World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

Federated learning: Challenges and future work

Md Boktiar Hossain [1,*] and Rashedur Rahman [2]

[1] Department of Information and Communication Engineering, University of Rajshahi, Rajshahi 6205, Bangladesh.
[2] Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh.

World Journal of Advanced Research and Reviews, 2022, 15(02), 850-862

Publication history: Received on 12 June 2022; revised on 21 August 2022; accepted on 29 August 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.2.0711

Abstract

This paper provides a comprehensive survey of Federated Learning (FL), an emerging paradigm in machine learning that allows multiple clients such as mobile devices or distributed data centers to collaboratively train shared models without exchanging raw data. By localizing data and transmitting only model updates, FL ensures data privacy, enhances security, and reduces the risks and costs associated with traditional centralized learning methods. The paper analyzes FL from five key dimensions: data partitioning strategies, privacy-preserving mechanisms, machine learning models, communication architectures, and system heterogeneity. In addition to exploring foundational concepts, the paper highlights enabling technologies and platforms that support FL, reviews widely used protocols, and presents real-world applications across industries such as healthcare, finance, and IoT. The authors also delve into the challenges of deploying FL in heterogeneous and large-scale environments, including issues related to communication efficiency, device reliability, and algorithmic fairness. Finally, the survey outlines open research directions and provides practical insights to help data scientists and engineers design more robust and privacy-preserving FL systems suitable for critical real-world deployments.

Keywords: Federated learning; Machine learning; Privacy protection; Personalized federated learning

1. Introduction

With the evolution of big data, privacy and data security have become critical concerns, driven by regulations like the EU's GDPR [4] and China's Cyber Security Law [5]. These laws prohibit unauthorized data use and require strict user consent, making centralized data collection and traditional machine learning increasingly impractical due to privacy risks and data silos [1–3], [6]. Federated Learning (FL) offers a promising solution by enabling decentralized model training across user devices without transferring raw data to a central server, thus ensuring compliance with privacy laws [7]. FL utilizes secure mechanisms such as homomorphic encryption, secure aggregation, and differential privacy to protect sensitive information during training [8,9]. FL is categorized based on data distribution: horizontal (shared features), vertical (shared users), and federated transfer learning (no overlap). Unlike conventional distributed learning, FL ensures complete user control over local data and supports privacy-preserving collaboration [10–13]. With advancements in edge computing and AI hardware, FL can now efficiently utilize client-side resources to train models across various domains including healthcare, IoT, defense, and mobile apps [14–16]. Despite its benefits, FL still faces technical challenges related to platforms, protocols, and privacy-preserving implementations [17–19]. This paper explores these aspects in depth and presents adaptable FL architectures for diverse industry applications [20–22].

* Corresponding author: Md Boktiar Hossain

2. Challenges

Federated Learning (FL) faces three main challenges: ensuring user privacy during model training, dealing with limited data on individual devices, and handling statistical heterogeneity, as data across devices is often non-IID, making global model training more difficult.

3. Contributions

This paper provides a comprehensive overview of Federated Learning (FL), focusing on its development, core components, challenges, and real-world applications. Unlike prior surveys, this work delves deeper into FL architectures, platforms, hardware, and software, aiming to give researchers and data scientists a practical blueprint for developing FL-based solutions. It highlights current use cases—particularly in healthcare—and outlines key technical challenges, best design practices, and future research directions to facilitate broader and more effective adoption of FL across industries. Figure-1 representing the general architecture of FL is shown below.

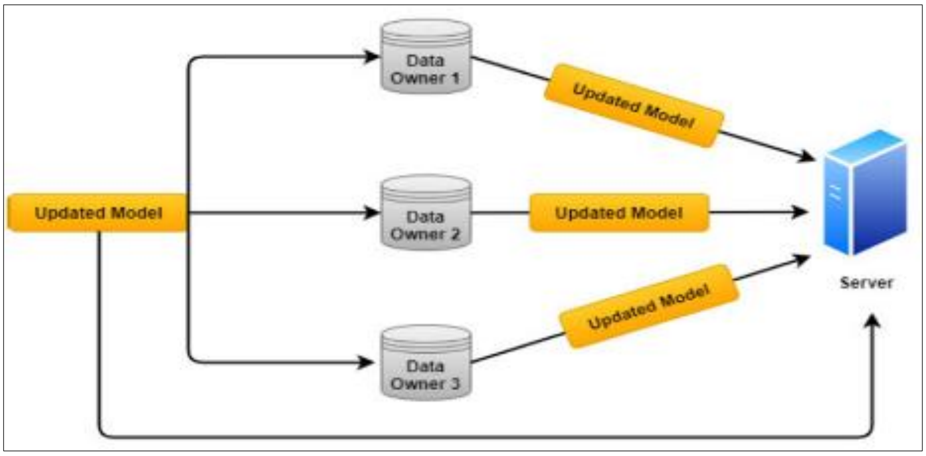

Figure 1 Federated learning architecture

4. Related works

Federated Learning (FL) is an encrypted distributed machine learning approach that enables participants to collaboratively build models without sharing their local data. By exchanging encrypted parameters, a shared virtual model is created, helping to overcome data silos. Though still emerging, FL is often compared to distributed, parallel, and deep learning, with several studies already exploring it in depth. Table 1 summarizes various works that tackle FL, along with other topics focusing on use-cases for FL.

Table 1 Summary of related works

Ref. No	Author(s)	Article Topic(s)
[23]	Y. Xia	
[24]	Tal Ben-Nun, T. Hoefler	Deep Learning
[25]	M.G. Poirot, et al.	
[26]	P. Vepakomma, et al.	HIPAA Guidelines for FL
[27]	P. Vepakomma, et al.	Drawbacks of FL
[28]	Kevin Hsieh	Traditional ML Methods
[29]	Qinbin Li, et al.	Data Privacy and Protection Future Direction of FL Challenges of FL
[30]	V. Kulkarni, et al.	Personalization techniques for FL
[31]	J. Geiping, et al.	Privacy of FL
[32]	Y. Liu, et al.	FL for 6G

5. Categorizations of federated learning

5.1. This section outlines five key categorizations of Federated Learning (FL)

Data partitioning, privacy mechanisms, applicable machine learning models, communication architecture, and methods to address heterogeneity. For easy understanding, we list the advantages and applications of these categorizations in Table 2.

Table 2 Categorizations of federated learning

Categorization	Methods	Advantage	Applications
Data partitioning	Horizontal federated learning	Increase user sample size	Android phone model update; logistic regression
	Vertical federated learning	Increase feature dimension	Decision tree; neural network
	Federated transfer learning	Increase user sample size and feature dimension	Transfer learning
Privacy mechanism	Model aggregation	Avoid transmitting the original data	Deep network federation learning; PATE method
	Homomorphic encryption	Users can calculate and process the encrypted data	Ridge regression; federated learning
	Differential privacy	Can successfully protect user privacy by adding noise	Traditional machine learning; deep learning
Applicable machine learning model	Linear models	Concise form, easy to model	Linear regression; ridge regression
	Tree models	Accurate, stable, and can map non-linear relationships	Classification tree; regression tree
	Neural network models	Learning capabilities, highly robust and fault-tolerant	Pattern recognition, intelligent control
Methods for solving heterogeneity	Asynchronous communication	Solve the problem of communication delay	Device heterogeneity
	Sampling	Avoid simultaneous training with heterogeneous equipment	Pulling Reduction with Local Compensation (PRLC)
	Fault-tolerant Mechanism	Can prevent the whole system from collapsing	Redundancy algorithm
	Heterogeneous Model	Can solve the corresponding heterogeneous device	(LG-FEDAVG) algorithm

5.2. Data partitioning

Based on the distribution of sample and feature spaces, FL can be classified into three types: horizontal FL, vertical FL, and federated transfer learning [36].

5.2.1. Horizontal federated learning

Horizontal FL applies when different datasets share similar features but involve mostly different users. It partitions data by user dimension aligning feature space while user identities differ allowing collaborative training without user overlap. This increases the training sample size and can enhance model accuracy. For example, two regional service providers may have different customer bases but similar user attributes, making them suitable candidates for horizontal FL. In this setup, each participant computes local gradients which are then sent to a central server for global model aggregation. Exchanging gradients can risk privacy breaches. To mitigate this, methods like homomorphic encryption [37], differential privacy [38], and secure aggregation [39] are commonly applied. A notable example is Google's 2016 federated model update system for Android devices [8,10], where users update model parameters locally and upload them to the cloud. This system leverages differential privacy [38] and secure aggregation to protect user data. Kim et al. [40] introduced BlockFL, a horizontal FL framework where devices update their local models through a blockchain network. Smith et al. [41] proposed MOCHA, a federated multitask learning framework that enables collaboration across sites while ensuring privacy and improving fault tolerance and communication efficiency. In approaches such as those in [11, 42], data is retained on the client side. Each client computes local gradients and sends them to the server, where the global model is updated—preserving data privacy and supporting distributed training

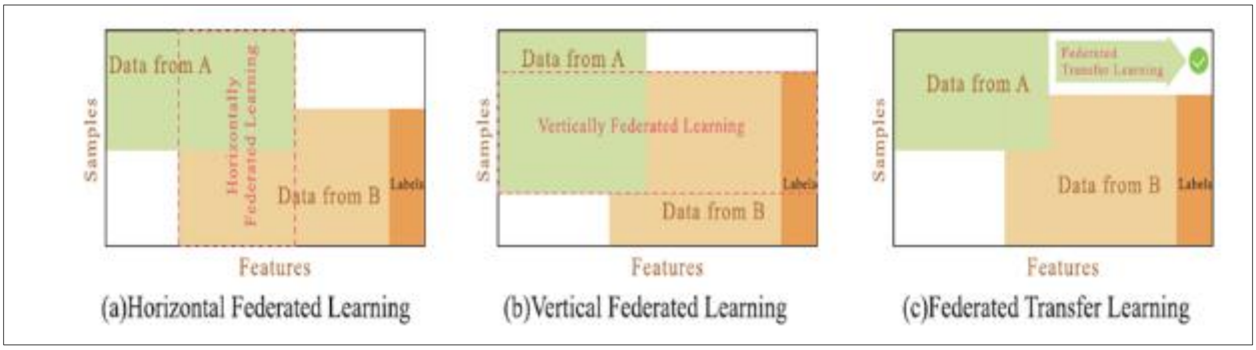

Figure 2 The distinct ways, in which data is divided in horizontal federated learning, vertical federated learning, and federated transfer learning

5.2.2. Vertical federated learning

Vertical federated learning is applicable when datasets share many of the same users but have largely different feature sets. In this approach, data is split vertically based on features, aligning on common users while combining different feature attributes from various sources. For instance, a local bank and an e-commerce platform may both serve the same regional user base. While the bank records financial and credit information, the e-commerce platform logs browsing and purchase behavior. By securely aggregating these distinct features, vertical FL enhances model learning without compromising data privacy. Various machine learning methods support vertically partitioned data, including classification [43], statistical analysis [44], gradient descent [45], and privacy-preserving linear regression [46,47], as well as data mining techniques [48]. For example, SecureBoost [49] enables collaborative model training using shared user data without information loss. Another work by Hardy et al. [50] introduced a privacy-preserving logistic regression model using vertical FL. This model combines entity alignment and distributed logistic regression, employing Paillier homomorphic encryption [51] to maintain data confidentiality while enhancing classification accuracy.

5.2.3. Federated transfer learning

When both users and features across datasets have minimal overlap, federated transfer learning becomes essential [9]. This method does not segment the data but instead applies transfer learning to address issues of limited data volume or sparse labels. For example, a Chinese e-commerce company and a U.S.-based social media platform may have little overlap in user base and feature data due to geographical and functional differences. In such cases, transfer learning enables knowledge sharing between these datasets, improving model performance despite data limitations. This approach is particularly useful when training data for a specific task is scarce but related data from other domains is available [52].

A practical example would be a hospital's radiology department lacking sufficient X-ray scans to train a diagnostic model. Here, transfer learning from related image recognition tasks can boost performance while preserving privacy. Thus, federated transfer learning not only protects user data but also enhances learning in data-constrained environments by leveraging auxiliary task knowledge.

5.3. Privacy mechanisms

The most important feature of federated learning is that cooperative clients can keep their own data locally, and need to share model information to train the target model, but the model information will also disclose some private information [53]. The common means to protect federal privacy are model aggregation [39], homomorphic encryption [50] and differential privacy [41].

5.3.1. Model aggregation

Model aggregation is a widely used privacy-preserving strategy in federated learning, where a global model is trained by collecting and combining model parameters from participating devices rather than sharing raw data. This approach ensures data privacy during training. For example, Shashi et al. [54] introduced an incentive-driven framework that enables multiple devices to contribute to federated learning. To maintain efficiency, real-time optimization of communication during parameter exchange is essential. In contrast to incentive mechanisms, Yu et al. [55] emphasized enhancing both privacy and model performance through techniques such as local fine-tuning, multi-task learning, and knowledge extraction. These methods help users achieve better results than standalone local models while maintaining privacy. McMahan et al. [42] proposed a deep federated learning framework based on iterative model averaging, which updates the global model in cycles by aggregating local updates. Another technique, PATE (Private Aggregation of Teacher Ensembles) [56], aggregates knowledge from multiple teacher models trained on separate data sources and transfers it to a student model, providing privacy protection by using a black-box approach. Yurochkin et al. [57] introduced a Bayesian nonparametric approach for federated neural networks, constructing a global model by aligning neurons across local models. Additionally, federated multitask learning [41] enables different users to train task-specific models locally and combine them through aggregation.

Lastly, studies such as [40, 58] have explored integrating blockchain with federated learning. In these systems, model updates are shared and aggregated through a blockchain network, ensuring secure and transparent parameter exchange under blockchain protocols.

5.3.2. Homomorphic encryption

Conventional encryption schemes primarily ensure the security of data during storage, preventing unauthorized users without the decryption key from accessing any information about the original data. These schemes do not allow for computations on the encrypted data, as attempting such operations typically results in failed decryption. In contrast, homomorphic encryption addresses this limitation by enabling secure data processing. Its key advantage is that it allows computations to be performed directly on encrypted data without revealing the underlying information. After processing, only the user with the appropriate decryption key can retrieve the final result, which matches the expected output. This capability makes homomorphic encryption particularly suitable for systems like Ridge regression [39,59], where privacy-preserving data processing is essential. Furthermore, it enhances both communication efficiency and computational performance.

5.3.3. Differential privacy

Differential Privacy [60], introduced by Dwork in 2006, offers a modern framework for protecting individual privacy in statistical databases. This approach ensures that the output of a computation remains largely unaffected by the inclusion or exclusion of any single data record. As a result, the presence of an individual record in the dataset has a minimal and controlled impact on the overall results, significantly reducing the risk of privacy leakage. An attacker, therefore, cannot accurately infer personal information by analyzing the output. In conventional machine learning [61] and deep learning [62] training processes, differential privacy is commonly implemented by introducing noise into the output during gradient iterations to safeguard user privacy. In practice, techniques such as the Laplace mechanism and the exponential mechanism are widely adopted to enforce differential privacy. Current research often focuses on balancing privacy protection with model utility, as excessive noise can compromise performance. One emerging trend is the integration of differential privacy with model compression techniques [63], aiming to enhance privacy while maintaining or even boosting performance.

6. Applicable machine learning models

Federated learning is increasingly being integrated with mainstream machine learning approaches, offering a means to preserve privacy while maintaining model efficiency. This section outlines three key categories of machine learning models commonly used within federated learning frameworks: linear models, decision trees, and neural networks.

6.1. Linear models

Linear models in federated learning are typically classified into three types: linear regression, ridge regression, and lasso regression. Du et al. [43] introduced a method for training linear models within a federated environment, effectively addressing security concerns related to entity parsing while maintaining accuracy comparable to non-private solutions. Nikolaenko et al. [64] developed a ridge regression system that incorporates homomorphic encryption and Yao's protocol [65], achieving superior performance. Linear models are generally straightforward to implement and serve as an efficient foundation for federated learning applications.

6.2. Tree-based models

Federated learning can be applied to train individual or ensembles of decision trees, including popular algorithms such as Gradient Boosting Decision Trees (GBDT) and Random Forests. GBDT has gained significant attention in recent years due to its strong performance across various classification and regression tasks. Zhao et al. [66] introduced a privacy-preserving GBDT system tailored for regression and binary classification, which securely aggregates regression trees from different data owners while protecting user privacy. Cheng et al. [49] proposed a framework called SecureBoost to train GBDT models on both horizontally and vertically partitioned data, enabling collaborative learning across decentralized datasets.

6.3. Neural network models

Neural networks represent a powerful class of machine learning models capable of addressing complex tasks, and their integration with federated learning is gaining traction. In scenarios involving UAVs (Unmanned Aerial Vehicles), tasks such as trajectory planning, target identification, and localization often rely on deep learning. Due to intermittent connectivity between UAV groups and ground stations, centralized training is not always feasible in real-time applications. Zeng et al. [67] were pioneers in implementing a distributed federated learning algorithm for UAV swarms, optimizing power allocation, scheduling, and convergence speed. Their approach involves a lead UAV aggregating locally trained models from peer UAVs to form a global model, which is then shared via intra-swarm communication. Bonawitz et al. [68] developed a scalable federated learning system for mobile devices using TensorFlow, enabling training across numerous distributed datasets. Yang et al. [70] established a federated deep learning framework based on data partitioning, with applications in enterprise-level data processing. In the public sector, traffic data often contains sensitive user information. To address this, Liu et al. [69] integrated Gated Recurrent Units (GRUs) with federated learning to forecast traffic flow, proposing a clustering-based FedGRU model that not only captures spatio-temporal dependencies more effectively but also outperforms traditional non-federated methods, as demonstrated on real-world datasets.

Although federated learning has achieved considerable progress across diverse machine learning models, the ongoing evolution of machine learning techniques continues to pose challenges in developing practical and high-performance federated learning solutions.

7. Challenges in federated learning

Federated Learning (FL) is an emerging branch of Artificial Intelligence developed for model training in distributed and heterogeneous edge environments. However, as illustrated in Fig. 3, FL is still in its early stages and has yet to gain strong trust within the research community, primarily due to several existing challenges and limitations.

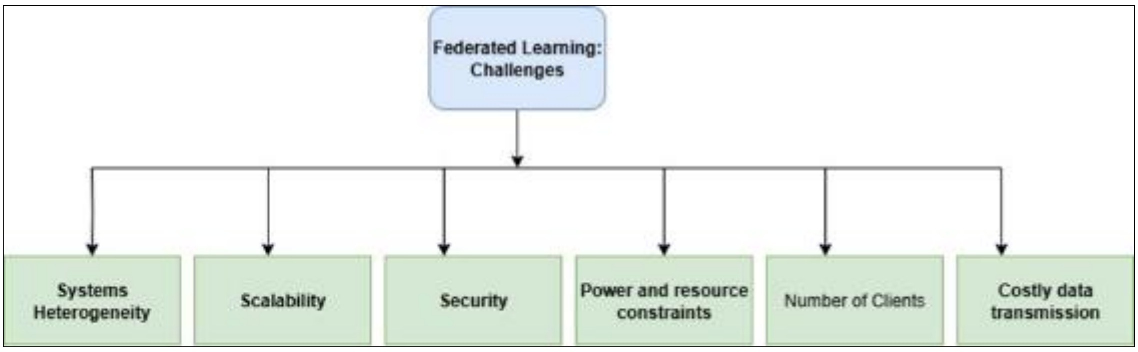

Figure 3 Challenges in Federated learning

7.1. Systems heterogeneity

Modern networks exhibit multiple layers of heterogeneity across hardware, network types (e.g., WLAN, WMAN, WWAN, WPAN), devices, applications, data storage, and battery levels. Device heterogeneity spans various platforms such as smartphones, tablets, laptops, and other mobile devices capable of intercommunication [71]. This complex heterogeneity presents significant challenges for federated learning (FL). In particular, the use of diverse data storage systems and the violation of the independent and identically distributed (I.I.D.) assumption complicate model training and analysis. Since devices generate data based on their unique usage and local environments, data distributions differ widely across participants [72]. For example, in tasks like next-word prediction, mobile users may use language differently, leading to non-I.I.D. data. Additionally, the volume of data available on each device may vary, and relationships may exist among devices and their local data distributions, further diverging from the I.I.D. assumption.

7.2. Scalability

Scalability is a common challenge in federated learning, especially as the number of participating devices grows beyond a certain threshold. One approach to mitigate this is the use of a parameter server, which can limit communication between participants and the server to a single round, thereby lowering the communication overhead per client [73]. Despite this benefit, relying on a parameter server still poses difficulties for communication-efficient distributed training, as both uploading and downloading model updates require effective compression techniques to minimize communication cost, time, and energy usage.

7.3. Power and resource constraints

In federated learning, participants are typically mobile devices, which often struggle with limited battery life and computing resources. Deep learning models, in particular, are resource-intensive, making even a single training iteration costly in terms of energy and memory usage [74]. The limited memory capacity of mobile devices further complicates the training of models locally. To address this, fog computing can serve as an intermediary layer between data processing units and storage systems, enabling real-time data processing closer to the source [75].

7.4. Security

Security remains a significant concern in federated learning (FL). Both the participants (clients) and the communication network can compromise core security principles such as authentication, integrity, and confidentiality. FL systems are vulnerable to various network threats, including malware, Trojan horses, viruses, spyware, worms, and phishing attacks. Moreover, malicious clients may expose sensitive information to unauthorized entities, such as intruders, third parties, or even impersonated central servers.

To mitigate these risks, FL emphasizes protecting user privacy by transmitting model updates instead of raw data. Techniques like secure multiparty computation and differential privacy can enhance both data privacy and model performance while maintaining low operational costs.

7.5. Number of clients

In federated learning, the number of participating clients plays a crucial role in storing and evaluating the collaboratively trained models. However, clients may refuse to participate either intentionally—due to a lack of interest—or unintentionally, owing to issues such as weak network connectivity, limited resources, or low battery power. Managing a large and dynamic set of clients is inherently difficult, making it a significant challenge in FL [76]. Therefore, ensuring consistent participation from clients is essential for the effectiveness of the federated learning process.

8. Future work

To address the challenges outlined above, several potential directions for future research are worth exploring:

8.1. Privacy restrictions

Due to the diverse nature of devices within a network, each comes with its own unique privacy constraints. Therefore, it is essential to define privacy requirements at a more granular level for groups of devices to ensure the protection of individual data samples and provide robust privacy guarantees. Developing privacy-preserving techniques tailored to the specific privacy needs of individual devices represents a promising and ongoing area for future research.

8.2. Optimization between communication efficiency and processing complexity

Balancing communication cost and computational load is a key challenge in federated learning. Efficiency in communication can be improved primarily through two strategies: sending smaller updates iteratively or reducing the total number of communication rounds. For instance, model compression techniques can help decrease the size of transmitted data. Alternatively, communication frequency can be reduced by selectively transmitting only the most important model updates. A combination of these approaches can significantly lower communication costs between mobile devices and servers. This often leads to increased computational demands on the devices. Identifying an optimal trade-off between communication overhead and computational burden remains a crucial focus for future research.

8.3. Multi-center federated learning

Heterogeneity remains a significant obstacle in federated learning. Recent studies [77–80] suggest that if device heterogeneity can be identified beforehand, mobile devices can be grouped based on their similarities, with a local central server assigned to each group. Models from devices within the same group can first be aggregated locally, and these intermediate models can then be sent to the main server for global aggregation. Exploring multi-center federated learning to address heterogeneity presents a promising avenue for future research [86].

8.4. Transitioning federated learning from research to production

Bringing federated learning (FL) into production presents several experimental challenges. These include issues such as data drift, where device behavior changes over time, and the cold start problem, where new devices initially lack sufficient data [92, 93]. As FL is still in its early stages, these challenges offer valuable opportunities for further research. Tools like LEAF, a modular benchmarking framework, support experimentation in FL by providing open-source federated datasets for evaluation and development [81-85, 94].

8.5. Heterogeneity diagnostics

Current approaches have quantified statistical heterogeneity using metrics such as neighborhood divergence and Earth Mover's Distance [95]. However, these metrics are difficult to compute across a federated network before training begins. This raises several important questions for future exploration:

- Can simple and efficient diagnostic tools be developed to quickly assess the level of heterogeneity in federated networks?
- Is it possible to design diagnostics that measure system-related heterogeneity in a similar manner?
- Can existing definitions of heterogeneity be leveraged to improve the design of federated optimization strategies?
- Are there practical diagnostics that can evaluate both system and data heterogeneity prior to model training?
- How can these diagnostics be effectively utilized to enhance the convergence of federated optimization methods?

These questions highlight the need for further research into heterogeneity assessment to improve the performance and robustness of federated learning systems.

Index Terms

- UAV: Unmanned Aerial Vehicle,
- GDPR: General Data Protection Regulation,
- I.I.D.: Independent and Identically Distributed,
- WWAN: Wireless Wide Area Network,
- WMAN: Wireless Metropolitan Area Network,
- WLAN: Wireless Local Area Network,
- WPAN: Wireless Personal Area Network,
- GBDT: Gradient Boosting Decision Tree,
- GRU: Gated Recurrent Unit,
- FedGRU: Federated Gated Recurrent Unit

9. Conclusion

Federated Learning (FL) is a decentralized machine learning approach that enables collaborative model training while preserving user privacy, making it highly relevant for sectors like healthcare, finance, and IoT. This paper provided a comprehensive overview of FL, including its types, privacy mechanisms, supported models, communication methods, and challenges such as heterogeneity, scalability, and security. Despite its advantages, FL faces obstacles like limited device resources, data variability, and complex client management. Future research should focus on optimizing privacy for heterogeneous devices, reducing communication costs, developing multi-center architectures, and improving diagnostic tools for heterogeneity. As FL moves toward real-world deployment, issues like data drift and cold starts must be addressed. Tools like LEAF and privacy-enhancing techniques offer promising solutions. Continued innovation is vital to realize FL's full potential in secure and scalable AI applications.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Zhang, C., Hu, X., Xie, Y., Gong, M., and Yu, B. (2020). A privacy-preserving multitask learning framework for face detection, landmark localization, pose estimation, and gender recognition. Frontiers in Neurorobotics, 13, 112.

[2] Gong, M., Feng, J., and Xie, Y. (2020). Privacy-enhanced multi-party deep learning. Neural Networks, 121, 484–496.

[3] Xie, Y., Wang, H., Yu, B., and Zhang, C. (2020). Secure collaborative few-shot learning. Knowledge-Based Systems, 2020, Article 106157.

[4] Albrecht, J. P. (2016). How the GDPR will change the world. European Data Protection Law Review, 2, 287.

[5] Parasol, M. (2018). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and smart city dreams. Computer Law and Security Review, 34(1), 67–98.

[6] Gray, W., and Zheng, H. R. (1986). General principles of civil law of the People's Republic of China. American Journal of Comparative Law, 34(4), 715–743.

[7] Gong, M., Xie, Y., Pan, K., Feng, K., and Qin, A. K. (2020). A survey on differentially private machine learning. IEEE Computational Intelligence Magazine, 15(2), 49–64.

[8] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., and Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the ACM Conference on Computer and Communications Security (CCS) (pp. 1175–1191).

[9] Liu, Y., Kang, Y., Xing, C., Chen, T., and Yang, Q. (2020). A secure federated transfer learning framework. IEEE Intelligent Systems, 35(4), 70–82.

[10] Liang, P. P., Liu, T., Ziyin, L., Allen, N. B., Auerbach, R. P., Brent, D., Salakhutdinov, R., and Morency, L.-P. (2020). Think locally, act globally: Federated learning with local and global representations (arXiv:2001.01523). Retrieved from http://arxiv.org/abs/2001.01523

[11] Zhuo, H. H., Feng, W., Lin, Y., Xu, Q., and Yang, Q. (2020). Federated deep reinforcement learning (arXiv:1901.08277). Retrieved from https://arxiv.org/abs/1901.08277

[12] Yu, H., Liu, Z., Liu, Y., Chen, T., Cong, M., Weng, X., Niyato, D., and Yang, Q. (2020). A fairness-aware incentive scheme for federated learning. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (pp. 393–399).

[13] Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., and Zhou, Y. (2019). A hybrid approach to privacy-preserving federated learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (AISec) (pp. 1–11).

[14] Süzen, A. A., and Simsek, M. A. (2020). A novel approach to machine learning application to protection of privacy data in healthcare: Federated learning. Namık Kemal Tıp Dergisi, 8(1), 22–30.

[15] Lin, S., Yang, G., and Zhang, J. (2020). Real-time edge intelligence in the making: A collaborative learning framework via federated meta-learning (arXiv:2001.03229). Retrieved from http://arxiv.org/abs/2001.03229

[16] Pandey, S. R., Tran, N. H., Bennis, M., Tun, Y. K., Manzoor, A., and Hong, C. S. (2020). A crowdsourcing framework for on-device federated learning. IEEE Transactions on Wireless Communications, 19(5), 3241–3256.

[17] Shao, R., He, H., Liu, H., and Liu, D. (2019). Stochastic channel-based federated learning for medical data privacy preserving (arXiv:1910.11160). Retrieved from http://arxiv.org/abs/1910.11160

[18] Alexander, A., Jiang, A., Ferreira, C., and Zurkiya, D. (2020). An intelligent future for medical imaging: A market outlook on Artificial Intelligence for medical imaging. Journal of the American College of Radiology, 17(1), 165–170.

[19] Bakopoulou, E., Tillman, B., and Markopoulou, A. (2019). A federated learning approach for mobile packet classification (arXiv:1907.13113). Retrieved from http://arxiv.org/abs/1907.13113

[20] Larson, D. B., Magnus, D. C., Lungren, M. P., Shah, N. H., and Langlotz, C. P. (2020). Ethics of using and sharing clinical imaging data for Artificial Intelligence : A proposed framework. Radiology, 295(3), Article 192536.

[21] Konečný, J., McMahan, H. B., Ramage, D., and Richtárik, P. (2016). Federated optimization: Distributed machine learning for on-device intelligence (arXiv:1610.02527). Retrieved from http://arxiv.org/abs/1610.02527

[22] Ilias, C., and Georgios, S. (2019). Machine learning for all: A more robust federated learning framework. In Proceedings of the 5th International Conference on Information Systems Security and Privacy (pp. 544–551).

[23] Liu, L., Zhang, J., Song, S. H., and Letaief, K. B. (2019). Client-edge-cloud hierarchical federated learning (arXiv:1905.06641). Retrieved from https://arxiv.org/abs/1905.06641

[24] Xia, Y. (2020). Watermarking federated deep neural network models (Master's thesis, G2 Pro Gradu, Diplomityö, Turku, Finland). Retrieved from http://urn.fi/URN:NBN:fi:aalto-202003222594

[25] Ben-Nun, T., and Hoefler, T. (2019). Demystifying parallel and distributed deep learning: An in-depth concurrency analysis. ACM Computing Surveys, 52(4), 1–43.

[26] Poirot, M. G., Vepakomma, P., Chang, K., Kalpathy-Cramer, J., Gupta, R., and Raskar, R. (2019). Split learning for collaborative deep learning in healthcare (arXiv:1912.12115). Retrieved from http://arxiv.org/abs/1912.12115

[27] Vepakomma, P., Swedish, T., Raskar, R., Gupta, O., and Dubey, A. (2018). No peek: A survey of private distributed deep learning (arXiv:1812.03288). Retrieved from http://arxiv.org/abs/1812.03288

[28] Vepakomma, P., Gupta, O., Swedish, T., and Raskar, R. (2018). Split learning for health: Distributed deep learning without sharing raw patient data (arXiv:1812.00564). Retrieved from http://arxiv.org/abs/1812.00564

[29] Hsieh, K. (2019). Machine learning systems for highly-distributed and rapidly-growing data (arXiv:1910.08663). Retrieved from http://arxiv.org/abs/1910.08663

[30] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., and He, B. (2019). A survey on federated learning systems: Vision, hype and reality for data privacy and protection (arXiv:1907.09693). Retrieved from http://arxiv.org/abs/1907.09693

[31] Kulkarni, V., Kulkarni, M., and Pant, A. (2020). Survey of personalization techniques for federated learning (arXiv:2003.08673). Retrieved from https://arxiv.org/abs/2003.08673

[32] Geiping, J., Bauermeister, H., Dröge, H., and Moeller, M. (2020). Inverting gradients: How easy is it to break privacy in federated learning? (arXiv:2003.14053). Retrieved from https://arxiv.org/abs/2003.14053

[33] O. A. Wahab, A. Mourad, H. Otrok and T. Taleb, "Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems," in IEEE Communications Surveys and Tutorials, vol. 23, no. 2, pp. 1342-1397, Secondquarter 2021, doi: 10.1109/COMST.2021.3058573

[34] McMahan, H. B., Moore, E., Ramage, D., and y Arcas, B. A. (2016). Federated learning of deep networks using model averaging. CoRR, abs/1602.05629. Retrieved from https://arxiv.org/abs/1602.05629

[35] J. Lee and H. -J. Yoo, "An Overview of Energy-Efficient Hardware Accelerators for On-Device Deep-Neural-Network Training," in IEEE Open Journal of the Solid-State Circuits Society, vol. 1, pp. 115-128, 2021, doi: 10.1109/OJSSCS.2021.3119554

[36] Yang, Q., Liu, Y., Chen, T., and Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.

[37] Aono, Y., Hayashi, T., Wang, L., and Moriai, S. (2017). Privacy-preserving deep learning via additively homomorphic encryption. IEEE Transactions on Information Forensics and Security, 13(5), 1333–1345.

[38] McMahan, B., Ramage, D., Talwar, K., and Zhang, L. (2018). Learning differentially private recurrent language models. In Proceedings of the International Conference on Learning Representations (ICLR).

[39] Chen, Y.-R., Rezapour, A., and Tzeng, W.-G. (2018). Privacy-preserving ridge regression on distributed data. Information Sciences, 451, 34–49.

[40] Kim, H., Park, J., Bennis, M., and Kim, S.-L. (2018). On-device federated learning via blockchain and its latency analysis. arXiv preprint arXiv:1808.03949. Retrieved from https://arxiv.org/abs/1808.03949

[41] Smith, V., Chiang, C.-K., Sanjabi, M., and Talwalkar, A. S. (2017). Federated multi-task learning. In Advances in Neural Information Processing Systems (NeurIPS) (pp. 4424–4434).

[42] McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the International Conference on Artificial Intelligence and Statistics (AISTATS), PMLR (pp. 1273–1282).

[43] Du, W., Han, Y. S., and Chen, S. (2004). Privacy-preserving multivariate statistical analysis: Linear regression and classification. In Proceedings of the Fourth SIAM International Conference on Data Mining (pp. 222–233). SIAM.

[44] Du, W., and Atallah, M. J. (2001). Privacy-preserving cooperative statistical analysis. In Annual Computer Security Applications Conference (ACSAC) (pp. 102–110). IEEE.

[45] Wan, L., Ng, W. K., Han, S., and Lee, V. C. (2007). Privacy-preservation for gradient descent methods. In Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 775–783).

[46] Gascón, A., Schoppmann, P., Balle, B., Raykova, M., Doerner, J., Zahur, S., and Evans, D. (2016). Secure linear regression on vertically partitioned datasets. IACR Cryptology ePrint Archive, 2016(892).

[47] Karr, A. F., Lin, X., Sanil, A. P., and Reiter, J. P. (2009). Privacy-preserving analysis of vertically partitioned data using secure matrix products. Journal of Official Statistics, 25(1), 125–138.

[48] Vaidya, J., and Clifton, C. (2002). Privacy preserving association rule mining in vertically partitioned data. In Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 639–644).

[49] Cheng, K., Fan, T., Jin, Y., Liu, Y., Chen, T., and Yang, Q. (2019). SecureBoost: A lossless federated learning framework. arXiv preprint arXiv:1901.08755. Retrieved from https://arxiv.org/abs/1901.08755

[50] Hardy, S., Henecka, W., Ivey-Law, H., Nock, R., Patrini, G., Smith, G., and Thorne, B. (2017). Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv preprint arXiv:1711.10677. Retrieved from https://arxiv.org/abs/1711.10677

[51] Schoenmakers, B., and Tuyls, P. (2006). Efficient binary conversion for Paillier encrypted values. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 522–537). Springer.

[52] Zhang, L. (2019). Transfer adaptation learning: A decade survey. arXiv preprint arXiv:1903.04687. Retrieved from https://arxiv.org/abs/1903.04687

[53] Bhowmick, A., Duchi, J., Freudiger, J., Kapoor, G., and Rogers, R. (2018). Protection against reconstruction and its applications in private federated learning. arXiv preprint arXiv:1812.00984. Retrieved from https://arxiv.org/abs/1812.00984

[54] L. Wulfert, C. Wiede and A. Grabmaier, "TinyFL: On-Device Training, Communication and Aggregation on a Microcontroller For Federated Learning," 2023 21st IEEE Interregional NEWCAS Conference (NEWCAS), Edinburgh, United Kingdom, 2023, pp. 1-5, doi: 10.1109/NEWCAS57931.2023.10198040

[55] Yu, T., Bagdasaryan, E., and Shmatikov, V. (2020). Salvaging federated learning by local adaptation. arXiv preprint arXiv:2002.04758. Retrieved from https://arxiv.org/abs/2002.04758

[56] Papernot, N., Abadi, M., Erlingsson, Ú., Goodfellow, I., and Talwar, K. (2017). Semi-supervised knowledge transfer for deep learning from private training data. In Proceedings of the International Conference on Learning Representations (ICLR).

[57] Yurochkin, M., Agarwal, M., Ghosh, S., Greenewald, K., Hoang, T. N., and Khazaeni, Y. (2019). Bayesian nonparametric federated learning of neural networks. In Proceedings of the 36th International Conference on Machine Learning (ICML), Vol. 97, PMLR, pp. 7252–7261.

[58] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.

[59] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, N. Taft, Privacy-preserving ridge regression on hundreds of millions of records, in: IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 334–348.

[60] C. Dwork, “Differential Privacy: A Survey of Results,” in Theory and Applications of Models of Computation (TAMC), Springer, 2008, pp. 1–19.

[61] R. Bassily, A. Smith, and A. Thakurta, "Private Empirical Risk Minimization: Efficient Algorithms and Tight Error Bounds," in Proceedings of the IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2014, pp. 464–473.

[62] M. Abadi, A. Chu, I. Goodfellow, H.B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with Differential Privacy," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2016, pp. 308–318.

[63] N. Agarwal, A.T. Suresh, F.X.X. Yu, S. Kumar, and B. McMahan, "CP-SGD: Communication-Efficient and Differentially-Private Distributed SGD," in Proceedings of the Annual Conference on Neural Information Processing Systems (NeurIPS), 2018, pp. 7564–7575.

[64] Nikolaenko, V., Weinsberg, U., Ioannidis, S., Joye, M., Boneh, D., and Taft, N. (2013). Privacy-preserving ridge regression on hundreds of millions of records. In IEEE Symposium on Security and Privacy (pp. 334–348). IEEE.

[65] Lindell, Y., and Pinkas, B. (2009). A proof of security of Yao's protocol for two-party computation. Journal of Cryptology, 22(2), 161–188.

[66] Zhao, L., Ni, L., Hu, S., Chen, Y., Zhou, P., Xiao, F., and Wu, L. (2018). InPrivate Digging: Enabling tree-based distributed data mining with differential privacy. In IEEE INFOCOM 2018 – IEEE Conference on Computer Communications (pp. 2087–2095). IEEE.

[67] Zeng, T., Semiari, O., Mozaffari, M., Chen, M., Saad, W., and Bennis, M. (2020). Federated learning in the sky: Joint power allocation and scheduling with UAV swarms. In IEEE International Conference on Communications (ICC) (pp. 1–6). IEEE.

[68] Bonawitz, K. A., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C. M., Konen, J., Mazzocchi, S., McMahan, B., Overveldt, T. V., Petrou, D., Ramage, D., and Roselander, J. (2019). Towards federated learning at scale: System design. In Proceedings of Machine Learning and Systems.

[69] Liu, Y., James, J., Kang, J., Niyato, D., and Zhang, S. (2020). Privacy-preserving traffic flow prediction: A federated learning approach. IEEE Internet of Things Journal, 19(5), 3241–3256.

[70] Yang, Q., Liu, Y., Chen, T., and Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.

[71] P. Singh, R. Agrawal, A game-theoretic approach to maximize payoff and customer retention for differentiated services in a heterogeneous network environment. Int. J. Wirel. Mob. Comput. 16(2), 146–159 (2019)

[72] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, V. Chandra, Federated learning with non-iid data. arXiv preprint arXiv:1806.00582 (2018)

[73] M. Asad, A. Moustafa, T. Ito, M. Aslam, Evaluating the communication efficiency in federated learning algorithms. arXiv preprint arXiv:2004.02738 (2020)

[74] F. Sattler, S. Wiedemann, K.R. Müller, W. Samek, Robust and communication-efficient federated learning from non-iid data. IEEE Transact. Neural Networks Learn. Sys. 31(9), 3400–3413 (2019)

[75] Singh, P., and Agrawal, R. (2021). An Overloading State Computation and Load Sharing Mechanism in Fog Computing. Journal of Information Technology Research (JITR), 14(4), 94-106.

[76] T. Nishio, R. Yonetani, Client selection for federated learning with heterogeneous resources in mobile edge, in ICC 2019-2019 IEEE International Conference on Communications (ICC), (IEEE, 2019), pp. 1–7

[77] M.S.H. Abad, E. Ozfatura, D. Gunduz, O. Ercetin, Hierarchical federated learning across heterogeneous cellular networks, in: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, IEEE, 2020, pp. 8866–8870.

[78] M. Duan, D. Liu, X. Ji, R. Liu, L. Liang, X. Chen, Y. Tan, Fedgroup: Ternary cosine similarity-based clustered federated learning framework toward high accuracy in heterogeneity data, 2020, arXiv preprint arXiv:2010. 06870.

[79] M. Xie, G. Long, T. Shen, T. Zhou, X. Wang, J. Jiang, Multi-center federated learning, 2020, arXiv preprint arXiv:2005.01026.

[80] H. Jiang, M. Liu, B. Yang, Q. Liu, J. Li, X. Guo, Customized federated learning for accelerated edge computing with heterogeneous task targets, Comput. Netw. 183 (2020) 107569.

[81] Azam, S., Huda, A. F., Shams, K., Ansari, P., Hasan, M. M., & Mohamed, M. K. (2015). Anti-inflammatory and anti-oxidant study of ethanolic extract of Mimosa pudica. Journal of Young Pharmacists, 7(3), 234.

[82] Rahaman, Md Zahedur, et al. "Assessment of thrombolytic, antioxidant and analgesic properties of a medicinal plant of Asteraceae family growing in Bangladesh." Discovery Phytomedicine 7.1 (2020): 47-52.

[83] Mondal, K. K. (2015). Potential investigation of anti-inflammatory activity and phytochemical investigations of ethanolic extract of Glycosmis pentaphylla leaves. American Journal of Biomedical Research, 3(1), 6-8.

[84] Ahammed, Md Salim, et al. "A Study on Hevea Brasiliensis for evaluation of phytochemical and pharmacological properties in Swiss Albino Mice." Discovery Phytomedicine 7.2 (2020): 72-75.

[85] Ansari, P., Shofiul, A. J., Sumonto, S., Kallol, K. M., Tasnim, T., & Sanjeeda, S. B. (2015). Potential investigation of anti-inflammatory and anti-oxidative properties of ethanolic extract of Ixora nigricans leaves. IJPR, 5(4), 104.

[86] Md Bahar Uddin, Md. Hossain and Suman Das, "Advancing manufacturing sustainability with industry 4.0 technologies", International Journal of Science and Research Archive, 2022, 06(01), 358-366.

[87] Kowsher, M., Tahabilder, A., Sanjid, M. Z. I., Prottasha, N. J., Uddin, M. S., Hossain, M. A., & Jilani, M. A. K. (2021). LSTM-ANN & BiLSTM-ANN: Hybrid deep learning models for enhanced classification accuracy. Procedia Computer Science, 193, 131-140.

[88] Javed Mehedi Shamrat, F. M., Ghosh, P., Tasnim, Z., Khan, A. A., Uddin, M. S., & Chowdhury, T. R. (2022). Human Face recognition using eigenface, SURF method. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021 (pp. 73-88). Singapore: Springer Nature Singapore.

[89] Javed Mehedi Shamrat, F. M., Tasnim, Z., Chowdhury, T. R., Shema, R., Uddin, M. S., & Sultana, Z. (2022). Multiple Cascading Algorithms to Evaluate Performance of Face Detection. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021 (pp. 89-102). Singapore: Springer Nature Singapore.

[90] Shamrat, F. J. M., Tasnim, Z., Chowdhury, T. R., Shema, R., Uddin, M. S., & Sultana, Z. (2022). Multiple Cascading Algorithms. Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021, 317, 89.

[91] A. S. M. Hasan and A. A. Ibrahim, "Improved WBAN EH_ MAC Protocol based on Energy Harvesting and Wake up - Sleep Duty Cycling Technique," 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2022, pp. 478-483, doi: 10.1109/ISMSIT56059.2022.9932730

[92] Yasmin Akter Bipasha, "Market efficiency, anomalies and behavioral finance: A review of theories and empirical evidence", World Journal of Advanced Research and Reviews, 2022, 15(02), 827-839.

[93] Li, T., Sahu, A. K., Talwalkar, A., and Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50-60.

[94] S. Caldas, S.M.K. Duddu, P. Wu, T. Li, J. Konečný, H.B. McMahan, A. Talwalkar, Leaf: A benchmark for federated settings. arXiv preprint arXiv:1812.01097 (2018)

[95] S. Vaswani, F. Bach, M. Schmidt, Fast and faster convergence of sgd for over-parameterized models and an accelerated perceptron, in The 22nd international conference on Artificial Intelligence and statistics, (PMLR, 2019), pp. 1195–1204