STM JOURNALS

Current Trends in
Information Technology

https://journals.stmjournals.com/ctit

ISSN: 2249-4707 (Online)
ISSN: 2348-7895 (Print)
Volume 14, Issue 3, 2024
September–December
DOI (Journal): 10.37591/CTIT

Research CTIT

Federated Learning: A Comprehensive Review of Models, Algorithms, and Business Applications

Nagendra Pratap Singh[1,*], Mamata Singh[2]

Abstract

In an age where data privacy is a significant concern, federated learning (FL) has become a game-changing method in machine learning. This decentralized model enables various parties to work together on training models without exchanging their raw data, effectively tackling the issues posed by data silos and privacy regulations. This article explores the current state of FL, including its underlying models and algorithms, practical applications, benefits, challenges, and future directions. NVIDIA's Clara Train SDK plays a crucial role in FL. By synthesizing recent research findings, we aim to comprehensively understand FL's impact on various industries and its potential to drive innovation. The article highlights the FL process. The article explores the current landscape of FL across multiple business domains, addressing its benefits, challenges, and prospects, ultimately emphasizing its role in creating a more efficient and privacy-preserving healthcare ecosystem. FL represents a significant leap forward in collaborative innovation, allowing businesses to leverage collective intelligence while maintaining data privacy. This decentralized approach opens new opportunities across various sectors, driving significant value and enabling organizations to balance privacy with powerful insights. As research and development in this area progress, FL is set to become a fundamental pillar in the future evolution of machine learning.

Keywords: Federated learning (FL), artificial intelligence (AI), decentralized model, machine learning, data privacy, algorithms

INTRODUCTION

As artificial intelligence (AI) continues to evolve, the need for effective data utilization while maintaining privacy has become increasingly critical. Conventional machine learning methods typically rely on centralized data storage, which presents considerable risks to data privacy and security. Federated learning (FL), first proposed by Google in 2016, offers a solution by enabling decentralized model training across multiple clients while keeping their data localized [1]. This study explores the fundamentals of FL, its algorithms, and its applications across various sectors, highlighting its transformative potential in data-driven decision making. The data-driven decision-making process is illustrated in Figure 1.

***Author for Correspondence**
Nagendra Pratap Singh
E-mail: nagendra.singh4565@gmail.com

[1]Associate Dean-Research, Department of Techno Centre Engineering, MS Ramaiah University of Applied Sciences, Bangalore, India
[2]Visiting Senior Scientist, Department of Medicine, Division of Infectious Disease, Mayo Clinic, Jacksonville, Florida, USA

Received Date: August 05, 2024
Accepted Date: August 28, 2024
Published Date: September 11, 2024

Citation: Nagendra Pratap Singh, Mamata Singh. Federated Learning: A Comprehensive Review of Models, Algorithms, and Business Applications. Current Trends in Information Technology. 2024; 14(3): 1–9p.

NVIDIA's Clara Train SDK integrates Federated Learning (FL), which is a groundbreaking approach that enables secure collaboration among healthcare institutions without compromising patient privacy. This method allows hospitals to train AI models on local data while only sharing model updates, thereby protecting sensitive information [2–4]. The server-client architecture facilitates efficient training, where a centralized server aggregates contributions from various clients, as shown in Figure 2.

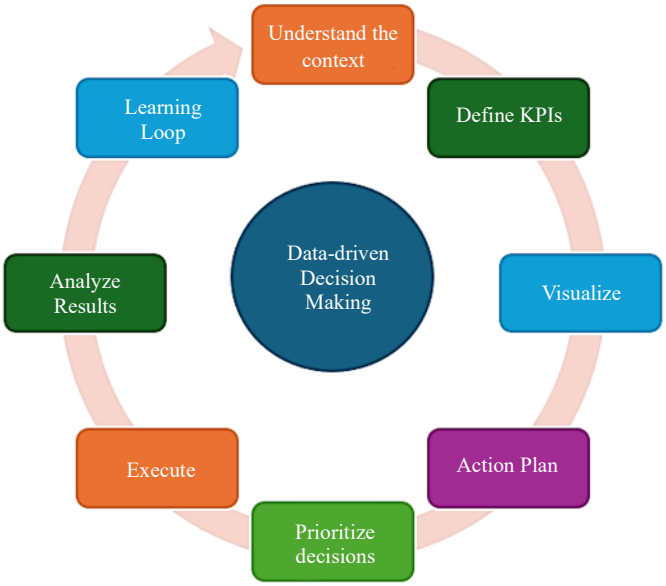

Figure 1. Data-driven decision making.

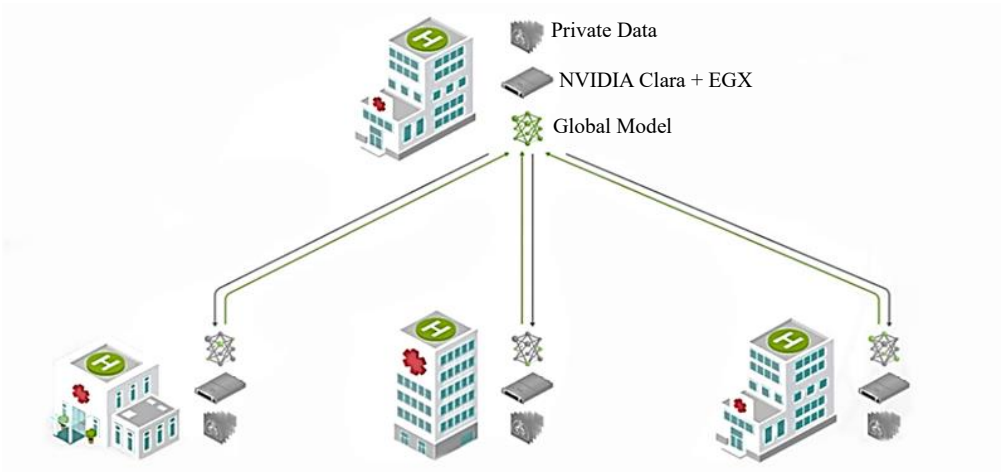

Figure 2. Federated learning: training AI models across multiple hospitals while keeping patient data private [5].

This innovative solution not only enhances model accuracy but also ensures compliance with privacy regulations, making it a significant advancement in medical AI [6, 7].

WHAT IS FEDERATED LEARNING?

Federated learning is a decentralized machine learning approach in which multiple clients (such as devices or organizations) collaborate on a shared model while maintaining control over their local data. Rather than sending sensitive data to a central server, each client trains a model locally and shares only model updates with the server. The central server then aggregates these updates to create a global model, leveraging the diversity of data sources while preserving data privacy and security [8].

The Federated Learning Process

The FL process can be summarized in the following steps:

1. *Model initialization:* A central server initializes the base model and distributes it to all participating clients.
2. *Local training:* Each client trains the model locally using its data that may contain sensitive information.

3. *Model update sharing:* After local training, clients send their model updates (not raw data) to the central server using secure communication channels.
4. *Aggregation:* The central server combines updates from all clients to enhance the global model, typically by averaging the model parameters.
5. *Iteration:* The improved global model is then sent back to the clients for additional local training, continuing the cycle to further increase the accuracy of the model.

This repetitive process enables the ongoing enhancement of the model, gradually increasing its accuracy and reliability over time while preserving data privacy [5].

ALGORITHMS USED IN FEDERATED LEARNING

Several algorithms are commonly employed in federated learning, each of which addresses specific challenges associated with decentralized training.

Federated Averaging (FedAvg)

This foundational algorithm averages the model updates received from clients to update the global model [1]. Federated Averaging (FedAvg) is a machine learning technique that enhances privacy and efficiency by training models across multiple clients while maintaining data on local devices. Here is how it works: The central server sends a global model to clients, who then train it on their data. Once completed, they sent the updated model parameters are sent back to the server. The server averages these updates to create a new global model. This process is repeated until the model converges, thereby reducing communication costs and ensuring that data remains private on local devices [9].

