iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82828

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Federated Learning: A Comprehensive Review of Concepts, Challenges, and Applications

Srikant Khator[1], Anurima Majumdar[2], Souvik Jana[3], Sovan Dey Sutradhar[4], Souvik Maiti[5], Souvik Das[6]
Department of Electronics and Communication Engineering, Guru Nanak Institute of Technology, Kolkata, India

Abstract: Federated Learning is a recent, distributed machine learning paradigm that allows multiple clients to collaboratively train a global model without explicit raw local data sharing. FL decentralizes the training process by reducing privacy risks, regulatory limitations, and hence improving large-scale learning over mobile, IoT, healthcare, and financial systems. This paper provides a comprehensive review of the foundational paradigm of FL, its architectures, optimization methods, security mechanisms, key challenges, especially in the case of non-IID data, communication cost, and system heterogeneity, and application domains. Recent advancements and open research directions are also outlined.
Keywords: Federated Learning, Distributed Learning, Privacy Preservation, Secure Aggregation, Edge Computing, IoT, Non-IID Data.

I. INTRODUCTION

Traditional machine learning relies on centralized data collection, but this model is often not practical because of user privacy needs, regulatory constraints, and cost of data transfer. FL overcomes these limitations by enabling distributed clients to collaboratively train a shared model without exposing private data [1]. Different from traditional distributed learning, FL prioritizes privacy, communication efficiency, and robustness across diverse clients.

FL has found rapid adoption in mobile devices, medical institutions, edge networks, and financial systems. Recent surveys emphasize the rapid expansion of FL in real-world applications and growth in research importance [1]-[4].

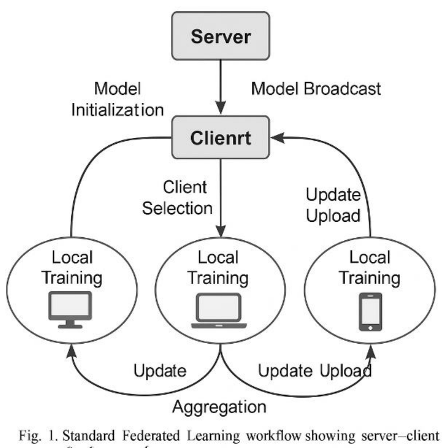


Figure 1:Federated Learning Workflow

In this paper, the fundamentals, challenges, optimization techniques, security considerations, and applications of FL are reviewed, discussing current research progress.

II. FUNDAMENTALS OF FEDERATED LEARNING

A. Federated Learning Workflow

FL works in an iterative fashion, usually via multiple rounds of communication between a central server and participating clients:

1) Model Initialization: The server initializes a global model.
2) Sampling of Client: Participants are selected based on availability.
3) Local Training: This involves the model's training on private datasets by clients.
4) Model Update: The client devices return gradients or model parameter updates.

5) Aggregation: The server carries out weighted averaging, such as FedAvg.
6) Broadcasting: Updated model is sent back to clients. This paradigm reduces privacy exposure because client data never leaves the device [1].

B. Types of FederateLearning

FL settings include:

1) Horizontal FL: Clients share the same feature space but differ in sample distribution [1].
2) Vertical FL: Clients share user IDs but possess different features (e.g., financial + e – commerce institutions) [2], [5].
3) Federated Transfer Learning: Used when both sample and feature spaces differ [2].

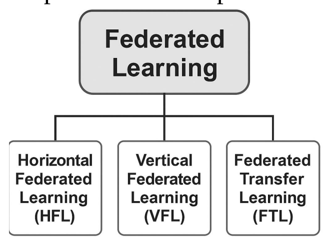


Figure 2: Types of Federated Learning

C. Deloyment Scenarios

- Cross-Device: Involves many mobile/IOT devices with unstable connectivity and limited resources [3].
- Vertical FL: Involves organizations with reliable connections and structured datasets [6].

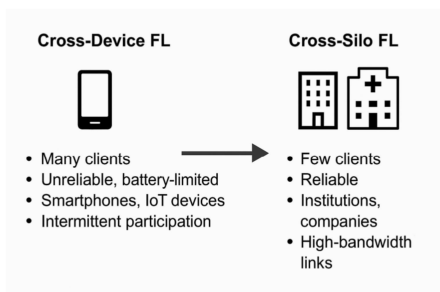


Figure 3: Cross-Device vs Cross-Silo Architecture

III. KEY CHALLENGES IN FEDERATED LEARNING

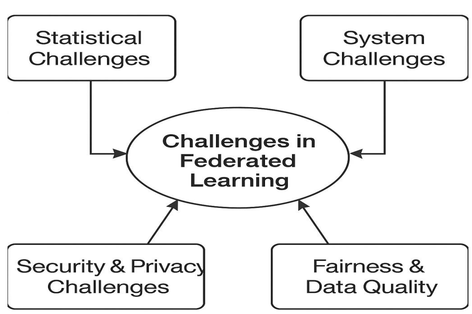


Figure 4: Challenges in Federated Learning

A. Data Heterogenity (Non-IID Data)

Non-IID data is recognized as the key obstacle in FL. In most cases, clients collect data from their personal usage patterns or organizational practices, leading to massive shifts in distributions, which substantially degrade model convergence and accuracy [4], [7], [8].

Experimental analyses have already shown that FL performance drastically degrades under label skew, feature skew, and quantity imbalance across clients [9], [10].

B. System Heterogenity

Client devices differ widely in processor capability, memory, and network bandwidth. This heterogeneity leads to idle time on the server while waiting for slower clients ("stragglers") and creates fairness challenges [3], [11].

C. Communication Overhead

FL requires frequent exchanges of model updates; this becomes overly costly when sending millions of parameters for deep neural networks. Model compression, quantization, and sparsification techniques mitigate this overhead but introduce trade-offs.

D. Privacy and Security Threats

Despite avoiding the transmission of raw data, FL is still susceptible to attacks such as:

- Model inversion
- Membership inference attacks
- Data poisoning and Byzantine attacks

Secure aggregation, differential privacy, and homomorphic encryption may provide protection but with higher computation and communication costs [6], [13], [14].

E. Privacy and Security Threats

Poor-quality or biased datasets from clients may degrade global performance. Ensuring model accuracy equitably for all participants is an essential pre-requisite for reliable FL deployment [7], [15].

IV.KEY CHALLENGES IN FEDERATED LEARNING

A. FedAvg and Algorithmic Variants

Federated Averaging (FedAvg) is the foundational FL algorithm. It reduces communication by performing multiple local epochs before transmitting updates [1]. However, FedAvg suffers under extreme non-IID conditions. Numerous extensions aim to improve robustness:

- FedProx: Adds proximal regularization to reduce client drift [3].
- SCAFFOLD: Uses control variates to correct for client update variance [8].
- FedNova and FedDvn: Improve convergence under heterogeneous updates [16].

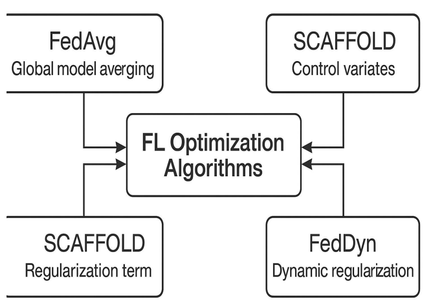


Figure 5: FL Optimization Algorithm

B. Optimization Under Non-IID Data

Studies show even small improvements in client update alignment significantly enhance global convergence. For example:

- Momentum-based FL improves training stability [9].
- Adaptive client selection reduces training variance [10].
- Variance-reduced aggregation techniques show measurable benefits [8], [16].

C. System Heterogenity

Personalized FL addresses the need for client-specific performance improvements. Approaches include:

- Fine-tuning global models
- Meta-learning, enabling fast adaptation
- Multi-task FL, where each client optimizes both shared and individual objectives [11], [17].

D. Privacy-Preserving Mechanisms

Key methods include:

- Secure Aggregation (SecAgg) to prevent the server from viewing individual updates [13].
- Differential Privacy (DP-FL) to obscure client contribution [14].
- Homomorphic Encryption allowing encrypted computation [6].

