A Survey on Federated Learning

Dhananjay Singh
dept. Computer Engineering)
Pune Institute of Computer Technology
Pune, India
sdhananjay0187@gmail.com

Tanishq Mohite
dept. Computer Engineering
Pune Institute of Computer Technology
Pune, India
mtanishq@yahoo.com

Aditya Bahiram
dept. Computer Engineering)
Pune Institute of Computer Technology
Pune, India
adityadb16@gmail.com

Chetan More
dept. Computer Engineering
Pune Institute of Computer Technology
Pune, India
chetanmore8605@gmail.com

Prof. Shital Girme
dept. Computer Engineering
Pune Institute of Computer Technology
Pune, India
sngirme@pict.edu

Sachin Gupta
dept. AI/ML
Vertias
Pune , India
sachin.gupta@vertias.com

***Abstract*—Federated learning (FL) has emerged as an intriguing model for collaborative machine learning that does not jeopardize data privacy. FL enables the building of robust models while keeping sensitive data localized by permitting distributed training across various devices or servers. This survey paper goes into the world of federated learning, taking an in-depth look at its fundamental concepts, frameworks, and applications. The paper begins with an overview of federated learning, detailing its key ideas and emphasizing its advantages over traditional centralized systems. It then digs into the vast universe of FL frameworks, evaluating their features and contrasting their advantages and disadvantages. The survey covers both open-source and proprietary frameworks, providing information about their applicability for diverse applications.**

***Index Terms*—Federated Learning, Decentralized Machine Learning, Privacy-preserving Machine Learning, Edge Computing, Distributed Learning, Secure Aggregation**

I. Introduction

Federated Learning is a groundbreaking approach in the field of machine learning that has gained considerable attention and significance in recent times. Unlike traditional centralized machine learning paradigms, allied literacy offers a decentralized and sequestration- conserving frame for model training. This innovative fashion enables multiple edge bias or data sources to collaboratively make a global model without the need to polarize sensitive data. In substance, it empowers associations and operations to influence the collaborative intelligence of distributed data sources, similar as mobile bias, Internet of effects(IoT) bias, and more, while securing individual sequestration and data security.

Federated Learning (FL) has gained popularity for training machine learning models, but there's no mature, dominant solution like PyTorch and TensorFlow for traditional machine learning. We provide standardized evaluations for existing open-source FL frameworks. This paper addresses two key questions: how to characterize FL frameworks and how to choose the best one for real-world applications. Their evaluation reveals significant qualitative differences among FL frameworks. Furthermore, training experiments on frameworks with various algorithm implementations indicate that the choice of model type has a more significant impact on performance than the algorithm or framework. Regarding system performance (training efficiency, communication efficiency, and memory usage), no single framework consistently outperforms the others, which is an interesting finding. Our measurement of system performance shows that, interestingly, when considering training efficiency, communication efficiency, and memory usage, there is no framework that consistently outperforms others.

II. Algorithms

An aggregation algorithm in federated learning is a fundamental technique that consolidates model updates from distributed clients. These algorithms are essential for the achievement of a global model while protecting data privacy, allowing for collaborative learning across distributed networks.

Federated Averaging, also known as FedAvg, serves as a key algorithm in federated learning. Its purpose is to facilitate collective model training while ensuring the confidentiality of data. In the FedAvg approach, several distributed clients (like mobile devices or edge servers) autonomously train their individual ML models using their own private data sets. These local models are periodically aggregated on a central server by calculating their weighted average. After receiving the updated global model from the central server, the clients undergo the same process repeatedly. There are two options for assigning weights to the clients in the aggregation: uniform weights or weighted weights. These weights are used to address differences in data distribution or computational resources among the clients. The privacy of data is upheld in FedAvg, where the clients retain their raw data and solely exchange model updates. The algorithm has proven its utility in multiple fields, encompassing healthcare, finance, and edge computing. Notably, it excels in scenarios where data privacy and distributed model training are of utmost importance.

