Federated Learning over Edge-Fog-Cloud Architectures for Distributed Intelligence

*Shairy Shairy and Rachit Garg

School of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab, India
*er.shairykalra@gmail.com, rachit.garg.in@gmail.com

Abstract. The high rate of Internet of Things (IoT) device growth has led to massive amounts of distributed data being created at the network edge, much of which is highly sensitive data about users. Traditional centralized machine learning models rely on aggregation of the raw data in a cloud server, which raises serious privacy, legal, communication, and latency concerns. Such restrictions have encouraged the development of federated learning (FL), a distributed machine learning model that enables collaborative model training while keeping raw data on the user devices. Meanwhile, the current computing infrastructures are shifting from a cloud-only model to encompass a continuum of edge, fog, and cloud computing. This hierarchy architecture supports low latency processing, optimized use of resources, and scalable coordination of distributed intelligence. Federated learning with an edge-fog-cloud architecture represents a beneficial solution to privacy-preserving, scalable, and real-time intelligent systems, especially in large-scale IoT and Industrial IoT systems. The paper explores federated learning on an edge-fog-cloud-based system in distributed intelligence. The key goals include the analysis of the architectural functions of edge, fog, and cloud layers in federated learning, the exploration of the communication-computation trade-offs, and the emphasis on the fact that hierarchical aggregation enhances the scale and efficiency. This study provides a systematic foundation for developing next-generation smart applications, which need safe, scalable, and privacy-conscious collaborative learning along the edge-fog-cloud spectrum.

Keywords: Federated Learning, Edge Computing, Fog computing, Cloud computing, Distributed Intelligence, Internet of things, (IoT), Privacy-preserving learning

1 INTRODUCTION

1.1 Background

The Internet of Things (IoT) devices, such as smartphones, wearable sensors, smart cameras, and industrial sensors, have expanded at a very high rate and this has made the magnitude of distributed data generation to rise sharply[1,

A. Agnihotri et al. (eds.), *Proceedings of the Conference on Bridging Engineering Disciplines with AI and Machine Learning (BEDAIML 2026)*, Advances in Intelligent Systems Research 209,
https://doi.org/10.2991/978-94-6239-697-5_23

2]. The new technologies of sensing, communication, and embedded computing have facilitated these devices to constantly receive huge amounts of data, the largest portion of which is sensitive information. At the same time, the maturity of machine learning (ML) and deep learning (DL) [3] methods has enhanced the need to use data-driven intelligence in the application of personalized recommendation, health care diagnostics, autonomous transportation, and smart city management. Conventional cloud-based machine learning models are based on aggregating raw data at remote locations in the form of distributed devices and learning to train models on centralized servers. Nevertheless, these solutions have a number of drawbacks, such as the presence of long communication latency, excessive bandwidth usage, the potential to leak privacy, and the disobedience of data protection laws, like GDPR[4]. Also, the establishment of data silos due to organizational, legal, and ownership limitations additional hinders the large-scale centralized learning.

Federated learning (FL) has become an appealing paradigm of distributed learning that can eliminate these issues because it allows joint training of the model without the transfer of raw data[5, 3]. Local devices in FL are trained on their own data and are only responsible to update the model with a coordinating server. Simultaneously, computing paradigms have developed towards edge and fog computing which can be considered a complement to cloud computing as it allows computing to be brought closer to the data sources. The federated learning combined with the Edge-Fog-Cloud continuum facilitates hierarchically distributed intelligence, less latency, enhanced scalability, and privacy protection[6].

1.2 Problem Statement

In spite of the benefits, the deployment of federated learning instead of heterogeneous Edge-Fog-Cloud infrastructures presents a number of challenges[7]:

- Data Privacy and Security: In spite of the fact that the raw data is local, model updates can also be affected by inference attacks, poisoning, and malicious users.
- Heterogeneous Resources: Edge devices, fog nodes and cloud servers change greatly in terms of computational storage capacity, potential and energy-related limitations.
- Communication and Computation Trade-offs: General communication costs in the form of frequent model updates, and general edge resources in the form of a limit on local training complexity.
- Scalability and Coordination: This requires a hierarchical aggregation and flexible management of resources in order to coordinate and manage millions of distributed devices.

2 ARCHITECTURE OVERVIEW

2.1 Edge-Fog-Cloud Architecture

The structuring of the proposed system will be hierarchical Edge-Fog-Cloud architecture[8] with three layers as depicted in Figure 1.

