。

4 人工智能与物联网应用的网络安全管理策略

4.1 加强网络安全管理体系和机制优化

在人工智能（AI）与物联网（IoT）深度融合的今天，网络安全管理体系和机制的加强旨在提升 AI 与 IoT 应用的网络安全防护能力。在加强网络安全管理体系的过程中，应确立网络安全责任制，明确各级管理人员在网络安全中的职责与义务，并制定详细的网络安全管理制度，包括但不限于安全策略、操作规范、应急预案等 [4]。同时，定期对 AI 与 IoT 应用进行风险评估，识别潜在的安全威胁和漏洞，实施实时安全监测，利用 AI 技术提升异常检测和响应速度。在对所有 AI 与 IoT 设备进行全面盘点和分类管理时，需要确保资产信息的准确性和完整性，实施严格的访问控制和权限管理，防止未经授权的访问和操作，通过制定详尽的网络安全应急预案，涵盖各种可能的安全事件场景。此外，定期进行应急演练，提升团队的应急响应能力和灾难恢复能力。总之，加强 AI 与 IoT 应用的网络安全管理体系和机制需要从多个方面入手，包括明确责任与制度、建立风险评估与监测机制、加强资产管理、强化应急响应与灾难恢复能力等。并通过实施具体的网络安全机制如访问控制、数据加密、漏洞管理、日志审计、安全培训和跨域隔离等，可以进一步提升系统的安全防护能力，如表 1 所示。

表 1 加强网络安全管理体系和机制优化措施

措施类别	具体措施	预期效果
访问控制	实施角色访问控制	确保只有授权用户才能访问特定资源
数据加密	对敏感数据加密存储和传输	防止数据在传输和存储中被窃取或篡改
漏洞管理	定期更新系统补丁，修复漏洞	减少因系统漏洞被利用的风险
日志审计	记录并分析所有网络活动日志	及时发现并追溯潜在的安全威胁
安全培训	定期对员工进行网络安全意识培训	提升全员网络安全素养和应急处理能力
跨域隔离	在不同网络区域实施物理逻辑隔离	防止安全威胁在网络间传播和扩散

4.2 加强网络安全防范意识能力

在人工智能与物联网应用的网络安全管理中，加强网络安全防范意识能力旨在提升网络安全防范意识，如表 2 所示。首先，在提升员工及用户网络安全意识方面，应定期网络安全培训，培训内容包括最新的网络威胁案例、防范技巧、安全政策等，通过培训后测试，确保员工掌握相关知识，增强防范意识。其次，在强化数据保护方面，使用 AES-256 等强加密算法对数据进行加密，确保所有敏感数据在传输和存储过程中均被加密。随后，在加强物理与逻辑安全防护方面，加强数据中心、物联网设备等的物理防护，如安装门禁系统、监控摄像头等，确保关键区域全天候无死角监控。同时，设置严格的访问控制策略，阻止未经授权的访问，部署入侵检测系统（IDS/IPS），及时发现并阻止网络攻击。最后，建立应急响应机制，明确应急响应流程、责任人、联系方式等，并建立网络安全事件响应团队，团队成员包括安全专家、IT 技术人员、法务人员等，确保目标在发现安全事件后 30 分钟内启动应急响应流程，以此实现提升人工智能与物联网应用领域的网络安全防范意识能力，降低安全风险，保障数据和系统的安全。

表 2 加强网络安全防范意识能力的措施及目标

措施类别	具体措施	目标 / 数据
员工培训	定期网络安全培训	每季度至少一次，90% 以上员工参与度
数据保护	数据加密	使用 AES-256 等强加密算法
	访问控制	基于角色的访问控制，定期审计访问记录
人工智能应用	智能安全监测	95% 以上威胁识别率
	行为分析	识别异常行为模式，降低安全风险
物理与逻辑安全	物理安全	加强数据中心、物联网设备等物理防护
	逻辑安全	配置防火墙，部署入侵检测系统
应急响应	制定应急响应计划	每年至少一次应急响应演练
	建立响应团队	快速响应，目标 30 分钟内启动应急流程

4.3 重视相关重要信息的安全管理水平

在人工智能与物联网的深度融合时代，对重要信息数据的安全管理成为了不容忽视的核心议题。为了确保网络系统中敏感与私密数据的安全性，需要采取一系列周密措施，对于那些关乎核心业务与用户隐私的数据，应严格遵循加密原则，采用高级别加密算法，并结合复杂的安全密钥与精细的等级权限管理机制，构建起多层次的防护网，有效提升了数据的私密性与防护能力，显著降低了数据泄露与丢失的风险 [5]。在信息数据的传输环节，在数据正式传输前，必先运行高效的杀毒程序，对传输环境进行全面清扫，确保信息通道的安全无虞。同时，积极拥抱技术创新，避免依赖传统、可能存在安全漏洞的数据传输方式，转而采用更为安全、高效的现代传输技术。此外，做好防火墙与安全管理系统是抵御外部威胁的第一道防线，因此需要不断加大投入，持续更新优化这些系统，确保防火墙与安全管理系统能够紧跟技术发展的步伐，有效抵御各类新型网络攻击。同时，建立定期的系统更新机制，将最前沿、最可靠的技术成果融入网络安全管理体系之中，不断提升人工智能与物联网应用的安全管理水平，为网络系统的稳定、健康运行提供坚实保障。

5 结语

人工智能与物联网应用的网络安全管理是一项复杂而系统的工程，需要政府、企业、科研机构及用户等多方共同努力。通过实施论文提出的综合性管理方法，包括构建多层防御体系、加强数据加密与隐私保护、引入智能监控与响应机制，并推动跨领域合作与标准化建设，才能有效应对 AI 与 IoT 环境下的网络安全挑战，保障技术的健康、安全发展。而随着技术的不断进步和威胁态势的演变，还应持续创新，不断优化和完善网络安全管理体系，为构建更加智能、安全、可信的数字世界贡献力量。

参考文献

[1] 卢胤舜.人工智能技术、消防物联网在消防安全标准管理中的应用[J].大众标准化,2022(22):10-12.

[2] 刘文艳,秦晔.人工智能技术、消防物联网在消防安全管理中的应用[J].消防界(电子版),2020,6(10):39-40.

[3] 姚克.基于人工智能和物联网应用的网络安全管理[J].计算机产品与流通,2020(4):155.

[4] 吴志雄.基于人工智能和物联网应用的网络安全管理[J].中国信息化,2019(9):64-65.

[5] 焦鹏.基于人工智能和物联网应用的网络安全管理[J].网络安全技术与应用,2018(10):109+133.