The FedProx (shortened to "FederatedProximal") machine learning algorithm is designed to address the issues associated with the non-identical and identical distribution of data across decentralized clients within a federated learning environment. The FedProx algorithm expands on the traditional federated averaging algorithm (such as FedAvg) by introducing the proximal term. This term serves to stabilize model parameters and accelerate the learning process in federated environments, even when client data distributions are significantly different. The goal of FedProx is to balance global model aggregation with local model adaptation in federated environments where traditional learning methods may not be sufficient. The algorithm has demonstrated promising results in terms of convergence and reduction of communication overhead within federated learning environments, making it an invaluable addition to the repertoire of privacy-protecting distributed machine learning techniques.

III. Literature Survey

The results of UniFed demonstrate that the selection of a particular Open Source Federation Learning (FL) framework can have an impact on the performance of the model. However, the different implementations of the same FL algorithm are comparable when it comes to training the same model type. The tree-based models are more effective in vertical environments, while the deep neural networks outperform the shallow ones. The shorter training times are attributed to either Flower or Flute, however Flower has a higher memory requirement than Flute. FedTree outperforms FATE as well as FedLearner in terms of performance, but none of the frameworks consistently outperform the others in all three dimensions. The authors caution that the selection of the model should be based on various scenarios and results from the tests conducted.[1]

FL works by sending a global model to each device, which then trains the model on its own data. The devices then send back updates to the central server, which aggregates the updates and updates the global model. This process is repeated until the model is converged. FL has a number of advantages over traditional machine learning techniques. First, it is more privacy-preserving, as devices do not need to share their data with the central server. Second, it is more data-efficient, as FL can train models on decentralized data. Third, FL is more scalable, as it can be used to train models on large datasets distributed across many devices. FL is a promising new machine learning technique that can be used to train models on decentralized data without compromising privacy. It has a number of advantages over traditional machine learning techniques, and it has a wide range of applications in healthcare, NLP, computer vision, IoT, and FinTech.[2]

In federated learning, multiple clients work together to solve machine learning challenges, coordinated by a central aggregator, and the training data is decentralized to ensure data privacy for each device. federated learning follows two main ideas: local computing, and model transmission. This reduces systematic privacy risks and costs associated with traditional centralized machine learning. The client's original data is stored locally and can't be exchanged or moved. In federated learning, devices use local data to train locally, upload the model for aggregation, and then send the model update to participants to meet the learning goal. In order to provide a comprehensive survey and facilitate future research, we systematically introduce existing works in federated learning from 5 perspectives: data partitioning; privacy mechanism; machine learning model; communication architecture; systems heterogeneity; current challenges; and future research directions for federated learning. Finally, we summarize existing federated learning characteristics and analyze the practical application.[3]

FL offers the potential to generate robust, accurate, secure, reliable and impartial models. By allowing multiple parties to collaborate without the need for data exchange or centralisation, FL neatly addresses the challenges associated with the transmission of sensitive medical data. This may open up new research and business opportunities, as well as the potential to enhance patient care worldwide. However, FL already has a significant impact on nearly all stakeholders and the overall treatment cycle, from enhanced medical image analysis to provide clinicians with more effective diagnostic tools, to true precision medicine by aiding in the identification of similar patients, to the collaborative and expedited drug discovery that reduces costs and time to market for pharma companies.[4]

The paper discusses the rising trend of wearable healthcare technology, such as smartphones and smart glasses, for monitoring daily activities and detecting cognitive diseases like Parkinson's. It addresses the challenges of data isolation and lack of personalization in wearable healthcare. To tackle these issues, the paper introduces FedHealth, a federated transfer learning framework. FedHealth constructs an initial cloud model using public datasets, distributes it to users, and refines it using their data through transfer learning. This approach balances personalized models and data privacy. The experiments conducted on a smartphone dataset demonstrate the effectiveness of FedHealth in auxiliary Parkinson's disease diagnosis, outperforming other methods. The framework leverages federated learning to create a more generalized cloud model on the server while enabling users to derive personalized models through transfer learning. FedHealth holds promise for advancing wearable healthcare and federated computing in the healthcare domain.[5]

