International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Towards Secure and Efficient Federated Learning for Wheat and Rice Disease Diagnosis

Shabad Kaur[1], Amandeep Kaur Virk[2]

[1]Research Scholar, Sri Guru Granth Sahib World University Fatehgarh Sahib, India
Email: *shabad.kaur15[at]gmail.com*

[2]Associate Professor, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India
Email: *amandeep_virk[at]sggswu.edu.in*

Abstract: ***Federated learning (FL) is a distributed machine learning paradigm that enables multiple clients (e.g. farms, sensors, or smartphones) to collaboratively train models without sharing raw data. This is highly relevant for agriculture, where data about crop health is sensitive and distributed across many smallholders. In India, wheat and rice – the country's two most important cereals – suffer huge losses from fungal diseases (rusts, blast, etc.). FL can leverage diverse image datasets from distributed fields (e.g. smartphone or drone imagery of leaves) to improve disease detection while preserving privacy. This paper introduces FL concepts and its role in plant disease diagnosis, traces FL's evolution, compares its advantages over centralized/cloud methods in agri-disease detection, reviews recent FL-agriculture research (including wheat/rice cases), and identifies research gaps and future directions in context of wheat and rice. A summary table compares representative FL-based approaches for diseased crops.***

Keywords: Federated Learning, Crop Disease Detection, Wheat, Rice, Edge Devices

1. Introduction

Crop disease detection in wheat and rice is essential for India because these crops underpin national food security, rural livelihoods, and agricultural productivity. Early detection using machine learning enables timely disease management, reduces yield losses, lowers pesticide use, and improves farmers' incomes. Manual monitoring of crops is time-consuming and costly, especially in large fields. Farmers often fail to detect the disease in its early stage, which leads to loss and affects yield prediction. AI based auto detect system can help farmer to predict disease at early stage and helps them to decide which pesticide will be use. By integrating such systems into smartphones or drones, the solution becomes scalable and accessible to rural farmers. Thus, there is a strong need to combine AI-based detection with privacy-preserving collaborative training so that farmers from different regions can benefit without fear of sharing their raw data.

Federated learning (FL) allows training an AI model across many edge devices (clients) without aggregating their data centrally. Instead of uploading all data to a server, each client (e.g. a farmer's smartphone, IoT sensor or edge node) trains locally and sends model updates to a central server for aggregation. Google introduced this concept in 2016. By keeping raw data on-device, FL embodies *data minimization* and significantly reduces the privacy risks and data-transfer costs of centralized ML. This is crucial when agricultural data are proprietary (e.g. yields, farm practices) or subject to regulations. In plant pathology, FL is promising for *crop disease detection*. For example, Mohanty *et al.* demonstrated that a deep convolutional neural network on a public plant-leaf image dataset can achieve >99% accuracy in identifying 14 crops and 26 diseases. Such high-performance models typically require massive datasets from many farms. However, farmers may not want to share raw images of their fields. FL enables them to collaboratively build a model for disease classification (e.g. for wheat rust or rice blast) by sending only weight updates, not images. Thus, FL can improve detection of diseases like wheat rusts (which can cause >50% yield loss) and rice blast (10–30% losses typically), while preserving each farm's data privacy. Wheat and rice are India's staple crops, accounting for a major share of calories. They are plagued by fungal diseases: wheat suffers stripe and stem rusts, blight and blast, while rice suffers blast, brown spot, sheath blight, etc. These diseases can devastate yields (over 10–50% loss). Early automated detection of symptoms (e.g. by leaf images) is key to management. Traditional ML models need pooled data from many farms; FL offers a decentralized alternative that is well-suited to India's small-farm context and privacy concerns. Recent studies have begun applying FL to agriculture (e.g., for crop yield prediction or plant disease detection) and show its viability. This paper reviews FL's history and key developments (Sec. II), highlights its FL in crop disease detection (Sec. III), surveys recent literature on FL for crop health (Sec. IV), and discusses research gaps and future opportunities specific to wheat and rice (Sec. V).

2. History of Federated Learning

The term *federated learning* was popularized by McMahan *et al.* in 2016–17. They proposed **FedAvg**, an algorithm that averages neural network weights from many local trainers, reducing communication cost and preserving privacy. Kairouz *et al.* later defined FL as a setting where "many clients (databases or devices) collaboratively learn a shared model under orchestration of a central server, while keeping the training data decentralized". Early FL research focused on mobile devices (e.g. next-word prediction on smartphones). Key milestones include: Google's FedAvg (2017); secure aggregation protocols (Bonawitz *et al.* 2017) for privacy; personalization and fairness algorithms (e.g. q-FedAvg); and convergence and communication-efficiency improvements (FedProx, FedOpt). In 2019 Kairouz *et al.* surveyed FL advances and open challenges. Since 2020, FL frameworks (e.g. TensorFlow Federated, PySyft) have proliferated, enabling FL in domains like healthcare and finance. More recently, FL has been adopted in Internet-of-Things (IoT) and smart agriculture contexts. Overall, FL evolved from a theoretical idea to a practical tool bridging edge computing and ML, with constant innovation in optimization, privacy (differential privacy, secure multiparty), and system design. Today it is an active field of research with growing applications, including initial proofs-of-concept in precision farming and plant pathology.

Advantages of Federated Learning for Crop Disease Detection

FL offers several key advantages in agricultural settings compared to conventional centralized or cloud-based ML:

- **Data Privacy and Security:** In centralized ML, farmers must upload raw data (images, sensor logs) to a server, risking exposure of sensitive information. FL keeps data local, sending only model updates (gradients/weights). This minimizes privacy leakage. Federated learning supports Data sovenity where privacy regulations would forbid data sharing. Kairouz *et al.* note that FL embodies data minimization and mitigates privacy risks inherent in centralized ML. In India, this is important since farm data (yields, disease incidence) can be proprietary.
- **Regulatory Compliance:** FL can ease adherence to data protection laws (GDPR, etc.) by design, since raw data never leave the owner. Compliance is particularly relevant as India and global agencies stress privacy in agri-tech. As Zhao *et al.* note, FL "ensures privacy by design" and avoids transmitting raw images, a GDPR-friendly approach.
- **Reduced Communication Costs:** Agricultural data (high-res images, video) is voluminous. Uploading terabytes to cloud is expensive in bandwidth and time. FL drastically cuts communication by transmitting compressed model updates. The central server only sends/receives model parameters each round, not raw images, reducing data transfer. This is advantageous in rural areas with limited connectivity: local model training and infrequent weight-sync are more feasible.
- **Scalability and Fault Tolerance:** FL can naturally scale to many farms or fields. It is robust to partial participation: if some clients are offline, remaining ones still improve the model. In contrast, centralized approaches can suffer if network failures interrupt data collection.but Federated Learning supports Edge FL with asynchronous or partially synchronous operation.
- **Local Relevance / Personalization:** Individual farms may have unique conditions (soil, climate, crop variety). FL enables local retraining on-site, potentially yielding personalized models. For example, a local FL client might fine-tune the global disease model on its own images. Hybrid FL methods (cross-silo vs cross-device) accommodate both many small farms and a few big institutions.
- **Computational Offloading:** On-device training spreads computation across many cheap devices instead of centralized servers. For instance, drones or smartphones can each handle local CNN training on images, collectively doing the work of a data center. This leverages idle edge resources and can lower infrastructure costs.
- **Knowledge Sharing without Raw Data:** By aggregating models, FL effectively shares learning while preserving secrecy of data. For example, a farm in Punjab can benefit from disease patterns learned by another in West Bengal without exchanging sensitive data. This collaborative approach yields better models than isolated local ML, yet protects each participant.

For Crop Disease Detection, FL outperforms by providing privacy, legal safety, communication efficiency, and collaboration among farms. These advantages are critical when farmers are reluctant to share images or records of their crops, or when network/bandwidth are limited.

3. Literature Review

Recent years have seen growing research applying FL to agriculture and plant disease detection. Table 1 summarizes representative studies, highlighting crop/disease focus, FL techniques and performance. Many studies demonstrate high accuracy and practical viability.

Table I: Review of federated Learning Models for Crop Disease Detection

Study	Year	Crops/Diseases	Method (Model, FL)	Key Results
Kabala *et al.* [1]	2023	Apple, Corn, etc. (PlantVillage)	CNNs (ResNet50), Vision Transformers (ViT) in FL	99.76% (ResNet50).
Nigam *et al.* [9]	2025	Wheat (leaf rust severity)	EfficientNet-B0 + CBAM via FL	Training acc.=99.51%, test=96.68% for disease severity.
Aggarwal *et al.* [11]	2023	Rice leaf diseases	EfficientNetB3 CNN in FL (non-IID)	99% (IID), 95% (non-IID).
Behera *et al.* [2]	2025	(Real-time IoT sensor and crop image dataset	CNNs, RNN, LSTM, GRU with IoT sensors	99% training and 94% test accuracy achieved in FL setting.
Chorney & Peng [4]	2025	Rice crop diseases	CNN-based FL model	Centralized classifier: Accuracy 83.24% ; FL preserves privacy, is cost- & comm.-efficient.
Piccialli *et al.* [5]	2025	Multiple plant leaf diseases	AGRIFOLD: ECA-VGG16 CNN in FL	High accuracy across 9 classes (leaf diseases+healthy) in 12 datasets with Acuracy 98.8%,
Zhao *et al.* [8]	2023	Tomato leaf diseases	Federated Transfer Learning (Graph–SNN)	Accuracy: 94.45% (lab), 62.02% (field) – highlights FL robustness under real conditions.

These studies illustrate FL's effectiveness. For instance, Kabala *et al.* found that ResNet50 under FL achieved near-centralized performance. Nigam *et al.* demonstrated that an Efficient Net-based model in FL could nearly match traditional training on wheat rust images. Aggarwal *et al.* showed that FL can train an Efficient Net on rice disease data distributed across clients, achieving 95% test accuracy despite non-IID splits. Notably, the tomato-leaf study underscores that FL-trained models generalize from laboratory to variable field conditions, although with some drop in accuracy.

Overall, these works indicate that FL enables high-performance plant disease classifiers while respecting data locality and privacy. Table highlight that FL systems typically use horizontal partitioning (data split by farm or device). More advanced approaches incorporate transfer learning or graph neural nets to cope with small local datasets.

4. Research Gaps and Future Opportunities

Despite progress, applying FL to Indian agriculture presents challenges and open research areas:

1) **Data Heterogeneity:** Farms differ by region, practice, and crop variety. Non-IID data can degrade FL training. Existing works (e.g. Chorney [4]) highlight that model architecture and fairness methods are crucial. Future work should develop FL algorithms robust to such heterogeneity common in multi-season Indian farms, possibly via personalized FL or federated multi-task learning.
2) **Resource Constraints:** Many Indian farmers lack high-end devices. Lightweight FL models (e.g. mobile CNNs) and efficient aggregation (fewer rounds, compression) are needed. Techniques like AGRIFOLD [5] point toward this, but more edge-optimized models and compression schemes would help.
3) **Connectivity Limitations:** Rural connectivity may be intermittent. Asynchronous FL and opportunistic communication (e.g. via local hubs or satellites) could allow training even with sparse networks. Research could explore hybrid models that combine local (on-device) inference with occasional cloud syncing.
4) **Incentive and Trust Models:** Collaborative FL requires trust among farmers. Mechanisms (possibly blockchain-based) to ensure fair contribution and model ownership could encourage adoption. Also, incentive structures or federated marketplaces might motivate farmers to participate.
5) **Domain-specific Models:** Tailored FL models for wheat and rice disease classes (e.g. rust detection, blast detection) are needed. This includes building or curating labeled image datasets from Indian fields, and potentially integrating multispectral imagery. Research should also merge FL with remote sensing (satellite/drone data) for regional disease monitoring.
6) **Policy and Education:** From a deployment perspective, awareness and training are needed. Research should address how to present FL solutions to farmers and agronomists, ensuring usability. Studies on socio-economic impacts of FL in farming communities (especially smallholders) would guide real-world implementation.
7) **Security and Privacy Guarantees:** Although FL is privacy-enhancing, vulnerabilities exist. Ensuring privacy under India's emerging data laws is also important.
8) **Cross-Domain Extensions:** FL in agriculture could extend to other tasks (yield estimation, resource optimization). For example, combining FL disease diagnosis with FL crop yield models could build holistic smart-farming systems. Interdisciplinary research bridging agronomy, data science, and policy will be valuable.

5. Conclusions and Future Work

Federated Learning holds great promise for Indian wheat and rice disease detection by enabling collaborative, privacy-preserving AI. Realizing its potential requires addressing heterogeneity, resource constraints, and integration into agrarian contexts. Future research should focus on designing FL algorithms and systems attuned to the practical realities of Indian agriculture, thereby improving disease surveillance and crop security across the nation.

References

[1] D. M. Kabala, A. Hafiane, L. Bobelin, and R. Canals, "Image-based crop disease detection with federated learning," Sci. Rep., vol. 13, Art. no. 19220, 2023, doi: 10.1038/s41598-023-46218-5.
[2] S. Behera, N. Padhy, R. Panigrahi, and S. K. Kuanar, "Crop disease prediction using deep learning in a federated learning environment: Ensuring data privacy and agricultural sustainability," Procedia Comput. Sci., vol. 254, pp. 137–146, 2025, doi: 10.1016/j.procs.2025.01.018.
[3] R. Janga and R. Dave, "Enhancing smart farming through federated learning: A secure, scalable, and efficient approach for AI-driven agriculture," arXiv preprint arXiv:2509.12363, 2025.
[4] W. J. Chorney and Z. Peng, "Federated learning for heterogeneous multi-site crop disease diagnosis," Mathematics, vol. 13, no. 9, Art. no. 1401, 2025, doi: 10.3390/math13091401.
[5] F. Piccialli, C. Della Bruna, D. Chiaro, P. Qi, and M. Savoia, "AGRIFOLD: AGRIculture federated learning for optimized leaf disease detection," Expert Syst. Appl., vol. 289, Art. no. 128371, 2025.
[6] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282, doi: 10.48550/arXiv.1602.05629.
[7] P. Kairouz *et al*., "Advances and open problems in federated learning," Found. Trends Mach. Learn., vol. 14, nos. 1–2, pp. 1–210, 2021, doi: 10.1561/2200000083.
[8] F. Zhao *et al*., "Federated transfer learning for tomato leaf disease detection using a neuro-graph hybrid model," Agriengineering, vol. 7, no. 12, Art. no. 432, 2023, doi: 10.3390/agriengineering7120432.
[9] S. Nigam *et al*., "Automated severity level estimation of wheat rust using an EfficientNet-CBAM hybrid model," Biology, vol. 12, no. 1, Art. no. 1, 2025, doi: 10.3390/biology12010001.
[10] M. Silveira, "Rice blast: A disease for global food security," J. Plant Biol., vol. 63, pp. 1–10, 2022, doi: 10.1007/s12374-022-09314-5.
[11] V. Aggarwal *et al*., "Lightweight federated learning for rice leaf disease classification using non-IID images," Sustainability, vol. 15, no. 16, Art. no. 12149, 2023, doi: 10.3390/su151612149.
[12] J. Xu *et al*., "Federated learning for crop yield prediction: A comprehensive review," Agronomy, in press, 2024.

[13] S. P. Mohanty, D. P. Hughes, and M. Salathé, "Using deep learning for image-based plant disease detection," Front. Plant Sci., vol. 7, Art. no. 1419, 2016, doi: 10.3389/fpls.2016.01419.
[14] S. Condran *et al*., "Machine learning in precision agriculture: A survey," IEEE Access, vol. 10, pp. 56899–56923, 2022, doi: 10.1109/ACCESS.2022.3177213.
[15] K. R. Žalik and M. Žalik, "A review of federated learning in agriculture," Sensors, vol. 23, no. 23, Art. no. 9566, 2023, doi: 10.3390/s23239566.
[16] K. Bonawitz *et al*., "Practical secure aggregation for privacy-preserving machine learning," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2017, pp. 1175–1191, doi: 10.1145/3133956.3133982.
[17] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in *Proc. Machine Learning and Systems (MLSys)*, 2020, pp. 429–450, doi: 10.48550/arXiv.1812.06127.
[18] Q. Yang, Y. Liu, T. Chen, and Y. Tong, *Federated Machine Learning: Concept and Applications*. San Rafael, CA, USA: Morgan & Claypool, 2019, doi: 10.2200/S00960ED1V01Y201907AIM043.
[19] G. A. Hard *et al*., "Federated learning for mobile keyboard prediction," in *NIPS Workshop on Distributed Machine Learning*, 2018.
[20] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2015, pp. 1310–1321, doi: 10.1145/2810103.2813687.
[21] Shabad Kaur and A. K. Virk, "AODV extension using genetic algorithm in VANET," Int. J. Sci. Res. (IJSR), vol. 4, no. 7, pp. 2420–2422, Jul. 2015, doi: 10.21275/SUB157062.
[22] M. J. Sheller *et al*., "Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data," Sci. Rep., vol. 10, Art. no. 12598, 2020, doi: 10.1038/s41598-020-69250-1.
[23] K. W. Church *et al*., "Federated learning on high-dimensional data," J. Big Data, vol. 6, Art. no. 113, 2019, doi: 10.1186/s40537-019-0285-6.
[24] H. B. McMahan *et al*., "A communication-efficient framework for federated learning," arXiv preprint arXiv:1602.05629, 2016.
[25] X. Li *et al*., "FedBN: Federated learning on non-IID data via local batch normalization," in *Proc. Int. Conf. Learning Representations (ICLR)*, 2020.