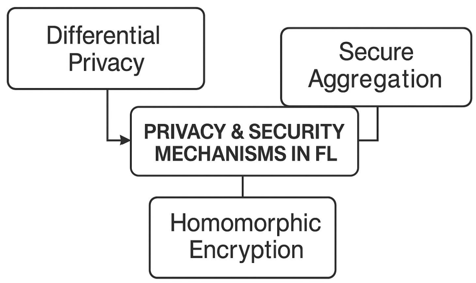


Figure 6: Privacy and Security Mechanism

E. Communiction Efficiency Approaches

To reduce communication cost, researchers propose:

- Gradient compression (e.g., quantization)
- Sparse update transmission
- Layer-wise updating
- Periodic averaging
- Partial client participation [12].

V. APPLICATIONS OF FEDERATED LEARNING

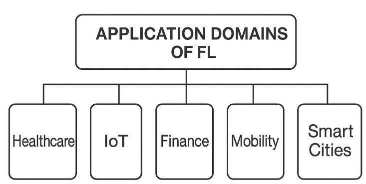


Figure 7: Application Domains of FL

A. Healthcare

FL assists in secure multi-institution collaboration in medical imaging, disease prediction, and patient outcome modelling without sharing sensitive health data [12], [18].

B. The Internet of Things (IoT) and Edge Computing

FL provides decentralized intelligence for smart sensors, vehicles, and industrial Iot devices. Lightweight FL frameworks allow model training under resource constraints [13], [19].

C. Mobile and Recommendation Systems

FL enables personalized services like next-word prediction, recommendation, and behavior modelling while preserving user privacy [1], [20].

D. Financial Services

Banks use FL to train fraud detection and credit risk scoring models together without sharing private user details [2], [5].

E. Smart Cities and Communicatio Networks

Example of use cases include traffic forecasting, smart-grid optimization and distributed decision making within 5G/6G networks [14], [21].

VI. RECENT ADVANCES IN FEDERATED LEARNING

Recent developments include:

- New taxonomies and systematic evaluation frameworks to benchmark FL algorithms [4], [9].
- Improved lightweight FL for edge and IoT systems using device-aware optimization [19].
- Stronger adversarial defenses and fair training approaches [7], [15].
- Enhanced vertical FL frameworks improving communication and privacy guarantees for organizational collaborations [5].

VII. RECENT ADVANCES IN FEDERATED LEARNING

Future work should focus on:

