Research Article

Review on Aggregation Frameworks For High-Performance Federated Learning

Dr. Anil Wanare[1*] , Ir.Dr. Pankaj Agarka[2] , Dr. Hemant A Wani[3] , Dr. Yogita D Kapse[4]

[1]Professor, E&TC Dept. JSPM's BSIOTR,SPPU, Pune. Eudoxia Research Centre, Guwahati, India. Email : anillaxman369@gmail.com
[2]Head of dept Computer Engineering, Lohegaon, Pune. Email : pmagarkar@gmail.com
[3]Associate Professor, E&TC Engg, JSPMs BSIoTR, Wagholi, Pune. Email : hawani_entc@jspmbsiotr.edu.in
[4]Assistant Professor, COEP Tech Univ Pune. Email : ydk.extc@coeptech.ac.in

Abstract:

Federated Learning (FL) enables collaborative model training across distributed clients while keeping their original data within local environments, thereby reducing the need for centralized data collection. Despite this advantage, the effectiveness of FL strongly depends on model aggregation, which determines how locally trained updates contribute to the global model. Conventional aggregation methods, particularly uniform or data-size-based averaging, may become ineffective when clients exhibit non-IID data distributions, class imbalance, unequal participation, device heterogeneity, client drift, variable update quality, and unreliable behaviour. This paper presents a systematic investigation of model aggregation strategies and organizes existing approaches into synchronous, asynchronous, hierarchical, adaptive, personalized, and robust aggregation frameworks. Their operating principles, advantages, limitations, and suitability for heterogeneous federated environments are comparatively examined. Particular emphasis is placed on aggregation mechanisms that account for local model performance, training loss, convergence behaviour, data contribution, statistical heterogeneity, and update quality when determining the influence of participating clients. The analysis reveals that fixed aggregation rules cannot adequately accommodate dynamically changing client and data characteristics. Accordingly, this work establishes the research direction toward an adaptive weighted aggregation framework in which client contributions are dynamically adjusted using multiple performance-related indicators. Such an approach is expected to improve global accuracy, convergence stability, fairness, minority-class representation, and robustness to low-quality updates, while retaining the privacy-preserving characteristics of FL. The study provides a foundation for developing reliable and scalable aggregation mechanisms for distributed applications including healthcare, intelligent transportation, smart cities, industrial systems, IoT, and next-generation communication networks.

Keywords: Federated Learning, Model Aggregation, Adaptive Aggregation, Non-IID Data, Class Imbalance, Client Heterogeneity, Personalized Federated Learning, Robust Aggregation.

Introduction

Machine Learning (ML) has become an important computational approach for extracting meaningful knowledge from complex data and supporting intelligent decision-making across domains such as healthcare, finance, business, transportation, and industrial applications [1]. Its ability to identify complex and nonlinear relationships has contributed significantly to the development of data-driven systems. However, conventional ML generally requires data from different sources to be collected and processed at centralized locations. Such centralized architectures introduce concerns related to privacy, security, confidentiality, data ownership, and unauthorized access, particularly when personal or proprietary information is involved [2]. These limitations have encouraged the development of distributed learning approaches in which useful models can be trained without directly centralizing the underlying data.

Federated Learning (FL) provides such a distributed learning paradigm by enabling multiple clients to collaboratively develop a shared model while retaining their original datasets within their local environments. The foundational FL framework was introduced by Google researchers to facilitate decentralized model training with improved communication efficiency [3]. Since then, FL has developed into an important privacy-oriented machine-learning approach. Different architectures have subsequently emerged, including decentralized FL [4] and blockchain-enabled FL [5]. Nevertheless, the conventional server–client architecture remains widely adopted, where a coordinating server manages the learning process and participating clients may represent mobile devices, IoT nodes, computers, edge devices, organizations, or institutions.

A typical FL process is performed through a sequence of communication rounds. At the beginning of each round, the server distributes the current global model to selected clients. Each client trains the received model using its locally available data and generates updated model parameters or gradients. These updates, rather than the original training data, are transmitted to the coordinating server. The server then performs model aggregation to combine the participating clients' updates and construct an improved global model. The

resulting model is redistributed for the subsequent training round, and this iterative procedure continues until the required convergence or termination criterion is achieved.