This paper introduces federated learning as an alternative to traditional server-based data collection and training in a commercial context. It demonstrates that the federated algorithm, leveraging client devices, can achieve superior prediction recall. The study uses a variation of LSTM called "Coupled Input and Forget Gate" (CIFG) to build language models, which efficiently manage information retention and improve mobile device performance. The FederatedAveraging algorithm combines client updates on the server to produce a global model. In experiments, the CIFG model trained through federated learning outperforms server-trained CIFG and baseline models for next-word prediction in a keyboard

application. The federated approach not only enhances model quality but also provides security and privacy benefits for users. This research highlights the potential of federated learning in improving language model performance while maintaining data privacy.[6]

Federated learning is a technique where statistical models are trained on devices or data centers located remotely, ensuring that the data remains localized. In the realm of standard federated learning, the primary challenge lies in acquiring knowledge from a solitary global statistical model that is trained using extensive data distributed across numerous remote devices, which could range from a mere tens to a staggering millions. The distributed optimization problem presents several core challenges, including expensive communication, systems heterogeneity, statistical heterogeneity, and privacy concerns. One can enhance communication efficiency through the utilization of local updating methods, compression schemes, and decentralized learning techniques. By incorporating model-compression techniques, it is possible to achieve both privacy advantages and reduced communication when utilizing differential privacy.[7]

In the field of Federated Learning, the authors have proposed an architecture that enables on-demand client deployment at the edge. In order to enable new devices to seamlessly and effectively join the learning process, the utilization of ”Containerization technology” has been employed. The usage of ”Kubeadm” is being observed by them. This tool enables the creation of Kubernetes clusters in an efficient manner. The architecture is composed of three layers: the server/service provider layer, the orchestrators/mini server layer, and the user devices layer. The server is in charge of making spontaneous decisions to determine which nodes should participate in cluster formation. It is supported by the orchestrator and also handles the management of the global model. Additionally, the server maintains a secure connection with the underlying layers. The utilization of orchestrator nodes involves the establishment of Kubeadm clusters, overseeing device movements within their vicinity, handling container deployment, and incorporating fresh clients into the cluster. In order to eliminate the risk of a single point of failure and to enhance efficiency, the addition of an orchestrator layer becomes crucial, particularly in highly dynamic scenarios. The disparity of 10% between the centralized and FL model proves to be a reasonable concession in exchange for safeguarding the confidentiality of the data.[8]

The Federated Learning (FL) framework is a distributed machine learning approach that generates a global model on a centralized aggregation server, taking into account local model parameters to address privacy concerns associated with the collection of training data. As the computational and communication capabilities of edge and Internet of Things (IoT) devices continue to increase, the use of FL for training machine learning models across heterogeneous devices is becoming a common practice. However, the traditional synchronous aggregation approach in the classical FL paradigm, especially in the heterogeneous device context, has limitations in terms of resource utilization as it necessitates waiting for slow devices to be aggregated in each training iteration. Additionally, the heterogeneous nature of the data across devices, such as data heterogeneity, has had a negative impact on the global model’s accuracy. As a result, a variety of asynchronous FL approaches have been adopted across different application contexts to improve efficiency, performance and privacy, and to address these issues. This survey provides a comprehensive analysis and summary of existing AFL variations, using a new classification scheme to cover device heterogeneity, data heterogeneity, privacy and security, and applications. Additionally, the survey reveals increasing challenges and presents potential research directions in an under-explored domain.[9]

