基于人工智能的物联网设备信息安全管理研究

胡建萍

广东广晟通信技术有限公司，广东 广州 510000

摘要：随着经济社会的持续蓬勃发展，我国在科学技术领域取得了显著的成就，并已稳步迈入信息化时代的大门。这一变革为行行业业的生产活动注入了较大的动力，极大地促进了效率以及创新的提升。与此同时，科学信息化时代带来了一系列前所未有的挑战，尤其是信息安全问题日益凸显。在这个信息高度透明的时代，信息的丢失和盗取成为了不容忽视的风险，对个人隐私、企业安全乃至国家安全都构成了潜在威胁。面对这些挑战，相关技术人员正积极投身于信息安全管理的深入研究与分析之中，致力于构建更加坚固的信息安全防线。在此过程中，人工智能技术的引入为物联网设备的信息安全管理提供了新的思路和解决方案。通过人工智能的智能化、自动化特性，我们可以更加精准地识别、监控和应对潜在的信息安全威胁，由此提升信息的安全性，防止技术信息的篡改和丢失。人工智能在物联网的设备信息安全管理中应用可以体现在许多方面。例如，利用人工智能技术，实现对物联网设备的实时监控，及时发现并处理异常行为；通过机器的学习算法，对大量的网络数据进行深度分析，挖掘出潜在的安全漏洞和攻击模式；人工智能也可以帮助我们构建更加智能的安全防御体系，实现对安全威胁的快速响应和较强有效遏制。综上所述，人工智能在物联网设备信息安全管理中的应用具有广阔的前景和巨大的潜力。我们应该充分利用这一先进技术，加强信息安全管理的研究与实践，为信息化时代的稳定发展提供有力的保障。我们也需要不断关注新技术的发展动态，及时调整和完善信息安全管理策略，以应对日益复杂多变的信息安全挑战。

关键词：人工智能；物联网设备；信息；安全管理

引言

在科学技术的迅速推进下，我国在自然科学人工智能技术已迈入了一个快速发展全新阶段。自 2015 年以来，该技术便呈现出稳步增长的态势，至 2018 年，其增长率已傲然突破了 54%的大关。这一连串的数据，无疑昭示着我国人工智能技术正日益走向成熟，其应用范畴也在不断地拓宽，现已广泛渗透至各行各业之中，为社会的进步与发展注入了强大的动力。物联网技术以及人工智能技术的日新月异，信息安全问题也日益凸显，且呈现出愈发严重的趋势。这些问题不仅仅威胁着个人隐私的安全，也对企业的运营乃至国家的安全稳定构成了潜在的隐患。对信息安全管理的深入研究与分析显得尤为迫切，成为信息化时代研究重要组成部分。利用人工智能技术来开展物联网设备的信息安全管理，便成为了解决问题的关键所在。通过人工智能技术，我们可以实现对物联网设备的智能化监控与管理，及时发现并处理潜在的信息安全隐患，从而确保信息的安全性与完整性。这不仅能够为物联网设备的稳定运行提供有力的保障，更能够推动信息化时代的持续健康发展。人工智能技术在物联网设备信息安全管理中的应用具有重大的意义。应该充分把握这一机遇，深入挖掘人工智能技术的潜力，将其与物联网设备的信息安全管理紧密结合，

