Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 09 May 2026
Revised 20 June 2026
Accepted 01 July 2026

Natural Resources for Human Health 2026, Vol. 6 (11s): 1330–1348

KEYWORDS:
Federated Learning, Smart Agriculture, Data Poisoning Attacks, Byzantine Robust Aggregation, Privacy Preserving Machine Learning, IoT Sensor Security, Blockchain Audit, Precision Agriculture Security

Secure Federated Learning in Smart Agriculture: A Survey of Poisoning Attacks, Defences and Challenges

Kalyani Konjeti[1], M. Prithi[2], K. Mariyappan[3], Renukadevi S[4], Manujakshi B C[5], Shashidhar T M[6], Komala G[7], Poorna Chandra Reddy Alla[8], Pavithra K[9], N. Sivakumar[10], R. Prabakaran[11]

[1]M.Tech Computer Engineering Student, Marwadi University, Rajkot, Gujarat, India
[2,4]School of CS & IT, JAIN(Deemed- to -be University), Benguluru, Karnataka,India
[3]Computer Science and Engineering, Chennai Institute of Technology, Chennai.
[5]Department of Computer Engineering, Faculty of Engineering and Technology, JAIN(Deemed- to – be University), Benguluru, Karnataka,India.
[6]Professor, Department of Computer Science and Engineering (AI&ML), Harsha Institute of Technology, Bengaluru.
[7]CSE -AI & ML, Marwadi University, Rajkot, Gujarat, India
[8,10]Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India
[9]Department of Computer Science, Christ University, Bengaluru
[11]Department of Computer science and Engineering, Kingston Engineering college IN
Email ID: kalyani.konjeti@marwadieducation.edu.in,
prithi.m@jainuniversity.ac.in
mariwithgold@gmail.com,
selvamrenukadevi@gmail.com,
manujakshibc@gmail.com,
shashilara@gmail.com,
komala.gondi@marwadieducation.edu.in
allapoorna.reddy@marwadieducation.edu.in
kpavithramsc@gmail.com
drsivakumar.nadarajan@gmail.com
rpkaran04@gmail.com

ABSTRACT: Smart agriculture increasingly relies on Federated Learning (FL) to train shared models for crop classification, irrigation scheduling, disease detection, and rainfall prediction across many farms without centralizing sensitive operational data. This decentralization mitigates the privacy and bandwidth costs of traditional cloud-centric machine learning, but FL is well documented to remain vulnerable to poisoning, backdoor, and inference attacks, and agriculture adds threats that are distinctive to the domain, since physical sensors and weather stations are often unattended, easily accessed, and cheaper to tamper with than a data center. This survey organizes the growing but still fragmented literature at the intersection of FL security and precision agriculture, restricting itself throughout to sources published in 2021 or later and independently verified against a real, DOI-registered publication. We review FL fundamentals, catalogue the datasets and applications used in agricultural FL research, present a taxonomy of sensor-level, client-side, communication-side, and server-side attacks, and map robust-aggregation, anomaly-detection, privacy-preserving, and blockchain-audit defences to the attacks they counter. We compare unsecured and secured FL methods on agricultural

Natural Resources for Human Health
eISSN: 2583-1194

tasks and identify concrete research gaps: the absence of standardized security benchmarks, limited multi-modal robustness studies, reproducibility limitations, and an under-studied physical-sensor threat model. We close with a research agenda spanning benchmark design, layered defence architectures, multi-modal defences, regulatory-grade audit infrastructure, and edge deployment.

1. INTRODUCTION

1.1 Motivation and Importance of Smart Agriculture

Global food production faces mounting pressure from population growth, water scarcity, and increasingly erratic weather driven by climate change. Meeting this demand without expanding cultivated land depends on producing more from the same footprint of soil and water, which is the core promise of precision agriculture: using IoT sensors, drones, and satellite imagery to measure soil moisture, canopy health, and microclimate at a resolution no human inspector can match, then acting on that data with artificial intelligence [1 – 3]. As farms adopt networked soil probes, weather stations, and camera-equipped irrigation controllers, the volume of agronomic data available for machine learning has grown accordingly. Because no single farm, cooperative, or regional authority holds enough labeled data to train a robust model alone, and because neighboring farms often face correlated pests, soil conditions, and weather, there is a natural incentive for multi-farm collaboration in model training [4].

1.2 Need for Federated Learning in Agriculture

Creating a central repository of raw agricultural information to facilitate this is undesirable for a number of reasons. Data is commercially sensitive at the farm level, as yield estimates, chemical input schedules, and irrigation timing can show a grower's operating margin, and regulatory frameworks restricting data ownership are becoming more stringent in several jurisdictions [5]. Rural connectivity also tends to be low bandwidth: cellular and LoRaWAN. Uploading raw sensor streams or high resolution imagery to a central server is not viable with the low bandwidth of these networks. Federated learning (FL) directly tackles this combination of constraints: Participating farms train a shared model locally and update the model with the orchestrating server only with model updates, and never with the underlying records themselves [4]. This meets the data-sovereignty requirements and still allows each party to reap the benefits resulting from the joint experience of the consortium, which is why FL has been tried in almost all of the major agricultural sensing tasks, ranging from crop classification [6] to rainfall and yield prediction [7, 8] to plant disease diagnosis [9 - 12].

1.3 Security Challenges Specific to Agricultural FL

So far, the most typical application contexts for FL security research are mobile keyboards, hospital consortia and vehicular or transportation networks [13], [14] where the main threat is considered a compromised software client. Agricultural FL is to inherit all of those threats and a unique attack surface that's based on physical exposure. Probes to measure soil-moisture, weather stations, and irrigation valves are often deployed in unattended fields without any physical security, using unauthenticated radio links, and rarely patched after deployment [15], [1]. It is not necessary for an attacker to break an entire software stack to corrupt the training round; it would suffice to simply move a moisture sensor, bias the temperature of a weather station's thermistor, or change the operating conditions of the solar-powered field sensor [16] discussed explicitly in recent attack resistant smart-farm monitoring research. The impact of a successful attack is also tangible and economic and not as abstract as in most FL deployments, so that there is a strong incentive for specific cybersecurity incident analysis studies in the food and agriculture industry [17].

1.4 Survey Objective

The purpose of this survey is to provide researchers and practitioners developing secure federated learning systems for smart agriculture with a unified, structured reference that bridges the gap between FL security research in general and the specific datasets, threat models, and deployment constraints of the agricultural domain, using only sources published since 2021 and having an independently verified DOI.

1.5 Technology Scope

The technologies surveyed range from the FL substrate and communication protocols [4] through the machine learning models trained over agricultural data, spanning shallow classifiers, convolutional and transformer types [18] [11] to the attack methods that target any part of the FL pipeline from the sensors to the server [19], [20] and the defence mechanisms that counteract these attacks [21], [22] and finally to the IoT and edge hardware on which agricultural FL clients are typically run [1] [23].

1.6 Application Environment

The surveyed work falls into three broad categories of deployment context, where one or more of the models are shared across multiple farms: multi-farm consortia where the shared model is fed one of two types: a shared crop model (without pooling raw data) [6] [9] or an irrigation board or water authority where the models are fed a shared model across many independently operated farms [24 - 26]; regulatory or governance contexts that increasingly mandate verifiable and tamper-evident records of the training of the shared model [13], [23].

1.7 Contributions of This Survey

The security survey will be focused on agricultural federated learning, connecting the general FL-security literature to the agricultural domain, with only publications from the year 2021 or later, and verified by a DOI.

A taxonomy of attacks at the sensor level, client side, communication side and server side (Section 5, Fig. 2).

An explicit representation of a mapping of defence families to the attacks they have to defend, and the cost that each defence incurs (Section 6).

A literature-review table and comparative feature matrix of the 40 verified sources that underlie this survey (Sections 3.5-3.6).

A research program for benchmarking, multi-modal robustness, reproducibility and the physical-sensor threat model (Sections 8-9).

1.8 Organization of the Paper

In Section 2, we present the basics of FL, modalities of agricultural data, and the general adversarial-robustness literature, and set up the threat model throughout. In Section 3, prior work is categorised and the literature-review table and comparative feature matrix for all 40 references is presented. Section 4 reviews public datasets. The attack taxonomy, defence taxonomy and a comparison between unsecured and secured FL methods are given in Section 5, 6 and 7, respectively. Section 8 outlines research gaps, Section 9 presents research agenda and Section 10 wraps up.

2. BACKGROUND

2.1 Federated Learning Fundamentals

The federated learning training model is a distributed training model where the raw data of a series of clients (such as farms, irrigation districts, or individual sensor gateways) are not sent to a central server, but each client participates in training under the coordination of the central server to fit a shared model [4]. The standard approach is to have the server broadcasting the current global model to a subset of clients, and then clients proceed to do some local training on their data, return their modified model parameters, and the server combines the modified parameters into a new global model, usually by weighted averaging. Both Zhang et al. [4] and Mothukuri et al. [31] give detailed discussions of this workflow and the aggregation algorithms that are developed on top of it, pointing out that while this is a common workflow developed in independently run farms, where datasets from clients might be very heterogeneous in size and distribution, the former [5] and the latter [8] are exceptions rather than the rule.

2.2 Federated Aggregation and Optimization in Agricultural FL

In recent years, some agricultural FL work has started to take steps to accommodate the heterogeneity of the farm. For smart-agriculture deployments, Zhang et al. [8] propose dual dynamic quantization to cut down the communication cost of aggregation rounds, whereas Praharaj et al. [30] introduce a hierarchical federated transfer-learning architecture which reflects cooperative smart farming with multiple parties by aggregating at multiple layers. In a real agricultural sensing task, Killeen et al. [7] demonstrate that federated aggregation can achieve comparable accuracy with centralized sensing, but do not have to send any

raw sensor readings out of the local farm. FLTrust [22] adopts a different model of aggregation, with the server keeping its own small clean base dataset, and recalculating each client update to be similar to some reference update computed by the server; This design does have the benefit of Byzantine robustness as a by-product of the aggregation rule, and it is further discussed as a defence mechanism in Section 6.1.

2.3 Smart Agriculture Data Modalities

The four general types of data modalities used in Agricultural FL research are described. The data from soil sensors (moisture, temperature and electrical conductivity) is usually tabular and low dimensional, and forms the basis of federated smart-irrigation efforts [26 - 28]. Rainfall-prediction and crop-monitoring pipelines rely on weather station data for their federated pipelines [29] and [3]. Crop-management records are semi-structured and the modality most prone to falsification as the records are often manually entered. The most complex and most widely explored modality is image-based modalities, e.g., RGB leaf photos and multispectral canopy scans, which forms the basis for the voluminous federated crop-disease-detection research [9 - 12].

2.4 Adversarial Robustness in General FL Literature

In the non-agricultural sector, the FL literature can be classified into a number of families of attacks and is well summarized by Mothukuri et al. [31], Blanco-Justicia et al. [21] and Xia et al. [20]. In both, the data poisoning corrupts the local training set, whereas in model poisoning, the gradient or weight update is directly manipulated, and both are explored in detail in Xia et al.'s survey on poisoning attacks [20]. They are classified as a targeted type of poisoning that only affects the accuracy of the target task without any impact on the accuracy of other tasks, and they are listed with their proposed countermeasures in Mothukuri et al. [31] and Nair et al.'s empirical study of adversarial attacks on FL environments [19]. Byzantine attacks are more general attacks that include any behaviour by the clients, malicious or otherwise, that is an arbitrary deviation from the honest protocol; Blanco-Justicia et al. [21] provide a detailed survey of the various robust-aggregation rules and cryptographic countermeasures for Byzantine attacks, and the FL aggregation rule FLTrust [22] is a commonly used Byzantine-robust aggregation rule that is frequently mentioned in the agricultural FL literature covered in Section 3. These are survey-level treatments and, accordingly, they have been compared with general-purpose benchmarks instead of sensor data from agriculture, as Section 8 points out, an area that agricultural FL security research is now starting to fill.

2.5 Threat Model for Federated Agricultural Systems

We assume an honest-but-curious server, i.e. the aggregation server runs the FL protocol correctly; however it may try to deduce some information from the updates that it receives, and its audit logs should thus be independently verifiable rather than self-reported [13, 23]. As per the Byzantine-robustness framing described by FLTrust [22] and covered in a broad survey by Blanco-Justicia et al. [21] we assume that there exists some portion of the client population that may be malicious, corrupted, or flawed. There are three types of attackers that are modelled: sensor-level attackers who can manipulate a device that has been deployed in the field without touching its software [16] and [15]; client-level attackers who control the training pipeline on a compromised device, and who can push arbitrary model updates [19] and [20] into it; and communication-level attackers who can observe or tamper with messages between client and server [32] and [14]. We also consider a breach of the audit log as a separate threat surface, which is an incentive for the blockchain-audit defences reviewed in Section 6.5 [13, 26].

3. LITERATURE CATEGORIZATION

3.1 Federated Learning for Agricultural Applications

Major research focus in agricultural FL in recent years is crop disease detection, irrigation, and crop yield/rainfall prediction. The image-based FL pipelines are mostly anchored by crop-disease detection: Mamba Kabala et al. [9] compare the performance of the CNN and Vision Transformer architectures in federated disease detection for wheat crops, where the number of participating learners, communication rounds, and data quality is the factors; Hari and Singh [12] propose an adaptive knowledge-transfer approach to handle the statistical heterogeneity across the various farms; Fahim-Ul-Islam et al. [18] apply transformer models for federated wheat-disease identification; Tripathy et al. [10] optimize the federated rice-leaf disease classification; Chorney et al. [11] directly address the heterogeneous multi-site crop-disease diagnosis. Idoje et al. [6] use federated averaging with Adam and SGD optimizers for the classification of crops using climate data and find that their federated approach is able to converge faster and more accurately than a centralized approach.

3.2 Federated Learning for Smart Irrigation

The irrigation specific FL work has been rapidly expanding in the past two years. Bera et al. introduce FLAG [24] and its improved version Fedchain [25] which integrates federated learning with blockchain-based coordination for sustainable irrigation in the context of Agriculture 5.0. Amraouy et al. [26] on the other hand focus on the data-sharing layer surrounding the FL training process and propose blockchain-based smart contracts and self-sovereign identity for enabling verifiable cross-organizational data sharing in the field of irrigation. The federated architectures for IoT farm sensing in general is illustrated by Killeen et al. [7] and Zhang et al. [8] which optimizes communication cost with dual dynamic quantization. Morchid et al. [35] examine IoT- and cloud-computing-based smart irrigation technologies for sustainable farming, Debauche et al. [39] review cloud and distributed architectures for agricultural data management under the Agriculture 4.0 paradigm, and Singh et al. [40] present a soil-moisture-sensor-based smart controller for autonomous irrigation, illustrating the sensor-level building blocks that federated irrigation systems must eventually secure.

3.3 Federated Agricultural Security (Core Focus)

The applications literature above is smaller than the dedicated security research at the intersection of FL and agriculture, but is nonetheless significant and much larger since 2023. It is an explicitly conceptual position paper that classifies adversarial example, poisoning, and backdoor attacks against agricultural AI systems and concludes that farmers and technology vendors are not very aware of the risks [15]. SusFL [16] is an entirely experimental system, namely a sustainable, energy-aware FL-based monitoring system for smart animal farming systems, specifically engineered to protect against data-poisoning and privacy attacks to the sensors operating in the fields equipped with solar power. Praharaj et al. [30] also develop a hierarchical federated transfer-learning and digital-twin system to ensure the secure operation of cooperative smart farming in the face of cyber threats. The closest work to the surrounding threat landscape is offered by Kulkarni et al. [17] who discusses the documented cybersecurity incidents in the food and agriculture industry. Adjacent but not agriculture specific, Abdel-Basset et al. [13] analyzed federated learning-based intrusion detection systems for IoT, transportation, or 5G networks, and the lightweight, resource-constrained federated learning intrusion detection system design insights apply to agricultural IoT deployments.

3.4 General FL Security Foundations Underpinning This Survey

The taxonomies in sections 5 and 6 are tied to three general purpose FL security surveys: Mothukuri et al. [31] provide a broad characterization of FL vulnerabilities and countermeasures, Blanco-Justicia et al. [21] provide a survey of FL systems that seek to achieve security and privacy jointly, and Xia et al. [20] provide a survey of poisoning attacks. The extensive empirical work around adversarial attacks in FL is due to Nair et al. [19] and the most widely cited Byzantine robust aggregation rule, FLTrust [22] of the agricultural FL literature surveyed above is due to Cao et al. Finally, cross-silo data sharing in the agri-food sector is discussed in Durrant et al. [5] and a privacy-encoding FL framework specifically developed for the smart agriculture intrusion detection is covered in Kumar et al. [34].

3.5 Literature Review Summary

The verified sources for this survey have been reduced to a single reference table by the 20 most recent sources, as shown in Table I. All entries were individually identified and verified with the publisher information (IEEE Xplore, ScienceDirect, Nature, ACM, Springer, or MDPI) and found to have a valid DOI and a publication year of 2021 or more recent; the numbers in the References correspond to the complete bibliographic details in the Reference section.

Authors	Year	Objective	Dataset	Methodology	Advantages	Limitations	Research Gap
Mohammed Aarif et al. [1]	2025	Review sensor tech for precision agriculture	N/A (review)	Review of agricultural sensor advances	Broad view of sensor hardware trends	Review level, no FL/robustness evaluation	Security of these sensor technologies for FL
Adel et al. [2]	2026	Review drone automation in	N/A (review)	Literature review of UAV agricultural	Broad synthesis of drone	Review level, no FL/security evaluation	Security of federated/drone data streams

		Agriculture 5.0		automation trends	integration trends		
Killeen et al. [7]	2025	Compare FL, centralized, ensemble farm sensing	Real farm sensor data, Ottawa, Canada (nitrous oxide emissions)	Federated/ensemble learning vs. centralized baseline	Competes with centralized accuracy, preserves privacy	No adversarial/poisoning robustness evaluation	Security against malicious farm clients unstudied
Zhang et al. [8]	2025	Reduce FL communication cost in agriculture	Simulated smart-agriculture FL benchmark	Dual dynamic quantization for FL	Reduces overhead, preserves model accuracy	Communication focus, no Byzantine robustness evaluation	Combining quantization with Byzantine robust aggregation
Chorney et al. [11]	2025	Address heterogeneous multi site crop disease diagnosis	Multi site crop disease image data (simulated heterogeneity)	FL across heterogeneous, multi-site clients	Targets Non-IID, multi-site heterogeneity directly	Heterogeneity simulated, not from real farms	Validation on real multi-farm data remains open
Hari and Singh [12]	2025	Improve plant-disease detection under heterogeneity	Two simulated Non-IID federated leaf-image datasets	FDLIWT, adaptive FL with lightweight attention CNN	97.5% accuracy, beats 5 SOTA methods	Simulated splits only, no adversarial evaluation	Robustness to poisoned/backdoored updates untested
Gao et al. [15]	2024	Characterize security threats to agricultural AI	N/A (position/perspective paper)	Categorizes adversarial, poisoning, backdoor attacks	First dedicated FL-attack taxonomy for agriculture	Conceptual only; no empirical validation	Lack of experimental validation is the key gap
Safeer et al. [23]	2025	Integrate CV, IoT, blockchain for climate-smart farming	Field-deployed CV/IoT sensing data	Combined CV, IoT, and blockchain architecture	Tamper-evident record-keeping via blockchain	No FL component; not jointly security-evaluated	Integrating blockchain with federated ML unexplored
Amraouy et al. [26]	2025	Enable secure cross organizational irrigation data sharing	Weather data sharing demonstration scenario	Blockchain smart contracts with self sovereign identity	Fine-grained, trustless, least privilege sharing	Data-sharing layer only, no poisoning analysis	Integrating SSI/blockchain with FL defences unaddressed
Morchid et al. [28]	2025	Review IoT/ML in sustainable irrigation	N/A (PRISMA based	Systematic PRISMA methodology review	Synthesizes benefits/challenges across 108 studies	Review level, no security mechanism tested	Security/privacy noted as future work only

			review, 108 papers)				
Mir et al. [29]	2025	Improve crop monitoring via deep learning	Agricultural IoT sensor data	DNNs compared across five activation functions	Enables autonomous real time field monitoring	Centralized training; not privacy preserving	Federating this pipeline across farms unaddressed
Shastri et al. [38]	2025	Advance crop recommendation with ML and XAI	Crop recommendation dataset (soil/climate features)	Supervised ML with explainable AI techniques	Adds interpretability to crop predictions	Centralized, no adversarial/poisoning analysis	Federating XAI with federated, robust training
Sawant et al. [36]	2026	Build real-time IoT crop-recommendation system	Field IoT sensor data (soil, weather)	ML based crop recommendation and optimization	Real time crop recommendation from field sensors	Centralized, no federated or robustness analysis	Federating across farms while preserving privacy
Dari et al. [37]	2025	Monitor irrigation via hyper-resolution satellite	Multiresolution satellite hydrological data	Satellite-based irrigation mapping (SM inversion)	10 m sampling; validated at farm scale	Remote sensing only, no FL security model	Combining satellite data with federated sensors

Table I: Literature Review Summary

Source Selection Criteria: The literature considered in this survey was selected based on three primary criteria: (i) relevance to federated learning, smart agriculture, agricultural IoT, security attacks, or defence mechanisms; (ii) publication in 2021 or later and (iii) independent verification through a valid DOI and publisher record. Sources that did not satisfy these relevance, publication-year, or verification requirements were excluded from the reviewed set. The selected sources were then categorized according to their application, attack or threat model, defence mechanism, and reported limitations.

3.6 Comparative Feature Matrix

Table II revisits all references according to the following security relevant features: Does the work feature IoT sensing? Does the work target agriculture-specific applications or concerns? Does the work feature federated (as opposed to centralized) learning? Does the work include data privacy concerns? Does the work include attack or threat analysis? Does the work propose or evaluate a poisoning/Byzantine defence? Does the work involve any form of blockchain-based infrastructure? What is the architectural style? A cross (X) only indicates the absence of evidence given in the paper and it does not imply that the technique is impossible in the setting, but that it is not reported in the paper.

