doi:10.6041/j.issn.1000-1298.2025.10.019

农业大数据与隐私计算技术研究综述

吴政娴　文　娟
（中国农业大学信息与电气工程学院，北京 100083）

摘要：近年来，随着传感器、遥感、互联网技术的快速发展，农业大数据呈现爆发式增长。传统的农业大数据集中处理方法是将多方农业数据存储在一起，然后进行作物生长评价和产量预测。然而，这些方法在数据传输过程中存在隐私泄露和共享效率低的问题。此外，多方数据还面临着数据版权保护等数据安全问题。为了解决上述问题，隐私计算作为一种新兴的数据安全技术，为在不泄露原始数据的情况下实现多方协同分析提供了可行的途径。本文首先从数据采集、预处理、存储管理、数据分析到农业大数据在精准农业、产量预测、病虫害监测、供应链溯源、农业金融等领域的关键应用，全面综述了农业大数据的发展现状。然后，系统总结了同态加密、安全多方计算、差分隐私、联邦学习等主流隐私计算技术的原理和应用场景。重点分析了隐私计算技术在农业领域的应用，概述了隐私计算在农业数据传输、病虫害检测、作物监测、产量预测等方面的研究进展，并总结了当前隐私计算技术存在的主要挑战，包括通信成本、计算复杂度、异构适应性、评估机制以及隐私保护与模型性能之间的权衡。最后，探讨了通信压缩、轻量加密、多模态建模、评估体系构建与隐私-性能优化等隐私计算技术，助力农业智能化发展。

关键词：农业大数据；智慧农业；隐私计算；数据安全
中图分类号：S24　　**文献标识码**：A　　**文章编号**：1000-1298(2025)10-0184-16　　**OSID**：

Review on Agricultural Big Data and Privacy Computing Technology

WU Zhengxian　WEN Juan
(*College of Information and Electrical Engineering*, *China Agricultural University*, *Beijing* 100083, *China*)

Abstract: In recent years, with the rapid development of sensors, remote sensing, and Internet technologies, agricultural big data has shown explosive growth. The traditional centralized processing methods integrated multi-party agricultural data for crop growth evaluation and yield prediction. However, these methods face great challenges with privacy leakage and low sharing efficiency in the process of data transmission. Moreover, multi-party data also faces data security issues such as data copyright protection. To address the above problems, privacy computing, an emerging data security technology, provides a feasible path to achieve multi-party collaborative analysis without disclosing the original data. Firstly, the landscape of agricultural big data was comprehensively reviewed from data acquisition, preprocessing, storage, and analysis to its key applications in precision farming, yield forecasting, pest monitoring, supply chain traceability, and agricultural finance. Then the principles and applicable scenarios of mainstream privacy computing technologies such as homomorphic encryption, secure multi-party computation, differential privacy, and federated learning were systematically summarized. To emphatically analyze the applications of privacy computing technology in the agricultural field, the advanced research of privacy computing was outlined in agricultural data transmission, pest and disease detection, crop monitoring, and yield prediction. Meanwhile, existing key challenges of the current privacy computing technology were summarized, including communication cost, computational complexity, heterogeneous adaptability, evaluation mechanism, and the trade-off between privacy protection and model performance. Finally, future directions of privacy computing technologies on communication compression, lightweight encryption, multimodal modeling, construction of evaluation systems, and privacy-performance optimization were explored to facilitate the intelligent development of agriculture.

Key words: agricultural big data; smart agriculture; privacy computing; data security

收稿日期：2025-07-10　修回日期：2025-07-30
基金项目：国家重点研发计划项目(2021QY2221-1)
作者简介：吴政娴(1999—)，女，博士生，主要从事信息安全与自然语言处理等研究，E-mail：wzxian@cau.edu.cn
通信作者：文娟(1982—)，女，副教授，博士生导师，主要从事信息安全与自然语言处理等研究，E-mail：wenjuan@cau.edu.cn

0　引言

近年来，传统农业模式已逐渐向以数据驱动为核心的智慧农业模式转型[1-2]。农业数据来源非常广泛，涵盖从田间生产到产业链末端的多类型信息资源。针对农业大数据的多源异构性与动态非平稳性，通过数据预处理流程可显著提升数据可用性与建模质量，并通过数据存储策略实现高频采集数据、遥感影像与结构化业务数据的统一存储与高效调度。

然而，在农业多主体协作日益频繁的背景下，农业数据还面临着严峻的隐私保护和数据治理挑战。农业多主体之间既拥有对本地数据的管理权和使用权，又对数据的外泄、误用或未经授权挖掘存在担忧。因此，农业数据呈现出典型的“数据孤岛”现象，严重制约了农业数据共享协同的有效开展。

隐私计算（Privacy computing）应运而生并逐步成为数据流通和智能利用的关键基础设施[3]，逐渐在农业领域展现出巨大潜力。然而，其在农业场景中仍然面临诸多技术与实践层面的挑战。

本文首先系统梳理农业大数据的采集与处理、存储与管理、挖掘与分析以及其应用场景。然后阐述隐私计算技术的发展脉络，归纳其在农业大数据中的典型应用进展，分析当前存在的技术瓶颈，并对未来发展提出探讨与展望。

1　农业大数据技术

随着智慧农业的不断发展，农业大数据逐渐成为现代农业发展的核心支撑资源。它不仅推动了传统农业向数字化、智能化转型，也为实现农业高质量发展、保障粮食安全和推动绿色低碳农业提供了坚实的数据基础。

1.1　数据采集技术

农业大数据的采集是实现农业智能化与精细化管理的关键基础，涵盖了从多源异构数据的获取与整合，到标准化处理与建模准备的全流程[4]。如图 1 所示，农业大数据的典型来源包括田间传感系统、遥感观测平台、农业生产管理服务平台、农产品供应链系统及金融服务机构等。数据形态方面，农业数据包括结构化数据（如作业记录、价格表格）和非结构化数据（如遥感图像与气象数据），构成一个多源、复杂、动态并具有时空耦合特征的数据体系[5]。

（1）田间传感系统。田间环境数据是农业生产精准感知的基础，主要依赖部署在农田中的土壤温湿度传感器、无人机平台和气象站等设备进行采集。



图 1　农业大数据分类与来源

Fig. 1　Classifications and sources of agricultural big data

典型参数包括温度、相对湿度、光照强度、风速、降水量及二氧化碳浓度等。通过无线传感网络与边缘计算节点的协同工作,可实现数据的高频采集、远程传输与本地初步分析,大幅提升采集数据的时效性与准确性。

(2)遥感观测平台。遥感平台通常分为卫星遥感、航空遥感和无人机遥感 3 类。其中,卫星遥感具备大范围、多光谱观测、高时序分辨率等优势,适用于宏观区域的作物分布识别与自然灾害监测。相比之下,航空与无人机遥感则具备高空间分辨率与机动性强的特点,适合地块级别作物长势分析与局部病虫害检测。遥感数据类型包括 RGB 图像、红外图像及多光谱图像,可用于计算归一化植被指数(NDVI)、绿度植被指数(GVI)等植被指数,为作物生长状态监测与健康评估提供关键输入。

(3)农业生产管理服务平台。农业机械(如播种机、收获机、无人拖拉机)与智能灌溉、施肥系统等农业设施系统可自动记录作业过程信息,生成作业轨迹、资源投入、作业时间、产出效率等结构化数据。此外,农业生产管理平台还可记录农事计划、用户反馈、监测任务日志等内容,为农业建模、生产过程分析及产量评估提供数据依据。

(4)农产品供应链系统及金融服务机构。农产品在流通过程中会产生大量市场与金融数据,包括价格行情、供需数据、金融借贷记录、农业保险保单等。这些数据多数来源于电商平台、物流系统与金融服务机构,其采集与利用涉及多平台 API 接口接入、数据脱敏处理与访问权限管理等流程,是构建农业经济模型与风险评估系统的重要数据支撑。

1.2 农业大数据的数据特征

农业大数据区别于其他行业的数据体系,具有鲜明的领域特征与复杂性,在数据结构、空间属性、时间维度、安全性等方面呈现出如下特点:

(1)强地域性:农业数据依赖于自然地理要素和生态条件,如气候带、土壤类型、海拔、地块分布等,对数据的空间位置高度敏感。

(2)多源异构性:农业大数据来源广泛,涵盖结构化数据与非结构化数据。同时,不同来源设备的采样频率、精度、格式存在差异,导致数据融合难度大,对标准化、预处理和语义对齐提出较高要求。

(3)强时序性与非平稳性:农业活动具有明显的周期性特征,如播种、生长、施肥、收获等环节均依季节与气候变化同步。采集的数据往往表现出时间连续性与动态波动性,且易受突发性天气、病虫害等外部因素影响,具有非平稳性。

(4)数据孤岛严重:农业数据通常由政府部门、农业企业、农户、科研机构等多主体掌握,分布在不同平台和系统中,缺乏统一的标准规范与共享机制,导致“数据可得而不可用”的情况普遍存在,难以形成统一的数据资产体系。

(5)隐私敏感性高:农业数据中包含大量与农户经营、耕地位置、金融行为等密切相关的敏感信息,特别是在精准农业与农业金融服务中,易引发数据泄露、滥用、歧视性定价等问题。

(6)价值潜力大:农业数据的单位价值通过深度挖掘与融合分析,其在农业生产优化、风险预警、政策支持与资源配置中的价值潜力巨大,尤其在粮食安全、绿色农业与碳中和背景下具有重要战略意义。

农业大数据在数据结构、空间属性、时间维度、安全性等方面的特征,对数据处理与安全提出了新的挑战与需求。

1.3 数据预处理与清洗

采集后的原始数据往往存在缺失、异常、重复及格式不一致等问题,需进行系统化预处理加以修正。常见的数据处理步骤主要包括:异常值检测与剔除(如传感器故障数据、GPS 漂移记录等异常值)[6]、缺失值填补(如时间插值填补、模型预测推断等填补)[7]、格式标准化(如单位转换、时间格式对齐等标准化)[8]、标注一致性处理(如统一作物编码与地块命名等一致性处理)[9]等。异常值检测与剔除可通过规则法、统计法或机器学习等方法实现,规则法与统计法的效率更高但鲁棒性差,机器学习的精度高但计算复杂。缺失值填补方法如时间插值和模型预测在效率与准确性之间存在权衡。格式标准化通过单位换算与时间对齐保障数据一致性,实施简单但对数据集成至关重要。标注一致性处理有助于提升多源数据融合能力,依赖统一的编码规范。整体而言,预处理质量直接影响后续建模效果与数据共享可用性。

此外,农业数据还存在时间不一致、空间尺度不同、语义标签不统一等问题。因此,数据集成过程需结合空间对齐[10]、时间对齐(基于时间戳)[11]等技术,实现数据在地块级、时间轴与语义维度的全面融合。通过多源数据的有机整合,良好的数据预处理是确保后续建模精度与可解释性的前提,为农业智能感知、精准分析与科学决策提供坚实支撑。

1.4 农业大数据的存储与管理

当前农业大数据通常采用分层、分布式、异构融合的存储策略进行系统管理。

(1)分层存储管理。分层存储主要依据数据访

问频率与访问延迟容忍度，将数据划分为热数据、温数据和冷数据，并部署在性能成本比最优的存储层中，形成“快-中-慢”三级响应机制[12]。典型实现机制包括冷热数据分层策略（Hot - Cold Tiering）[13]，在农业感知数据平台中动态调度高频访问（如实时湿度数据）至高性能节点，而将历史归档或低频访问数据自动迁移至廉价存储区，从而优化性能与成本结构。调度过程常借助 Least recently used（LRU）或 Least frequently used（LFU）策略实现自动化分层迁移与缓存淘汰。

（2）分布式存储管理。分布式存储强调横向扩展能力与跨节点数据冗余能力，适用于农业场景中区域分布广、数据接入点多的特征[14]。该类管理机制多采用主从复制 + 分区分片机制（如 Hadoop HDFS[15] 和 Apache Cassandra[16] 等），支持农业数据的容错、分片负载均衡与并行处理。

（3）异构融合存储管理。异构融合强调多种数据库引擎与存储引擎之间的统一协调调度能力，解决农业大数据中不同数据结构、不同来源系统难以共存的问题[17]。常见机制包括多模型统一访问框架[18]，通过元数据编排与统一查询接口对接结构化数据库（如 PostgreSQL）[19]、非结构化对象存储（如 OSS）[20] 等异构后端，实现统一视图与跨源联合查询。在智慧农业中，常采用该机制将农机作业日志、遥感图像、农户反馈信息等异构数据源整合至统一分析平台，从而提高数据可用性与融合度。

1.5　数据挖掘与分析

农业大数据的挖掘与分析是实现智慧农业、精准管理和科学决策的核心手段。通过对多源、异构、大规模农业数据的深入建模与知识提取，可以实现从感知数据到应用价值的转化。该过程通常涵盖数据集成、特征提取、建模分析与可视化解释等关键环节，具体方法和技术路径呈现出多样化与交叉融合的趋势。

根据应用目标从农业大数据中提取多维度特征，包括时间序列特征（如作物生长曲线）、空间特征（如地块土壤类型）与图像特征（如遥感 NDVI 纹理特征）等[21]。在此基础上可结合主成分分析（PCA）、互信息分析或深度特征编码等手段进行特征选择与降维，提升建模效率[22]。

农业大数据分析中常用的建模方法可分为传统机器学习方法和深度学习方法。传统机器学习方法包括支持向量机（SVM）[23]、随机森林（RF）[24]、K 近邻（KNN）[25] 等，常用于作物识别、产量预测、病虫害分类等场景。深度学习方法包括卷积神经网络（CNN）[26]、循环神经网络（RNN）[27] 和 Transformer 架构[28]，逐渐在遥感图像识别、时序数据建模和农田边界提取等任务中取得优异性能。

农业数据具有明显的时间序列性与空间异质性，因而需要专门的时空分析方法支持。基于 UVA 遥感技术[29] 和 GIS[30] 等技术可实现农田监控、种植结构分布动态展示与灾害扩散模拟。

1.6　数据应用场景举例

农业大数据作为智慧农业体系的核心基础，正广泛应用于农业生产、管理、服务与政策等多个环节。以下总结具有代表性的应用场景，以展示其在实践中的多维价值。

（1）精准农业管理。依托传感器网络、遥感观测与地块级管理系统，农业大数据可实现作物精准施肥[31]、灌溉[32] 与病虫害防控[33] 等关键环节的智能化管理。腰彩红等[34] 提出基于模糊自适应 PID 控制的温室草莓智能灌溉系统，有效提升了灌溉精度与响应性能。仿真结果显示，该系统能显著减小超调量并降低稳态误差，达到节水与精细控制的双重目标。

（2）农作物产量预测。结合遥感影像、历史气象数据和田间管理记录，农业大数据可用于构建产量预测模型，提前评估作物收成情况，支持农业保险、储运调度与价格制定等下游环节。陈柏青等[35] 构建了基于 APSIM - Cotton 模型与多源气象数据融合的新疆棉花产量动态预测方法，实现了全生育期滚动预测，产量预测误差整体稳定在 4% 以内。模型在昌吉地区不同密度下表现出良好精度，棉花生育期、生物量和产量的 NRMSE 分别为 5.18%、19.60% 和 6.08%，为智慧农业决策提供了可靠的数据支撑。

（3）农业灾害预警与风险评估。基于实时遥感监测与历史灾情数据，农业大数据支持农业自然灾害（如干旱、洪涝、病虫害）的早期识别与风险等级评估。祁卓平[36] 提出了一种结构优化、成本较低的山区气象远程监测预警系统，基于微电子检测与 4G 通信技术，实现了气象与图像数据的稳定远程同步采集与传输。实地测试结果表明，系统数据平均传输速率达 406 KB/s，图像传输时延约 1 s，无丢包或卡顿现象。采用混合传输机制可将流量消耗降低至传统轮询机制的 60%，有效提升数据传输效率与可靠性。

（4）农产品质量溯源与供应链管理。农业大数据可支持构建基于区块链的溯源系统，记录作业环节、物流路径与仓储环境信息，提升食品安全透明度与供应链效率。李梦琪等[37] 设计了一种基于主从多链架构的水产品区块链溯源管理系统，有效提升

了数据安全性与溯源透明度。该系统可实现隐私数据分层存储与溯源信息的高效管理,较传统单链结构在性能与可扩展性方面具有明显优势。

(5)数字农业金融服务。农业大数据通过建模分析农户经营行为、作业记录与风险状况,为农业保险、农贷等金融服务提供数据支撑。李兵等[38]围绕农业金融振兴乡村的目标,系统探讨了卫星遥感与智能技术在农业金融中的创新应用,重点展示了在作物长势监测、估产评估与灾害预警等方面的关键成果。研究表明,融合遥感大数据与人工智能技术可显著提升农业金融服务的精准性与风险管控能力,为推进乡村振兴和农业现代化提供了新路径与技术支撑。

综上所述,农业大数据作为智慧农业发展的关键驱动力,涵盖了从采集、处理、存储、挖掘到应用的完整技术链条,呈现出多源异构、强时空耦合与高价值潜力等鲜明特征。通过引入先进的传感技术、分布式存储架构与智能分析算法,农业数据得以高效采集、精准建模与深度挖掘,支撑了作物精准管理、产量预测、灾害预警、供应链溯源与农业金融等多个核心应用场景。由于数据规模庞大、质量参差、系统分散,农业大数据的存储与传输体系正面临多维挑战,包括网络基础设施薄弱、异构系统协同困难、数据一致性难以保障以及存储-计算解耦带来的资源孤岛等问题。

2 隐私计算

隐私计算是一种新兴的计算范式,其目的是在数据处理过程中保护数据安全传输与隐私安全,从而实现多方数据协同建模、分布式计算与可信分析[39-40]。传统的数据集中存储与共享模式难以满足对数据主权、隐私保护与合规性的要求,制约了农业数字化的进一步深化。隐私计算技术则为农业大数据的安全流通提供了关键支撑。如表 1 所示,隐私计算可大致分为同态加密、安全多方计算、差分隐私和联邦学习。

表 1 隐私计算技术归纳

Tab. 1 Summary of privacy computation technology

项目	提出时间	核心原理	数据是否可见	目标	优点	缺点	应用场景	代表框架
同态加密	1978 年[41]	在加密数据上直接计算,结果解密后仍然正确	始终不可见	防止在计算过程中泄露数据	安全性强,支持密文计算(全同态)	效率低、计算成本高	云计算、区块链等加密传输	Microsoft SEAL[42]、IBM HELib[43]、Paillier[44]
安全多方计算	1982 年[45]	多方协同参与计算,各方保留输入隐私,仅获得最终输出	仅参与方本地可见持有数据	防止在协同计算中泄露数据	支持复杂逻辑计算	通信复杂、难以扩展到大规模参与方	拍卖、投票等多方协同系统	SPDZ[46]、ABY[47]、EMP - toolkit[48]、Sharemind[49]
差分隐私	2006 年[50]	在数据或查询结果中添加噪声,防止个体隐私识别	加噪后可见	防止推断个体隐私数据	理论清晰,计算高效,可控制隐私预算	数据加噪影响计算精度	数据发布、查询系统	Google DP library[51]、OpenDP[52]
联邦学习	2016 年[53]	本地分布式训练模型,仅上传本地模型参数/梯度,聚合后返回总参数/梯度	仅参与方本地可见持有数据	防止在集中化训练中泄露数据	分布式训练	参数可能泄露,依赖通信与聚合机制	边缘设备参与的分布式模型训练	Google FedAvg[54]、PySyft[55]、FATE[56]、Flower[57]

2.1 同态加密

同态加密(Homomorphic encryption,HE)是一种特殊的加密技术[58]。如图 2 所示,同态加密技术可以将隐私信息加密为密文数据进行传输,同时直接对密文数据进行数学运算得到的密文结果解密后与对原始明文直接运算的结果相同[41]。根据密文可支持的计算程度,同态加密可分为半同态加密(Partially homomorphic encryption, PHE)[59]和全同态加密(Fully homomorphic encryption, FHE)[60],如表 2 所示。

近年来,随着加密算法与计算资源的发展,半同态加密和全同态加密不断取得了理论与工程突破,



图 2 同态加密流程图

Fig. 2 Progress of homomorphic encryption

逐步向实用化迈进。特别是在农业数据安全传输场景中,同态加密展现出显著优势。KULALVAIMOZHI 等[65]在农业遥感图像传输中,利用同态加密和增强型离散小波变换对遥感图像进行加密、压缩、解压缩和解密。MAHATO 等[66]对传感器采集的农田数据进行本地同态加密,仅上传加密数据进行远程诊断分析。SHEN 等[67]对土壤湿度、

表 2　同态加密技术分类

Tab. 2　Classification of homomorphic encryption technology

同态加密类型	支持计算	优点	缺点	代表算法
半同态加密(PHE)	加法或乘法(单一)	效率高、计算复杂性低	无法支持通用计算	RSA[61]、Paillier[44]
全同态加密(FHE)	加法和乘法(任意)	计算开销大、加解密速度慢	支持任意计算	Gentry[62]、BGV[63]、CKKS[64]

温度、肥力等数据进行同态加密处理，分布式训练的模型参数也采用同态加密处理，实现远程协作的分布式模型训练。尽管同态加密在隐私保护方面具有理论上的完备性，其在农业场景中的推广仍面临挑战，例如计算开销大、处理速度慢、密文体积庞大等问题限制了其在实时性与资源受限环境下的应用。

2.2　安全多方计算

安全多方计算(Secure multi-party computation，SMPC)是一种密码学技术。如图 3 所示，假设 N 个参与方都持有各自的敏感信息。第 N 个参与方的敏感信息为 x_N，在各参与方互不信任且不泄露各自私有数据的前提下，共同计算函数 f 的结果，并得到对应的输出 y_N[45]。在整个计算过程中，所有参与方的原始输入数据对其他方始终保持不可见性。

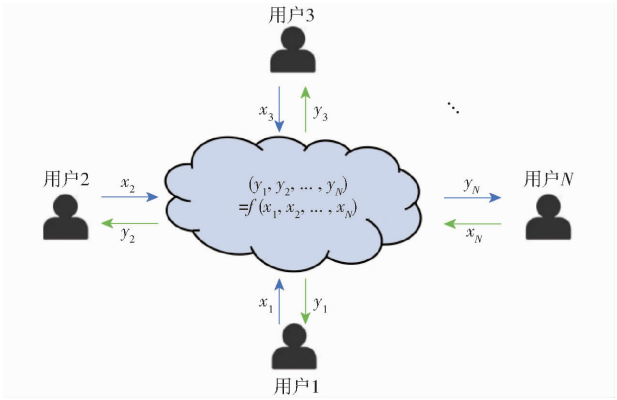


图 3　安全多方计算原理图

Fig. 3　Principle of secure multi-party computation

AKBAR 等[68]将安全多方计算与联邦学习相结合，在各农场互不泄露原始数据的前提下，进行跨组织模型协作。ZHU 等[69]在农业供应链等分布式环境中采用多方安全计算，以避免单点数据暴露。SINGH 等[70]将安全多方计算嵌入到农业自动化的机器学习模型中，保护无人机路径规划、喷灌控制等关键数据，防止恶意推理攻击或训练数据反演。尽管安全多方计算能够在不泄露各方私有数据的前提下实现农业数据的精确共享与联合计算，确保数据隐私与安全性，但其计算开销较大，协议复杂度高，往往导致通信和计算资源的显著消耗，限制了其在资源受限或大规模数据处理场景中的广泛应用。

2.3　差分隐私

差分隐私(Differential privacy，DP)是一种数学意义上可量化的隐私保护技术。如图 4 所示，在发布或使用统计数据时，对个体隐私信息进行加噪模糊，最终的数据结果与未处理的数据结果几乎不变，以最大限度减少对个体隐私的泄露[50]。

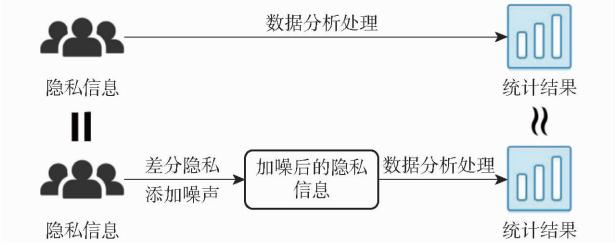


图 4　差分隐私原理图

Fig. 4　Principle of differential privacy

差分隐私技术广泛应用于医疗安全等领域。虽然差分隐私技术已逐渐引入农业领域，但现阶段研究较少。ZILLER 等[71]提出差分隐私随机梯度下降(DP－SGD)算法，对每个样本独立计算梯度、进行 L_2 范数裁剪、添加高斯噪声，并采用高斯差分隐私(GDP)进行精确隐私预算评估，从而实现对任意网络结构的通用支持和严格隐私保障。ZHANG 等[72]采用计算属性间相关性的方法，结合差分隐私保护模型和树模型，提出了一种基于属性关联的差分隐私分类树数据发布方法(ACDP－Tree)，在不泄露隐私信息的情况下保障数据发布后的数据有效性。

差分隐私因其在保护个体敏感信息方面的理论保障，已被广泛应用于多个数据共享与分析场景。然而，在实际应用中，差分隐私仍面临一些关键挑战：引入的随机噪声可能导致模型或数据分析结果的精度显著下降，影响其实用性；如何在不同应用场景下合理设计噪声机制以平衡隐私保护强度与数据可用性，仍是一项具有挑战性的任务。

2.4　联邦学习

联邦学习(Federated learning，FL)是一种分布式机器学习技术。如图 5 所示，多个参与方在本地数据上训练各自的模型，并将其参数传输给公共方进行汇总。最终各参与方在不共享本地数据的前提下，共同训练一个全局模型[53]。根据各参与方本地数据集的数据分布特征，联邦学习可分为 3 类：横向联邦学习、纵向联邦学习和迁移联邦学习(表 3)。

康孟珍等[76]将联邦学习与区块链相融合提出了农业 AI 框架，该框架可以实现数据可控、安全的数据建模。许继平等[77]采用横向和纵向联邦学习框架，针对粮食供应链场景有效保障供应链各环节

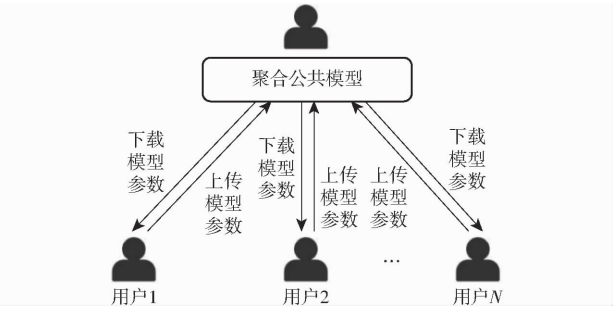


图 5 联邦学习原理图

Fig. 5 Principle of federated learning

的数据安全协作。联邦学习结合同态加密、安全多方计算和差分隐私等技术,能够在不直接交换原始数据的前提下有效保护本地数据的隐私安全。然而,联邦学习在实际部署中仍面临若干挑战:联邦学习依赖于频繁传输模型参数或梯度,尤其是在大规模参与节点或复杂模型场景下,显著增加了通信开销;为实现有效的模型聚合,联邦学习通常要求所有参与方采用一致的模型结构与训练流程,这在异构设备或跨机构合作中可能难以满足,从而限制了其灵活性和适应性。

表 3 基于特征分布的联邦学习分类

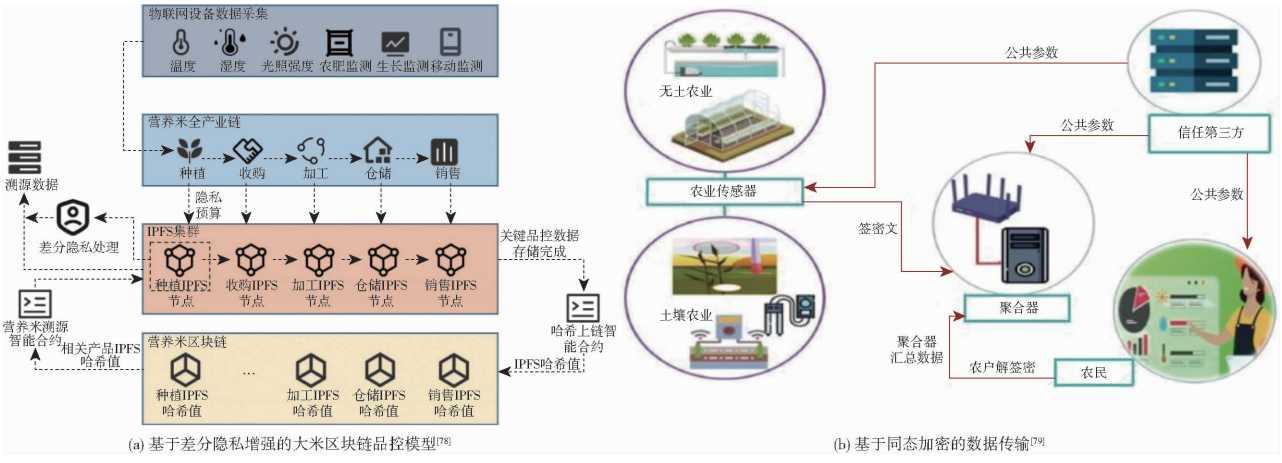
Tab. 3 Federated learning classification based on feature distribution

联邦学习类型	数据特征	应用示例	文献序号
横向联邦学习(Horizontal FL)	特征重叠、样本不重叠	多个农户拥有相似的作物种类、传感器指标,但农田位置不同,需要各自训练产量预测模型	[73]
纵向联邦学习(Vertical FL)	特征不重叠、样本重叠	农业银行和农业保险公司对同一农户拥有不同数据(征信或保单)联合训练信用模型	[74]
迁移联邦学习(Federated Transfer/Hybrid FL)	特征、样本部分重叠或不重叠	不同地区农场使用不同农机和作物,但希望共享知识构建共通病虫害识别模型	[75]

3 隐私计算在农业大数据中的应用

3.1 数据传输与发布

由于农业数据来源高度分散,其在采集、传输发布过程中面临诸多隐私与安全挑战。随着传感器、无人机、遥感设备及农机终端的大规模部署,农业数据呈现出实时性强、分布广泛、敏感性高等特点,涵盖作物生长信息、土壤环境参数、农户行为数据及交易记录等。这些数据的传输若缺乏有效的加密与保护机制,容易在网络中被窃取、篡改或滥用,进而损害数据拥有者的利益与数据系统的可信性。为此,研究者将隐私计算技术引入农业领域以安全传输与发布数据。图 6 展示了隐私计算在数据传输中的应用,表 4 展示了基于隐私计算的数据传输的部分研究成果。



(a) 基于差分隐私增强的大米区块链品控模型[78]

(b) 基于同态加密的数据传输[79]

图 6 隐私计算在数据传输和区块链中的应用

Fig. 6 Research of data transmission and block-chain based on privacy computing

首先,苗玉霞[80]以农产品供应链为对象,采用 Paillier 同态加密算法对物联网节点属性数据加密,并在中心节点进行聚合关联分析,并通过异常检测算法抵御恶意攻击。研究结果显示该方案在保障隐私的同时具备较低的计算与通信开销。类似地,王炎[81]提出一种基于同态加密的多函数安全数据融合方案(HMDA),支持多种统计查询,并在映射与编码阶段实现数据与顺序保护。研究结果表明,HMDA 方案能有效抵御多种攻击,保障融合精度与网络负载均衡,同时降低通信开销。为了实现多方供应链的数据安全,PENG 等[82]针对稻米供应链,提出多区块链精细化监管模型(MBRRSM),融合混

表 4　基于隐私计算的农业数据传输与发布研究成果

Tab. 4　Research of agricultural data transmission and release based on privacy computing

发表时间	研究对象	隐私计算	原理	文献序号
2017 年	农产品供应链	同态加密	引入 Paillier 同态加密进行聚合与关联分析	[80]
2019 年	传感器数据	同态加密	结合同态加密技术保护网络融合的数值与顺序	[81]
2022 年	稻米供应链	安全多方计算	结合混合加密、安全多方计算和 SPOP 共识机制保障数据传输、存储与使用安全	[82]
2024 年	大米区块链	差分隐私	利用差分隐私技术模糊隐私信息，保护数据隐私安全	[78]
2024 年	传感器数据	同态加密	利用同态加密、混沌 Logistics 序列和模糊加权聚类，存储无线传感器网络数据与动态存储结构优化	[79]

合加密、安全多方计算与 SPOP 共识机制，构建数据传输、存储与使用体系。研究表明，MBRRSM 在保障数据隐私与监管精度方面表现优异，助力可持续农业与粮食安全战略实施。为了缓解同态加密与多方安全计算与通信开销较大的问题，吴国栋等[78]提出一种差分隐私增强的大米区块链品控模型，结合 IPFS 分布式存储与差分隐私机制，解决数据上链效率低与隐私泄露问题。研究结果表明，该系统单环节数据存储平均耗时 1.125 s，追溯查询平均耗时 0.691 s，较传统系统存储效率提升 6.64%、查询效率提升 16.44%，实现品控数据的高效、安全与可追溯管理。为了保障准确率与实现数据加密和动态存储结构优化，TAJI 等[79]提出一种基于同态加密的无线传感器网络数据安全存储方法，结合混沌 Logistics 序列与模糊加权聚类，实现数据加密与动态存储结构优化。研究结果显示，该方法抗攻击概率平均为 95.24%，显著提升了数据存储的安全性与空间均衡。

总体而言，现阶段的研究充分展示了同态加密及其与其他隐私保护技术结合在农产品供应链与农业数据管理中的广阔应用前景，在保障数据隐私、安全传输与融合精度的同时，也兼顾了系统的计算效率与通信开销，为实现智慧农业和粮食安全战略提供了坚实技术支撑。尽管部分方案在计算与通信方面进行了优化，同态加密本身仍具有较高的计算成本。虽然部分研究保障了数据隐私，但可能在一定程度上影响数据分析的精度或可解释性。未来的工作可以进一步聚焦于低资源消耗下的隐私保护机制、跨场景通用架构设计以及隐私保护与数据效能之间的优化平衡。

3.2　作物病虫害检测

在智慧农业体系中，作物病虫害检测是保障农业生产安全与提高产量质量的关键环节。借助遥感技术、图像识别、无人机巡检与物联网感知设备，农业系统能够实时采集大田作物的叶面状态、气候数据及土壤环境信息，并通过人工智能模型实现对病虫害的快速识别与预警。然而，病虫害检测模型的构建通常依赖于大量的图像与环境数据，其中不乏地理位置信息、农户种植行为、作物健康状况等敏感内容。若未经保护即被集中上传或共享，可能导致农场信息泄露、农产品竞争情报暴露，甚至引发数据滥用和农户权益受损的问题。为了防止数据泄露，研究者在作物病虫害检测中引入了分布式联邦学习。图 7 展示了联邦学习在苹果病虫害检测中的应用，表 5 展示了基于隐私计算的病虫害检测部分研究成果。

首先，DENG 等[83]基于联邦学习与改进的 Faster R－CNN，针对苹果病害提出病虫害检测方

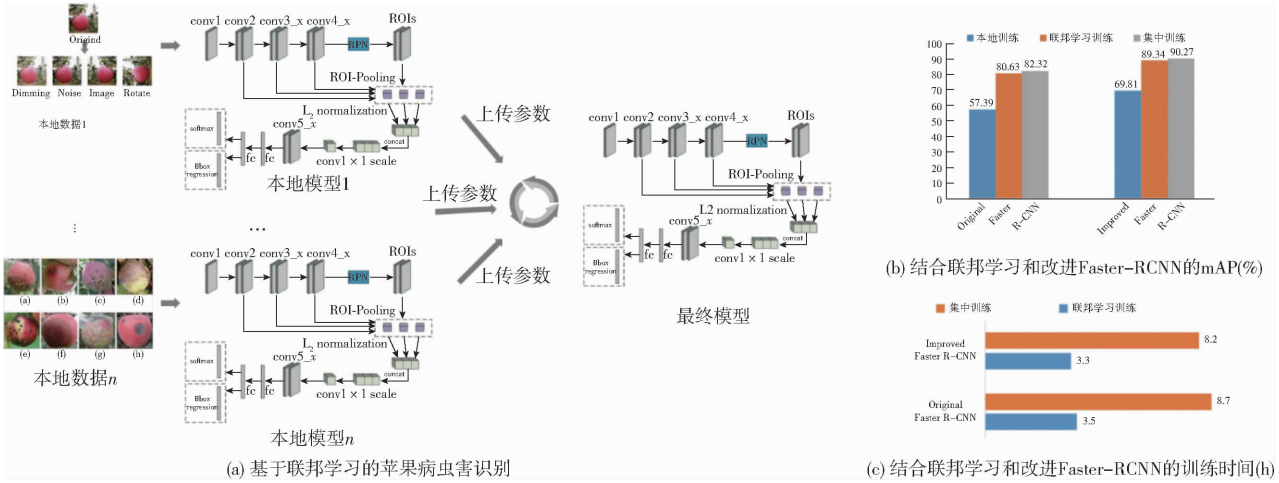


图 7　基于联邦学习的苹果病虫害检测研究[83]

Fig. 7　Research of apple pest and disease detection based on federated learning

表 5 基于联邦学习的作物病虫害检测研究成果

Tab. 5 Research of crop pests and diseases detection based on federated learning

发表时间	研究内容	原理	性能	文献序号
2022 年	苹果病害	引入 OHEM、Soft - NM 和分布式联邦学习分布式训练 ResNet - 101 检测苹果病害	mAP 为 90.27% FL 下的 mAP 为 89.34%	[83]
2023 年	小麦病害	结合 TensorFlow Federated 框架与 CNN 模型,利用 FedAvg 聚合分布式训练模型	精准率为 94.8% F1 分数为 94.6%(加权平均)	[84]
2024 年	草莓叶片病害	构建 4 级病害严重程度分类体系,利用联邦平均融合聚合 6 个客户端 CNN 模型	平均精准率为 96.91%	[85]
2024 年	香蕉叶片病害	采用加权平均聚合 5 个 CNN 模型以缓解不平衡分类	精准率 97% ~99%	[86]
2024 年	水稻病害	在独立同分布(IID)和非独立同分布(Non - IID)数据集上检测水稻病虫害	IID 数据的精准率为 99.05% Non - IID 数据的精准率为 98.48%	[87]
2024 年	玉米叶片病害	利用 DeepClusterV2 自监督预训练与梯度策略,缓解异构数据下的过拟合问题	精准率为 96.37%	[88]

法。该方法引入 ResNet - 101 替换 VGG - 16 以解决小目标检测困难的问题,同时还引入了在线困难样本挖掘增强(OHME)和软非极大值抑制优化(Soft - NMS)以提升复杂环境中多尺度目标检测精度。研究表明,基于联邦学习的改进后 Faster R - CNN 模型将 mAP 提升至 89.34%,训练速度提升 59%,单图像检测仅需 0.05s。类似地,MEHTA 等[84]针对小麦病虫害提出一种基于联邦学习的卷积神经网络方法,该方法在分散的终端设备上分布式训练模型。研究结果显示该方法的准确率达到 94.8%,加权平均后的 F1 分数为 94.6%。为了进一步提升准确性,THAPLIYAL 等[85]还针对草莓叶片病害问题,提出一种基于卷积神经网络与联邦学习的检测方法,利用来自不同地区、不同农业技术条件下的图像数据,实现跨客户端的全局知识提取。研究结果显示平均准确率为 96.91%。为了解决不平衡分类,SURYAVANSHI 等[86]结合联邦学习与 CNN,提出一种针对香蕉叶病害识别的分布式诊断方法,通过各客户端本地训练与参数聚合构建全局模型,实现隐私保护与高效分类。研究结果显示加权平均准确率为 96.32%,表明该方法在多源异构数据环境下的准确性与可扩展性,展示出其在农业病害检测中的应用潜力。类似地,黄炯炯[87]针对智能农业中水稻病虫害分类问题,提出基于联邦学习的方案以解决数据孤岛并保护设备隐私,利用 7 种预训练模型进行特征提取并评估性能。研究结果显示,VGG19 模型在 IID 与 Non - IID 数据下准确率分别达 99.05% 与 98.48%,联邦学习使设备准确率提升 4.36 个百分点,且模型稳定性随参与设备数量增加而增强,验证了其在实际应用中的高效性与鲁棒性。为了缓解模型过度拟合本地特征差异数据,赵盎然等[88]针对玉米叶片病害识别问题,提出一种基于联邦学习的分布式病害识别方法(GFedAvg),通过改进梯度更新策略与引入自监督预训练,解决数据异构引发的模型漂移与过拟合问题。研究结果表明,GFedAvg 在无需上传数据的前提下实现与集中式模型相近的识别性能,显著提升了准确率(96.37%)与收敛速度,并降低了波动性。

总体而言,现阶段研究在作物病虫害检测任务中积极引入联邦学习框架,将隐私保护与模型性能有效结合,为智能农业提供了更安全、高效的解决方案。这些研究不仅在多源异构数据环境下实现了高准确率(普遍超过 94%),还有效解决了数据孤岛、模型漂移、小目标识别等实际问题,显示出联邦学习在农业检测领域的广阔应用前景和技术先进性。尽管其无需上传原始数据,降低了数据泄露风险,但模型参数的共享仍可能引发潜在的隐私泄露风险。而对模型参数进行隐私加密,则面临数据传输普遍存在的通信开销问题。因此,未来的研究可进一步聚焦于部署结构的简化、通信与计算效率的提升、对异构数据的鲁棒性增强,同时建立统一的评估体系,并引入更强的隐私保护机制,以推动联邦学习在农业病虫害智能识别中的持续发展与实际应用。

3.3 作物监测

作物监测是智慧农业中的基础性任务,涵盖作物生长状态的动态感知、营养诊断等关键环节,对于实现精准种植、科学施肥、风险防控等目标具有重要意义。近年来,隐私计算技术在作物监测任务中的应用逐渐展开,并取得了积极进展。图 8 展示了联邦学习在作物监测系统中的应用研究,表 6 展示了基于隐私计算的作物监测部分研究成果。

为了提高农业自动化响应精度,ABU-KHADRAH 等[89]结合联邦学习机制提出了一种可修改的多功能传感器控制系统(AMFSC),通过历史最佳传感数据优化当前农业传感与驱动策略,实现对土壤、气候和作物健康的精准响应。研究表明,该

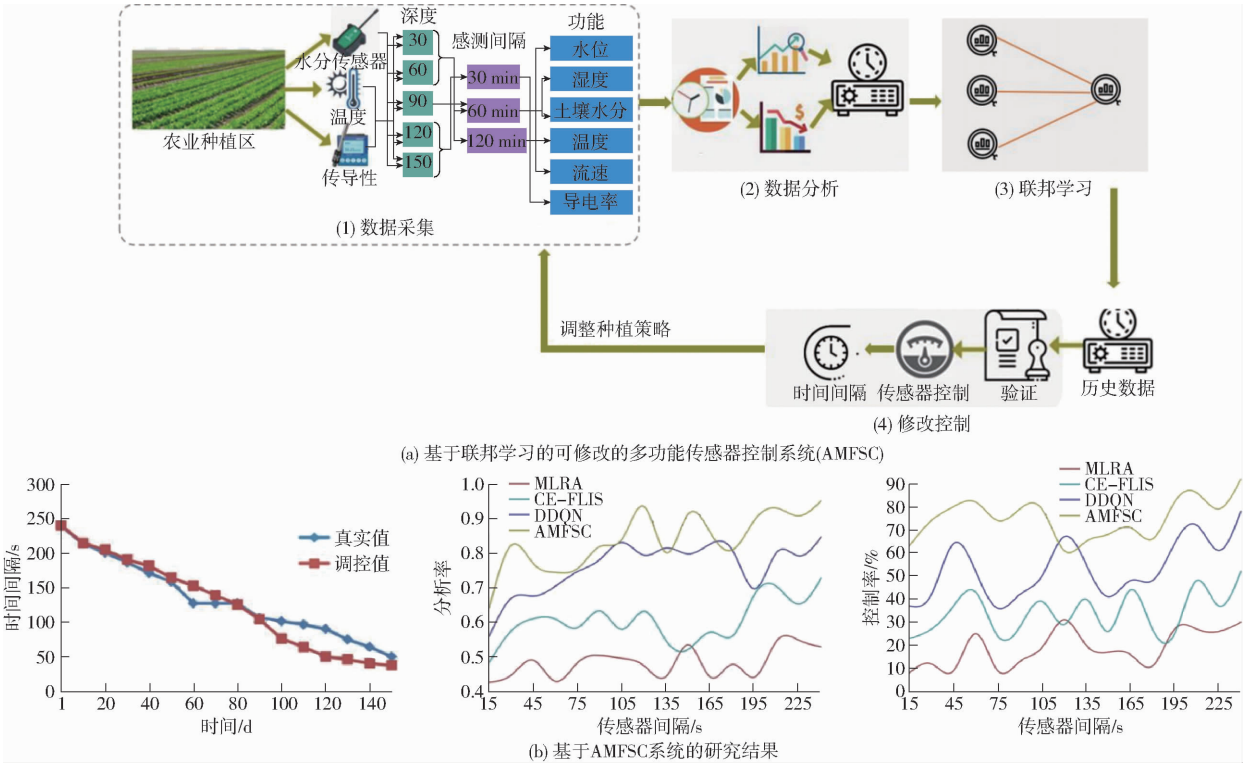


图 8　基于联邦学习的作物监测系统研究[89]

Fig. 8　Research of crop monitoring system based on federated learning

表 6　基于隐私计算的作物监测研究成果

Tab. 6　Research of crop monitor based on privacy computing

发表时间	研究内容	原理	性能	文献序号
2023 年	自动化监测系统	利用联邦学习优化多传感器分析与控制策略，提高农业自动化响应精度	分析率提升 12.52%；控制率提升 7%；延迟下降 8.97%	[89]
2024 年	健康监测	结合联邦学习与博弈论机制设计策略，实现自动化健康监测	能耗下降 10%；MTBF 上升 34%	[90]
2025 年	作物与杂草检测	基于联邦学习框架进行分布式模型训练，实现农场间数据主权保护	在同质数据中，mAP50 为 85.6%；在异质数据中，mAP50 为 64.8%	[91]

系统在不同时间间隔下优化传感与控制动作，可将分析率提高 12.52%、控制率提高 7%、适应性提升 9.65%，同时减少分析时间 7.12%、驱动滞后 8.97%，显著提升农业生产效率与适应性。为了降低能耗，CHEN 等[90]提出一种基于能源感知联邦学习的智能农业系统 SusFL，利用太阳能传感器与博弈论机制设计实现动物健康监测中的客户端选择优化，有效应对能量波动与对抗性攻击。研究表明，SusFL 在能耗降低 10%、社会福利提升 15%、平均故障间隔时间增加 34% 的同时，提升了全局模型预测精度，验证了其在智能农场中的高效性与可持续性。为了实现农场间数据主权保护，HUSSAINI 等[91]提出结合联邦学习与 YOLO v8 目标检测模型，采用 FedAvg 算法在不集中数据的前提下实现模型训练。研究表明，在同质数据场景中，联邦学习模型的 mAP50 约 85.6%；在异质数据条件下，通过优化本地训练轮数可显著提升模型效果，mAP50 约 64.8%。

总体而言，当前研究表明，联邦学习在作物监测领域的应用已初步展现出良好的效果，能够在保障数据隐私的前提下，实现多终端协同建模和高精度感知分析。无论是在作物健康状态评估、动物监测，还是在田间杂草识别等任务中，隐私计算技术均有效提升了系统的智能化水平与资源利用效率。然而，不同数据分布条件下模型性能的波动、设备异构性带来的训练不一致问题仍有待进一步研究。未来可从模型自适应优化、低能耗算法设计以及跨场景部署能力提升等方面持续推进，为构建高效、可信、可持续的智能农业监测体系提供支持。

3.4　产量预测

产量预测是农业生产管理和政策制定中的核心任务，对于粮食安全评估、农产品市场调控、农业保险理赔及供应链优化具有重要意义。通过融合多源异构数据（遥感影像、历史气象记录、土壤信息、农

艺操作记录及作物生长过程监测等)集中式训练机器学习与深度学习模型,能够实现对不同时空尺度下作物产量的高精度估计。然而集中式训练涉及数据传输,面临数据泄露、滥用或用于不当目的的风险,尤其在农户数据权属不清、农业服务平台多方参与的背景下,数据隐私保护问题尤为突出。为了防止数据泄露,研究者将隐私计算引入产量预测的回归任务。图 9 展示了联邦学习与随机森林相结合在产量预测中的应用研究,表 7 展示基于隐私计算的产量预测部分研究成果。

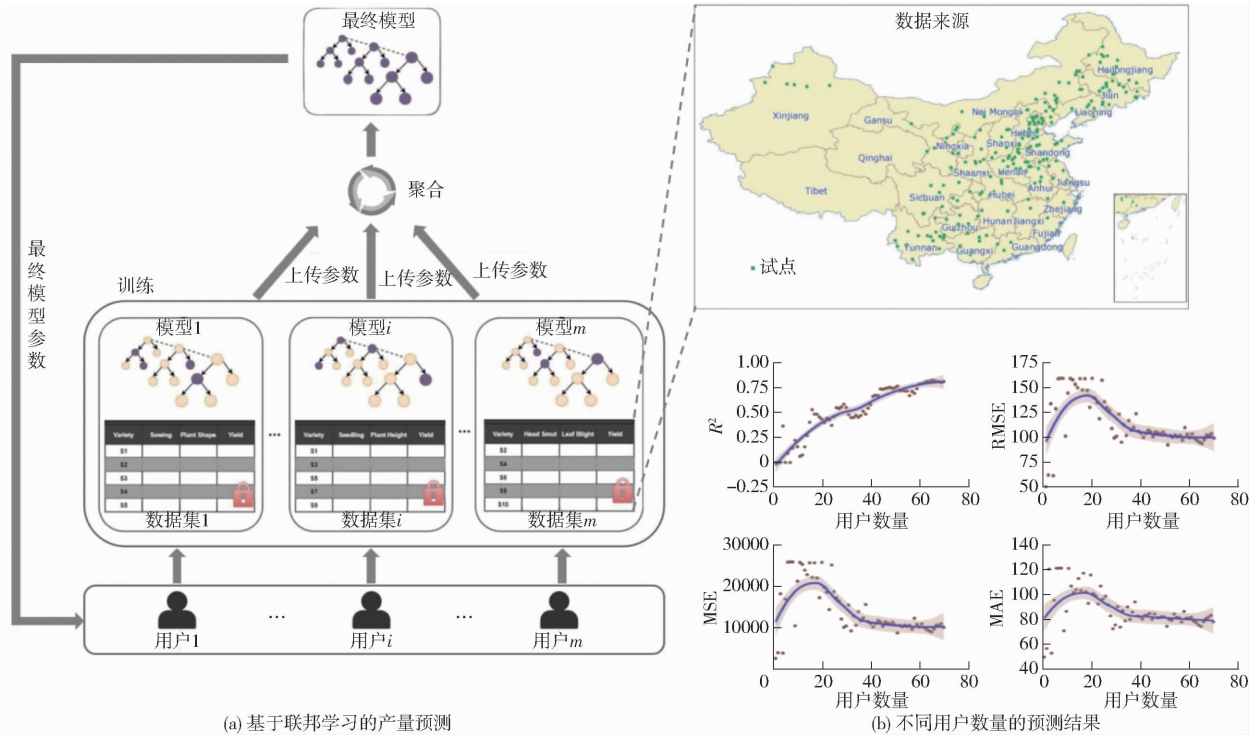


图 9 基于联邦学习和随机森林的产量预测应用研究[92]

Fig. 9 Research of yield prediction based on federated learning and random forest

表 7 基于隐私计算的产量预测应用研究成果

Tab. 7 Research of yield prediction based on privacy computing

发表时间	研究内容	原理	性能参数	文献序号
2022 年	草莓产量预测	结合同态加密与 CNN 框架实现不公开数据的草莓产量预测	MAPE 为 8.0%(7 d)、14.7%(14 d)、22.3%(21 d)	[93]
2022 年	大豆产量预测	结合 ResNet 模型与联邦学习实现分布式模型训练	R^2 为 0.92	[94]
2023 年	玉米产量预测	将随机森林与联邦学习结合,利用编码、DM5 加密与服务端协调保障数据隐私	R^2 为 0.803 5	[92]
2025 年	多作物产量预测	将 FLyer 框架与 LSTM、边缘计算、数据加密相结合实现产量预测	准确率超 99%,平均延迟降低 39%,能耗降低 40%,泄露率小于等于 0.038	[95]

为了保护数据安全传输,ONOUFRIOU 等[93]提出一种结合全同态加密(FHE)与自动参数化神经网络的隐私保护深度学习方法,构建了基于 MS-SEAL CKKS 方案的多向图计算框架,并开发了兼容 FHE 的 CNN 模型,用于草莓产量预测任务。研究结果表明,在预测 7、14、21 d 产量的任务中,该方法的平均绝对百分比误差(MAPE)分别为 8.0%、14.7%、22.3%,在保障数据完全加密的前提下取得了可接受的预测性能。为了适应多主体协作并保护各方数据隐私,MANOJ 等[94]将联邦学习引入产量预测任务,通过在分布式客户端设备上训练深度残差网络模型(如 ResNet-16 和 ResNet-28)并聚合各客户端参数来解决数据孤岛问题并提升大豆产量预测精度。研究结果表明,采用 Adam 优化的 ResNet-16 在联邦学习环境中表现最佳,其预测性能 R^2 为 0.92,显著优于传统集中式模型,展现了在分散数据场景下的部署可行性与实用价值。虽然联邦学习在保护各主体数据安全的同时解决了数据孤岛问题,但聚合模型所需要的分布式模型参数在传输过程中也面临着数据泄露的风险。ZHANG 等[92]结合联邦学习和随机森林,构建了联邦随机森林框架,该框架支持 HFL 和 VFL 混合情境使育种机构在不共享原始数据的前提下协同建模,利用本地数据(包括表型和气象信息)实现联合预测。同时,引入

编码、DM5 加密与服务端协调方式保障数据安全传递。该研究基于 2017—2021 年中国国家玉米品种试验的 248 个试点数据进行试验。研究结果表明，该方法准确率达到 80.35%，几乎不比集中式模型性能差，且显著优于各单独模型。DEY 等[95]提出基于联邦学习与边缘计算的作物产量预测框架 FLyer，利用 LSTM 模型在本地处理土壤与环境数据，并通过 AES－256 进行梯度加密和 RSA/AES 进行数据加密以保护数据隐私。研究结果显示，FLyer 在准确率超 99% 的同时，将延迟降低约 39%、能耗降低约 40%，本地模型准确率也超过 94%，同时其数据泄露率低于 0.038。

总体而言，现有基于隐私计算的产量预测方法在保障数据安全的同时，实现了较高的预测精度和良好的多方协同效果，展现出较强的应用潜力。尤其是联邦学习与加密技术的结合，有效缓解了数据孤岛问题，提升了模型在异构环境下的泛化能力。但与此同时，现有方法仍面临通信开销大、计算复杂度高、模型在非独立同分布数据下鲁棒性不足等问题。此外，缺乏统一的评估体系也限制了不同方法的横向比较和推广。未来研究可以聚焦于轻量化模型设计、通信与计算效率优化、异构数据适应能力提升，并构建隐私与性能兼顾的综合评估框架，以推动隐私计算在产量预测中的高效落地与持续发展。

4　存在问题与展望

4.1　存在问题

为了应对多主体协同工作的需求以及日益严峻的数据隐私安全问题，农业大数据逐渐融合隐私计算技术，旨在改善传统的数据传输与模型训练方式，并在实际应用中取得了显著成效。然而，当前隐私计算在农业领域的研究仍处于起步阶段，相关工作数量有限，且存在一定的局限性，主要体现在以下方面：

（1）通信开销大：隐私计算，尤其是联邦学习、安全多方计算等框架，往往需要在各参与方之间频繁传输模型参数或加密数据，导致通信资源消耗显著，难以适应部分农业场景中带宽受限、网络不稳定的实际条件。

（2）计算复杂度高：为保障数据安全，引入的加密机制（如同态加密、差分隐私等）在计算上相对复杂，对终端设备的计算能力要求较高，制约了其在资源受限的农业设备（如边缘设备或传感器）中的部署与应用。

（3）对异构数据适应性弱：农业数据类型多样，包括图像、文本、时间序列与结构化表格数据等，来源分散且格式不一。现有隐私计算方案多针对特定数据类型优化，尚未形成适应多模态、异构数据处理的统一解决方案。

（4）评估体系不健全：目前缺乏统一的评估指标和测试标准来衡量隐私计算方案在农业场景中的性能、隐私保障强度及部署可行性，影响了其在不同农业子领域之间的横向比较与推广。

（5）隐私保护与模型性能的权衡问题：在保障数据隐私的同时，如何最大程度保持模型的预测准确性，仍是一个关键挑战。部分方法在增强隐私保护的同时，模型性能出现明显下降，限制了其实用价值。

4.2　未来展望

未来研究可进一步聚焦于开发轻量级、适应性强的隐私计算模型，提升算法效率与可扩展性，并加强与农业场景深度融合，以推动隐私计算在农业智能化发展中的广泛落地与应用。未来研究有以下发展方向：

（1）发展通信高效的协同计算框架。未来可重点发展通信压缩与异步更新机制，如梯度量化、稀疏更新、局部更新与模型分层同步等策略，减少模型传输频率和数据量。同时，可探索端边协同计算与层次式联邦学习架构，将部分计算任务下沉至边缘节点，减轻中心节点压力，提升在低带宽、间歇性连接农业环境中的适应性。

（2）推进轻量化与硬件友好的加密机制。为降低对计算资源的依赖，需开发轻量级加密方法，如优化的差分隐私机制、硬件加速的同态加密模块或混合加密策略（如局部敏感加密结合扰动机制）。此外，可研究与农业设备硬件紧密耦合的隐私计算模块设计，实现算法与芯片协同优化，推动隐私计算在低功耗设备上的可部署性。

（3）构建多模态联合学习框架。未来可设计面向多模态数据的隐私保护学习框架，支持图像、文本、传感器时序、结构化数据等多类型输入的协同处理。可借助联邦多模态学习、跨模态表示对齐、隐私增强型自监督学习等技术，打破数据源异构带来的割裂，提升整体建模效果与适应性。

（4）建立标准化评估与测试平台。建议构建面向农业隐私计算的基准测试平台与评估体系，涵盖隐私强度、预测性能、计算效率、通信开销等多维指标。可制定统一的数据集、评估流程与指标体系，推动农业隐私计算研究的标准化、可比性与工程化发展，促进不同方法在实际农业应用中的可复用与落地。

（5）探索动态可调与自适应机制。未来可探索

动态隐私预算分配策略与隐私-性能联合优化框架，根据模型训练阶段、数据敏感性及任务要求灵活调整隐私强度，实现个性化保护与性能最优化的平衡。同时，引入强化学习或贝叶斯优化方法自动寻找最优隐私参数配置，提升方法的实用性与自动化程度。

参 考 文 献

[1] 姜侯，杨雅萍，孙九林. 农业大数据研究与应用[J]. 农业大数据学报，2019，1(1)：5－10.
JANG Hou，YANG Yaping，SUN Jiulin. Research and application of big data in agriculture[J]. Journal of Agricultural Big Data，2019，1(1)：5－10.（in Chinese）

[2] 顾生浩，温维亮，卢宪菊，等. 作物智慧栽培学——信息-农艺-农机深度融合的新农科[J]. 农学学报，2023，13(2)：67－76.
GU Shenghao，WEN Weiliang，LU Xianju，et al. Smart crop cultivation：a new agricultural science toward deep integration of information，agronomy and machinery[J]. Journal of Agriculture，2023，13(2)：67－76.（in Chinese）

[3] KAMILARIS A，KARTAKOULLIS A，PRENAFETA-BOLDÚ F X. A review on the practice of big data analysis in agriculture[J]. Computers and Electronics in Agriculture，2017，143：23－37.

[4] COBLE K H，MISHRA A K，FERRELL S，et al. Big data in agriculture：a challenge for the future[J]. Applied Economic Perspectives and Policy，2018，40(1)：79－96.

[5] OSINGA S A，PAUDEL D，MOUZAKITIS S A，et al. Big data in agriculture：between opportunity and solution[J]. Agricultural Systems，2022，195：103298.

[6] 苑严伟，徐玲，冀福华，等. 农业机械作业大数据清洗方法与试验优化[J]. 农业机械学报，2021，52(6)：35－42.
YUAN Yanwei，XU Ling，JI Fuhua，et al. Experimental optimization of big data cleaning method for agricultural machinery[J]. Transactions of the Chinese Society for Agricultural Machinery，2021，52(6)：35－42.（in Chinese）

[7] 刘政宇. 基于大数据的数据清洗技术及运用[J]. 数字技术与应用，2019，37(4)：92－94.
LIU Zhengyu. Data cleaning technology and application based on big data[J]. Digital Technology and Application，2019，37(4)：92－94.（in Chinese）

[8] 王湛迪. 大数据环境下数据清洗与预处理技术研究[J]. 数码设计，2024(9)：73－75.
WANG Zhandi. Research on data cleaning and preprocessing technology in big data environment[J]. Digital Insige，2024(9)：73－75.（in Chinese）

[9] 凌芝拓. 大数据技术在数据清洗与预处理中的应用研究[J]. 互联网周刊，2024(19)：42－44.

[10] 陈跨越，王保云. 基于改进 Resnet18 网络的火灾图像识别[J]. 河南师范大学学报(自然科学版)，2024，52(4)：101－110.
CHEN Kuayue，WANG Baoyun. Fire image recognition based on improved Resnet18 network[J]. Journal of Henan Normal University(Natural Science Edition)，2024，52(4)：101－110.（in Chinese）

[11] 李广盛，郑建立，车霞静. 降低数据稀疏性的多维时序序列时间戳对齐方法[J]. 智能计算机与应用，2022，12(4)：135－139.
LI Guangsheng，ZHENG Jianli，CHE Xiajing. Timestamp alignment method of multi-dimensional time series sequence to reduce data sparsity[J]. Intelligent Computer and Applications，2022，12(4)：135－139.（in Chinese）

[12] SIDDIQA A，KARIM A，GANI A. Big data storage technologies：a survey[J]. Frontiers of Information Technology & Electronic Engineering，2017，18：1040－1070.

[13] GUAN Y，MA Z，LI L. HDFS optimization strategy based on hierarchical storage of hot and cold data[J]. Procedia CIRP，2019，83：415－418.

[14] 张剑波，夏灯城，赵加奥，等. 分布式计算环境下的栅格数据存储策略[J]. 国防科技大学学报，2017，39(6)：51－58.
ZHANG Jianbo，XIA Dengcheng，ZHAO Jiaao，et al. Storage strategy of raster data under the distributed computing environment[J]. Journal of National University of Defense Technology，2017，39(6)：51－58.（in Chinese）

[15] HANNAN S A. An overview on big data and hadoop[J]. International Journal of Computer Applications，2016，154(10)：29－35.

[16] CHEBOTKO A，KASHLEV A，LU S. A big data modeling methodology for Apache Cassandra[C]//2015 IEEE International Congress on Big Data. IEEE，2015：238－245.

[17] 沈志宏，赵子豪，王华进，等. PandaDB：一种异构数据智能融合管理系统[J]. 软件学报，2021，32(3)：763－780.
SHEN Zhihong，ZHAO Zihao，WANG Huajin，et al. PandaDB：intelligent management system for heterogeneous data[J]. Journal of Software，2021，32(3)：763－780.（in Chinese）

[18] 李跃鹏，温亮明，黎建辉. 基于查询语言转换的多源数据统一访问框架[J]. 计算机系统应用，2021，30(9)：53－61.
LI Yuepeng，WEN Liangming，LI Jianhui. Framework for heterogeneous data unified access based on language translating[J]. Computer Systems & Applications，2021，30(9)：53－61.（in Chinese）

[19] MAKRIS A，TSERPES K，SPILIOPOULOS G，et al. MongoDB Vs PostgreSQL：a comparative study on performance aspects[J]. GeoInformatica，2021，25：243－268.

[20] 马泽. 对象存储服务对空间非结构化数据存储的探讨——以阿里云 OSS 为例[J]. 江西科学，2018，36(2)：347－352.

MA Ze. Discussion on object storage service to spatial unstructured data storage—to Ali Cloud OSS as an example[J]. Jiangxi Science, 2018, 36(2):347 – 352. (in Chinese)

[21] AIT ISSAD H, AOUDJIT R, RODRIGUES J J P C. A comprehensive review of data mining techniques in smart agriculture [J]. Engineering in Agriculture, Environment and Food, 2019, 12(4): 511 – 525.

[22] 徐畅, 丁俊琦, 赵聃桐, 等. 基于 LightGBM 和处方数据的番茄病害诊断方法[J]. 农业机械学报, 2022, 53(9):286 – 294.
XU Chang, DING Junqi, ZHAO Dantong, et al. Tomato disease diagnosis method based on LightGBM and prescription data [J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(9):286 – 294. (in Chinese)

[23] 张亚军. 基于改进支持向量机算法的农业害虫图像识别研究[J]. 中国农机化学报, 2021, 42(2):146 – 152.
ZHANG Yajun. Image recognition of agricultural pest based on improved support vector machine[J]. Journal of Chinese Agricultural Mechanization, 2021, 42(2):146 – 152. (in Chinese)

[24] KAUR A, KUKREJA V, AGGARWAL P, et al. Amplifying apple mosaic illness detection: combining CNN and random forest models[C]//2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI). IEEE, 2024: 1 – 5.

[25] 陈旸. 基于机器学习的农业害虫识别与分类[J]. 农业灾害研究, 2023, 13(10):61 – 63.
CHEN Yang. Identification and classification of agricultural pests based on machine learning[J]. Journal of Agricultural Catastrophology, 2023, 13(10):61 – 63. (in Chinese)

[26] KUNDURACIOGLU I. CNN models approaches for robust classification of apple diseases[J]. Computer and Decision Making: An International Journal, 2024, 1: 235 – 251.

[27] KHAKI S, WANG L, ARCHONTOULIS S V. A CNN – RNN framework for crop yield prediction[J]. Frontiers in Plant Science, 2020, 10: 1750.

[28] LIU Y, WANG S, CHEN J, et al. Rice yield prediction and model interpretation based on satellite and climatic indicators using a transformer method[J]. Remote Sensing, 2022,14(19):5045.

[29] 苏秀永, 杨杰, 李星华, 等. 基于 UAV 遥感技术的高标准农田耕种状况监测与时空分析[J]. 江西农业学报, 2025, 37(6):68 – 72.
SU Xiuyong, YANG Jie, LI Xinghua, et al. Monitoring and spatiotemporal analysis of high-standard farmland cultivation status based on UAV remote sensing technology[J]. Acta Agriculturae Jiangxi, 2025, 37(6):68 – 72. (in Chinese)

[30] 王长委, 胡月明, 谢健文, 等. 基于 GIS 稻飞虱种群变化时空分析[J]. 农业工程学报, 2009, 25(10):171 – 175.
WANG Changwei, HU Yueming, XIE Jianwen, et al. Spatio-temporal analysis of planthoppers population based on GIS[J]. Transactions of the CSAE, 2009, 25(10):171 – 175. (in Chinese)

[31] LU Y, LIU M, LI C, et al. Precision fertilization and irrigation: progress and applications[J]. AgriEngineering, 2022, 4(3): 626 – 655.

[32] ABIOYE E A, ABIDIN M S Z, MAHMUD M S A, et al. A review on monitoring and advanced control strategies for precision irrigation[J]. Computers and Electronics in Agriculture, 2020, 173: 105441.

[33] 朱惠斌, 王明鹏, 白丽珍, 等. 基于视觉识别的玉米病虫害检测与精准变量喷药系统研究[J]. 农业机械学报, 2024, 55(增刊 2):210 – 221.
ZHU Huibin, WANG Mingpeng, BAI Lizhen, et al. Maize pest and disease detection and precise variable spraying system based on visual recognition[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(Supp. 2):210 – 221. (in Chinese)

[34] 腰彩红, 李扬, 王建春, 等. 温室草莓精准灌溉系统的设计与试验[J]. 河北农业大学学报, 2024, 47(6):17 – 23, 39.
YAO Caihong, LI Yang, WANG Jianchun, et al. Design and experiment of precision irrigation system of greenhouse strawberry [J]. Journal of Agricultural University of Hebei, 2024, 47(6):17 – 23, 39. (in Chinese)

[35] 陈柏青, 张悦, 王科, 等. 基于 APSIM 的新疆棉花生长与产量动态预测方法[J]. 农业机械学报, 2025, 56(5):82 – 90.
CHEN Baiqing, ZHANG Yue, WANG Ke, et al. Dynamic predictions of cotton growth and yield in Xinjiang based on APSIM model[J]. Transactions of the Chinese Society for Agricultural Machinery, 2025, 56(5):82 – 90. (in Chinese)

[36] 祁卓平. 农业气象灾害远程智能预警系统设计[J]. 农业工程, 2022, 12(4):54 – 57.
QI Zhuoping. Design of remote intelligent early warning system for agrometeorological disasters[J]. Agricultural Engineering, 2022, 12(4):54 – 57. (in Chinese)

[37] 李梦琪, 杨信廷, 徐大明, 等. 基于主从多链的水产品区块链溯源信息管理系统设计与实现[J]. 渔业现代化, 2021, 48(3):80 – 89.
LI Mengqi, YANG Xinting, XU Daming, et al. Design and implementation of aquatic product blockchain traceability information management system based on master-slave multi-chain[J]. Fishery Modernization, 2021, 48(3):80 – 89. (in Chinese)

[38] 李兵, 罗涛, 施佳子, 等. 卫星遥感大数据赋能农业金融[J]. 地理空间信息, 2023, 21(10):28 – 31.
LI Bing, LUO Tao, SHI Jiazi, et al. Satellite remote sensing big data empowers agricultural finance[J]. Geospatial Information, 2023, 21(10):28 – 31. (in Chinese)

[39] DEMBANI R, KARVELAS I, AKBAR N A, et al. Agricultural data privacy and federated learning: a review of challenges and

opportunities[J]. Computers and Electronics in Agriculture, 2025, 232: 110048.
[40] GAVAI A K, BOUZEMBRAK Y, XHANI D, et al. Agricultural data privacy: emerging platforms & strategies[J]. Food and Humanity, 2025, 4: 100542.
[41] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169 - 180.
[42] FAWAZ S M, BELAL N, ELREFAEY A, el al. A comparative study of homomorphic encryption schemes using Microsoft SEAL[J]. Journal of Physics: Conference Series, 2021, 2128(1): 012021.
[43] HALEVI S, SHOUP V. Bootstrapping for helib[J]. Journal of Cryptology, 2021, 34(1): 7 - 45.
[44] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1999: 223 - 238.
[45] YAO A C. Protocols for secure computations[C]// 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). IEEE, 1982: 160 - 164.
[46] DAMGÅRD I, PASTRO V, SMART N, et al. Multiparty computation from somewhat homomorphic encryption[C]// Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology. Springer Berlin Heidelberg, 2012: 643 - 662.
[47] DEMMLER D, SCHNEIDER T, ZOHNER M. ABY—a framework for efficient mixed-protocol secure two-party computation[C]// Network and Distributed System Security Symposium (NDSS15), 2015.
[48] WANG X, MALOZEMOFF A J, KATZ J. EMP-toolkit: efficient multi-party computation toolkit[EB/OL]. https://github.com/emp-toolkit.
[49] BOGDANOV D, LAUR S, WILLEMSON J. Sharemind: a framework for fast privacy-preserving computations[C]// Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 2008: 192 - 206.
[50] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]// Theory of Cryptography: Third Theory of Cryptography Conference. Springer Berlin Heidelberg, 2006: 265 - 284.
[51] ERLINGSSON Ú, PIHUR V, KOROLOVA A. Rappor: randomized aggregatable privacy-preserving ordinal response[C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.
[52] HAY M, GABOARDI M, VADHAN S. A programming framework for OpenDP[C]// 6th Workshop on the Theory and Practice of Differential Privacy (TPDP 2020), 2020.
[53] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]// Artificial Intelligence and Statistics. PMLR, 2017: 1273 - 1282.
[54] CASELLA B, ESPOSITO R, CAVAZZONI C, et al. Benchmarking fedavg and fedcurv for image classification tasks[J]. arXiv Preprint, arXiv:2303.17942, 2023.
[55] ZILLER A, TRASK A, LOPARDO A, et al. Pysyft: a library for easy federated learning[J]. Federated Learning Systems, 2021, 965: 111 - 139.
[56] YANG L, TAO F, TIANJIAN C, et al. An industrial grade federated learning framework[J]. The Journal of Machine Learning Research, 2021, 22(1): 10320 - 10325.
[57] BEUTEL D J, TOPAL T, MATHUR A, et al. Flower: a friendly federated learning research framework[J]. arXiv Preprint, arXiv:2007.14390, 2020.
[58] ALAYA B, LAOUAMER L, MSILINI N. Homomorphic encryption systems statement: trends and challenges[J]. Computer Science Review, 2020, 36: 100235.
[59] RYU J, KIM K, WON D. A study on partially homomorphic encryption[C]// 2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM). IEEE, 2023: 1 - 4.
[60] MARCOLLA C, SUCASAS V, MANZANO M, et al. Survey on fully homomorphic encryption, theory, and applications[J]. Proceedings of the IEEE, 2022, 110(10): 1572 - 1609.
[61] BONEH D. Twenty years of attacks on the RSA cryptosystem[J]. Notices of the AMS, 1999, 46(2): 203 - 213.
[62] GENTRY C. A fully homomorphic encryption scheme[M]. Stanford University, 2009.
[63] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. Leveled fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory (TOCT), 2014, 6(3): 1 - 36.
[64] CHEON J H, KIM A, KIM M, et al. Homomorphic encryption for arithmetic of approximate numbers[M]// TAKAGI T, PEYRIN T. Advances in cryptology—ASIACRYPT 2017. Lecture notes in computer science. Springer, Cham, 2017.
[65] KULALVAIMOZHI V P, ALEX M G, PETER S J. A novel homomorphic encryption and an enhanced DWT (NHE - EDWT) compression of crop images in agriculture field[J]. Multidimensional Systems and Signal Processing, 2020, 31(2): 367 - 383.
[66] MAHATO G K, BANERJEE A, CHAKRABORTY S K, et al. Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption[J]. Applied Soft Computing, 2024, 167: 112405.
[67] SHEN R, ZHANG H, CHAI B, et al. BAFL - SVM: a blockchain-assisted federated learning-driven SVM framework for smart agriculture[J]. High-Confidence Computing, 2025, 5(1): 100243.
[68] AKBAR N A, LENZITTI B, TEGOLO D. Proof of federated learning contribution (PoFLC) for secure agri-data sharing and

collaborative model training[C]// 2024 7th International Conference on Information and Communications Technology (ICOIACT). IEEE, 2024: 258 - 263.

[69] ZHU J, SHANG Y, ZHANG X. Decentralized information resource management: leveraging blockchain for sustainable development and security[C]//2024 International Conference on Computers, Information Processing and Advanced Education (CIPAE). IEEE, 2024: 638 - 644.

[70] SINGH A K, KHARBAS V K, KUMAR S B V. Enhancing security and privacy of machine learning algorithms in agricultural automation[C]//2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2024: 1 - 6.

[71] ZILLER A, USYNIN D, BRAREN R, et al. Medical imaging deep learning with differential privacy[J]. Scientific Reports, 2021, 11(1): 13524.

[72] ZHANG S, LI X. Differential privacy medical data publishing method based on attribute correlation[J]. Scientific Reports, 2022, 12(1): 15725.

[73] LIU D, BAI L, YU T, et al. Towards method of horizontal federated learning: a survey[C]// 2022 8th International Conference on Big Data and Information Analytics (BigDIA). IEEE, 2022: 259 - 266.

[74] LIU Y, KANG Y, ZOU T, et al. Vertical federated learning: concepts, advances, and challenges[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(7): 3615 - 3634.

[75] LIU Y, KANG Y, XING C, et al. A secure federated transfer learning framework[J]. IEEE Intelligent Systems, 2020, 35(4): 70 - 82.

[76] 康孟珍, 王秀娟, 李冬, 等. 基于联邦学习的分布式农业组织[J]. 智能科学与技术学报, 2022, 4(2):288 - 297.
KANG Mengzhen, WANG Xiujuan, LI Dong, et al. Distributed agricultural organization based on federated learning[J]. Chinese Journal of Intelligent Science and Technology, 2022, 4(2):288 - 297. (in Chinese)

[77] 许继平, 李卉, 王浩宇, 等. 基于联邦学习的粮食供应链隐私数据要素协同计算研究[J]. 智慧农业, 2023, 5(4): 79 - 91.
XU Jiping, LI Hui, WANG Haoyu, et al. Collaborative computing of food supply chain privacy data elements based on federated learning[J]. Smart Agriculture, 2023, 5(4): 79 - 91. (in Chinese)

[78] 吴国栋, 胡全兴, 刘旭, 等. 差分隐私增强的大米区块链品控模型[J]. 智慧农业, 2024, 6(4):149 - 159.
WU Guodong, HU Quanxing, LIU Xu, et al. Differential privacy-enhanced blockchain-based quality control model for rice[J]. Smart Agriculture, 2024, 6(4):149 - 159. (in Chinese)

[79] TAJI K, GHANIMI F. Enhancing security and privacy in smart agriculture: a novel homomorphic signcryption system[J]. Results in Engineering, 2024, 22: 102310.

[80] 苗玉霞. 农产品供应链的物联网安全[J]. 江苏农业科学, 2017, 45(10):188 - 193.

[81] 王炎. 无线传感器网络中面向多数据查询的安全数据融合算法[J]. 电子设计工程, 2019, 27(7):138 - 143.
WANG Yan. Secure data aggregation algorithm for multi-data query in wireless sensor networks[J]. Electronic Design Engineering, 2019, 27(7):138 - 143. (in Chinese)

[82] PENG X, ZHANG X, WANG X, et al. A refined supervision model of rice supply chain based on multi-blockchain[J]. Foods, 2022, 11(18): 2785.

[83] DENG F, MAO W, ZENG Z, et al. Multiple diseases and pests detection based on federated learning and improved Faster R-CNN[J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 1 - 11.

[84] MEHTA S, KUKREJA V, VATS S. Empowering farmers with AI: federated learning of CNNs for wheat diseases multi-classification[C]//2023 4th International Conference for Emerging Technology (INCET). IEEE, 2023: 1 - 6.

[85] THAPLIYAL N, KUKREJA V, GARG N, et al. Empowering farmers: federated learning CNN for accurate strawberry leaf disease[C]//2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, 2024: 1 - 6.

[86] SURYAVANSHI A, KUKREJA V, MEHTA S, et al. Agriculture advances: federated learning CNN's for combatting banana leaf diseases[C]//2024 5th International Conference for Emerging Technology (INCET). Belgaum, 2024: 1 - 6.

[87] 黄炯炯. 智慧农业下基于联邦学习的水稻病虫害分类研究[J]. 电子技术应用, 2024, 50(11):89 - 98.
HUANG Jiongjiong. Research on rice pest and disease classification based on federated learning under smart agriculture[J]. Application of Electronic Technique, 2024, 50(11):89 - 98. (in Chinese)

[88] 赵盎然, 兰鹏, 任洪泽, 等. 基于联邦学习的玉米叶片病害识别方法[J]. 山东农业大学学报(自然科学版), 2024, 55(5):740 - 749.
ZHAO Angran, LAN Peng, REN Hongze, et al. Identification of maize leaf diseases based on federated learning[J]. Journal of Shandong Agricultural University(Natural Science Edition), 2024, 55(5):740 - 749. (in Chinese)

[89] ABU-KHADRAH A, ALI A M, JARRAH M. An amendable multi-function control method using federated learning for smart sensors in agricultural production improvements[J/OL]. ACM Transactions on Sensor Networks, 2023. https://doi.org/10.1145/358201.

(下转第 276 页)

the future agriculture[J]. Computers in Industry, 2020, 117: 103187.
[159] BHAT S A, HUANG N F. Big data and AI revolution in precision agriculture: survey and challenges[J]. IEEE Access, 2021, 9: 110209 - 110222.
[160] OSINGA S A, PAUDEL D, MOUZAKITIS S A, et al. Big data in agriculture: between opportunity and solution[J]. Agricultural Systems, 2022, 195: 103298.
[161] KHATOON P S, AHMED M. Semantic interoperability for IoT agriculture framework with heterogeneous devices[C]// Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Springer Singapore, 2021: 385 - 395.
[162] STERGIOU C, PSANNIS K E, KIM B G, et al. Secure integration of IoT and cloud computing[J]. Future Generation Computer Systems, 2018, 78: 964 - 975.
[163] SAGAR S, N BIRJE M. Precision agriculture using Internet of Things and cloud computing: a review[J]. SN Computer Science, 2025, 6(4): 1 - 18.
[164] VANI P D, RAO K R. Measurement and monitoring of soil moisture using cloud IoT and android system[J]. Indian Journal of Science and Technology, 2016, 9(31): 1 - 8.
[165] NAMASUDRA S, ROY P, BALUSAMY B. Cloud computing: fundamentals and research issues[C]// 2017 Second International Conference on Recent Trends and Challenges in Computational Models. IEEE, 2017: 7 - 12.
[166] TABRIZCHI H, KUCHAKI RAFSANJANI M. A survey on security challenges in cloud computing: issues, threats, and solutions[J]. The Journal of Supercomputing, 2020, 76(12): 9493 - 9532.
[167] BOTTA A, DE DONATO W, PERSICO V, et al. Integration of cloud computing and Internet of Things: a survey[J]. Future Generation Computer systems, 2016, 56: 684 - 700.
[168] HOLZ R, AMANN J, MEHANI O, et al. TLS in the wild: an internet-wide analysis of TLS-based protocols for electronic communication[J]. arXiv Preprint, arXiv:1511.00341, 2015.
[169] DENG R, LU R, LAI C, et al. Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption[J]. IEEE Internet of Things Journal, 2016, 3(6): 1171 - 1181.

(上接第 199 页)

[90] CHEN D, YANG P, CHEN I R, et al. SusFL: energy-aware federated learning-based monitoring for sustainable smart farms[J]. arXiv Preprint, arXiv:2402.10280, 2024.
[91] HUSSAINI M, VOIGT M, THEISS J, et al. Federated learning for data-sovereign training of weed and crop detection machine learning models[C]// 45. GIL-Jahrestagung, Digitale Infrastrukturen für eine nachhaltige Land-, Forst-und Ernährungswirtschaft. Gesellschaft für Informatik eV, 2025: 59 - 70.
[92] ZHANG Q, ZHAO X, HAN Y, et al. Maize yield prediction using federated random forest[J]. Computers and Electronics in Agriculture, 2023, 210: 107930.
[93] ONOUFRIOU G, HANHEIDE M, LEONTIDIS G. EDLaaS: fully homomorphic encryption over neural network graphs for vision and private strawberry yield forecasting[J]. Sensors, 2022, 22(21): 8124.
[94] MANOJ T, MAKKITHAYA K, NARENDRA V G. A federated learning-based crop yield prediction for agricultural production risk management[C]//2022 IEEE Delhi Section Conference (DELCON). IEEE, 2022: 1 - 7.
[95] DEY T, BERA S, MUKHERJEE A, et al. FLyer: federated learning-based crop yield prediction for agriculture 5.0[J]. IEEE Transactions on Artificial Intelligence, 2025, 6(7):1943 - 1952.