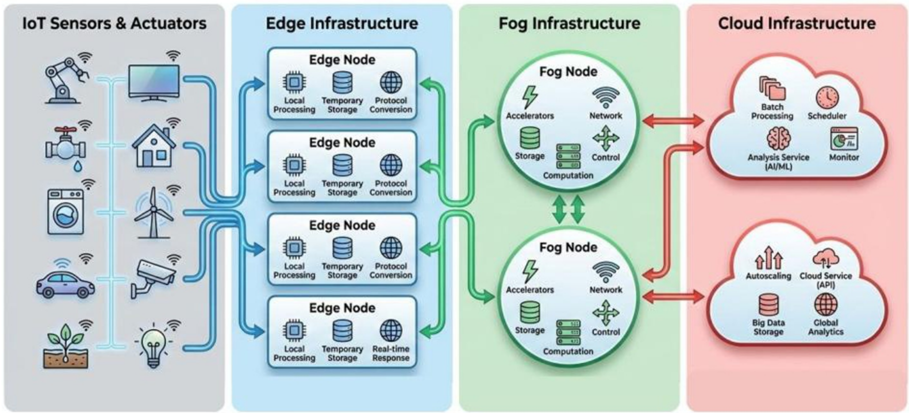

Fig. 1. Architecture of Edge-Fog-Cloud

Edge Layer: Data generated form devices like IoT sensors[9], smartphones, wearables, smart cameras and embedded systems contain in edge layer. These devices conduct the local model training on the basis of private data to produce model updates. Edge computing provides high bandwidth consumption, low latency and high data privacy [6].

Fog Layer: The layer of fog comprises of intermediate nodes including gateways, base stations and local servers. Fog nodes receive updates on models of a group of edge devices, combine model updates with other edge devices, coordinate devices, and offload communication to the cloud. This layer allows hierarchical federated learning to be scaled and made efficient[10].

Cloud Layer: Cloud layer is an example of centralized data centers that have high-performance computing capabilities. It does aggregation of global models, assessment, long term storage and coordination of many fog nodes. The cloud provides world-wide consistency and scalability of federated learning systems of large scale[11].

2.2 Federated Learning Process

The federated learning workflow is hierarchically trained and aggregated on the Edge-Fog-Cloud architecture.

- **Local Training on Edge:** In this step every edge device transfers a local model using its own data.

- **Intermediate Aggregation on Fog:** Fog nodes receive and add model updates by multiple edge devices in this part.
- **Global Aggregation at Cloud:** The cloud takes the updates of the fog nodes to form a global model.
- **Model Distribution:** In the next training round new world global model is sent back through the fog layer to edge devices.

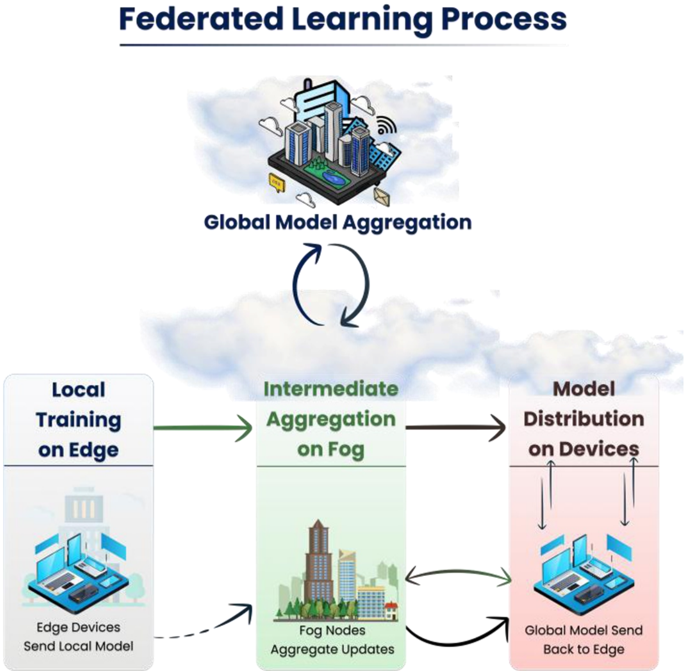

Fig. 2. Federated Learning Process

Table 1. Comparison of Edge, Fog, and Cloud Computing in Federated Learning

Feature	Edge	Fog	Cloud
Location	Near data source	Between edge and cloud	Centralized center
Role in FL	Local training	Partial aggregation	Global aggregation
Data Privacy	Very high	High	Medium
Scalability	Limited	Good	Excellent
Compute Power	Low	Medium	Very high
Communication Cost	Very low	Medium	High
Latency	Very low	Low	High
Example	Mobile phone	Local server	Cloud server

3 LITERATURE REVIEW

The concept of Federated Learning (FL) is one of the potentially effective paradigms of distributed machine learning, where the training of models is not based on the aggregation of data in the centralized format. This feature is especially appropriate in Edge–Fog–Cloud (EFC) architectures, where data is produced by spatially dispersed, resourceful edge computers and acted upon in numerous hierarchical steps. This literature review will take the thematic methodology in synthesizing the results of 30 research papers identified to reveal the key research themes, challenges, and gaps in federated learning based on edge/ fog/ cloud architectures.

3.1 Federated learning architectures in edge fog cloud environments

A number of articles are devoted to the architectural designs, which use FL with edge, fog, and cloud layers. These papers consider hierarchical FL architectures in which local models are trained on the edge devices, aggregated on the fog nodes and coordinated on a global scale by the cloud servers. The purpose of such architectures is to minimize the use of communication overhead, enhance scalability and real-time intelligence. FL models that are hierarchical and have multi-layers are often considered to be an effective way to handle the heterogeneity of devices and networks in EFC systems. The literature, however, shows that there are no standardized architectural frameworks that can be applied in different fields of application[5, 8, 12].

3.2 Resource Management and Communication Efficiency

Several papers suggest gradient compression and adaptive communication solutions to overcome bandwidth limitations in between the edge, fog, and cloud layers. FL mechanisms that are aware of resource availability are developed to be able to balance computation, energy usage, and latency, notably at the edge layer. Although these were made, there are gaps in the research in dynamically optimizing communication and computation across all three layers jointly, especially when the network is highly dynamic[13–15].

3.3 Trust Management, Privacy and Security

A number of articles discuss secure aggregation protocol, differential privacy, and encryption-based methods to safeguard sensitive data at the edge devices. Other security threats, including model poisoning, inference and Byzantine failures are also considered in EFC-based FL systems. his literature shows that there is a need to have light and yet powerful security that can be resource-aware to edge and fog nodes with constrained resources since the available mechanisms usually come with large computing overheads[14, 6, 16].

3.4 Managing Heterogeneity of Data and Systems

It is a well-established fact that non-IID data distribution and heterogeneity in the system are issues in the FL-enabled EFC architectures. Various research works suggest adaptive aggregation, dedicated FL algorithms and clustering methods to address the issue of poor performance due to the heterogeneity related to the data and abilities of devices[17–19]. Nevertheless, the majority of available literature is constrained to simulated settings, which means that there is a gap in research conducted to validate and test the solutions in the real world, as well as in the large-scale deployment studies.

3.5 Federated Learning in EFC Application-Oriented

The papers reviewed reveal the relevance of FL to edge fog clouds, compared to other systems, including smart cities, health, Internet of Things (IoT), autonomous cars, and industrial automation. All these studies highlight the prospects of FL to facilitate distributed intelligence and achieve the latency and privacy needs. However, there are few cross-domain comparative analyses, and the majority of the works refer to isolated application cases[20–22].

Table 2. Summary of Federated Learning Studies

No	Author	Year	Arch.	Method	Contribution	Limitation
1	Saha et al.	2021	EFC	Energy-aware FL	Reduces IoT energy	Limited scale
2	Nguyen et al.	2022	FC	Network-aware FL	Optimized communication	Needs network estimation
3	Rajagopal et al.	2023	EFC	End-to-end FL	Healthcare framework	Small experiments
4	Zhang et al.	2024	EC	Blockchain FL	Privacy improvement	Crypto overhead
5	Savoia et al.	2024	Edge	Eco-FL	Energy efficiency	Accuracy tradeoff
6	Choppara et al.	2025	FC	Distributed FL	Fault tolerance	System complexity

4 Literature Gaps

Although federated learning has made substantial improvements over Edge–Fog–Cloud (EFC) architectures, the literature indicates that several critical research gaps and open challenges still need to be addressed to enable practical and large-scale deployment.

4.1 Lack of Unified and Standardized Architectures

Most existing studies propose application-specific or customized federated learning frameworks for the EFC setting. However, a unified and standardized architectural model that can be generalized across multiple domains such as healthcare, smart cities, and industrial IoT is still lacking [6, 1, 17].

4.2 Lack of Practical Implementation and Measurement

A majority of current research relies on simulations or small-scale testbeds. There is a scarcity of large-scale real-world implementations that realistically capture network dynamics, device failures, mobility, and non-IID data distributions [24, 26, 27].

4.3 Joint Optimization of Communication, Computation, and Energy

Existing solutions often focus on optimizing a single aspect, such as communication efficiency, computational cost, or energy consumption. Joint optimization across edge, fog, and cloud layers in a holistic manner remains an open challenge, particularly in highly dynamic environments [8, 13, 28].

4.4 Scalability and Coordination of Massive IoT Systems

Adaptive aggregation strategies, efficient client selection, and intelligent scheduling mechanisms are still underexplored in hierarchical federated learning systems. These aspects are crucial for coordinating millions of heterogeneous and intermittently connected IoT devices [15, 29, 27].

4.5 Lightweight and Adaptable Security Mechanisms

Although privacy-preserving techniques such as secure aggregation and differential privacy have been proposed, they often incur high computational and communication overhead. Designing lightweight, adaptive, and resource-aware security mechanisms suitable for edge and fog environments remains a significant research challenge [5, 16, 30].

4.6 Handling Data and System Heterogeneity

Non-IID data distributions, device mobility, and hardware heterogeneity significantly degrade model performance in federated learning systems. Current approaches provide only partial solutions and lack robustness under extreme heterogeneity conditions [19, 18, 20].

5 Conclusion and Future Research Directions

This paper presented a comprehensive thematic review of federated learning over Edge–Fog–Cloud architectures for distributed intelligence. The review examined key architectural designs, resource management strategies, security mechanisms, and application-driven solutions that collectively support privacy-preserving and scalable intelligence at the network edge.The analysis indicates that federated learning significantly benefits from hierarchical Edge–Fog–Cloud infrastructures by enabling reduced latency, enhanced privacy preservation, and improved scalability. However, existing solutions are largely fragmented, predominantly experimental, and lack large-scale practical validation.

Future research should focus on developing standardized EFC-based federated learning frameworks, large-scale real-world deployments, and unified optimization strategies that jointly address communication efficiency, energy consumption, and computational constraints. Additionally, next-generation intelligent systems require adaptive security mechanisms and robust solutions to manage extreme device heterogeneity and mobility. Overall, federated learning over

Edge–Fog–Cloud architectures remains a promising yet evolving research domain with substantial opportunities for innovation in both theoretical modeling and practical system design.

References

1. Bao G, Guo P (2022) Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. *Journal of Cloud Computing* 11. https://doi.org/10.1186/s13677-022-00377-4
2. Perifanis NA, Kitsios F (2022) Edge and fog computing business value streams through IoT solutions: A literature review for strategic implementation. *Information* 13. https://doi.org/10.3390/info13090427
3. Yurdem B, Kuzlu M, Gullu MK, et al. (2024) Federated learning: Overview, strategies, applications, tools and future directions. *Heliyon* 10:e38137. https://doi.org/10.1016/j.heliyon.2024.e38137
4. Kale GS, Pervez MS, Gaikwad KM, et al. (2025) A federated learning approach to real-time AI-assisted laparoscopic surgery with privacy preservation. *Journal of Neonatal Surgery* 14:762–771. https://doi.org/10.52783/jns.v14.2751
5. Makris I, Karampasi A, Radoglou-Grammatikis P, et al. (2025) A comprehensive survey of federated intrusion detection systems: Techniques, challenges and solutions. *Computer Science Review* 56. https://doi.org/10.1016/j.cosrev.2024.100717
6. Hasan BT, Idrees AK (2024) Federated learning for IoT/edge/fog computing systems. In: *Federated Learning: Principles, Paradigms and Applications*, pp. 47–76. https://doi.org/10.1201/9781003497196-3
7. Grataloup A, Kurpicz-Briki M (2024) A systematic survey on the application of federated learning in mental state detection and human activity recognition. *Frontiers in Digital Health* 6:1–15. https://doi.org/10.3389/fdgth.2024.1495999
8. Saha R, Misra S, Deb PK (2021) FogFL: Fog-assisted federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal* 8:8456–8463. https://doi.org/10.1109/JIOT.2020.3046509
9. Wang Z, Goudarzi M, Gong M, Buyya R (2025) A knowledge distillation-empowered adaptive federated reinforcement learning framework for multi-domain IoT application scheduling.
10. Choppara P, Mangalampalli SS (2025) Adaptive task scheduling in fog computing using federated DQN and K-means clustering. *IEEE Access* 13:75462–75488. https://doi.org/10.1109/ACCESS.2025.3563487
11. Rajendran S, Obeid JS, Binol H, et al. (2020) Cloud-based federated learning implementation across medical centers. *JCO Clinical Cancer Informatics* 5:1–11. https://doi.org/10.1200/CCI.20
12. Tsai YH, Chang DM, Hsu TC (2022) Edge computing based on federated learning for machine monitoring. *Applied Sciences* 12. https://doi.org/10.3390/app12105178
13. Savoia M, Prezioso E, Mele V, Piccialli F (2024) Eco-FL: Enhancing federated learning sustainability in edge computing through energy-efficient client selection. *Computer Communications* 225:156–170. https://doi.org/10.1016/j.comcom.2024.07.014
14. Saha R, Misra S, Chakraborty A, et al. (2023) Data-centric client selection for federated learning over distributed edge networks. *IEEE Transactions on Parallel and Distributed Systems* 34:675–686. https://doi.org/10.1109/TPDS.2022.3217271