FedDyn

This algorithm adapts the regularization term for local losses based on the data statistics of each client, thereby minimizing global loss more effectively [10]. FedDyn is an innovative federated learning algorithm that enhances training efficiency by dynamically aligning local device solutions with a global solution. It can effectively manage device heterogeneity, partial participation, and unbalanced data. The key features of this algorithm are shown in Figure 3.

However, FedDyn is prone to training instability without additional techniques such as gradient clipping. In summary, FedDyn is a state-of-the-art federated learning algorithm that offers high accuracy and robust performance. However, it requires more computational resources and may face stability issues in certain scenarios [11].

Secure Aggregation

Techniques are implemented to ensure that model updates are aggregated securely, preventing data leakage during communication [12]. Secure aggregation utilizes cryptographic methods to securely combine model updates from various clients, as shown in Figure 4.

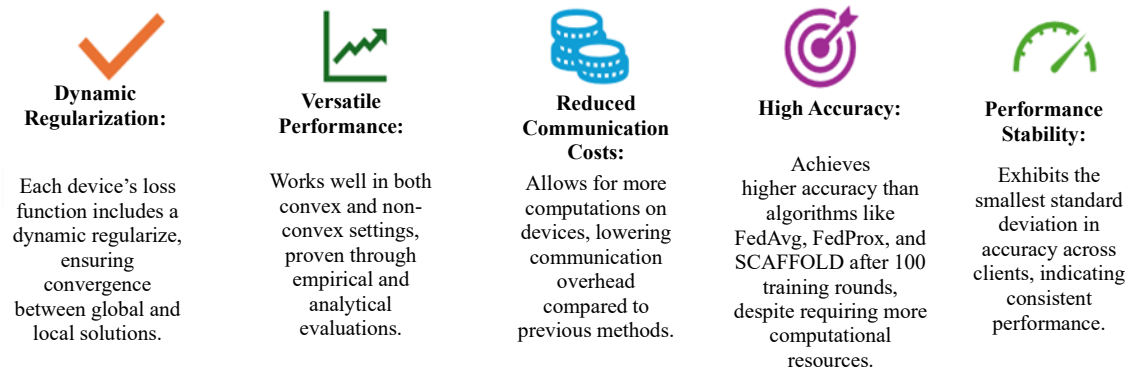

Figure 3. Key features of the FedDyn.

The primary goal is to compute a global model update based on local updates while ensuring that no individual client data are exposed during the aggregation process. This is especially crucial in federated learning contexts where data privacy is critical, such as healthcare or personal finance applications. Implementing secure aggregation in federated learning presents several challenges including client dynamics and scalability.

Personalized Federated Learning

This approach tailors the global model to better fit individual clients by allowing some degree of personalization based on local data characteristics [13]. The benefits of personalized FL are shown in Figure 5.

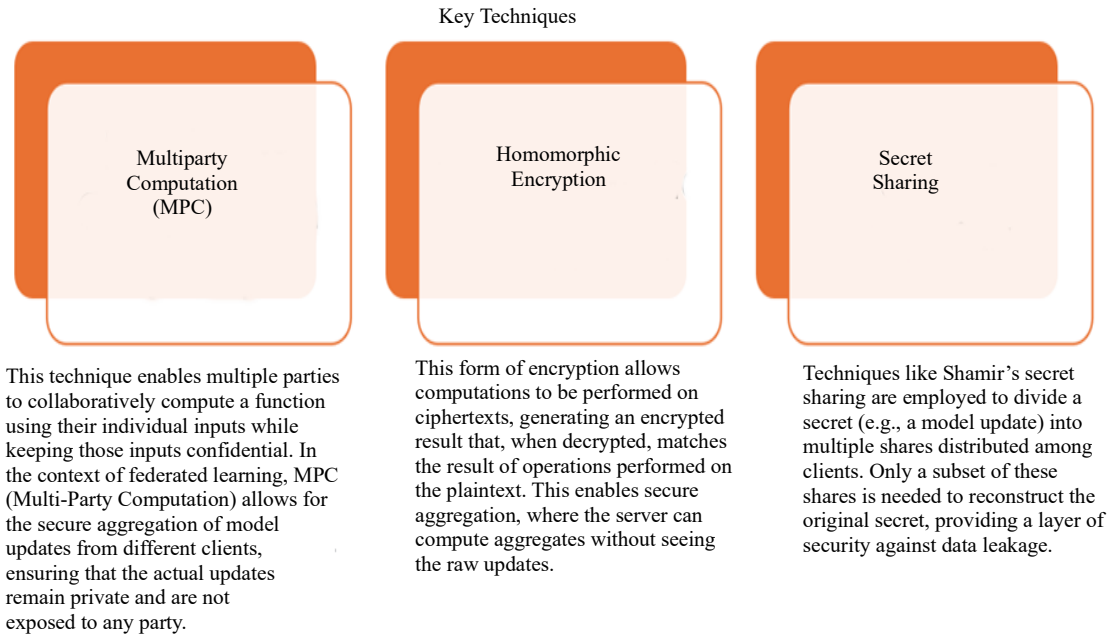

Figure 4. Key secure aggregation techniques.

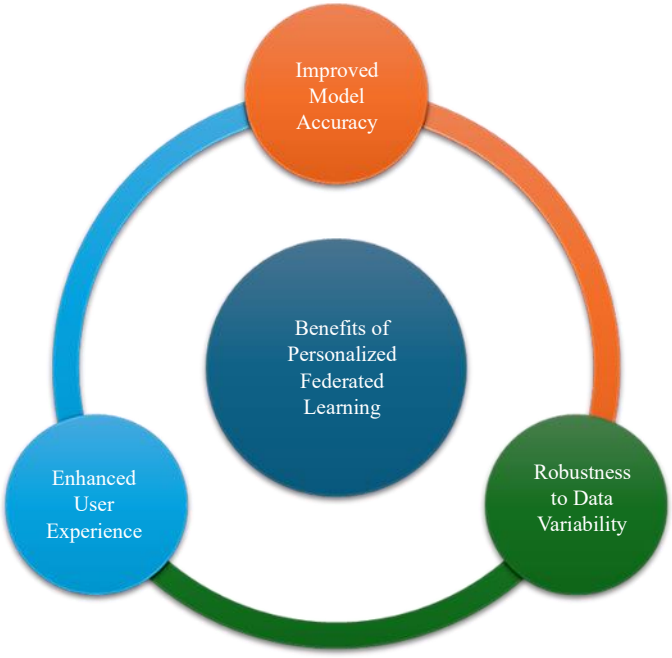

Figure 5. Benefits of personalized FL

APPLICATIONS OF FEDERATED LEARNING

Federated learning has found applications across various sectors by leveraging unique capabilities to enhance data privacy and collaboration.

Healthcare

In healthcare, FL enables collaborative research, while preserving patient confidentiality. For instance, hospitals can jointly train models for disease prediction without sharing sensitive patient data [14]. This collaborative method may result in better patient outcomes and more effective treatment strategies. The primary application of FL is illustrated in Figure 6.

Federated learning transforms healthcare by facilitating collaborative machine learning while safeguarding patient privacy. In conventional healthcare systems, sharing data between institutions carries substantial risks such as breaches of sensitive information. FL addresses these issues by enabling hospitals and medical facilities to develop AI models using local data, without sending it to a central server. This decentralized method ensures adherence to regulations such as HIPAA and improves data security. Recent studies have highlighted FL's applications of FL in various healthcare domains, such as remote patient monitoring, biomedical image analysis, and identification of COVID-19 traits, showing its potential to improve diagnostic accuracy and treatment personalization [15].

Moreover, FL facilitates the integration of artificial intelligence into healthcare, which can lead to innovative solutions to complex medical challenges. By aggregating model updates from multiple sources, FL creates a robust global model while maintaining the confidentiality of individual datasets.

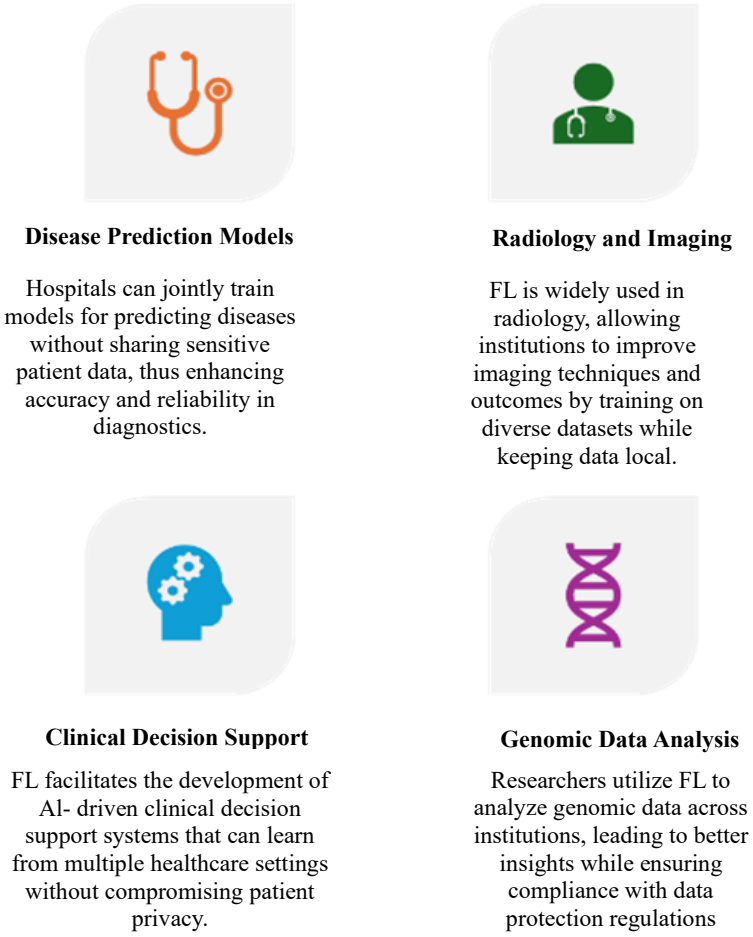

Figure 6. Key applications of FL in healthcare.

Finance

In the financial sector, FL can facilitate joint fraud detection and risk assessment, without exposing sensitive customer information. By collaborating in model training, financial institutions can enhance their ability to detect fraudulent activities while maintaining compliance with data protection regulations [7].

Internet of Things (IoT)

FL is particularly well-suited for IoT applications, where devices can learn from local data to optimize performance and enhance security. For example, smart home devices can collaboratively improve their predictive capabilities without compromising user privacy [16].

Smart Cities

In smart city initiatives, FL can enable various stakeholders to collaborate on urban planning and resource management, while protecting citizen data. By aggregating insights from multiple sources, cities can make informed decisions that enhance the quality of life [17].

BENEFITS OF FEDERATED LEARNING

Federated learning provides multiple benefits compared to traditional centralized machine learning methods:

1. *Enhanced data privacy:* Raw data remains local, ensuring confidentiality and compliance with regulations [8].
2. *Reduced data transmission costs:* Minimizing data sharing decreases bandwidth requirements, making FL more efficient [5].
3. *Increased model accuracy:* Collective knowledge from diverse data sources enhances predictive capabilities [1].
4. *Improved collaboration:* FL facilitates seamless partnerships and accelerates innovation across sectors [10].

Challenges and Future Directions

Despite its promise, federated learning faces several challenges that must be addressed before its widespread adoption.

Communication Overhead

The communication overhead associated with exchanging model updates can be significant, particularly when the number of clients increases. Optimizing data exchange to minimize latency is crucial for improving the efficiency of FL systems [5].

Data Heterogeneity

Data heterogeneity among clients can lead to model drifts and reduced accuracy. Addressing variations in data formats, quality, and distribution is essential for effective collaboration [8].

Model Convergence

Ensuring that the global model is accurate, stable, and reliable remains a challenge. Research into algorithms that can enhance model convergence is ongoing [1].

Security and Trust

Establishing robust safeguards and fostering trust among collaborators is vital for successful implementation. As FL systems become more prevalent, addressing security threats, and ensuring data integrity will become paramount [5].

PRIVACY AND SECURITY CHALLENGES IN FEDERATED LEARNING

Although federated learning is a promising framework for privacy-preserving machine learning, it has its own set of challenges. The security of FL systems is of paramount importance because

vulnerabilities can expose sensitive data and undermine trust among participants. Several key challenges include the following.

Privacy Threats

Despite the inherent privacy protection offered by FL, there are still risks associated with parameter leakage and malicious attacks. Research has shown that even encrypted model updates can potentially reveal sensitive information about underlying data [18]. Differential privacy techniques have been proposed to mitigate these risks by adding noise to model updates, thereby obscuring individual contributions while maintaining overall model accuracy.

Communication Overhead

The communication overhead in FL can be substantial, particularly when many clients are involved. This overhead can exceed the computational costs associated with the local training, leading to the system [5]. Strategies to compress model updates and reduce communication frequency are essential for enhancing the practicality of FL.

Heterogeneity of Data

Data heterogeneity among clients is a major challenge. Variations in data distribution can lead to global model drift, where the aggregated model becomes less representative of the underlying data [8]. Techniques, such as personalized federated learning, aim to address this issue by allowing individual clients to adapt the global model to better fit their local data.

Security Mechanisms

To address these challenges, various security mechanisms have been developed. These include secure multiparty computation (SMC), homomorphic encryption, and differential privacy [15]. Each of these techniques offers unique advantages and trade-offs in terms of computational overhead and security guarantees.

FUTURE DIRECTIONS FOR FEDERATED LEARNING

As federated learning continues to evolve, several future directions warrant exploration:

Improved Algorithms

There is a need to develop more efficient algorithms that can address issues related to communication overhead, data diversity, and model convergence more effectively. Research into adaptive learning rates and dynamic aggregation strategies may enhance the performance of FL systems [1].

Broader Applications

Extending the use of FL to emerging fields such as autonomous vehicles, smart manufacturing, and environmental monitoring could generate substantial benefits. Tailoring FL techniques to meet the specific needs of these industries is essential for successful implementation.

Enhanced Security Measures

As the threat landscape continues to evolve, research on robust security measures is critical. Developing techniques that can withstand sophisticated attacks while maintaining usability is of paramount importance for the widespread adoption of FL [18].

Interdisciplinary Collaboration

Collaboration among researchers in machine learning, cybersecurity, and privacy law is essential to address the multifaceted challenges of FL. By leveraging insights from diverse fields, comprehensive solutions that balance performance, privacy, and security can be developed.

CONCLUSION

Federated learning represents a significant advancement in collaborative innovation, enabling businesses to harness the power of collective knowledge while safeguarding sensitive information. By facilitating decentralized model training, FL unlocks new business opportunities and drives unprecedented value across various sectors. As organizations such as Google demonstrate, the potential applications of federated learning are vast, paving the way for a future in which data privacy and collaborative intelligence coexist harmoniously. Ongoing research and development in this area are crucial for addressing current challenges and fully harnessing the potential of federated learning.

REFERENCES

1. Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, et al. Advances and open problems in federated learning. Found Trends® Mach Learn. 2019;4(1). DOI: 10.48550/arXiv.1912.04977.
2. Jacobs J, Van Moll J, Krause P, Kusters R, Trienekens J, Brombacher A. Exploring defect causes in products developed by virtual teams. Inf Softw Technol. 2005;47:399–410. DOI: 10.1016/j.infsof.2004.09.006.
3. Altun A. Understanding hypertext in the context of reading on the web: Language learners' experience. Curr Issues Educ. 2003;6(12):1-15. Available from: https://cie.asu.edu/ojs/index.php/cieatasu/article/view/1685.
4. Hoffman M, Blake J. Computer literacy: Today and tomorrow. J Comput Sci Coll. 2003;18:221–33.
5. Wen Y, Li W, Roth H, Dogra P. (2019). Federated Learning powered by NVIDIA Clara. [online] NVIDIA Technical Blog. Available from: https://developer.nvidia.com/blog/federated-learning-clara/.
6. Li W, Milletarì F, Xu D, Rieke N, Hancox J, Zhu W, Baust M, Cheng Y, Ourselin S, Cardoso MJ, Feng A. Privacy-preserving federated brain tumour segmentation. In: Machine Learning in Medical Imaging [10th international workshop]. Proceedings of the 10, MLMI 2019, Held in Conjunction with MICCAI, Vol. 13, 2019. October: Shenzhen, China. Springer International Publishing, pp. 133–141.
7. NVIDIA developer blog (2021). Using Federated Learning to Bridge Data Silos in Financial Services. [online] Available from: https://developer.nvidia.com/blog/using-federated-learning-to-bridge-data-silos-in-financial-services/.
8. Sun C, Duan X, Qiu L, Shi Q, Li T. RLIM: Representation learning method for influence maximization in social networks. Int J Mach Learn Cybern. 2022;13:3425–40. DOI: 10.1007/s13042-022-01605-8.
9. Sun T, Li D, Wang B. Decentralized federated averaging. IEEE Trans Pattern Anal Mach Intell. 2023;45:4289–301. DOI: 10.1109/TPAMI.2022.3196503. PubMed: 35925850.
10. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated learning aggregation algorithms; strategies, contributions, limitations, and future perspectives. Electronics. 2023;12:2287. DOI: 10.3390/electronics12102287.
11. Acar DA, Zhao Y, Navarro RM, Mattina M, Whatmough PN, Saligrama V. Federated learning based on dynamic regularization. [Preprint]. ArXiv:2111.04263 (2021 Nov 8). DOI: 10.48550/arXiv.2111.04263.
12. Bonawitz K. Towards Federated Learning at Scale: System Design. [Preprint]. ArXiv:1902.01046 (2019). DOI: 10.48550/arXiv.1902.01046.
13. Fallah A, Mokhtari A, Ozdaglar A. Personalized federated learning: A meta-learning approach. arXiv Preprint ArXiv:2002.07948 (2020 Feb 19). DOI: 10.48550/arXiv.2002.07948.
14. Sheller MJ, Edwards B, Reina GA, Martin J, Pati S, Kotrotsou A, et al. Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. Sci Rep. 2020;10:12598. DOI: 10.1038/s41598-020-69250-1. PubMed: 32724046.

15. Rahman A, Hossain MS, Muhammad G, Kundu D, Debnath T, Rahman M, et al. Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. Cluster Comput. 2022;1–41. DOI: 10.1007/s10586-022-03658-4. PubMed: 35996680.
16. Yang A, Ma Z, Zhang C, Han Y, Hu Z, Zhang W, et al. Review on application progress of federated learning model and security hazard protection. Digit Commun Netw. 2023;9:146–58. DOI: 10.1016/j.dcan.2022.11.006.
17. Zhang C, Xie Y, Bai H, Yu B, Li W, Gao Y. A survey on federated learning. Knowl Based Syst. 2021;216:106775. DOI: 10.1016/j.knosys.2021.106775.
18. Wen J, Zhang Z, Lan Y, Cui Z, Cai J, Zhang W. A survey on federated learning: Challenges and applications. Int J Mach Learn Cybern. 2023;14:513–35. DOI: 10.1007/s13042-022-01647-y. PubMed: 36407495.