共同构建起一个安全、稳定、高效的信息化环境，为社会的进步与发展贡献更多的力量。

1 研究背景

在新时代背景下，物联网（IoT）技术已深度融入社会的各个角落，与生产活动、日常生活以及学习教育紧密相连，对社会的整体发展产生了深远的影响。物联网技术的广泛应用，如智能家居的普及、工业自动化的推进等，无疑为社会的进步带来了显著的积极影响，并推动了物联网设备数量的逐年攀升。然而，在这一繁荣景象的背后，也伴随着一系列挑战与潜在风险，其中最为突出的便是信息安全问题。面对物联网设备信息安全的严峻挑战，如何有效利用人工智能技术来加强信息安全管理，已成为当前学术界与产业界共同关注的焦点。据相关调查研究显示，物联网技术的广泛应用，全球物联网安全市场呈现出逐年增长的态势，这一增长趋势与物联网设备数量的增加呈现出正相关的关系。网络攻击的复杂性与多样性也在不断增加，进一步凸显了物联网设备信息安全管理的重要性与紧迫性。本文旨在深入探讨人工智能技术在物联网设备信息安全管理中的应用优势，并基于当前的实际情况，提出一系列具有针对性的有效策略。这些策略旨在在满足数据共享需求的同时，确保信息的安全性，有效防范信息泄露、盗取等风险，从而维护物联网网络环境的安全稳定，为后续的运行与发展提供坚实的保障。人工智能技术在物联网设备信息安全管理中的应用，可以凭借其强大的数据处理与分析能力，实现对物联网设备的实时监控与预警，及时发现并应对潜在的安全威胁。通过机器学习等先进技术，人工智能还可以不断优化和完善安全防御策略，提高物联网设备对复杂网络攻击的防御能力。

2 基于人工智能技术的物联网设备信息安全管理存在的问题

对于当前阶段来说，物联网设备的应用尤为常见，但是随之而来的是一系列的信息安全问题，对物联网设备运行的稳定性造成了严重的不良影响，本文基于此对当前存在的问题进行统计，具体如下所示：

2.1 缺乏安全防护

物联网设备在运行的过程中，涉及到多种内容，整体环境较为复杂，且会受到诸多因素的影响，最终导致出现物联网设备信息丢失的问题，对此技术人员进行探究与分析，发现主要是因为缺乏安全防护，无法对互联网设备开展保护，最终出现安全问题。在开展物联网设备信息管理的过程中，安全防护系统的应用尤为重要，但是大部分并未建设安全防护系统，即使建设了安全防护系统，其运行有效性较低，无法发挥安全防护作用，病毒与黑客等依然会共计物联网设备信息系统，影响整体运行安全性[1]。

2.2 数据采集与处理效果较低

在物联网设备信息安全管理的广阔领域中，数据采集与处理环节扮演着至关重要的角色，它们是确保物联网设备稳定运行与信息安全防护的基石。从当前管理工作的实践状况来审视，我们发现一个不容忽视的问题：工作人员在实施管理时，未能充分发掘并有效利用人工智能技术的强大潜力，这一疏忽直接导致了系统运行效率的低下，进而对物联网设备的整体安全性能构成了潜在威胁。

具体而言，在数据采集与处理的实践过程中，传统方法依然占据主导地位。这种方法不仅效率低下，而且难以保证数据的完整性和准确性，传统手段在处理复杂多变的数据流时往往力不从心，容易造成数据丢失或错误解读。更为严重的是，传统数据采集方式需要投入大量的时间与人力资源，这不仅增加了运营成本，还限制了数据处理的时效性，使得关键信息无法及时得到分析和利用，从而影响了数据采集与处理的最终效果。传统数据采集流程还面临着响应速度迟缓的问题。在快速变化的物联网环境中，信息的时效性至关重要。由于传统方法在处理数据时耗时较长，往往无法及时捕捉到

最新的安全威胁或异常行为，这无疑为物联网设备的安全运行埋下了隐患。当前物联网设备信息安全管理在数据采集与处理方面存在的问题不容忽视。为了提升管理效率，确保数据安全，我们必须重新审视并优化管理流程，积极引入人工智能技术，以智能化、自动化的手段替代传统方法，从而实现对数据的高效、精准采集与处理，为物联网设备的稳定运行与信息安全提供有力保障。

2.3 入侵检测系统落后

在开展物联网设备信息安全管理的过程中，工作人员已经意识到入侵检测的重要性，并建立入侵检测系统，当前网络环境较为复杂，病毒入侵种类层层增加，传统入侵检测系统不能满足当前安全管理的需求[2]。传统入侵检测主要以单一的规则库为基础开展检测，整体检测内容较多，且检测难度较大，无法保证入侵检测的可靠性和精准性，于此同时检测效率比较低，后续工作的过程造成一定的影响，导致物联网设备处于不安全的运行环境之中。

3 基于人工智能技术的物联网设备信息安全管理有效措施

3.1 搭建安全防护系统

通过应用人工智能技术，可建立安全防护系统，实现物联网设备信息安全防护的目的，有效避免出现信息泄露以及丢失的情况。对于安全防护系统来说，其中最为重要的一项内容就是硬件的开发与设计，可将计算机较为常用的 Windows 系统作为基础，利用 Python 语言作为系统开展语言，并利用大数据加密技术对数据库进行加密处理，实现数据安全防御与保护的目的[3]，具体配置如表 1 所示。

表 1 硬件配置

项目	配置参数
交换机	中央处理器 1GB；硬盘空间 50GB
中控台	中央处理器 1GB；硬盘空间 50GB
传感器	微处理器驱动
网络适配器	1000M
数据服务器	开设 Docker 服务
处理器	256GB

在人工智能技术的支持下，可保证安全防护的有效性，且其功能更为全面，在实际运行的过程中，可收集大量数据信息，并通过智能化的方式进行识别、分类与处理，同时，在物联网设备遭到病毒或者是其他攻击行为时，可自动开启智能化防护，以此保证信息安全，也可提升计算机网络的安全性，其功能设计如图 1 所示。

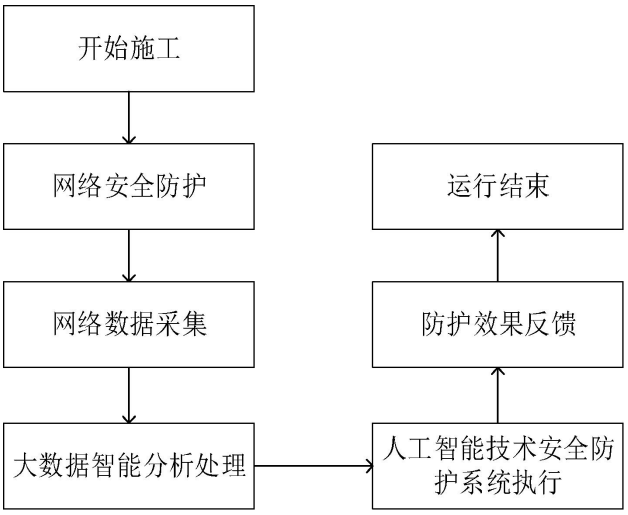

图 1 物联网设备信息安全防护系统功能设计示意图

3.2 优化数据采集与处理

对于物联网设备信息安全管理工作的开展来说，需做好数据采集与数据处理，其是保证数据信息安全管理质量的关键，也是避免病毒污染以及攻击行为的重点，此时需引进人工智能化技术，通过智能化以及自动化的方式开展数据采集与处理，可保证工作质量以及工作效率，并保证数据信息的全面性以及可靠性[4]。

（1）数据采集：在当今信息化时代下，物联网设备实际运行的过程中会产生大量数据信

息，倘若人工方式进行数据采集，消耗大量的精力以及时间，无法保证数据信息的全面性以及完整性。在人工智能技术的支持下，可根据物联网设备的实际需求，利用网络软件以及硬件资源，开展数据采集。通过此种方式，可提升数据采集的自动化以及智能化，节约时间资源，无需将大量人力资源用于数据采集之中，同时可保证数据信息的全面性和完整性，但是需要注意的一点是要做好网络安全保护。在数据采集系统的支持下，可针对访问数据进行分析与处理，并将其储存在不同的子系统之中，同时需要利用人工智能技术进行数据过滤，以此提升数据采集的速率，也可保证数据信息的精准性，避免出现重复数据信息。

（2）数据处理：在完成数据采集之后，需及时对数据进行处理与分析。系统完成网络数据采集之后会自动上传数据，并对数据进行自动化分类，随后将其分配到对应的功能单元。完成数据分配之后，各模块启动工作，并对不同类型的病毒进行识别与分析，以此保证网络数据信息的精准性、可靠性以及智能化[5]。在实际开展数据处理的过程中，需要针对收集的数据信息进行预处理，随后将处理结果进行比对与分析，判断数据信息是否已经被病毒感染，以此明确当前物联网设备存在的风险与问题，并将可能存在的风险向防护单元进行反馈，随后防护单元针对风险制定具有针对性的解决方案。

3.3 入侵检测

在当今这个信息化高速发展的时代，信息环境的复杂程度日益加深，这无疑给物联网设备的运行带来了前所未有的挑战。网络病毒与黑客攻击如同潜藏的暗流，时刻威胁着物联网设备的安全稳定运行。传统的入侵检测系统，在面对这些日益复杂和多样化的威胁时，已显得力不从心，无法满足当前信息安全管理的迫切需求。积极探索和应用人工智能技术来强化入侵检测，成为了保障物联网设备信息安全的关键所在。人工智能技术的引入，为入侵检测带来了智能化和自动化的革新。借助大数据技术，人工智能能够深入分析入侵病毒和攻击行为，精准识别病毒类型，甚至对新型病毒也能进行有效识别，并迅速采取防御措施。这一智能化入侵检测系统，其核心在于从入侵原理出发，深入剖析入侵途径和变化趋势，针对不同病毒类型进行精准打击。由于入侵机理的相对固定性，这一方法能够从源头上有效遏制病毒入侵和其他攻击行为。

一旦检测到病毒或攻击行为，智能化入侵检测系统能够立即启动病毒入侵程序，迅速实现病毒抵御，从而有效保护信息安全。即便面对未被纳入规则库的新型病毒，人工智能化入侵检测系统也能凭借其强大的分析能力和学习能力，对其进行有效检测和防御，确保物联网设备始终处于安全运行状态。这一系统不仅建立了弹性防线，还实现了物联网设备的长期安全监控。人工智能化入侵检测系统还能与传统算法实现有机融合，通过算法对数据源进行深入分析，进一步提升病毒识别的精准度和可靠性。在设计过程中，系统还增设了入侵警报系统，一旦感知到病毒或攻击行为，便能立即发出警报，并迅速启动识别、响应和处理机制，确保在最短时间内完成病毒和攻击的处理，最大限度地降低对物联网设备安全的影响。

4 结语

综上所述，物联网设备运行的过程中会产生一定处理的信息，但是由于当前网络环境较为复杂，需做好信息安全管理，而传统管理模式无法满足当前运行需求，可引进人工智能技术，以此为基础开展信息安全管理。在实际开展信息安全管理的过程中，在人工智能技术的支持下，可从安全防护、数据采集与处理以及入侵检测 3 方面入手，以此保证信息安全性，有效避免出现信息泄露等不良问题。

参考文献

[1]张雯,周子航,周明升.基于物联网和人工智能的园区安全运营管理平台[J].计算机时代,2023(2):132-136

[2]干光磊,黄娟,徐乃娟,等.基于人工智能物联网的多维度手术设备管控平台的构建与应用评价[J].中国医学装备, 2024, 21(1):130-134.

[3]徐卫卫.基于物联网的智能环境监控新型设备设计研究[J].现代计算机,2022,28(3):117-120

[4]王厚奎.人工智能和物联网应用的网络安全管理方法[J].石河子科技,2023(1):44-45

[5]李建华.基于人工智能和物联网应用的网络安全管理分析[J].中国科技期刊数据库 工业A,2022(1):288-291