Although FL reduces the requirement for centralized data collection, its distributed architecture introduces several challenges. One of the most significant is statistical heterogeneity, where client datasets may follow different distributions rather than the conventional independent and identically distributed (IID) assumption [6]. Such non-IID data can cause inconsistent local updates, client drift, reduced global accuracy, and slower or unstable convergence [7]. In addition, device heterogeneity results from differences in computational capability, storage, communication bandwidth, energy availability, and network conditions among participating clients. These variations can produce unequal participation and delays during collaborative training. FL has also gained considerable importance in edge-computing environments [8], where increasing computational capabilities of mobile phones, wearable devices, IoT nodes, drones, and autonomous systems enable learning closer to the data source [9]. Integrating FL with edge computing allows data to remain at distributed devices while locally trained model updates are collaboratively aggregated. This architecture provides an effective mechanism for coordinating large numbers of geographically distributed devices while reducing direct movement of sensitive data. Despite these advantages, the effectiveness of FL is strongly influenced by the mechanism used to combine local updates. Model aggregation therefore represents a central component of the federated learning process, directly affecting global-model accuracy, convergence, fairness, communication efficiency, and robustness. Conventional averaging strategies may not adequately represent individual client contributions when clients differ substantially in data distribution, class balance, data quality, computational capability, or local training behaviour. Consequently, the development of adaptive and intelligent aggregation mechanisms that evaluate client-specific characteristics before determining aggregation weights represents an important research direction. This work therefore investigates model aggregation strategies with particular emphasis on mechanisms capable of adapting to non-IID data, class imbalance, client heterogeneity, convergence behaviour, data contribution, update quality, and unreliable client participation, providing a foundation for more accurate, stable, fair, and robust Federated Learning systems. Existing research has explored FL across healthcare [10], intelligent transportation [11], wireless networks [12], and IoT [13], along with large-scale federated systems [14]. Studies have also addressed data heterogeneity [15], model aggregation [16], and practical applications [17]. Following the introduction of FedAvg [18], model aggregation became a significant research area. However, existing surveys [19], [20] provide limited aggregation-focused coverage. Therefore, this study systematically reviews model aggregation methods from 2017–2023 and develops a structured taxonomy of synchronous, asynchronous, hierarchical, adaptive, personalized, and robust aggregation, while identifying key challenges, research gaps, and future directions. The study is guided by six research questions focusing on existing FL model aggregation methods and their advantages and limitations, the influence of ML/DL algorithms on aggregation, systematic taxonomy of aggregation techniques, major publication venues, application domains and domain-specific aggregation requirements, and key challenges encountered during the model aggregation process.

Research methodology: To evaluate the applications and impact of aggregation methods in Federated Learning (FL), a systematic literature review (SLR) was conducted using a scientific, transparent, and reproducible approach [30]. The review followed the guidelines proposed by Siddaway et al. [18] and the PRISMA framework by Moher et al. [30]. The SLR process involved formulating research questions, defining inclusion and exclusion criteria, conducting the literature search, screening relevant studies, extracting data, assessing study quality, synthesizing the findings, and reporting the results. PRISMA guidelines were further used to ensure systematic and transparent reporting of the review process. The predefined research questions guided the overall review, while the search strategy and selection criteria were applied to identify studies relevant to FL model aggregation.

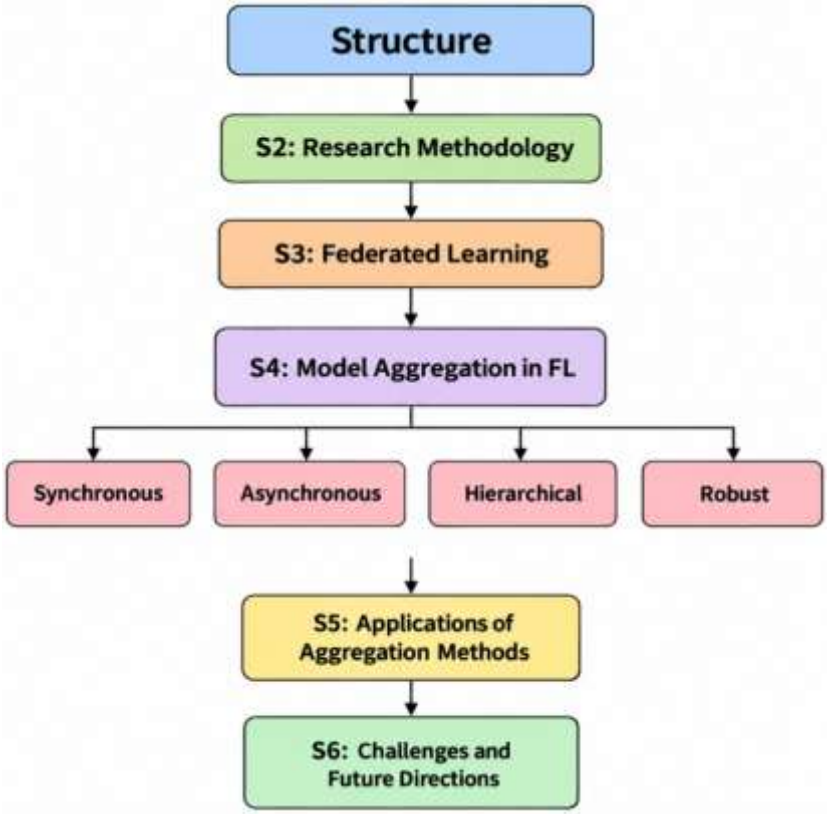

Fig. 1. The survey presents the research methodology, FL aggregation fundamentals, a comprehensive taxonomy of aggregation methods, their applications across diverse data and scenarios, and future research directions.

Federated learning: This section provides a brief overview of Federated Learning (FL), focusing on its fundamental principles, key characteristics, and major categories. Principles of Federated Learning. Federated Learning (FL) is a distributed machine learning approach in which N clients $\{C_1, C_2, \ldots, C_n\}$ collaboratively train a global model while keeping their local datasets $\{D_1, D_2, \ldots, D_n\}$ decentralized. The FL process consists of three main steps: (1) Initialization, where clients receive the current global model w^t from the server; (2) Local Training, where each client C_k trains the model using its private dataset D_k to obtain an updated local model w_k^{t+1}; and (3) Model Aggregation, where the server combines the received local models using an aggregation function, $global^{t+1} = Agg(w_k^{t+1})$. This iterative process enables collaborative model development without directly sharing raw client data, thereby supporting data privacy and decentralized learning.

Literature Review

Federated Learning (FL) has emerged as an effective privacy-preserving distributed machine-learning paradigm, enabling multiple clients to collaboratively train a shared model without transferring raw data to a central server. Earlier studies by Jordan and Mitchell and Paleyes et al. discussed the expanding role of machine learning and the practical difficulties of deploying scalable, reliable, and continuously monitored ML systems in real-world environments [1],[2]. These concerns are particularly significant in FL because training occurs across geographically distributed, resource-constrained, and heterogeneous devices. Communication efficiency is a fundamental issue in FL. Konečný et al. proposed compression and structured-update techniques to reduce communication overhead, whereas McMahan et al. introduced Federated Averaging (FedAvg), which aggregates local models according to client data size and reduces the number of communication rounds [3], [16]. Bonawitz et al. further examined the practical requirements of large-scale FL deployment, including client availability, fault tolerance; secure aggregation, and communication management [12]. For decentralized environments, Pappas et al. proposed IPLS, which removes dependence on a central aggregation server and enables peer-to-peer model exchange and aggregation [4]. Data and system heterogeneity remain major barriers to reliable FL performance. Li et al. proposed FedProx, which incorporates a proximal regularization term to improve convergence when clients have non-IID data and unequal computational capabilities [5]. Sattler et al. introduced a communication-efficient and robust approach based on update compression and

client selection for heterogeneous settings [13]. Zhu et al. classified different forms of non-IID data and analysed their effect on client drift and aggregation performance [21]. Similarly, Kulkarni et al. reviewed personalized FL approaches designed for scenarios in which a single global model may not perform equally well for all clients [20]. Recent studies have increasingly focused on adaptive and contribution-aware aggregation. Liu et al. proposed Projected Federated Averaging for heterogeneous differential privacy, while Bai et al. introduced FedEWA using elastic weighted averaging [28]. Deng et al. developed FAIR by combining update quality, user incentives, and aggregation, whereas Hong et al. used example-forgetting events to address label-imbalanced non-IID data. Ye et al. proposed FedDisco for discrepancy-aware collaboration, and Tang et al. employed local Shapley values to estimate the contribution of each client. These approaches indicate that performance-aware, fairness-oriented, privacy-aware, and contribution-driven weighting can improve global-model quality under heterogeneous conditions. However, an integrated aggregation framework that simultaneously considers class imbalance, convergence behaviour, privacy, fairness, unreliable clients, and malicious updates is still needed. Security and privacy are equally important in FL because local model updates may reveal sensitive information or be manipulated by adversarial participants. Mothukuri et al. reviewed attacks such as model poisoning, inference attacks, backdoor attacks, and Sybil attacks, along with their defence mechanisms [18]. Yin et al. presented a taxonomy of privacy-preserving FL mechanisms, including differential privacy, homomorphic encryption, and secure aggregation [19]. Kumar et al. combined blockchain and homomorphic encryption for privacy-preserving aggregation in medical-image applications, while Ji et al. proposed LAFED, a lightweight authentication mechanism for blockchain-enabled FL [8], [4]. These works demonstrate the importance of secure and trustworthy aggregation, although security mechanisms may increase computational and communication costs. FL has also been widely applied in edge computing, IoT, healthcare, wireless networks, and intelligent transportation systems. Shi et al. established the fundamental vision of edge computing and identified challenges related to communication, computation, resource management, and security [6]. Lim et al. surveyed FL in mobile-edge networks, while Nguyen et al. reviewed FL applications in IoT systems [7], [11]. In healthcare, Xu et al. and Nguyen et al. discussed privacy-preserving collaborative learning, clinical applications, healthcare datasets, and deployment challenges [15], [23]. Wang et al. proposed vehicle selection and resource allocation for FL in the Internet of Vehicles, whereas Chen et al. investigated in-network aggregation in multihop wireless networks to reduce latency and transmission overhead [9], [10].