Training ML models which are fair across different demographic groups is of critical significance due to the increased integration of ML in pivotal decision- making scripts similar as healthcare and reclamation. Federated literacy has been viewed as a promising result for collaboratively training machine literacy models among multiple parties while maintaining their original data sequestration. still, allied literacy also poses new challenges in mollifying the implicit bias against certain populations(e.g., demographic groups), as this generally requires centralized access to the sensitive information(e.g., race, gender) of each datapoint. Motivated by the significance and challenges of group fairness in allied literacy, in this work, we propose FairFed, a new algorithm for fairness-apprehensive aggregation to enhance group fairness in allied literacy. Our proposed approach is garçon- side and agnostic to the usable original debiasing therefore allowing for flexible use of different original debiasing styles across guests. We estimate FairFed empirically versus common nascences for fair ML and allied literacy and demonstrate that it provides fairer models, particularly under largely miscellaneous data distributions across guests. We also demonstrate the benefits of FairFed in scripts involving naturally distributed real- life data collected from different geographical locales or departments within an association.[10]

The paper ”A Performance Evaluation of Federated Learning Algorithms” explores the conception of allied literacy, which involves training machine literacy models by adding up locally trained models from distributed guests. The paper focuses on bracket tasks using Artificial Neural Networks(ANNs) and evaluates three allied literacy algorithms Federated Averaging(FedAvg), Federated Stochastic Variance Reduced grade(FSVRG), and hutch. The evaluation compares their performance against a centralized literacy approach using the MNIST dataset. The results indicate that FedAvg achieves the loftiest delicacy among the allied algorithms, anyhow of how the data was partitioned. still, the centralized approach outperforms FedAvg when dealing withnon-i.i.d. data. The paper also addresses challenges related to data sequestration and communication in allied literacy, proposing results to minimize data transfer and cover sequestration.[11]

Federated literacy is a machine literacy paradigm that emerges as a result to the sequestration- preservation demands in artificial intelligence. As machine literacy, allied literacy

is hovered by inimical attacks against the integrity of the literacy model and the sequestration of data via a distributed approach to attack original and global literacy. This weak point is aggravated by the attainability of data in allied literacy, which makes the protection against inimical attacks harder and evidences the need to furtherance the exploration on defence styles to make allied learning a real result for securing data sequestration. In this paper, we present an expansive review of the pitfalls of allied literacy, as well as as their corresponding countermeasures, attacks versus defences. This check provides a taxonomy of inimical attacks and a taxonomy of defence styles that depict a general picture of this vulnerability of allied literacy and how to overcome it. Likewise, we expound guidelines for opting the most acceptable defence system according to the order of the inimical attack. either, we carry out an expansive experimental study from which we draw farther conclusions about the geste of attacks and defences and the guidelines for opting the most acceptable defence system according to the order of the inimical attack. Eventually, we present our learned assignments and challenges.[12]

This study explores the field of federated learning (FL) and the tools used to implement FL pipelines that can significantly accelerate research in this field. The study provides a comprehensive overview of open source solutions and offers two rankings based on tool popularity and readiness. The main goal is to guide users, including non-experts, to adopt FL solutions, promote their use and accelerate research and development in the field. One of the main findings of the study is that the tools most commonly used in the community are not necessarily the most mature skills. By conducting multiple searches over nearly a year, the researchers gained valuable insight into the growth rates of these tools, allowing them to make clear recommendations to end users starting their FL research journey.[13]

This research paper introduces Federated Learning (FL), a privacy-preserving machine learning approach used in various domains like finance, healthcare, and edge computing. Unlike traditional distributed machine learning, FL involves localized data training and collaborative model creation, ensuring individual data privacy. The paper outlines the common workflow of FL, involving local model updates, parameter aggregation, and model distribution, with researchers focusing on improving specific steps for various scenarios.

To address the inefficiencies in FL algorithm implementations, the paper introduces FedLab, a highly customizable framework for FL simulations. FedLab offers flexibility, scalability, and standardized FL implementation schemes, simplifying the development of FL algorithms. It provides data partition tools, standard FL system templates, benchmarks, and open-source resources for continuous maintenance.