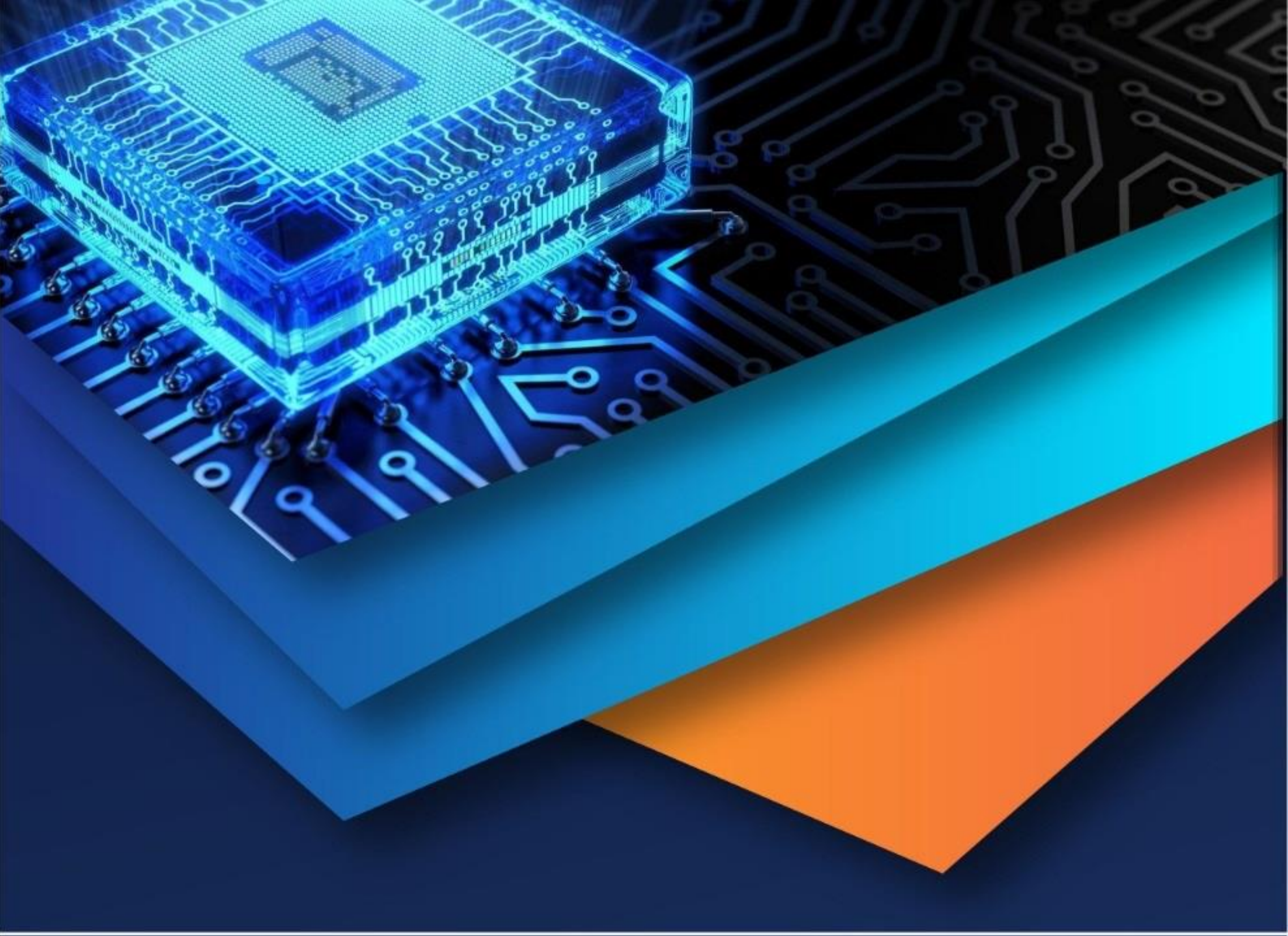
1) Robust non-IID solutions for extreme distribution shifts.
2) Energy-efficient FL architectures for IoT and edge devices.
3) Integrated security + privacy frameworks combining DP, encryption, and robust aggregation.
4) Fairness-aware FL ensuring ethical model deployment.
5) Interoperable cross-domain FL for real-world collaboration between institutions.
6) Standardized benchmarks and evaluation protocols.

VIII. CONCLUSION

Federated Learning provides a compelling framework for privacy-preserving distributed computation across diverse and decentralized data sources. While optimization, privacy, personalization, and communication reduction have seen progress, challenges remain in addressing non-IID data, heterogeneity, fairness, and real-world scalability. Continued research and innovations in systems will make FL more reliable and widespread in industries such as healthcare, finance, communication, and smart cities.

REFERENCES

[1] C. Zhang et al., A Survey on Federated Learning.
[2] Q. Li et al., A Survey on Federated Learning Systems.
[3] T. Li et al., "Federated Optimization in Heterogeneous Networks."
[4] Y. Kang et al., "Federated Learning: Challenges, Methods, and Future Directions."
[5] J. Xie et al., "Efficient Communication in Vertical Federated Learning."
[6] K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving ML."
[7] M. Mohri et al., "Fairness in Federated Learning."
[8] S. Karimireddy et al., "SCAFFOLD: Stochastic Controlled Averaging for FL."
[9] Z. Cheng et al., "Momentum Benefits Non-IID Federated Learning."
[10] M. Haller et al., "Handling Non-IID Data in Federated Learning."
[11] A. Smith et al., "Federated Multi-Task Learning."
[12] A. Rieke et al., "Federated Learning in Healthcare."
[13] S. Pokhrel et al., "FL for Edge-IoT Systems."
[14] M. Chen et al., "FL in 6G Networks."
[15] D. Ji et al., "Fairness and Bias in Federated Learning."
[16] T. Reddi et al., "Adaptive Optimization in Federated Learning."
[17] Ye et al., "Personalized Federated Multi-Task Learning."
[18] Choi et al., "Federated Learning in Medical Imaging."
[19] Baqer et al., "Lightweight Federated Learning for IoT."
[20] Hard et al., "Federated Learning for Mobile Keyboard Prediction."
[21] Shen et al., "FL for Smart Cities and Intelligent Transportation."



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY