第 4 卷◆第 1 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

物联网感知数据质量治理与安全利用协同研究

徐浩
中国联合网络通信有限公司青岛市分公司
DOI:10.32629/acair.v4i1.19354

[摘　要] 随着信息技术的快速发展,物联网作为全新的信息技术组成部分,正以前所未有的速度改变着人们的生活与生产方式。而在物联网蓬勃发展的当下,海量感知数据不断生成,其质量和安全利用成为当今社会热议的话题之一。基于此,本文就物联网感知数据质量治理与安全利用协同展开探究分析,通过构建融合数据质量评估模型与安全防护策略的协同框架,以此实现对数据质量的提升和安全保障的有机统一,以更好地推动物联网在各行业的深度应用与创新发展。
[关键词] 物联网；感知数据；质量治理；安全利用
中图分类号：TP393.4　**文献标识码**：A

Collaborative Research on IoT Sensing Data Quality Governance and Secure Utilization

Hao Xu
China United Network Communications Co., Ltd.

[Abstract] With the rapid development of information technology, the Internet of Things (IoT), as a new component of information technology, is changing people's lives and production methods at an unprecedented pace. In the current booming development of IoT, massive amounts of sensor data are constantly being generated, and its quality and secure utilization have become hot topics in society. Based on this, this paper explores and analyzes the synergistic governance and secure utilization of IoT sensor data. By constructing a collaborative framework that integrates data quality assessment models and security protection strategies, it aims to achieve an organic unity between improving data quality and ensuring security, thereby better promoting the deep application and innovative development of IoT in various industries.
[Key words] Internet of Things; Sensing data; Quality governance; Secure utilization

物联网感知数据在带来巨大机遇的同时,也存在诸多挑战,受感知设备精度限制以及数据隐私、机密等问题的影响,当物联网感知数据被泄露或者不完整时,必然会给个人、社会以及企业带来重大的损失。因此,开展物联网感知数据质量治理与安全性的协同研究,对推动物联网技术的健康发展具有至关重要的作用。

1 物联网感知数据质量治理与安全利用概述

1.1物联网感知数据

物联网感知数据是一种基于物联网系统,通过各种感知设备,如传感器、摄像头、射频识别等标签,对物理世界中的各种对象以及环境进行感知、采集而获取到的数据[1]。因此,物联网感知数据具有海量性特点,并随着物联网设备的大量部署,可产生出的数据规模呈爆炸式增长。而感知数据由感知设备采集,并通过网络传输,或有线、无线等方式,最终到达数据中心,其传输中还会因设备故障,格式不兼容等出现数据的丢失、错误等问题。

1.2数据质量治理理论

数据质量是指数据满足明确和隐含需求程度的综合性特征,关系到数据能否有效支撑业务的决策和运营。常用数据质量维度具有丰富性和多样性特点,能确保数据反映真实情况。同时,数据质量的完整性要求数据完整无缺失,涵盖所需全部信息。对于数据质量评估环节,则可通过抽样检测、指标分析等多种手段衡量数据的质量现状,最终共同构建完整的数据质量治理流程,以提升数据价值。

1.3协同理论概述

协同理论是指元素与元素之间的相互干扰、相互作用,并通过协调合作产生整体大于部分之和的效应。协同理论的基本原理中,协同效应作为核心,是指系统内各子系统相互配合,从而使系统从无序走向有序,产生新的功能和结构[2]。而将协同理论应用于物联网感知数据治理时,由于物联网感知数据来源广泛、类型多且质量治理和安全利用涉及到多个环节与主体,因此,通过协同,能充分发挥各部分的优势,以推动物联网感知数据更好地服务于各个领域。

2 物联网感知数据质量现状分析

2.1数据质量问题表现

在物联网广泛应用的当下，其感知数据质量问题变得日益凸显，以智能交通领域的交通流量监测为例，部分路段部署的传感器由于长时间的运行，会出现数据的缺失情况。这种数据错误的情况屡见不鲜，如在工业生产中的温度监测环节，传感器可能因干扰或故障，将实际50℃的温度错误记录为80℃，若按照此错误数据调整生产参数，必然会严重影响到产品的品质。此外，数据重复问题也同样存在，在物流仓储管理时，货物标签扫描设备会因操作不当或系统故障，对同一货物进行多次扫描，生成重复数据，严重干扰到库存统计的准确性，大幅增加管理成本。

2.2数据问题产生原因

从感知设备层面来看，设备精度不足会引发数据质量问题。部分低成本传感器为了降低成本，在设计和制造时，必然会导致精度受限，很难精准捕捉物理量的细微变化，致使采集的数据与实际值存在偏差。而在网络传输环节，网络干扰问题不可忽视，对于复杂的电磁环境，如工厂车间内众多设备同时运行时，电磁信号之间相互干扰，会使物联网感知数据在传输中出现丢包、乱码等问题[3]。而一些数据处理算法在面对海量、复杂的物联网数据时，难以有效处理异常数据值和噪声数据，以至于数据清晰不彻底，进一步影响到数据的质量。

2.3数据质量问题影响

就数据质量问题的影响，在智能决策方面，数据是决策的基础，数据质量问题会严重影响到智能决策的准确性。例如，在智能医疗中，当患者生命体征监测数据存在缺失或错误时，医生依据这些不准确的数据制定治疗方案，很可能会延误患者病情的治疗。而在智能电网中，电力负荷监测数据的不准确，会导致电力调度系统做出错误的决策，从而引发电网故障，影响到电力供应的可靠性。此外，在成本控制方面，数据质量问题会增加企业的运营成本，最终降低企业的经济效益和市场竞争力。

3 物联网感知数据安全现状分析

3.1数据安全威胁类型

在物联网数据感知安全威胁中，主要分为外部攻击和内部人员违规操作两种类型。首先，在外部攻击威胁中，黑客通常会利用物联网设备存在的漏洞发起攻击，如通过恶意软件感染设备，篡改感知数据，干扰设备的正常运行[4]。例如，当智能摄像头被入侵后，黑客可获取监控画面，侵犯用户的隐私，甚至会导致拒绝服务，导致设备难以正常为用户提供监控服务。其次，内部人员违规操作威胁中，由于部分员工的疏忽或故意泄露，导致内部信息数据被外泄，如在医疗物联网中，患者信息的泄露，会给患者带来精神伤害和潜在的风险。在这两种威胁类型中，相对而言，外部攻击具有隐蔽性和突发性，而内部违规则具有随意性和难以防范性，两者都会严重威胁到物联网感知数据的安全。

3.2数据安全防护现状

针对物联网感知数据的安全防护，在技术层面，目前采用的是加密技术，这种技术能够对数据传输和存储进行加密，以保障数据的保密性需求，常用的方式以对称加密和非对称加密结合为主。同时，访问控制技术则通过设置权限，用于限制用户对数据的访问，防止非法访问，而身份认证技术则确保只有合法用户能接入系统，如基于生物特征的认证[5]。但这些防护存在诸多问题，其安全防护技术较为单一，缺乏综合防护体系，对于新兴威胁的应对能力严重不足，且难以协同工作。

4 物联网感知数据质量治理与安全利用协同框架构建

4.1协同框架设计目标与原则

在物联网感知数据质量治理与安全利用协同框架的构建过程中，设计目标与原则的科学界定对系统效能的优化具有决定性作用。从目标维度审视，首要任务在于系统性提升数据质量。物联网感知数据因来源多元、类型异构，常伴生数据缺失、错误、冗余等典型问题，亟需通过协同框架集成数据清洗、校验等技术机制，有效提升数据的准确性、完整性和一致性，为后续分析与应用提供高可靠性基础支撑。同时，数据安全保障构成核心目标，鉴于感知数据中密集包含个人隐私、企业机密等敏感信息，协同框架须构建涵盖数据加密、访问控制、安全审计的多层次防护体系，以严密防范数据泄露、篡改、滥用风险，确保数据在采集、传输、存储及应用全生命周期中的安全性。此外，质量治理与安全利用的协同优化是框架设计的内核目标，二者存在动态互馈关系而非割裂状态，质量治理需在安全约束下有序实施，安全利用须依托高质量数据精准开展，通过消除机制壁垒实现整体效能的最大化。

在设计原则上，整体性原则要求将质量治理与安全利用整合为有机统一体系，实施全局性规划与协同推进策略，避免局部优化导致整体效益失衡。层次性原则强调基于物联网系统分层架构的差异化特征，制定针对性的质量治理与安全利用策略，实现分层管控与精准施策[6]。动态性原则注重物联网环境的实时演化特性，要求框架具备高度的适应性与弹性，能够动态响应数据质量问题与安全威胁的动态变化，确保机制时效性。开放性原则保障框架的可扩展性，支持无缝集成新兴技术与方法论，持续驱动数据质量治理与安全利用水平的迭代升级。上述目标与原则的协同作用，为构建高效、安全、可持续的物联网数据治理体系奠定了理论基础与实践路径。

4.2协同框架总体架构

物联网感知数据质量治理与安全利用协同框架的总体架构由数据采集层、数据传输层、数据处理层及数据应用层构成，并集成数据质量评估、数据清洗、安全防护与协同管理等核心模块。数据采集层作为基础支撑，负责从各类物联网感知设备中获取原始数据，数据传输层确保数据在跨网络环境中的可靠传输与高效流通，数据处理层执行数据清洗、校验及质量优化等深度处理任务，数据应用层则将处理后的数据转化为可操作的应

用价值。各层与模块之间通过协同机制实现功能整合与动态适配,形成有机联动的系统架构,有效保障框架的稳定性与可持续性,为物联网感知数据的质量治理与安全利用提供结构化支撑与全链路保障。

而物联网感知数据质量治理与安全利用协同框架中,数据采集层作为系统输入的初始环节,依托部署于物理环境的传感器、摄像头等感知设备,实时捕获环境物理参数,为后续处理提供原始数据输入。数据传输层通过有线或无线网络基础设施,实现数据从采集端至处理中心的高效、可靠传输,其传输稳定性直接制约数据的完整性与时效性。数据处理层为核心功能模块,运用数据挖掘与机器学习算法对原始数据进行清洗、特征提取及质量优化,显著提升数据的可用性与可靠性。数据应用层将处理后的数据集成至智能交通系统、工业自动化控制等具体领域,实现数据驱动的决策支持与价值转化。各层次间形成递进式依赖关系,通过协同机制构建完整的物联网数据价值链,确保质量治理与安全利用的系统性整合。

此外,数据质量评估模块依据预设的质量标准,对输入的原始数据实施系统性评估,生成结构化质量评估报告,为后续数据处理流程提供量化依据。数据清洗模块基于评估结果识别的质量缺陷,执行数据修正、缺失补全及冗余消除等操作,输出高可靠性数据集[7]。安全防护模块通过数据加密、访问控制策略及完整性校验等技术机制,确保数据在传输与存储全链路中的机密性、完整性和可用性,有效抑制数据泄露与篡改风险。协同管理模块统筹协调各功能模块的运行机制,依据质量评估动态结果与安全需求参数,实时优化处理策略配置,实现质量治理与安全利用的动态协同与效能最大化。

4.3协同机制设计

为实现物联网感知数据质量治理与安全利用的高效协同,构建实时动态的信息交互机制具有关键性作用。该机制依托网络化感知与智能分析技术,建立数据质量态势与安全风险信息的双向流通通道。在数据采集端,感知设备在获取原始物理参数的同时,同步记录质量维度指标及安全环境参数,并通过加密专用通道实现信息的毫秒级传输。信息交互平台对多源异构数据进行语义化分类整合与深度态势分析,生成结构化质量评估报告与安全风险预警信息,并实时推送至质量治理模块、安全防护单元及管理决策层。此机制通过闭环反馈机制确保各环节对数据全生命周期状态的动态感知,为协同决策提供高时效性、高精度的量化依据,有效规避因信息时序偏差或完整性缺失导致的治理失效与安全风险。

为实现物联网感知数据质量治理与安全利用的协同优化目标,构建基于实时共享数据质量与安全信息的科学化决策机制构成核心环节。该机制系统整合数据质量多维特征指标及安全风险参数,依托海量历史数据与实时流数据的深度挖掘与多维关联分析,精确量化不同治理策略与安全防护措施对数据质量态势及安全风险的动态影响。决策层依据此量化评估结果,生成协同优化的治理策略,例如,针对数据质量薄弱环节与安全高风险区域实施资源动态配置,优先部署数据清洗强化与安全加固措施。同时,通过闭环反馈机制实现策略的实时动态调优,确保质量治理与安全利用在全生命周期内实现协同效能最大化,从而在保障物联网系统安全可靠运行的前提下,持续输出高可靠性数据服务。

与此同时,协同决策的高效实施需依托系统化的协同执行机制,在任务分配层面,依据决策策略对任务进行结构化分解,明确各执行单元的职责边界与量化绩效目标。资源调度环节实施动态资源配置策略,基于任务需求统筹人力、物力及计算资源,确保执行过程的充分保障。流程控制机制对执行全过程实施实时监测与动态优化,通过异常检测与即时干预机制识别并修正执行偏差,保障决策执行的精确性与连续性。该机制通过任务-资源-流程的闭环协同,有效支撑物联网感知数据质量治理与安全利用的协同目标实现,确保系统在安全可靠运行的前提下持续提供高可靠性数据服务。

4.4具体实施策略

物联网感知数据质量治理与安全利用协同框架的构建需实施系统性多维整合策略,以实现治理效能与安全防护的有机统一。首先,在数据标准层面,构建统一的标准化体系,明确定义数据质量核心维度指标,包括准确性、完整性、一致性及时效性。而安全规范参数包括访问控制策略、加密强度等级,以确保多源异构数据在语义与格式层面实现互操作性,有效规避因标准碎片化引发的数据异构性风险与安全漏洞[8]。其次,技术架构采用分层协同设计范式,在数据采集层部署高精度感知设备并集成安全防护模块,从源头保障数据质量与采集过程安全性。数据传输层构建鲁棒网络通道,运用数据压缩编码与前向纠错技术降低传输误差率,辅以防火墙与入侵检测系统实现传输链路的完整性与机密性防护。然后,数据处理层集成数据清洗算法与机器学习模型优化质量特征,通过动态身份认证与敏感数据脱敏技术强化数据安全边界。数据应用层开发定制化智能应用系统,实时反馈数据使用效能与安全异常,驱动全链路动态优化。最后,管理机制方面,建立跨部门协同治理组织,明晰权责边界与标准化工作流程,构建数据质量与安全量化评估体系,基于周期性指标分析实施策略动态调优,强化人员专业能力建设,系统提升数据治理与安全利用的理论素养与实操技能,为框架可持续运行提供机制保障与人力资源支撑,最终实现物联网感知数据的高质量获取、安全化应用与全生命周期协同优化目标。

5 结语

构建协同框架、运用多种技术手段,可实现数据质量的提升与安全保障的有机结合。而随着物联网技术的不断发展,感知数据的规模和复杂度也在持续增加,数据质量治理与安全利用协同研究依旧面临着诸多问题。需提高其适应性和扩展性,以应对不断变化的物联网环境,才能促进物联网感知数据质量治理与安全利用的标准化发展,以推动物联网技术在各行业的广泛应用。

[参考文献]

[1]谢硕.物联网感知数据在断层带微震监测中的应用[J].北斗与空间信息应用技术,2025,(06):100-102.

[2]陈述,孙宇航.基于物联网的多场景文物安全感知数据智能融合模型研究[J].无线互联科技,2025,22(22):15-19.

[3]黄幼姑.多源感知数据融合的城市公共安全风险评估与应急响应机制[J].张江科技评论,2025,(09):143-145.

[4]卢贤玲,马龙江,王珂.基于物联网多源感知数据的突发事件谣言溯源方法研究[J].物联网技术,2025,15(18):103-105.

[5]陈刚.基于物联网的煤矿井下无人机巡视信息感知研究[J].自动化应用,2025,66(16):257-259.

[6]杨庭,占娜,王溪.基于改进最大熵算法的配电站房设备全状态量线上感知方法[J].微型电脑应用,2025,41(6):273-276.

[7]张萍.基于物联网技术的供电企业用户用电计量数据实时采集方法[J].办公自动化,2025,30(12):89-91.

[8]冯光升,於志文.海洋感知网络:从单点观测到多域协同感知[J].计算,2025,1(02):80-87.

作者简介：

徐浩(1977--),男,汉族,山东烟台人,大学本科,工程师,研究方向：计算机网络专业方向。