In summary, the paper presents FedLab as a versatile framework for FL research, making it easier for researchers to work on specific components of FL algorithms and facilitating the standardization of FL simulations.[14]

Federated Learning (FL) is a promising machine learning approach that enables multiple clients to train a shared model without sharing their data. However, FL can still be vulnerable to privacy attacks, where an adversary can infer private information from the uploaded model parameters. To address this challenge, this paper proposes a novel FL framework called Noisy Before Model Aggregation FL (NbAFL). NbAFL adds artificial noise to the model parameters at the client side before aggregation, which effectively prevents information leakage while still allowing the model to converge. The authors prove that NbAFL satisfies differential privacy (DP), a rigorous mathematical framework for ensuring privacy in machine learning. They also develop a theoretical convergence bound for NbAFL, which reveals the tradeoff between convergence performance and privacy protection. To further improve convergence performance, the authors propose a K-client random scheduling strategy, where K clients are randomly selected from the overall set of clients to participate in each aggregation. They show that this strategy also retains the above three properties, and that there is an optimal K that achieves the best convergence performance at a fixed privacy level. Evaluations demonstrate that the authors' theoretical results are consistent with simulations. This work facilitates the design of various privacy-preserving FL algorithms with different tradeoff requirements on convergence performance and privacy levels. Potential applications of NbAFL: NbAFL can be used in a variety of applications where FL is used to train models on sensitive data, such as: Healthcare: NbAFL can be used to train models on patient data without exposing the data to the server or to other clients. Finance: NbAFL can be used to train models on financial data without exposing the data to the server or to other clients. Government: NbAFL can be used to train models on government data without exposing the data to the server or to other clients. Overall, NbAFL is a promising new FL framework that can help to protect client privacy while still enabling the training of effective models.[15]

METHODOLOGY

Federated Learning involves a structured approach to design, implement, and evaluate federated learning systems. Below is a comprehensive outline of the steps and considerations involved in such a methodology:

1) Problem Formulation and Goal Definition:
   - Clearly define the problem that federated learning aims to solve.
   - Set specific goals and objectives for the federated learning project.
2) Data Preprocessing:
   - Prepare and preprocess data at the client nodes to ensure consistency and compatibility.
   - Address data quality issues, anonymization, and data distribution disparities.
3) Client Selection:
   - Determine the selection criteria for participating clients.

- Consider factors such as device capabilities, data quality, and willingness to participate.

4) Model Selection and Design:
   - Choose appropriate machine learning models for the federated learning task.
   - Design the global model architecture, considering privacy and communication constraints.
5) Privacy Preservation:
   - Implement privacy-preserving techniques, such as secure aggregation, federated averaging, or encryption, to protect sensitive data during model updates.
6) Communication Protocol:
   - Define the communication protocol for exchanging model updates between the server and clients.
   - Optimize communication frequency and bandwidth usage.
7) Model Initialization:
   - Initialize the global model and distribute it to client nodes.
   - Define a strategy for aggregating client updates.
8) Training and Optimization:
   - Train the global model iteratively using client updates.
   - Monitor convergence, stability, and efficiency of the federated learning process.
   - Experiment with hyperparameter tuning and optimization strategies.
9) Evaluation Metrics:
   - Select appropriate evaluation metrics to assess the performance of the global model.
   - Include metrics that measure model accuracy, fairness, and robustness.
10) Validation and Testing:
   - Validate the federated learning system using validation datasets.
   - Conduct testing for model robustness, scalability, and security.
11) Performance Analysis:
   - Analyze the performance of federated learning with respect to the defined goals and objectives.
   - Continuously improve the system based on the analysis results.

SYSTEM ARCHITECTURE

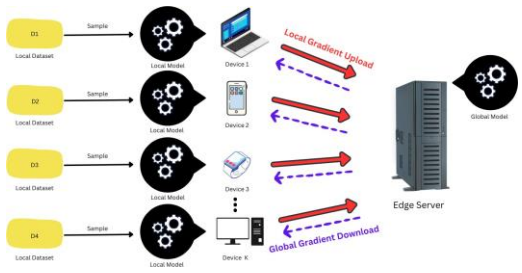

Fig. 1. Federated Learning Architecture

CONCLUSION

This research project involves conducting a survey of available open-source solutions. The primary objective is to offer guidance to users, including those who may not be experts in the field, in the adoption of FL solutions. This guidance aims to encourage the use of FL tools, facilitate their utilization, and accelerate progress in research and development within this domain. An important observation made in this study is that the tools most commonly embraced by the community may not necessarily represent the most mature options. By conducting research it provides valuable insights into the growth trajectories of these tools, enabling the provision of clear recommendations to users embarking on their FL research journey.

REFERENCES

[1] X. Liu, T. Shi, C. Xie, Q. Li, K. Hu, H. Kim, X. Xu, B. Li, D. Song, " UniFed: A Benchmark for Federated Learning Frameworks ", arXiv preprint arXiv:2207.1030, 2022.
[2] M. Khan, F. Glavin, M. Nickles, " Federated Learning as a Privacy Solution - An Overview ", Procedia Computer Science, Volume 217, Ireland, Elsevier, 2023, Pages 316-325.
[3] C. Zhang , Y. Xie b , H. Bai , B. Yu, "A survey on federated learning", China ,Knowledge-Based Systems ,2021.
[4] N. Rieke ,J. Hancox , W. Li , F. Milletar`ı , "The future of digital health with federated learning",Italy, Npjdigitalmed,2020.
[5] Y. Chen, X. Qin, J. Wang, C. Yu and W. Gao, "FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare," in IEEE Intelligent Systems, vol. 35, no. 4, pp. 83-93, 1 July-Aug. 2020.
[6] A. Hard, K. Rao, R. Mathews, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, D. Ramage, "Federated Learning for Mobile Keyboard Prediction ", Mountain View, CA, U.S.A, Google LLC, 2018.
[7] T. Li, A. K. Sahu, A. Talwalkar and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions" in IEEE Signal Processing Magazine, Volume 37, Issue 3, pp. 50-60, May 2020.
[8] M. Chahoud, S. Otoum, A. Mourad. "On the feasibility of Federated Learning towards on-demand client deployment at the edge". Information Processing and Management, Volume 60, Issue 1. Lebanon, United Arab Emirates, United Arab Emirates. Elsevier, 2023.
[9] C. Xu, Y. Qu, L. Gao,"Asynchronous federated learning on heterogeneous devices: A survey", Computer Science Review, Volume 50, November 2023.
[10] S. Yan, C. He ,E. Ferrara,"FairFed: Enabling Group Fairness in Federated Learning",Proceedings of the AAAI Conference on Artificial Intelligence,Vol. 37 No. 6: AAAI-23 Technical Tracks 6, November 2023.
[11] A. Nilsson, S. Smith, G. Ulm, "A Performance Evaluation of Federated Learning Algorithms", Norway, DIDL'20,2020.
[12] N. Rodríguez-Barroso,D. Jiménez-López,M. Victoria Luzón,"Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges",Information Fusion,Volume 90, Pages 148-173 , February 2023.
[13] W. Riviera, I. B. Galazzo and G. Menegaz, "FeLebrities: A User-Centric Assessment of Federated Learning Frameworks," in IEEE Access, vol. 11, pp. 96865-96878, 2023.
[14] D. Zeng, S. Liang, X. Hu, H. Wang, Z. Xu, "FedLab: A Flexible Federated Learning Framework", Journal of Machine Learning Research 24, 2023.
[15] K. Wei, J. Li, M. Ding, C. Ma, H. Yang, F. Farokhi, S. Jin, T. Quek, H. Poor, "Federated Learning With Differential Privacy: Algorithms and Performance Analysis," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3454-3469, 2020.

[16] J. Hernandez-Ramos, G. Karopoulos, E. Chatzoglou, V. Kouliaridis, E. Marmol, A. Gonzalez-Vidal, G. Kambourakis, "Intrusion Detection based on Federated Learning: a systematic review",arXiv preprint arXiv:2308.09522v1, 2023.
[17] S. Tyagi, I. S. Rajput and R. Pandey, "Federated learning: Applications, Security hazards and Defense measures," 2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT), Dehradun, India, 2023.
[18] L. Lyu, H. Yu, X. Ma, C. Chen, L. Sun, J. Zhao, Q. Yang, P. Yu, "Privacy and Robustness in Federated Learning: Attacks and Defenses," in IEEE Transactions on Neural Networks and Learning Systems, 2022.
[19] A. Rahman. M. Hossain, G. Muhammad, D. Kundu, T. Debnath, M. Rahman, M. Khan, P. Tiwari, S. Band, "Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues", Cluster computing 26, no. 4, 2023.
[20] D. Chen, V. Tan, Z. Lu, E. Wu, J. Hu, "OpenFed: A Comprehensive and Versatile Open-Source Federated Learning Framework", Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2023.
[21] Y. Zhang, D. Ramage, Z. Xu, Y. Zhang, S. Zhai, P. Kairouz, "Private Federated Learning in Gboard", arXiv preprint arXiv:2306.14793, 2023.
[22] Z. Danish, I. Khan, Danish, Zargar, and Ihtiram Raza Khan. "A review of Federated Learning." In ICIDSSD 2022: Proceedings of the 3rd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2022, 24-25 March 2022, New Delhi, India, 2023.
[23] Y. Chen, S. Huang, W. Gan, G. Huang, Y. Wu, "Federated Learning for Metaverse: A Survey", arXiv preprint arXiv:2303.17987, 2023.
[24] M. Chahoud, H. Sami, A. Mourad, S. Otoum, H. Otrok, J. Bentahar, M. Guizani, "On-Demand-FL: A Dynamic and Efficient Multicriteria Federated Learning Client Deployment Scheme," in IEEE Internet of Things Journal, vol. 10, no. 18, pp. 15822-15834, 15 Sept.15, 2023.
[25] O. Wehbi, O. A. Wahab, A. Mourad, H. Otrok, H. Alkhzaimi and M. Guizani, "Towards Mutual Trust-Based Matching For Federated Learning Client Selection," 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 2023.
[26] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, B. He, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3347-3366, 1 April 2023
[27] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications", Information processing and management 59, no. 6, 2022.
[28] P. Kairouz, H. McMahan, B. Avent, A. Bellet, M. Bennis, A. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, R. D'Oliveira, H. Eichner, S. Rouayheb, D. Evans, J. Gardner, Z. Garrett, A. Gascón, B. Ghazi, P. Gibbons, M. Gruteser, Z. Harchaoui, C. He, L. He, Z. Huo, B. Hutchinson, J. Hsu, M. Jaggi, T. Javidi, G. Joshi, M. Khodak, J. Konecný, A. Korolova, F. Koushanfar, S. Koyejo, T. Lepoint, Y. Liu, P. Mittal, M. Mohri, R. Nock, A. Özgür, R. Pagh, H. Qi, D. Ramage, R. Raskar, M. Raykova, D. Song, W. Song, S. Stich, Z. Sun, A. Suresh, F. Tramèr, P. Vepakomma, J. Wang, L. Xiong, Z. Xu, Q. Yang, F. Yu, H. Yu, S. Zhao, "Advances and Open Problems in Federated Learning", Foundations and Trends® in Machine Learning: Vol. 14: No. 1–2, pp 1-210, 2021.
[29] F. Lai, Y. Dai, S. Singapuram, J. Liu, X. Zhu, H. Madhyastha, M. Chowdhury,"FedScale: Benchmarking Model and System Performance of Federated Learning at Scale", Proceedings of the 39th International Conference on Machine Learning, PMLR 162:11814-11827, 2022.
[30] P. Foley, M. Sheller, B. Edwards, S. Pati, W. Riviera, M. Sharma, P. Moorthy, S. Wang, J. Martin, P. Mirhaji "OpenFL: the open federated learning library", Physics in Medicine and Biology, 67(21), p.214001, 2022.