Universe Scientific Publishing
机械工程 (5)2024,6
ISSN: 2661-3530(Print)； 2661-3549(Online)

人工智能和物联网应用的网络安全管理方法

解晓丽
（宁夏财经职业技术学院学院　宁夏银川　750021）

摘　要：随着人工智能和物联网应用的蓬勃发展，网络安全问题日益凸显。本文探讨了人工智能和物联网应用面临的主要网络安全隐患，针对这些安全隐患，文章提出了相应的网络安全管理办法，如加强数据隐私保护、增强系统安全性、防范误导信息和恶意软件等。此外，制定完善的安全政策和标准也是确保人工智能和物联网应用网络安全的关键措施。本文为提高人工智能和物联网应用的网络安全水平提供了有益借鉴。

关键词：人工智能；物联网；网络安全；管理方法

引言：

在当前信息时代，人工智能和物联网技术已广泛应用于各个领域，显著提高了生活和工作的便利性。与此同时，网络安全问题也随之而来，给人工智能和物联网应用的发展带来新的挑战。网络攻击手段日益复杂，安全威胁形式多样化，如何妥善管理网络安全风险，确保人工智能和物联网应用的可靠运行，已成为需要解决的重要课题。

一、人工智能和物联网应用的网络安全隐患

（一）数据隐私与泄露风险

人工智能和物联网应用极大依赖于海量数据的收集和处理。一方面，这些数据中蕴含着大量个人隐私信息，如姓名、地址、联系方式、财务状况、健康记录等。一旦发生数据泄露，将给个人带来名誉和财产损失的风险。此外，企业运营数据、技术秘密、商业模式等商业机密若遭泄露，也将对企业的竞争力和发展造成重创。另一方面，人工智能算法训练所使用的数据集，可能存在数据偏差或数据污染等问题。例如，训练集中包含了种族、性别等方面的偏见信息，那么训练出的人工智能模型在做出决策时，也可能继承并放大这些偏见，导致歧视性的结果。此类算法偏差会严重影响人工智能决策的公平性和准确性，给个人和社会带来潜在伤害。

（二）系统脆弱性与黑客攻击风险

人工智能和物联网系统由各种硬件和软件模块组成，任何一个环节存在漏洞或弱点，都可能被黑客利用实施攻击。物联网设备安全性能通常较低，计算能力和存储空间有限，安全防护措施薄弱，很容易被攻击者入侵和控制。一旦大量物联网设备被黑客控制，将形成僵尸网络，对网络基础设施和关键信息系统造成严重威胁。人工智能系统的决策模块也是黑客攻击的重点目标。攻击者可以通过投毒训练数据、构造对抗性样本等手段，使人工智能系统产生误判和失控。例如，若自动驾驶汽车的感知模块被攻击，就可能导致严重的交通事故。

（三）误导性信息与恶意软件风险

人工智能系统对输入数据的质量和真实性极为敏感，任何误导性或被篡改的信息，都可能导致人工智能做出错误的决策。例如，在自然语言处理任务中，若输入的文本包含虚假谣言，那么人工智能的文本理解和判断就会受到影响。在计算机视觉任务中，对抗性对象可以欺骗物体识别模型。此外，恶意软件也可能潜伏在物联网设备或人工智能系统中，对系统造成破坏。恶意软件可能来自黑客入侵，也可能在设备供应链环节被植入。一旦被恶意软件感染，系统可能遭到勒索或数据窃取，甚至被远程控制执行违法操作。

二、人工智能和物联网应用的网络安全管理办法

（一）加强数据隐私与泄露风险管理

确保个人隐私和企业机密数据的安全，是网络安全管理的重中之重。应当采取严格的加密和访问控制措施，对数据的全生命周期进行全方位保护，包括数据收集、传输、存储和使用等各个环节。同时，政府应当制定并执行严格的隐私保护法律法规，规范数据处理行为，明确数据处理者的义务和责任，并对违规行为实施有力惩处。除了技术手段和法律约束之外，还需加强隐私保护意识的宣传教育，增强全社会的隐私保护意识。企业和组织也应树立良好的数据道德和合规文化，自觉遵守法律法规，恪守商业道德，切实保护用户和客户的隐私权益。

例如在数据收集环节，可以采用匿名化技术，避免收集过多的个人身份信息；在数据传输环节，需要使用端到端加密技术；在数据存储环节，需要对数据进行分类存储、加密和访问控制。具体来说，对于较为敏感的数据，如个人身份信息、财务数据、健康记录等，应当使用高强度加密算法，限制访问权限，只有授权人员才能查阅。同时，需要建立完善的访问审计机制，记录每一次数据访问的时间、人员和目的，防止数据被滥用或泄露。在数据使用环节，也要加强管控，明确规定数据的使用场景和目的，禁止将数据用于

非授权的其他用途。

（二）增强系统脆弱性与黑客攻击风险管理

对于系统漏洞和黑客攻击风险，需要采取主动发现、及时修复的方式。定期对人工智能和物联网系统进行安全性评估和漏洞扫描，全面检测各类漏洞和弱点。一旦发现漏洞，需要立即修复，并推送安全补丁更新。对于物联网设备和工控系统等资源受限的环境，由于无法及时更新补丁，容易遭受攻击和入侵，所以还需采取其他保护措施，如隔离高风险设备、部署专用防火墙和入侵监测系统等。同时应当加强对物联网设备的认证和访问控制，提高设备的安全性能，从根本上降低被攻击的风险。及时发现和修复系统漏洞，是防患于未然的根本举措，需要运维人员和安全专家的长期努力和持续投入，方能真正确保系统的安全可靠运行。

例如，2021 年 5 月，全球遭受了史上最大规模的勒索软件攻击“暗网熊猫”。该勒索软件利用了微软 Exchange 服务器的一个漏洞，成功入侵了全球数万台系统，加密了大量数据，并勒索赎金。这个事件引发的损失高达数十亿美元，影响范围遍及全球上百个国家和地区，政府机构、医疗卫生、教育、金融等关键基础设施系统均遭到了严重攻击。事后调查发现，微软早在两个月前就发布了相关补丁，但许多用户和组织疏于更新，才导致了如此惨重的后果。因此，除了要主动发现漏洞之外，及时安装补丁更新同样至关重要。

（三）防范误导性信息与恶意软件风险

针对误导性信息和恶意软件的威胁，需要加强对人工智能输入数据的检验和过滤，及时发现并清除错误和恶意信息。同时构建健全的软件和固件更新机制，确保及时为物联网设备推送最新的安全补丁和反病毒签名库。对于误导性信息的防范，除了基于事实查证、谣言检测等技术手段之外，更重要的是培养用户的辨识能力，提高信息鉴别素养。定期开展网络安全教育和培训，教育公众如何识别虚假信息和钓鱼陷阱，是一项长期的系统工程。同时，也需要加强舆论引导，及时辟谣，营造良好的网络环境。此外，对于涉及重要决策的人工智能系统，还可以引入人机协作的模式，确保系统输出符合预期且可控。

例如，在自然语言处理任务中，可以先对输入文本进行事实查证、谣言识别等处理，剔除虚假和不当内容。此外，还需要引入多样化的反病毒和防火墙技术，有效阻挡恶意软件的入侵和传播。具体来说，可以通过部署实时在线扫描系统，自动检测和拦截恶意软件和钓鱼网站。针对已知的恶意软件家族，也需及时更新病毒特征库和拦截规则。此外，应用沙箱等隔离技术，可以对未知威胁进行行为分析，及时发现并阻止恶意行为。

（四）制定安全政策和标准

网络安全是一项系统工程，需要政府、企业、技术机构等各方的通力合作。应当共同制定出行之有效的网络安全政策、标准和规范，为人工智能和物联网应用的安全可靠运行提供顶层设计和制度保障。网络安全需要大量高素质的安全专业人才，以及先进的检测、防护、应急响应等技术装备，还需要政府、企业、科研机构的长期持续投入。政策和标准的制定需要与时俱进，持续跟进技术发展的新动向，并加大资金和人才的投入，为网络安全建设提供充足的硬件和软件支持。只有从法律、技术、资源等多方面入手，网络安全管理才能行之有效。

例如，美国政府于 2019 年发布了“人工智能系统的可信赖人工智能框架”，为人工智能系统的安全性、透明度、公平性等提出了具体的原则和实践方法。欧盟则在 2021 年颁布了“人工智能法案”草案，旨在规范人工智能的开发和使用，确保其安全可靠。这些政策和法规为人工智能系统的网络安全管理提供了统一的指导方针。除了政府主导制定顶层政策外，业界标准化组织也发挥了重要作用。例如，IEEE 在 2016 年成立了“人工智能与自主系统伦理规范工作组”，旨在制定符合伦理道德的技术标准；新加坡在 2019 年发布了“人工智能治理实践指南”。这些政策法规和技术标准，为人工智能和物联网应用在产品开发、算法设计、系统部署、运营维护等各个环节的网络安全管理提供了可操作的规范性要求。

结束语：

随着信息技术的不断创新，人工智能和物联网必将得到更广泛地应用。然而，网络安全风险却无处不在，需要各方共同努力加以防范。本文分析了人工智能和物联网应用面临的主要网络安全隐患，并针对性地提出了管理对策，为相关领域的网络安全防护提供了参考。网络安全是一项永恒的系统工程，需要政府、企业、技术机构和用户的通力合作，方能最终达成安全、高效、可靠的人工智能和物联网应用。

参考文献：

[1]尚学艳.人工智能在网络空间安全中的应用策略[J].中国建设信息化,2023(23):70-73.

[2]郭金辉.新形势下网络安全威胁与防御策略[J].信息与电脑(理论版),2023,35(23):180-183.

[3]全斌,王晨.人工智能技术在网络安全防御体系中的应用[J].信息系统工程,2023(02):51-53.

[4]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(04):155.

作者简介：

姓名：解晓丽（1978.10.29），性别：女，民族：汉，籍贯：宁夏中卫，单位：宁夏财经职业技术学院，职称：副教授，学历：大学，研究方向：人工智能，网络安全，计算机应用。