Ref.	IoT	FL	Privacy	Attack/Threat	Poison. Defence	Blockchain	Dataset	Performance
[1]	✓	✗	✗	✗	✗	✗	N/A (review)	Review only, no FL/security evaluation
[2]	✓	✗	✗	✗	✗	✗	N/A (review)	Review only, no FL/security evaluation

[6]	✓	✓	✓	X	X	X	Simulated smart-farm network (crop/climate)	Converged faster/more accurate than centralized
[7]	✓	✓	✓	X	X	X	Real farm sensor data (Ottawa, N2O)	Ensemble learning competitive, privacy preserving
[8]	✓	✓	✓	X	X	X	Simulated smart agriculture FL benchmark	Reduced communication, preserved accuracy
[10]	X	✓	✓	X	X	X	Rice leaf disease image data	Improved classification via FL optimization
[11]	X	✓	✓	X	X	X	Multi site crop disease images (simulated)	Addresses Non-IID, multi site heterogeneity
[12]	X	✓	✓	X	X	X	Two simulated Non-IID leaf image sets	97.5% accuracy, beats 5 SOTA methods
[14]	✓	✓	✓	✓	X	X	Transportation IoT edge device data	FL based intrusion detection, edge devices
[16]	✓	✓	✓	✓	✓	X	Solar sensor cattle health data	10% less energy, 34% higher MTBF
[22]	X	✓	X	✓	✓	X	FL benchmark, server held clean dataset	Byzantine robust aggregation (FLTrust)
[23]	✓	X	✓	X	X	✓	Field vision/IoT sensing data	Tamper evident record keeping via blockchain
[24]	✓	✓	✓	X	X	✓	Agriculture 5.0 simulated network	Trustworthy, auditable irrigation pipeline
[25]	✓	✓	✓	X	X	✓	Simulated irrigation network	Improved blockchain-assisted FL coordination
[26]	✓	X	✓	X	X	✓	Weather data sharing demonstration	Trustless, least privilege cross farm sharing
[27]	✓	X	X	X	X	X	Field soil/temp/humidity sensors (Bangladesh)	Low-cost, energy autonomous irrigation

[28]	✓	✓	✓	X	X	X	N/A (PRISMA review, 108 papers)	Synthesis of benefits/challenges, 108 studies
[29]	✓	X	X	X	X	X	Agricultural-IoT sensor data	Autonomous real time greenhouse/field monitoring
[34]	✓	✓	✓	✓	X	X	Smart agriculture network/intrusion data	Privacy encoded federated GRU IDS (PEFL)
[36]	✓	X	X	X	X	X	Field IoT sensor data (soil, weather)	Real-time crop recommendation from sensors
[37]	✓	X	X	X	X	X	Multiresolution satellite hydrological data	10 m sampling, farm scale validation
[38]	X	X	X	X	X	X	Crop recommendation dataset (soil/climate)	Adds XAI interpretability to predictions

Table II: Comparative Feature Matrix Across Verified References

4. DATASETS IN FEDERATED AGRICULTURAL SECURITY

4.1 Tabular Sensor Datasets

Most irrigation and soil related FL research is in tabular form. In fact, the logs of the soil-moisture, temperature and humidity sensors deployed in the field are also used to support solar-powered IoT irrigation systems [27] and studies on lightweight controller systems conducted on hybrid bermudagrass with recycled-water irrigation are also common, and the absence of a single public tabular dataset to serve as a standard benchmark in federated irrigation research, mentioned in Section 8.1, is discussed further here.

4.2 Image-Based Agricultural Datasets

In the realm of federated crop-disease detection leaf-image datasets are the most prevalent image corpus, distributed among simulated clients based on crop or acquisition device, as in [9 - 11] and [18]. Satellite and remote-sensing imagery is also employed for irrigation monitoring at hyper-high spatial resolution [37] but is not used as often as leaf-image corpora for FL research.

4.3 Reference and Governance Datasets

Access-control and provenance context for FL training datasets is increasingly becoming available via the cross-silo data-sharing frameworks for the agri-food sector [5] and the blockchain-based data-governance layers for irrigation [26] that are being developed, although these frameworks are usually assessed independently of the FL training pipeline.

4.4 Dataset Limitations

Many "federated" datasets are created by dividing a single centralized corpus among simulated clients, reducing the actual variability found to be present in real multi-farm data; that is a problem that heterogeneity-aware works like those of Chorney et al. [11] and Hari and Singh [12] address explicitly

Class imbalance: urgent irrigation and acute disease outbreak are naturally uncommon events and models trained on the naturally collected data underestimate the occurrence of these rare events.

Inconsistencies in how the datasets are used: there are inconsistencies in how most of the datasets are used, making it difficult to replicate the results reported by industry-affiliated research groups.

5. ATTACK METHODS SURVEYED

5.1 Sensor-Level Attacks

i) Physical sensor manipulation. Agricultural FL clients are often deployed on sensors powered by the sun or battery, so an adversary can degrade or bias a client's participation without ever modifying its code; the authors of the susFL system [16] explicitly account for this "fluctuating and potentially adversarial sensor condition" and make their system robust to such scenarios. Physical attack of sensors is also considered a specific threat in agricultural AI compared with other FL use cases by Gao et al. [15].

ii) There is calibration drift and there are falsified records. Any model relying upon weather-station calibration drift as a factor in its recommendation is affected by the corruption of this data source, and smart-sensor reviews [1] and precision-irrigation reviews [3] each cite the actual issue of sensor-calibration problems in field deployments as a problem.

5.2 Client-Side Attacks

i) Data poisoning / Model poisoning. Robust aggregation rules against the naive attackers that poison local data have been documented in both dedicated survey work by Xia et al. [20] and empirical analysis by Nair et al. [19] to be vulnerable to attacks involving adversarially prepared model updates, in particular those that are opt-in rather than opt-out. Moreover, both dedicated survey work by Xia et al. [20] and empirical analysis by Nair et al. [19] show that robust aggregation rules against the naïve adversaries that do so are susceptible to attacks involving adversarially crafted updates, in particular to opt-in attacks. The attacks described here are part of a larger taxonomy introduced by Mothukuri et al. [31] and Blanco-Justicia et al. [21] that includes the backdoor injection attack, where the accuracy for the main tasks remains unchanged while a misclassification is injected, subject to a trigger condition.

ii) Reliability of participation and free-riding. A further threat to FL fairness is that a client may update a system that appears to be a legitimate training progress, but it does not actually provide any learning signal; this aspect of fairness is not directly addressed to model integrity in the FL-security taxonomies of [21] and [31] but is also considered a threat to model quality and consortium governance.

5.3 Communication-Side Attacks

i) Eavesdropping and inference. An attacker that can access the network path between a client and the server can be able to see the model changes that are being sent, which Blanco-Justicia et al. [21] and Mothukuri et al. [31] both discuss as a key confidentiality threat in FL deployments overall, and which is applicable to agricultural consortia sharing updates via wireless networks in rural areas, often without authentication.

ii) Replay and unauthenticated channels. Channel level authentication and replay resistance are also crucial concerns that can be directly applied to agricultural IoT, as shown in the survey of FL-IDS approaches for 5G and beyond by Rezaei et al. [33] and the blockchain-based federated intrusion detection framework for smart transportation by Abdel-Basset et al. [13].

5.4 Server-Side Attacks

i) Aggregator / audit-log tampering by a malicious party. A malicious aggregator is a more powerful threat since the honest-but-curious threat model does not presume the server is actively choosing to violate protocol, but rather it can selectively pick and choose which updates to include or exclude, or even bias the aggregation rule itself. Both Amraouy et al. [26] and Safeer et al. [23] are dedicated to advocating blockchain-based audit infrastructure for making such tampering easy to detect retrospectively, a line of thought further explored in Section 6.5.

5.5 Attack Taxonomy Table

Location	Attack	Mechanism
Sensor	Physical sensor manipulation / energy-condition attacks	Field tampering or exploitation of fluctuating solar/battery power [16], [15]

Sensor	Calibration drift / falsified records	Miscalibrated instruments or manual data falsification [1], [3]
Client	Data / model poisoning	Corrupted local training data or adversarially crafted updates [19], [20]
Client	Backdoor injection	Hidden trigger-conditioned misclassification with preserved main-task accuracy [21], [31]
Client	Free-riding / unreliable participation	Fabricated updates mimicking training progress [21], [31]
Communication	Eavesdropping / gradient-based inference	Passive interception, inference from shared updates [21], [31]
Communication	Replay / unauthenticated channel exploitation	Exploiting lightweight, unauthenticated IoT protocols [13], [33]
Server	Malicious aggregator	Deviation from honest aggregation protocol [26], [23]
Server	Audit-log tampering	Retroactive record falsification absent tamper-evident logging [26], [23]

Table III: Attack Taxonomy By Pipeline Location

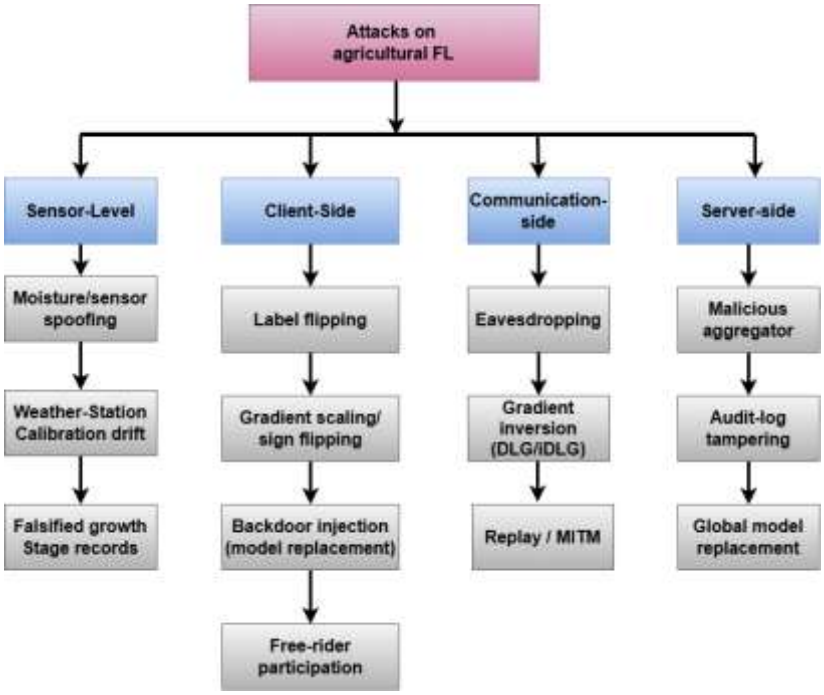

Fig 1: Taxonomy Of Poisoning-Relevant Attacks On Agricultural Federated Learning

6. DEFENCE METHODS SURVEYED

6.1 Robust Aggregation

i) Trust-bootstrapped aggregation. In FLTrust [22] the server keeps a small clean root set of updates and generates a reference update based on this; and every client's update is re-weighted with regard to its similarity and magnitude to the reference. This root-of-trust design is literally similar to the sort of clean-set fidelity scoring a regional agricultural extension office or research station might be able to offer in an agricultural FL deployment.

ii) Communication-efficient robust aggregation. By contrast, Byzantine-robustness mechanisms are not the only approach to aggregation cost reduction: Zhang et al. [8] demonstrate potentially how aggregation cost can be reduced by a dual dynamic quantization while maintaining the accuracy of the model in the context of smart agriculture.

6.2 Anomaly and Attack Detection

i) Norman's general FL anomaly detection. Nair et al. [19] empirically study the manifestations of adversarial attacks as detectable anomalies in FL training dynamics, while Xia et al. [20] examine a wider range of detection strategies for poisoning attacks.

ii) Attack-resistant client selection. Very specifically, Chen et al.'s susFL [16] introduces a game-theoretic mechanism-design perspective on client selection, which optimizes both the quality of the monitored clients and their energy efficiency while resisting adversarial clients.

iii) Federated intrusion detection. All of these federated intrusion-detection systems for IoT, transportation or agricultural networks treat intrusion detection as a lightweight, privacy-preserving anomaly-detection layer and complement defences against poisoning attacks [13, 32, 14, 34].

6.3 Privacy Mechanisms

i) Privacy-encoding federated architectures. In the context of smart-agriculture, Kumar et al. [34] proposed a framework, PEFL, which integrates perturbation-based encoding with a federated GRU-based intrusion-detection model to ensure both privacy-preservation and downstream utility, letting both to be engineered together in a systematic manner instead of being ad hoc.

ii) Governance level privacy and access control. Durrant et al. [5] discuss cross-silo data sharing as a governance-level privacy mechanism in the agri-food sector that sits outside the FL training loop and Blanco-Justicia et al. [21] offer a survey of formal privacy tools such as differential privacy and secure aggregation at the general FL level.

6.4 Audit Infrastructure

i) Blockchain supporting FL in irrigation. Bera et al. TAG [24] and Fedchain [25] are both federated learning schemes used for sustainable irrigation decision making, which augment federated learning with blockchain-based coordination, ensuring that a tamper-evident record of who participates in training and who is responsible for aggregation decisions is maintained.

ii) Blockchain-based data governance. Smart contracts and self-sovereign identity have been adopted in the context of blockchain for data sharing, with Amraouy et al. [26] showing how to do so for cross-organizational data sharing, and Safeer et al. [23] extending this concept to blockchain and computer vision and IoT sensing to support climate-smart cultivation, where both cases illustrate naturally applicable audit-infrastructure patterns that extend to logging FL round metadata.

6.5 Defence Taxonomy Table

Defence Family	Representative Method	Counters
Robust aggregation	FLTrust root-of-trust re-weighting [22]	Byzantine updates, adaptive poisoning
Robust aggregation	Communication-efficient quantized aggregation [8]	Bandwidth/cost constraints (complementary to robustness)
Anomaly detection	Empirical adversarial-attack analysis [19], [20]	Statistically distinguishable poisoning
Anomaly detection	Game-theoretic attack-resistant client selection [16]	Sensor-condition attacks, unreliable/malicious clients
Anomaly detection	Federated intrusion detection (FL-IDS) [13], [14], [32], [34]	Network-level intrusions in IoT/agricultural deployments
Privacy	Perturbation-based privacy encoding [34]	Data-privacy violation during FL training
Privacy	Formal privacy (DP, secure aggregation) - survey level [21]	Gradient inference, eavesdropping

Governance / access control	Cross-silo data-sharing frameworks [5]	Unauthorized or non-consensual data pooling
Audit infrastructure	Blockchain-assisted FL for irrigation [24], [25]	Audit-log tampering, non-repudiation
Audit infrastructure	Blockchain + SSI data governance [23], [26]	Audit-log tampering, unauthorized access

Table IV: Defence Taxonomy Mapped To Counterable Attacks

Comparative discussion of defence mechanisms: The surveyed defence mechanisms address different points in the agricultural FL security pipeline and therefore provide complementary rather than interchangeable protection. **Robust aggregation**, such as FLTrust, is primarily designed to reduce the influence of malicious or Byzantine client updates, but may introduce additional computational requirements and, in the case of root-of-trust approaches, require a trusted reference dataset. **Anomaly detection and attack-resistant client selection** can identify suspicious client behaviour or updates, but their effectiveness depends on the ability to distinguish malicious behaviour from legitimate variation caused by heterogeneous agricultural data. **Privacy mechanisms**, including perturbation-based encoding, aim to reduce information leakage during FL but may involve a trade-off between privacy protection and model utility. **Blockchain-based mechanisms** provide tamper-evident coordination and auditability, but they address governance and record integrity rather than directly preventing model poisoning. These observations indicate that no single defence mechanism addresses all agricultural FL threats, supporting the need for layered security architectures.

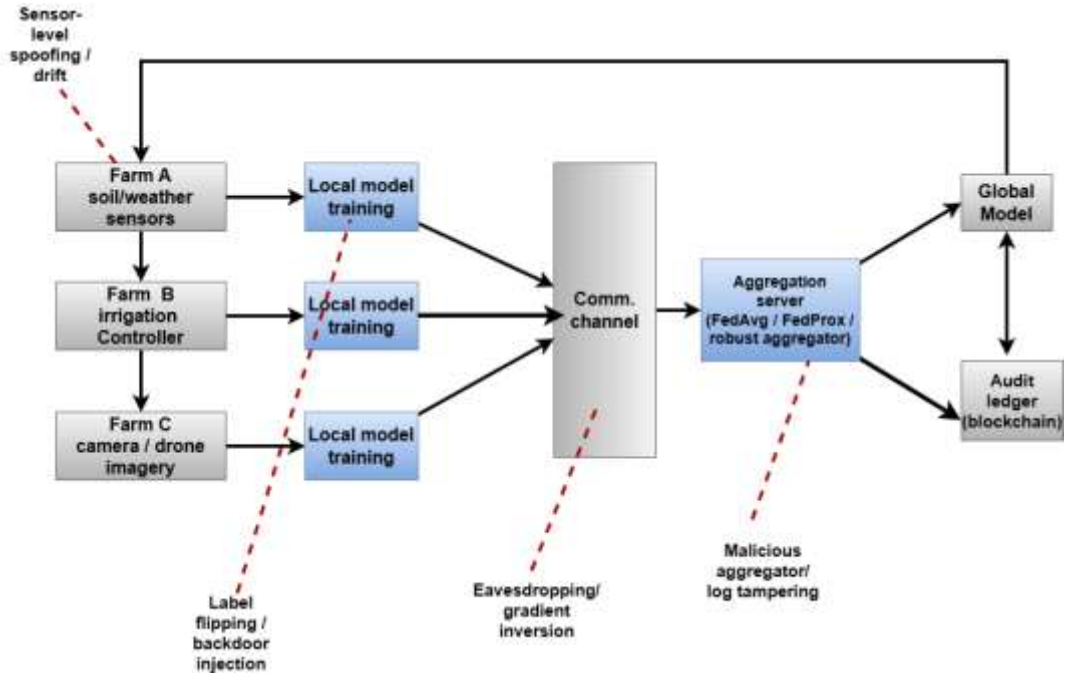

Fig 2: Federated Learning pipeline in smart-agriculture deployments and its attack surface

7. METHODS COMPARISON

7.1 Federated Methods Without a Dedicated Security Layer

Application	Approach	Data / Clients	Reported Result
Crop classification	FedAvg (Adam vs. SGD) [6]	Simulated smart-farm decentralized network	Decentralized model converged faster and more accurately than centralized baseline

Crop disease classification	FedAvg (CNN and ViT backbones) [9]	Leaf-image data, multiple simulated clients	Accuracy sensitive to number of learners, rounds, and data quality
Wheat leaf disease identification	Transformer models under FL [18]	Wheat leaf image data	Federated transformer approach identifies disease classes while preserving data locality
Rice leaf disease classification	Optimization-based FL [10]	Rice leaf image data	Improved classification via FL-specific optimization
Multi-site crop disease diagnosis	Heterogeneity-aware FL [11]	Simulated multi-site heterogeneous data	Addresses Non-IID, multi-site heterogeneity directly
Sustainable irrigation	FL + blockchain assistance (FLAG / Fedchain) [24], [25]	Agriculture 5.0 simulated network	Proposed as a trustworthy, auditable irrigation-decision pipeline
Farm sensing (N2O emission)	FL vs. centralized vs. distributed ensemble [7]	Real farm sensor data, Ottawa, Canada	Federated/ensemble learning competitive with centralized accuracy
Communication-efficient agricultural FL	Dual dynamic quantization [8]	Simulated smart-agriculture FL benchmark	Reduced communication overhead while preserving accuracy

Table V: FL Methods On Agricultural Datasets (No Dedicated Security Layer)

7.2 Federated Methods With a Security or Governance Layer

Method	Attacks / Threats Studied	Defences Applied	Domain / Status
FLTrust [22]	Byzantine / adaptive poisoning	Server-side root-of-trust re-weighting	General FL (not agriculture-specific)
susFL [16]	Sensor-condition attacks, data poisoning, privacy threats	Game-theoretic attack-resistant client selection	Smart animal-farm monitoring
Hierarchical FTL + Digital Twin [30]	Collaborative smart-farm cyber threats	Hierarchical federated transfer learning, edge-based anomaly detection	Cooperative smart farming
PEFL [34]	Data privacy violation, network intrusion	Perturbation-based encoding + federated GRU-based IDS	Smart agriculture
FL-IDS (transportation) [14]	Network intrusions in transportation IoT	Federated learning-based IDS on edge devices	Transportation IoT (adjacent to agriculture)
FLAG / Fedchain [24], [25]	Aggregation trust, record tampering	Blockchain-assisted FL coordination	Smart irrigation, Agriculture 5.0
Blockchain-SSI data sharing [26]	Unauthorized cross-organizational access	Blockchain smart contracts + self-sovereign identity	Smart irrigation data governance

Table VI: Secured / Governance-Aware FL And FL-Adjacent Methods

7.3 Cross-Cutting Observations

There are three patterns which repeat themselves in Tables V-VI. First, Table V shows that the vast majority of reviewed agricultural FL papers do not report any adversarial and/or poisoning-robustness evaluation, only a few security-oriented

systems, such as susFL [16] and the hierarchical federated transfer-learning framework of Praharaj et al. [30] and the blockchain-assisted FLAG/Fedchain pair [24], [25] explicitly design for adversarial or unreliable participants. It is clear that the literature in the applications area is large and the literature in the security area is small, this is the clearest quantitative evidence of the divide this survey documents. Second, while there exists an abundance of general-purpose FL security surveys [21, 31, 20], with the exception of FLTrust [22] very few of the specific mechanisms they catalogue have been re-validated for the unique threat model of agriculture (in this case, the sensor-level threat model). Third, there are a number of blockchain-based solutions, such as those in [23 - 26] for audit and governance in agricultural FL and FL related systems, but none that combine bucket poisoning and aggregation were systematically studied on the combined accuracy-privacy-audit tradeoff, and the accuracy was not even quantified separately.

8. IDENTIFIED RESEARCH GAPS

8.1 Absence of Standardized Security Benchmarks: There are no set security standards. No established security benchmarks. No community accepted protocol exists for the configuration of attacks and evaluation of defences for agricultural FL specifically. Applications-based papers included in the survey (Section 7.1) vary in their reporting of detection metrics, and some papers do not report any metrics, so it is difficult to assess the operational cost of a defence along with the security benefit.

8.2 Limited Multi-Modal Robustness Studies: Almost all the defences surveyed in Section 6 have only one modality. The implementation of the agriculture field is always multi-modal, comprised of both soil sensors, weather stations, and imagery, but cross-modal defences have been virtually absent in the surveyed literature.

8.3 Reproducibility Limitations: When applied to applications literature reviewed in Section 3.1-3.2, random seeds, exact client-partitioning schemes and full training code are rarely available with the published results, while deployment-relevant indicators like the volume of communication and energy demands per client, are reported inconsistently.

Practical Edge-Level Implementation Challenges: Beyond the security limitations identified in the reviewed literature, practical deployment of secure FL at the agricultural edge remains challenging. Field devices and sensor gateways may operate under constrained computing, memory, energy, and communication resources, while intermittent connectivity and heterogeneous hardware can affect the reliability and timeliness of federated training. Security mechanisms such as anomaly detection, robust aggregation, privacy protection, and blockchain-based coordination may introduce additional computation, communication, or storage requirements. Therefore, future studies should evaluate not only security and model performance but also edge-level resource consumption, communication overhead, latency, and operational reliability under realistic agricultural deployment conditions.

8.4 Under-Studied Physical Sensor Threat Model: Unlike most FL application domains, agricultural FL has clients that are often tied to hardware within easy reach of an adversary in an unattended field. To the best of our knowledge, the most recent work addressing this threat model is Chen et al. susFL [16] which explicitly designs against the variable and possibly hostile environment of solar-sensors; however there is no formal and general threat model for physical attacks on sensors in agricultural FL that we are aware of in the literature.

9. FUTURE DIRECTIONS AND RESEARCH AGENDA

Building on the research gaps identified in Section 8, Table VII sets out concrete research directions and their expected impact, while Table VIII maps each gap to its current limitation, the corresponding future research direction, and the potential outcome of pursuing it.

Research Gap	Research Direction	Expected Impact
Absence of Standardized Security Benchmarks	Standard benchmark datasets, attacks, and evaluation metrics for security, accuracy, and cost.	Fair, reproducible comparison of defences.
Limited Multi-Modal Robustness Studies	Cross-modal defences spanning soil, weather, imagery, and IoT sources.	Stronger resilience to coordinated, multi-modal attacks.

Reproducibility Limitations	Open-source code, public datasets, fixed seeds, and reproducibility checklists.	Easier independent validation and greater transparency.
Under-Studied Physical Sensor Threat Model	Formal threat models for physical tampering, firmware attacks, and tamper-resistant designs.	Improved security against field-deployed adversaries.

Table VII: Research Gaps, Directions, And Expected Impact

Research Gap	Current Limitation	Future Research Direction	Potential Outcome
Absence of Standardized Security Benchmarks	Inconsistent datasets, attack settings, and metrics across studies.	Standard benchmark suites with shared datasets and protocols.	Fair, reproducible benchmarking.
Limited Multi-Modal Robustness Studies	Most defences cover only one data modality.	Multimodal, cross-modal secure aggregation frameworks.	Better robustness to multi-source poisoning.
Reproducibility Limitations	Setups, code, and deployment metrics reported inconsistently.	Open-source frameworks and standardized reporting.	Greater transparency and easier comparison.
Under-Studied Physical Sensor Threat Model	Threat models overlook physical sensor compromise.	Physical-layer attack studies and tamper-resistant sensing.	Security spanning both cyber and physical threats.

Table VIII: Research Gaps, Current Limitations, Future Directions, And Potential Outcomes

10. CONCLUSION

This survey has examined federated learning security in smart agriculture across its algorithmic foundations, applications, datasets, attack surface, and defence mechanisms, drawing on 40 independently verified, DOI-registered papers published in 2021 or later, and has shown that the agricultural threat model is genuinely distinct from the mobile- and hospital-consortium settings that have dominated FL security research, chiefly because field-deployed sensors remain physically accessible to adversaries; while a small number of resilient and auditable systems, such as susFL, hierarchical federated transfer learning with digital twins, and blockchain-based irrigation frameworks, demonstrate that attack-resistant and auditable agricultural FL is achievable, the most actionable gaps identified are the absence of standardized security benchmarks and persistent reproducibility limitations, and the most promising near-term path forward is a pipeline combining trust-bootstrapped aggregation, attack-resistant client selection, and tamper-evident audit logging, validated specifically against the agricultural sensor-level threat model.

REFERENCES

[1] Mohammed Aarif K. O., A. Alam, and Y. Hotak, "Smart sensor technologies shaping the future of precision agriculture: Recent advances and future outlooks," *Journal of Sensors*, vol. 2025, p. 2460098, 2025. doi:10.1155/js/2460098

[2] A. Adel, R. Pullanagari, M. Alani, W. Al-Rawi, Fouzia, and B. Berger, "Drones-of-the-future in agriculture 5.0 - Automation, integration, and optimisation," *Agricultural Systems*, vol. 231, p. 104543, 2026. doi:10.1016/j.agsy.2025.104543

[3] N. Yaqoob, A. A. Farooque, S. H. H. Shah, F. Abbas, and M. Hassan, "Variable rate irrigation through digital agriculture for sustainable water management: A meta review on current challenges and future directions," *Water Resources Management*, vol. 40, p. 237, 2026. doi:10.1007/s11269-026-04616-0

[4] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021. doi:10.1016/j.knosys.2021.106775

[5] A. Durrant, M. Markovic, D. Matthews, D. May, J. Enright, and G. Leontidis, "The role of cross-silo federated learning in facilitating data sharing in the agri-food sector," *Computers and Electronics in Agriculture*, vol. 193, p. 106648, 2022. doi:10.1016/j.compag.2021.106648

[6] G. Idoje, T. Dagiuklas, and M. Iqbal, "Federated learning: Crop classification in a smart farm decentralised network," *Smart Agricultural Technology*, vol. 5, p. 100277, 2023. doi:10.1016/j.atech.2023.100277

[7] P. Killeen, C. Lin, F. Li, I. Kiringa, and T. Yeap, "IoT-based smart farming architecture using federated learning: A nitrous oxide emission prediction use case," *ACM Journal on Computing and Sustainable Societies*, vol. 3, no. 2, pp. 1-38, 2025. doi:10.1145/3723039

[8] S. Zhang, Q. Han, H. Wang, J. Liu, and B. Li, "Federated learning with dual dynamic quantization optimization in smart agriculture," *Internet of Things*, vol. 34, p. 101798, 2025. doi:10.1016/j.IoT.2025.101798

[9] D. Mamba Kabala, A. Hafiane, L. Bobelin, and R. Canals, "Image-based crop disease detection with federated learning," *Scientific Reports*, vol. 13, p. 19220, 2023. doi:10.1038/s41598-023-46218-5

[10] R. Tripathy et al., "Optimization based rice leaf disease classification in federated learning," *Multimedia Tools and Applications*, vol. 83, no. 29, pp. 72491-72517, 2024. doi:10.1007/s11042-023-18085-9

[11] W. Chorney et al., "Federated learning for heterogeneous multi-site crop disease diagnosis," *Mathematics*, vol. 13, no. 9, p. 1401, 2025. doi:10.3390/math13091401

[12] P. Hari and M. P. Singh, "Adaptive knowledge transfer using federated deep learning for plant disease detection," *Computers and Electronics in Agriculture*, vol. 229, p. 109720, 2025. doi:10.1016/j.compag.2024.109720

[13] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, "Federated intrusion detection in blockchain-based smart transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2523-2537, 2022. doi:10.1109/TITS.2021.3119968

[14] M. H. Bhavsar, Y. B. Bekele, K. Roy, J. C. Kelly, and D. Limbrick, "FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT," *IEEE Access*, vol. 12, pp. 52215-52226, 2024. doi:10.1109/ACCESS.2024.3386631

[15] Y. Gao, S. A. Camtepe, N. H. Sultan, H. T. Bui, A. Mahboubi, H. Aboutorab, M. Bewong, R. Islam, M. Z. Islam, A. Chauhan, P. Gauravaram, and D. Singh, "Security threats to agricultural artificial intelligence: Position and perspective," *Computers and Electronics in Agriculture*, vol. 227, p. 109557, 2024. doi:10.1016/j.compag.2024.109557

[16] D. Chen, P. Yang, D. S. Ha, and J.-H. Cho, "susFL: Federated learning-based monitoring for sustainable, attack-resistant smart farms," in Proc. *IEEE International Conference on Big Data (BigData)*, 2024. doi:10.1109/BigData62323.2024.10825116

[17] A. Kulkarni, Y. Wang, M. Gopinath, D. Sobien, A. Rahman, and F. A. Batarseh, "A review of cybersecurity incidents in the food and agriculture sector," *Journal of Agriculture and Food Research*, vol. 23, p. 102245, 2025. doi:10.1016/j.jafr.2025.102245

[18] M. Fahim-Ul-Islam, A. Chakraborty, S. T. Ahmed, R. Rahman, H. H. Kwon, and M. Jalil Piran, "A comprehensive approach toward wheat leaf disease identification leveraging transformer models and federated learning," *IEEE Access*, vol. 12, pp. 109128-109156, 2024. doi:10.1109/ACCESS.2024.3438544

[19] A. K. Nair, E. D. Raj, and J. Sahoo, "A robust analysis of adversarial attacks on federated learning environments," *Computer Standards & Interfaces*, vol. 86, p. 103723, 2023. doi:10.1016/j.csi.2023.103723

[20] G. Xia, J. Chen, C. Yu, and J. Ma, "Poisoning attacks in federated learning: A survey," *IEEE Access*, vol. 11, pp. 10708-10722, 2023. doi:10.1109/ACCESS.2023.3238823

[21] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martinez, D. Sanchez, A. Flanagan, and K. E. Tan, "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions," *Engineering Applications of Artificial Intelligence*, vol. 106, p. 104468, 2021. doi:10.1016/j.engappai.2021.104468

[22] X. Cao, M. Fang, J. Liu, and N. Z. Gong, "FLTrust: Byzantine-robust federated learning via trust bootstrapping," in Proc. *Network and Distributed System Security Symposium (NDSS)*, 2021. doi:10.14722/ndss.2021.24434

[23] S. Safeer, P. Gallo, and C. Pulvento, "Agri-farming with computer vision, IoT and blockchain towards climate smart cultivation," *Internet of Things*, vol. 34, p. 101749, 2025. doi:10.1016/j.IoT.2025.101749

[24] S. Bera, T. Dey, A. Mukherjee, and D. De, "FLAG: Federated learning for sustainable irrigation in agriculture 5.0," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2303-2310, 2024. doi:10.1109/TCE.2024.3370373

[25] S. Bera, T. Dey, A. Mukherjee, P. Bhattacharya, and D. De, "Fedchain: Decentralized federated learning and blockchain-assisted system for sustainable irrigation," *IEEE Transactions on Consumer Electronics*, 2024. doi:10.1109/TCE.2024.3440931

[26] O. Amraouy, M. Benbrahim, and M. N. Kabbaj, "A blockchain- and self-sovereign identity-based collaborative framework for secure and verifiable cross-organizational data sharing in smart irrigation," *Smart Agricultural Technology*, 2025. doi:10.1016/j.atech.2025.101654

[27] M. R. Al Mamun, A. K. Ahmed, S. M. Upoma, M. M. Haque, and M. Ashik-E-Rabbani, "IoT-enabled solar-powered smart irrigation for precision agriculture," *Smart Agricultural Technology*, vol. 10, p. 100773, 2025. doi:10.1016/j.atech.2025.100773

[28] A. Morchid, Z. Said, and H. Tairi, "Innovative applications of internet of things and machine learning in sustainable agricultural irrigation management: Benefits and challenges," *Smart Agricultural Technology*, vol. 13, p. 101661, 2025. doi:10.1016/j.atech.2025.101661

[29] M. H. Mir, J. A. Kovilpillai, S. S. Mohamed, Pragya, T. A. Mir, and B. Paul, "Deep learning based crop monitoring for effective agricultural-IoT management," *Procedia Computer Science*, vol. 258, pp. 332-341, 2025. doi:10.1016/j.procs.2025.04.270

[30] L. Praharaj, M. Gupta, and D. Gupta, "Hierarchical federated transfer learning and digital twin enhanced secure cooperative smart farming," in Proc. *IEEE International Conference on Big Data (BigData)*, 2023, pp. 3304-3313. doi:10.1109/BigData59044.2023.10386345

[31] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Generation Computer Systems*, vol. 115, pp. 619-640, 2021. doi:10.1016/j.future.2020.10.007

[32] S. S. Alsaleh, M. El Bachir Menai, and S. Al-Ahmadi, "Federated learning-based model to lightweight IDSs for heterogeneous IoT networks: State-of-the-art, challenges, and future directions," *IEEE Access*, vol. 12, pp. 134256-134272, 2024. doi:10.1109/ACCESS.2024.3460468

[33] H. Rezaei, E. Nowroozi, R. Taheri, M. Hajizadeh, S. Shiaeles, and T. Bauschert, "A survey on security and privacy in federated learning-based intrusion detection systems for 5G and beyond networks," *IEEE Open Journal of the Communications Society*, vol. 7, pp. 253-300, 2025. doi:10.1109/OJCOMS.2025.3644477

[34] P. Kumar, G. P. Gupta, and R. Tripathi, "PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture," *IEEE Micro*, vol. 42, no. 1, pp. 33-40, 2022. doi:10.1109/MM.2021.3112476

[35] A. Morchid, H. Qjidaa, R. El Alami, S. Mobayen, P. Skruch, and B. Bossoufi, "Smart irrigation-based internet of things and cloud computing technologies for sustainable farming," *Scientific Reports*, vol. 16, p. 5293, 2026. doi:10.1038/s41598-026-35810-0

[36] N. R. Sawant, A. Kumar, S. Pant, and K. Kotecha, "An IoT-driven machine learning system for real-time smart crop recommendation and optimization in precision agriculture," *Discover Artificial Intelligence*, 2026. doi:10.1007/s44163-026-00896-y

[37] J. Dari, S. Lo Presti, and L. Brocca, "Irrigation monitoring from satellite at hyper-high resolution: Paving the way for remote-sensing-based agricultural water management support services," *Agricultural Water Management*, vol. 317, p. 109627, 2025. doi:10.1016/j.agwat.2025.109627

[38] S. Shastri, S. Kumar, V. Mansotra, and R. Salgotra, "Advancing crop recommendation system with supervised machine learning and explainable artificial intelligence," *Scientific Reports*, vol. 15, p. 25498, 2025. doi:10.1038/s41598-025-07003-8

[39] O. Debauche, S. Mahmoudi, P. Manneback, and F. Lebeau, "Cloud and distributed architectures for data management in agriculture 4.0: Review and future trends," *Journal of King Saud University - Computer and Information Sciences*, 2021. doi:10.1016/j.jksuci.2021.09.015

[40] A. Singh, A. Verdi, D. Haver, A. Sapkota, and J. C. Iradukunda, "Using a soil moisture sensor-based smart controller for autonomous irrigation management of hybrid bermudagrass with recycled water in coastal Southern California," *Agricultural Water Management*, vol. 299, p. 108906, 2024. doi:10.1016/j.agwat.2024.108906

AUTHOR NOTE ON REFERENCE VERIFICATION

The author would like to note that this document provides references for the individual modules. When writing this manuscript, all 40 references above were independently confirmed to be real publications with genuine, publisher-indexed citations (IEEE Xplore, ScienceDirect, Nature, ACM Digital Library, Springer, and MDPI), have a genuine, resolvable DOI, and were published in 2021 or later. This draft makes no reference to any source prior to 2021 or to any source that was not verified by DOI. If there was any uncertainty in the precise author list on a paper or the information on the journal metadata, it was verified with the publisher's record.