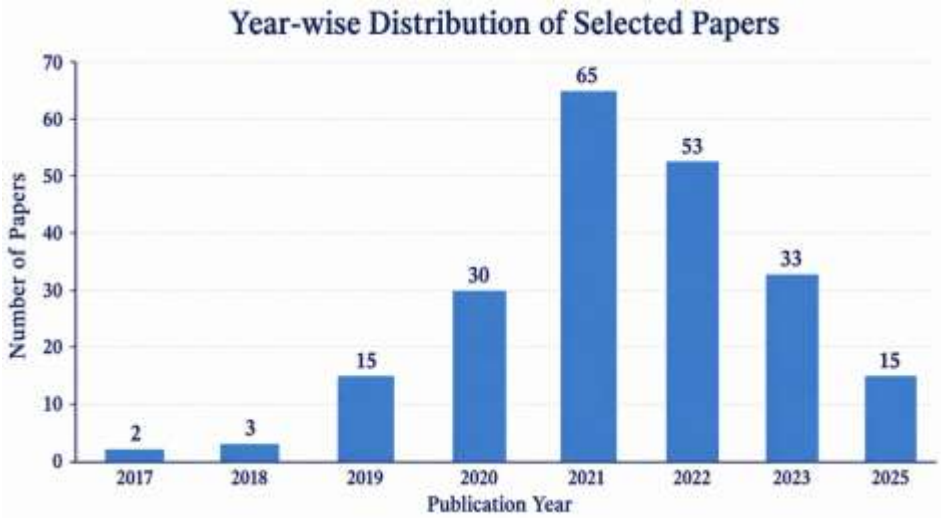

Fig. 2. Year-wise distribution of papers on the subject area of model aggregation in FL.

Although existing surveys examine FL architectures, privacy, security, communication efficiency, applications, and individual aggregation methods, limited work provides an integrated taxonomy specifically focused on model aggregation. Therefore, this survey systematically reviews and classifies FL aggregation methods, analyses the impact of heterogeneity and domain-specific requirements, and identifies challenges related to communication, privacy, security, robustness, and adaptability.

Methodology / Proposed Approach

At communication round t, the central server maintains the current global model w^t and distributes it to the selected participating clients: $w_k^t \leftarrow w^t$, $k \in S_t$. Each selected client independently trains the received model using its private dataset. For a learning rate η, a gradient-based local update can be expressed as:
$w_k^{t+1} = w_k^t - \eta \nabla F_k(w_k^t)$.
After one or more local training epochs, each client sends only its updated model parameters or model update to the server; the underlying raw data remain local. The server combines the received client models using an aggregation function Agg(·) to construct the next global model:
$w^{t+1} = Agg(\{w_k^{t+1} \mid k \in S_t\})$
For the conventional FedAvg method, aggregation is commonly represented as:
$w^{t+1} = \Sigma_{k \in S_t} (n_k / \Sigma_{j \in S_t} n_j) w_k^{t+1}$
Through repeated communication rounds, the global model progressively learns from distributed client knowledge without requiring centralized collection of raw data. This makes FL particularly suitable for privacy-sensitive and geographically distributed applications. The aggregation strategy is therefore a critical component of FL because it determines how individual client contributions influence the global model.

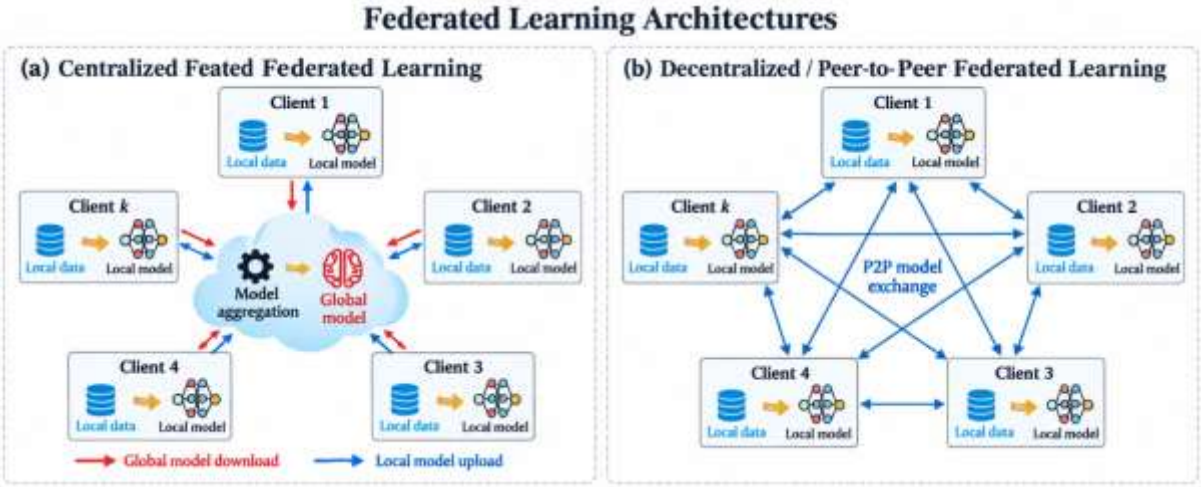

Fig. 3. Primary FL network structures: (a) **Centralized FL** uses a central server for model aggregation and synchronization in a star topology. (b) **Decentralized FL** enables direct peer-to-peer (P2P) communication among clients without a central server, forming a mesh topology and improving resilience to server failures and communication disruptions.

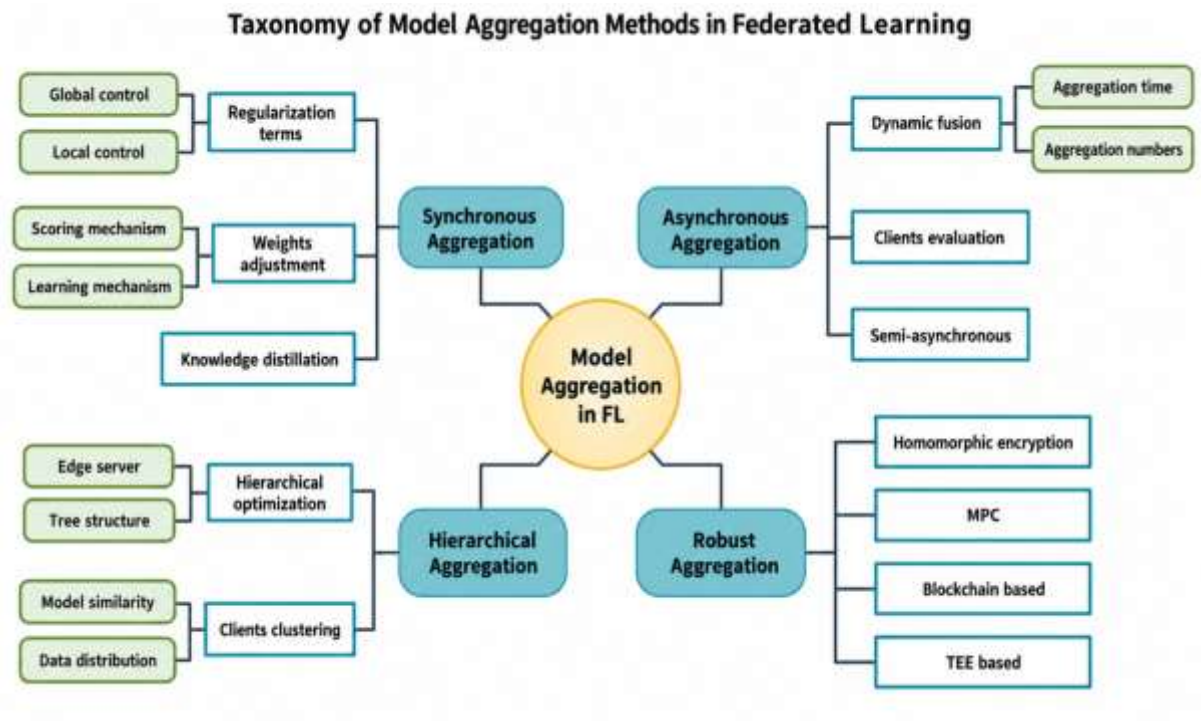

Fig. 3. Proposed taxonomy of model aggregation techniques in Federated Learning

Results and Discussion

Horizontal Federated Learning (HFL), also known as sample-based FL, is applied when participating clients have the same feature space but different samples. In this setting, clients store data with similar attributes collected from different individuals, institutions, or geographical locations, as shown in Fig. 4(a).

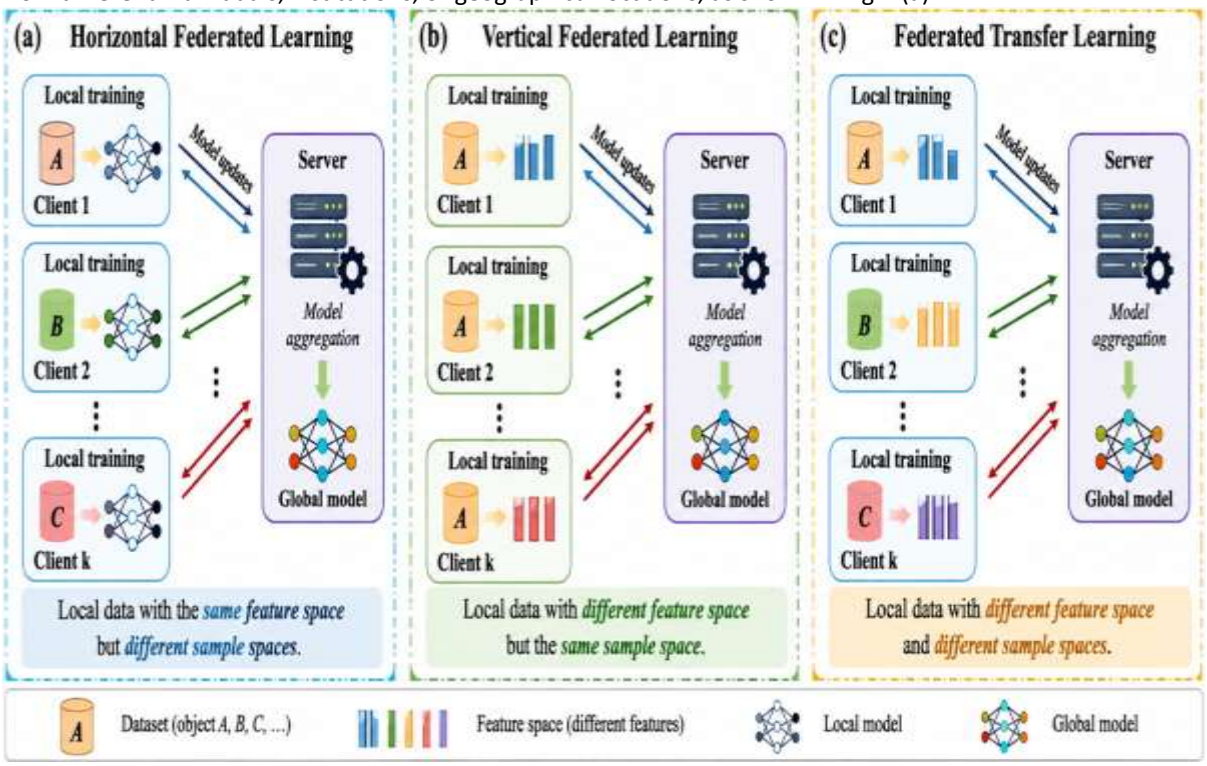

Fig. 4. Data partition in FL: (a) Horizontal FL, (b) Vertical FL and (c) Federated transfer learning.

For example, multiple hospitals may collaboratively train a COVID-19 detection model using chest CT images from different patients while retaining a common set of imaging features. Vertical Federated Learning (VFL), or feature-based FL, is suitable when clients have overlapping samples but different feature spaces. Different organizations may possess complementary attributes about the same users; therefore, VFL aligns common entities and enables collaborative training without sharing raw data, as illustrated in Fig. 4(b). It is useful in customer analysis, personalized recommendation, and financial services. Federated Transfer Learning (FTL) is designed for situations in which clients differ in both sample space and feature space, as shown in Fig. 4(c). It uses transfer-learning techniques to share useful knowledge across heterogeneous datasets while preserving local-data privacy. For instance, FedHealth applies FTL to adapt a reference model to wearable healthcare data and develop personalized client models.

Model aggregation is a central process in Federated Learning that combines information generated by participating clients during each communication round to update the global model. Instead of transferring raw data, clients share model-related information, thereby maintaining data privacy and confidentiality. Aggregation may be parameter-based, where local model weights, gradients, or parameter updates are combined at the server [29], [30], or output-based, where compact outputs such as logits, predictions, embeddings, sketches, or binary masks are combined . For example, FedMask [28] aggregates locally learned binary masks rather than complete model parameters, reducing communication and computational overhead.

Based on the aggregation architecture, FL can be categorized as centralized or decentralized. In centralized FL, a server collects locally trained model updates, aggregates them to construct an updated global model, and redistributes the model to clients for subsequent training rounds. Although this approach supports efficient coordination and synchronization, it can introduce communication bottlenecks, scalability concerns, and a single point of failure. In decentralized FL, clients exchange and combine updates directly through peer-to-peer communication without relying on a central server. This improves decentralization and fault tolerance but creates challenges related to network topology, synchronization, convergence, communication overhead, and unreliable clients.Various aggregation algorithms have been developed to address data heterogeneity, client drift, communication cost, convergence, privacy, and robustness in FL. Among these, SCAFFOLD addresses

client drift under non-IID data by introducing control variates for variance reduction. It maintains a client-specific control variable ckc_k and a global server control variable cc. During local optimization, the difference between these variables corrects the local gradient direction, reducing deviation from the global optimization objective. This mechanism improves convergence stability and learning performance in heterogeneous environments.

Experimental setup, evaluation metrics, tables/graphs, comparison with existing methods, interpretation of results, and limitations. The comparative analysis demonstrates that the effectiveness of Federated Learning aggregation algorithms depends significantly on data heterogeneity, convergence, robustness, and personalization**.** Under non-IID conditions, FedAvg shows considerable performance degradation, whereas FedProx and FedNova provide greater stability. SCAFFOLD and MOON achieve stronger performance under severe heterogeneity, indicating improved handling of client drift and diverse data distributions. Regarding convergence, SCAFFOLD requires fewer communication rounds, while Zeno involves higher computational and communication requirements due to its validation mechanism. Robustness analysis indicates that conventional approaches remain vulnerable to unreliable or malicious updates, whereas Zeno provides better resistance by filtering suspicious client contributions. For personalization, Per-FedAvg achieves the strongest client-specific performance, with gains of up to 10–15%**,** while SCAFFOLD provides a balanced compromise between global accuracy and personalization. Overall, no single aggregation method performs optimally across all FL scenarios. These findings highlight the need for an adaptive aggregation framework that dynamically considers client performance, convergence behaviour, data heterogeneity, contribution quality, and robustness to achieve a more accurate, stable, and reliable global model.

Conclusion and Future Scope

This study presents a systematic and comprehensive analysis of model aggregation techniques in Federated Learning (FL)**,** recognizing aggregation as a fundamental component that determines the effectiveness of collaborative learning while preserving decentralized data privacy. The study is motivated by the need for a structured understanding and taxonomy of aggregation mechanisms, as existing research has largely addressed individual FL challenges and aggregation approaches independently.

Based on their operational characteristics, model aggregation techniques are systematically organized into four major categories: synchronous, asynchronous, hierarchical, and robust aggregation. This classification provides a structured framework for understanding how different aggregation mechanisms coordinate client updates and address diverse federated environments. The analysis also demonstrates the practical significance of these approaches across application domains, including smart healthcare, intelligent transportation, smart cities, industrial systems, finance, network security, education, and recommendation systems.

Despite substantial progress, several challenges continue to limit the effectiveness of FL aggregation. Statistical heterogeneity can result in client drift and unstable convergence, while communication bottlenecks increase training latency and resource consumption in large-scale networks. Furthermore, security and privacy threats, including model poisoning, Sybil attacks, and inference attacks, emphasize the need for reliable and secure aggregation mechanisms. Emerging technologies and approaches such as adaptive aggregation, AirComp, IRS, 6G communication, blockchain, and trusted environments provide promising directions for addressing these limitations. Overall, the study indicates that no single aggregation strategy can optimally address all federated learning conditions. Future research should therefore focus on developing adaptive, intelligent, communication-efficient, and secure aggregation frameworks capable of dynamically responding to client heterogeneity, model performance, convergence behaviour, communication constraints, and update reliability. Such developments can improve the accuracy, convergence, robustness, scalability, fairness, and practical applicability of FL and provide a strong foundation for next-generation privacy-preserving distributed intelligent systems.

Challenges and Future Directions

Despite significant advances in Federated Learning (FL) aggregation, several challenges remain. Statistical heterogeneity caused by non-IID and imbalanced client data can reduce model accuracy, fairness, and convergence stability. Communication bottlenecks arise from frequent model exchanges among distributed clients, increasing bandwidth requirements and training latency. Secure aggregation is also essential because model updates may be exposed to privacy leakage, poisoning, or other adversarial attacks. Future research should therefore focus on adaptive and intelligent aggregation strategies that dynamically account for data heterogeneity, client contribution, communication efficiency, and update reliability while ensuring privacy and

security. Such approaches can enable more accurate, robust, scalable, and efficient FL systems for real-world applications.

References

[1] A. Paleyes, R.-G. Urma, and N. D. Lawrence, “Challenges in deploying machine learning: A survey of case studies,” ACM Comput. Surv., 2020.

[2] M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” Science, vol. 349, no. 6245, pp. 255–260, 2015.

[3] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, et al., “Federated learning: Strategies for improving communication efficiency,” arXiv preprint, 2016.

[4] C. Pappas, D. Chatzopoulos, S. Lalis, and M. Vavalis, “IPLS: A framework for decentralized federated learning,” in Proc. IFIP Networking Conf., IEEE, 2021, pp. 1–6.

[5] S. Ji, J. Zhang, Y. Zhang, Z. Han, and C. Ma, “LAFED: A lightweight authentication mechanism for blockchain-enabled federated learning system,” Future Gener. Comput. Syst., vol. 145, pp. 56–67, 2023.

[6] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, 2020.

[7] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, et al., “Federated optimization in heterogeneous networks,” in Proc. Mach. Learn. Syst., vol. 2, pp. 429–450, 2020.

[8] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, 2016.

[9] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, et al., “Federated learning in mobile edge networks: A comprehensive survey,” IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 2031–2063, 2020.

[10] R. Kumar, J. Kumar, A. A. Khan, H. Ali, et al., “Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images,” Comput. Med. Imag. Graph., vol. 102, Art. no. 102139, 2022.

[11] S. Wang, F. Liu, and H. Xia, “Content-based vehicle selection and resource allocation for federated learning in IoV,” in Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW), 2021, pp. 1–7.

[12] X. Chen, G. Zhu, Y. Deng, and Y. Fang, “Federated learning over multihop wireless networks with in-network aggregation,” IEEE Trans. Wireless Commun., vol. 21, no. 6, pp. 4622–4634, 2022.

[13] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, et al., “Federated learning for Internet of Things: A comprehensive survey,” IEEE Commun. Surveys Tuts., vol. 23, no. 3, pp. 1622–1658, 2021.

[14] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, et al., “Towards federated learning at scale: System design,” in Proc. Mach. Learn. Syst., vol. 1, pp. 374–388, 2019.

[15] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, “Robust and communication-efficient federated learning from non-IID data,” IEEE Trans. Neural Netw. Learn. Syst., vol. 31, no. 9, pp. 3400–3413, 2019.

[16] L. Zhang, L. Shen, L. Ding, D. Tao, and L.-Y. Duan, “Fine-tuning global model via data-free knowledge distillation for non-IID federated learning,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), 2022, pp. 10174–10183.

[17] J. Xu, B. S. Glicksberg, C. Su, P. Walker, et al., “Federated learning for healthcare informatics,” J. Healthc. Inform. Res., vol. 5, no. 1, pp. 1–19, 2021.

[18] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proc. Int. Conf. Artif. Intell. Statist. (AISTATS), 2017, pp. 1273–1282.

[19] C. Zhang, Y. Xie, H. Bai, B. Yu, et al., “A survey on federated learning,” Knowl.-Based Syst., vol. 216, Art. no. 106775, 2021.

[20] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, et al., “A survey on security and privacy of federated learning,” Future Gener. Comput. Syst., vol. 115, pp. 619–640, 2021.

[21] X. Yin, Y. Zhu, and J. Hu, “A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions,” ACM Comput. Surv., vol. 54, no. 6, pp. 1–36, 2021.

[22] V. Kulkarni, M. Kulkarni, and A. Pant, “Survey of personalization techniques for federated learning,” in Proc. 4th World Conf. Smart Trends Syst., Security Sustainability (WorldS4), IEEE, 2020, pp. 794–797.

For IEEE thesis/paper writing, cite them in the text numerically, for example: “FedAvg provides a communication-efficient approach for decentralized learning [18], while subsequent studies have focused on heterogeneous data [7], [15], communication efficiency [3], [14], and security and privacy [20], [21].”

[23] H. Zhu, J. Xu, S. Liu, and Y. Jin, “Federated learning on non-IID data: A survey,” Neurocomputing, vol. 465, pp. 371–390, 2021.

[24] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, “Federated learning: A survey on enabling technologies, protocols, and applications,” IEEE Access, vol. 8, pp. 140699–140725, 2020.
[25] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, et al., “Federated learning for smart healthcare: A survey,” ACM Comput. Surv., vol. 55, no. 3, pp. 1–37, 2022.
[26] S. Niknam, H. S. Dhillon, and J. H. Reed, “Federated learning for wireless communications: Motivation, opportunities, and challenges,” IEEE Commun. Mag., vol. 58, no. 6, pp. 46–51, 2020.
[27] M. P. Sah and A. Singh, “Aggregation techniques in federated learning: Comprehensive survey, challenges and opportunities,” in Proc. 2nd Int. Conf. Advance Computing and Innovative Technologies in Engineering, IEEE, 2022, pp. 1962–1967.
[28] L. U. Khan, W. Saad, Z. Han, E. Hossain, et al., “Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges,” IEEE Commun. Surveys Tuts., 2021.
[29] G. Antonella, F. Giancarlo, G. Gianluigi, and M. Marcello, “Data and model aggregation for radiomics applications: Emerging trend and open challenges,” Inf. Fusion, Art. no. 101923, 2023.
[30] B. Kitchenham, “Procedures for performing systematic reviews,” Keele Univ., Keele, U.K., Tech. Rep., vol. 33, pp. 1–26, 2004.