15. Kumar A, Srirama SN (2025) FedStrag: Straggler-aware federated learning for low resource devices. *Digital Communications and Networks* 11:1214–1224. https://doi.org/10.1016/j.dcan.2024.12.004
16. Zhang F, Zhang Y, Ji S, Han Z (2024) Secure and decentralized federated learning framework with non-IID data based on blockchain. *Heliyon* 10. https://doi.org/10.1016/j.heliyon.2024.e27176
17. Ayeelyan J, Utomo S, Rouniyar A, et al. (2025) Federated learning design and functional models: Survey. *Artificial Intelligence Review* 58. https://doi.org/10.1007/s10462-024-10969-y
18. Gao J, Li Y, Zhao Y, Campbell B (2024) H-FedSN: Personalized sparse networks for efficient and accurate hierarchical federated learning for IoT applications.
19. Lee S, Tavallaie O, Chen S, et al. (2025) Personalizing federated learning for hierarchical edge networks with non-IID data.
20. Cremonesi F, Planat V, Kalokyri V, et al. (2023) The need for multimodal health data modeling: A practical approach for a federated-learning healthcare platform. *Journal of Biomedical Informatics* 141. https://doi.org/10.1016/j.jbi.2023.104338
21. Tripathy SS, Bebortta S, Chowdhary CL, et al. (2024) FedHealthFog: A federated learning-enabled approach towards healthcare analytics over fog computing platform. *Heliyon* 10:e26416. https://doi.org/10.1016/j.heliyon.2024.e26416
22. Zwiers LC, Grobbee DE, Uijl A, Ong DSY (2024) Federated learning as a smart tool for research on infectious diseases. *BMC Infectious Diseases* 24. https://doi.org/10.1186/s12879-024-10230-5
23. Sadilek A, Liu L, Nguyen D, et al. (2021) Privacy-first health research with federated learning. *npj Digital Medicine* 4. https://doi.org/10.1038/s41746-021-00489-2
24. Rajagopal A, Redekop E, Kemisetti A, et al. (2023) Federated learning with research prototypes: Application to multi-center MRI-based detection of prostate cancer. *Academic Radiology* 30:644–657. https://doi.org/10.1016/j.acra.2023.02.012
25. Almogadwy B, Alqarafi A (2025) Fused federated learning framework for secure and decentralized patient monitoring in healthcare 5.0 using IoMT. *Scientific Reports* 15. https://doi.org/10.1038/s41598-025-06574-w
26. Sah DK, Vahabi M, Fotouhi H (2025) Federated learning at the edge in industrial Internet of Things: A review. *Sustainable Computing: Informatics and Systems* 46:101087. https://doi.org/10.1016/j.suscom.2025.101087
27. Wang S, Hosseinalipour S, Aggarwal V, et al. (2023) Toward cooperative federated learning over heterogeneous edge/fog networks. *IEEE Communications Magazine* 61:54–60. https://doi.org/10.1109/MCOM.005.2200925
28. Wang F, Wang K (2025) Federated learning-based trust and energy-aware routing in fog–cloud computing environments for IoT. *Scientific Reports* 16:1–28. https://doi.org/10.1038/s41598-025-32010-0
29. Hiremani V, Devadas RM, Preethi, et al. (2025) Federated learning for crop yield prediction: A comprehensive review of techniques and applications. *MethodsX* 14:103408. https://doi.org/10.1016/j.mex.2025.103408
30. Zhan S, Huang L, Luo G, et al. (2025) A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration.