# 农业物联网中的数字安全治理：挑战、策略与未来趋势分析

程龙瑞，王俊

安徽汽车职业技术学院，安徽 合肥 230000

**摘　　要：** 农业的数字化转型，尤其是通过物联网（IoT）技术的应用，为农业带来了前所未有的精准管理和效率提升。然而，这种进步也伴随着严峻的数字安全挑战和治理需求。农业物联网的数据密集性与开放性使其易受网络攻击，对关键农业设施构成威胁。为了实现有效整合和数据实时监控（如土壤湿度和作物生长预测），农业组织需要确保设备安全，同时政府需作为监管者和政策制定者介入。首要任务是建立健全的数据保护法规和标准，保障数据隐私和知识产权，例如通过实施数据加密技术如 TLS（Transport Layer Security）或 AES（Advanced Encryption Standard）来确保数据在传输过程中的安全性。政府还需投资研发并提供激励措施，推动农业组织采用这些安全措施，同时积极参与国际标准的制定。

**关 键 词：** 农业物联网；数字安全；数据加密

# Digital Security Governance In The Agricultural Internet Of Things: Challenges, Strategies And Future Trends Analysis

Cheng Longrui, Wang Jun

Anhui Automobile Vocational and Technical College, Hefei, Anhui 230000

**Abstract:** The digital transformation of agriculture,especially through the application of Internet of Things (IoT) technology,has brought unprecedented precision management and efficiency improvements to the industry.However,this progress also comes with serious digital security challenges and governance needs.The data-intensive and open nature of agricultural IoT makes it vulnerable to network attacks,posing a threat to critical agricultural facilities.To achieve effective integration and real-time monitoring of data such as soil humidity and crop growth predictions,agricultural organizations need to ensure device security,and governments need to intervene as regulators and policy makers.The primary task is to establish sound data protection laws and standards to safeguard data privacy and intellectual property rights.This can be done by implementing data encryption technologies such as TLS (Transport Layer Security) or AES (Advanced Encryption Standard) to ensure the security of data during transmission.Governments also need to invest in research and development and provide incentives to promote agricultural organizations to adopt these security measures,while actively participating in the development of international standards.

**Keywords:** agricultural Internet of Things; digital security; data encryption

## 一、引言

农业物联网（Agricultural Internet of Things,IoT in Agriculture）的兴起可以追溯到21世纪初，随着信息技术、传感器技术以及大数据处理能力的快速发展，传统农业开始向智能化和精准化转型[1]。农业物联网的核心理念在于通过实时数据采集和分析，对农业生产过程进行精细化管理。此过程中数字安全治理也是非常重要的，有效的农业数字安全管理体系能够及时响应和恢复，减少经济损失，保护农业产业的稳定运行[2]。

## 二、农业物联网的数字安全现状

物联网设备在现代农业中的应用展现出了巨大的潜力，然而其脆弱性也使得其一旦遭受攻击，可能带来严重的现实影响，诸如农业生产中断、基础设施管理混乱（如灌溉系统失效、电力供应受阻、温室温度调控失常，甚至是农作物病虫害的远程操控导致大面积损失），以及环境质量的恶化，甚至可能威胁到人员生命和健康[3]。尤其在农业物联网的感知层，如利用无线传感器网络（WSN）进行作物监测，其路由协议的局限性可能导致数据安全问题，读写器与无线信号的复制易导致数据泄露[4]。网络层面临的威胁，如分布式拒绝服务攻击、身份欺骗和篡改，进一步加大了保障数据完整性的挑战。农业物联网设备的异质性和规模庞大性，使得它们极易成为黑客活动的目标，构成大规模的僵尸网络，这与我国当前物联网安全防护体系的发展水平不匹配[5]。

## 三、农业物联网数字安全治理策略与实践

### （一）基于云计算和区块链的解决方案

农业物联网（Agricultural Internet of Things,IoT）的数字安全治理策略与实践涉及了技术与管理的深度融合，旨在保护农业数据、设备以及整个农业生态系统的安全性。云计算和区块链技术在这方面的应用扮演了关键角色[6]。

1. 云计算

一方面，云计算提供了大规模的数据中心，用于存储农业物联网产生的海量传感器数据，通过分布式计算优化资源利用率，同时保证数据的安全备份和访问控制。另一方面农业物联网可以通过边缘计算将部分数据分析处理任务放到物联网设备或靠近现场的边缘节点，减少了数据传输中的安全风险，并提高响应速度[7]。不可忽略的是安全服务，云服务提供商通常会提供加密通信、身份验证和访问控制等安全机制，防止未经授权的访问[8]。

2. 区块链技术

区块链通过分布式账本记录所有交易和数据，确保信息的透明性和完整性，防止数据被恶意篡改。并且智能合约自动执行基于预设规则的合同，简化交易流程，减少人为错误和欺诈风险。最后通过加密和共识机制，确保只有授权用户能够访问特定的农业信息，保障数据隐私。

### （二）安全技术应用：物联网安全网关、加密通信等

在现代农业物联网系统中，物联网安全网关（IoT Security Gateway）和加密通信技术起着至关重要的作用，特别是在保障数据安全方面。这些技术的应用旨在确保农业生产过程中的各类数据，如环境监测、作物生长数据、设备状态等，免受未经授权的访问、篡改和泄露。

首先，物联网安全网关作为连接物联网设备与核心网络的关键组件，它扮演了防火墙的角色[9]。其次，加密通信技术是保护数据传输安全的核心手段，确保在设备之间以及网关与云端服务器之间的通信过程中，数据以密文形式传输，难以被中间人拦截或解析，从而降低了信息泄露的风险。再者，由于农业物联网设备可能分布在广阔的农田区域，因此还涉及零信任网络架构（Zero Trust Network）的应用，这种架构强调无论设备的位置如何，始终验证所有请求。这有助于提高系统的整体安全性，并在面对潜在的安全威胁时快速响应。

### （三）农业组织和政府的角色与责任

农业组织作为行业的实践者，如合作社、农场和专业服务机构，它们负责应用物联网技术，如传感器网络、远程监控和数据分析系统，以提高生产效率，精确农业管理，例如土壤湿度监测、作物生长预测等。这些组织需确保设备的有效集成和数据的实时收集，从而支持决策制定[10]。

政府的角色则更为宏观和战略。它在农业物联网中扮演监管者和政策制定者的双重角色。一方面，需要制定相关的法规和标准，确保物联网设备的兼容性和数据隐私，保护农民的知识产权，同时促进数据共享与互通。此外，政府还应投资于研发，支持农业物联网技术的研发，并提供财政激励措施，鼓励农业组织采用这些先进技术。

在数据安全方面，政府和农业组织共同承担责任。他们需建立完善的数据管理系统，防止未经授权的访问、篡改或泄露[11]。这涉及网络安全策略的制定，如防火墙建设、数据加密、身份验证机制以及定期的安全审计。同时，教育农民和农业从业人员关于数据安全的重要性和操作规范，提升他们的信息安全意识。

## 四、面临的挑战与未来发展趋势

### （一）技术更新带来的新挑战

在农业生产领域，随着智能化和精准农业的发展，传统的生产设施和环境已无法满足现代农业对高效、节能、实时数据监控的需求。设备的低功耗设计以及稳定的数据传输能力变得至关重要[12]。现代物联网（IoT）技术，如无线传感器网络（WSN）、智能传感器和边缘计算，被广泛应用到农田管理、作物监测、灌溉控制等各个环节中。

WSN，作为基础设施，其节点需要在田间环境中长时间运行，这就要求设备具有极低的功耗，以减少电池更换的频率，同时保证信号传输的可靠性，避免因通信中断而影响决策支持系统的实时响应。此外，为了应对大面积农田的信息收集，网络的扩展性和带宽优化也是关键技术挑战。边缘计算的引入使得数据处理分析可以在传感器网络的近端进行，极大地提高了响应速度，减少了数据回传至云端的压力。

然而，这种即时分析也带来了新的数据安全风险。一方面，因为设备数量众多，且分布广泛，数据集中点可能成为攻击者的目标，数据泄露或篡改的风险增大。另一方面，边缘计算的本地处理可能会暴露一些敏感信息，如作物病虫害预测模型或农场操作策略，需要强大的加密技术和隐私保护机制来防止信息被盗用或滥用。

为了应对这些挑战，农业物联网需要结合区块链技术[13]，提供不可篡改的交易记录和数据来源追踪，增强透明度和可追溯性。此外，利用人工智能的威胁检测和行为分析技术，能够及时发现并阻止潜在的网络安全威胁。

### （二）法规适应性与国际标准

农业物联网的数据安全是现代农业信息化的关键环节，涉及多个主体的法律遵从和标准化实践[14]。首先，农业生产者需要遵循国家及国际的相关数据保护法规，如欧盟的 GDPR（General Data Protection Regulation）或中国的《网络安全法》。他们需保证收集、处理和分享农业传感器数据时，用户的隐私权得到尊重，并对数据进行适当加密以防止未经授权的访问。农业供应商与采购商在交易中涉及的物联网数据，可能涉及商业秘密和合同义务，因此他们需要了解并遵守电子商务法、电子合同法以及数据交换和共享的行业规范[15]。

数字化企业作为物联网平台提供商，需遵守各地的数据保护法规，构建符合 SGDPR 或 CCPA（California Consumer Privacy Act）等的隐私保护框架，并积极参与制定和推动行业数据安全标准，如物联网设备安全标准和数据安全协议。

## 五、结论

农业物联网的发展依赖于数据收集和分析，但这也带来了数字安全的风险。数据驱动决策是农业的核心，但信息安全和数据隐私保护不容忽视。有效的农业数字安全治理对于基于云计算的决策支持系统至关重要，能够提升农业生产效率，保障资源合理利用，并促进可持续发展。

*参考文献：*


[1] 罗述斌. 基于5G 和物联网的智慧农业大数据管理平台建设策略［J］. 农业工程技术，2023,43(08):22-23.

[2] 张继群，李斌，赵斌. 基于区块链的农业物联网 AI 大数据平台［J］. 物联网技术，2024,14(02):121-122+126.

[3] 葛礼姣，程玉静，仇亮，等. 农业物联网技术在温室大棚生产中的应用进展［J］. 浙江农业科学，2024,65(01):242-248.

[4] 张珂，蔡熙桐，霍洪双. 基于2.4G 无线收发模块的低成本农业物联网节点软件设计［J］. 齐齐哈尔大学学报 ( 自然科学版 ),2023,39(06):53-57.

[5] 苏兵. 基于边缘计算的农业物联网数据流处理设计［J］. 信息技术与信息化，2023,(08):102-105.

[6] 薛寅乐. 农业物联网技术在农业经济信息化中的应用与发展［J］. 农业工程技术，2023,43(23):75-76.

[7] 徐秋. 关于农业物联网技术的应用及创新研究［J］. 佳木斯职业学院学报，2023,39(07):182-184.

[8] 章小宝. 基于移动通信网络的农业物联网数据稳定传输研究［J］. 长江信息通信，2023,36(06):54-56+60.

[9] 陈可. 基于虚拟化攻击模块优先级评估的自动攻击框架研究［D］. 广州大学，2023.

[10] 李淑萍. 浅析农业物联网技术提升农业机械化向数字化转型［J］. 农业机械，2023,(05):58-60+64.

[11] 曹梦川，伍丹，杜朋轩. 基于非对称加密算法的农业物联网数据加密解密模块的研究［J］. 信息与电脑 ( 理论版 ),2022,34(15):224-228.

[12] 李航，董安明，禹继国，等. 基于前后端分离架构的智慧农业物联网系统设计［J］. 现代电子技术，2022,45(14):63-68.

[13] 史恒，雷莹慧，何正方，等. 区块链技术在农业物联网防伪溯源的应用研究［J］. 计算机时代，2022,(06):32-36.

[14] 张文正. 基于农业物联网的数据管理系统［D］. 南京邮电大学，2021.

[15] 安强. 农业物联网时序数据处理平台的设计与实现［D］. 北京邮电大学，2020.