ARTICLE

JOURNAL`S UNIVERSITY OF BABYLON FOR ENGINEERING SCIENCES (JUBES)

مـــجلـة جـــامعة بـــــابـل للعلـــــوم الهندسية

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

Literature Review of Federated Learning in Various Applications, Challenges, and Emerging Research Directions

Tiba Saad Mohammed[1], Hilal Al-Libawy[2]

[1,2]of Electrical Engineering, College of Engineering, University of Babylon, Babel, Iraq

Email:.[1] tiba.mohammed@student.uobabylon.edu.iq , [2] eng.hilal_al-libawy@uobabylon.edu.iq

Received:	26/9/2023	Accepted:	27/11/2023	Published:	15/4/2024

Abstract

Federated Learning (FL) is an emerging technology recently used collaboratively with machine learning approaches. It has been the key to an effective solution to the major global problem of protecting sensitive data. The data is trained locally within the clients, the server collects the models trained from the clients and the global model is generated. They have been used in many applications, particularly in applications that require data protection, such as medical applications whose data is legally protected. This paper discusses standardized learning applications that are still in their infancy due to the many challenges facing researchers. The latest developments in Federated Learning and open fields are outlined for researchers to develop this technology. It has been concluded that the most critical area researchers seek to develop is improving the global model. The main causes and challenges affecting the quality of global models were clarified. Finally, some proposals are presented to improve the Federated Learning technology.

Keywords: Federated learning, Internet of Medical Things, Heterogeneous data, Server, Client.

1. Introduction

FL aims to construct a cohesive machine-learning model by harnessing data from numerous decentralized locations.. These strategies are expected to significantly impact advancing AI to the next stage when models can be constructed in a collaborative, secret, and privacy-preserving manner. We can compare the traditional centralized Machine Learning (ML) and Federated Learning (FL) as the following . In ML, the training has occurred on centralized data located on the cloud or central server. The training takes place primarily in the cloud in machine learning and cannot operate on heterogeneous data, and the data privacy is low. FL has been suggested to solve all of Machine Learning's problems. The training process is done on distributed data. Moreover, this data stays with its owner and has high user data privacy. Training happens cross-silos/ cross-devices and can operate on heterogeneous data. FL is a way of ML in which multiple entities, called "clients," work together to solve Machine Learning problems while being watched by a central server or service provider. [2], as depicted in Figure 1.

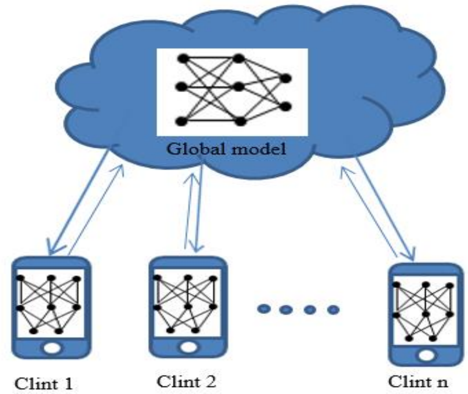

Figure 1: Federated learning work principle.

The raw data of each individual client is saved in a local repository, as opposed to being shared or downloaded. Instead, utilizing targeted updates enables the rapid aggregation of data to attain the desired learning outcome. In contrast to conventional machine learning algorithms, the Federated Learning (FL) algorithm encompasses three primary constituents: a learning algorithm and training methodology, a mechanism for safeguarding data privacy, and a participant incentive mechanism. Following the local training of each client, the server employs an iterative aggregation process, which is often known as the learning algorithm and training technique. The collaborative model training utilizes a data privacy protection mechanism and an incentivization system to foster client engagement.

There exist three various classifications of Federated Learning (FL) methodologies. depending on how data is stored in different clients. Figure 2 is an illustration of three types of FL.

1. Horizontal FL: Both datasets share the same feature space but differ in the sample ID space. For example, a tiny user intersection exists between two banks in different regions. The business is comparable to the feature space.[2]

2. Vertical FL: The sample ID space is the same in both datasets; however, the feature space differs. In the same city, for example, banks and hospitals. Users frequently cross paths because its user base may include most of the community's people. Banks and hospitals, however, do not do business the same way, so the feature space is different.[3]

3. Transfer FL: The sample sizes of the two datasets and the number of features they contain differ. It could be in China, a bank, or a hospital in the United States. To consider a financial institution in the People's Republic of China and a healthcare facility in the United States of America. The intersections between the sample space and feature space are pretty limited.[4]

Additional studies have been conducted on the training and configuration of the horizontal Federated Learning (HFL) model. There are numerous unresolved inquiries around Vertical

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

Federated Learning (VFL) and Transfer Federated Learning (TFL) . Future research is anticipated to contribute to developing the remaining two categories .

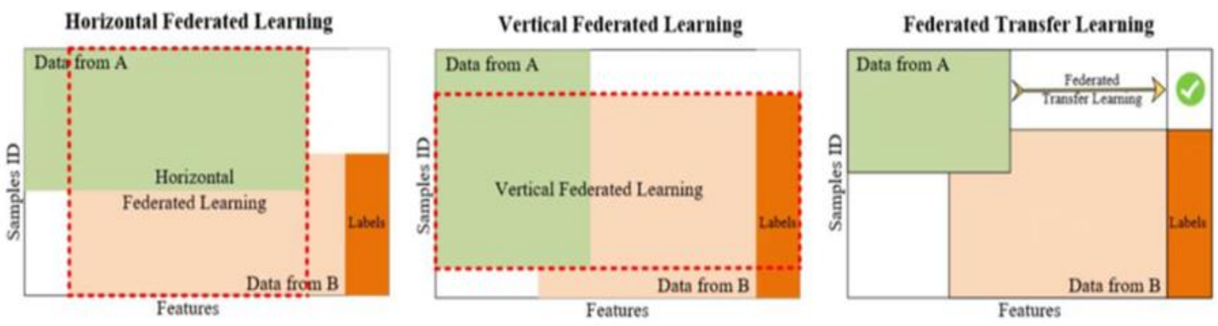

Figure 2: Types of federated learning.

The remaining sections of the paper will provide the most important applications used in this technology (see section 2) , a literary review of previous works in FL (see section 3) , the mechanism of the training process in the FL (see section 4) and the most important challenges facing researchers (see section 5).

2. Application of federated learning

The difficulties that FL addresses are diverse, illustrating the versatility of FL, similar to other AI technologies, in its applicability across multiple industries, as depicted in Figure 3. However, there are significant data privacy issues that need to be addressed by FL. As a result, there is still a need for research into using FL to deal with actual challenges in other fields. One of this research aims is to review the prevailing applications and guide future researchers towards other engineering industry applications. The most famous applications that have been used in the Federated Learning technique is :

1. Healthcare [6,7].
2. Internet of Things and Edge Computing[8]
3. Physical Information System [9]
4. Internet and Finance [10]
5. Urban Computing and Smart Cities [11]
6. Industrial Manufacturing [12]

In the medical field, data privacy is essential. In all hospitals and health centers, they contain records of patient information. Still, this data is legally protected, and it is not allowed to be used even to benefit from it scientifically in the field of artificial intelligence. Therefore,

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

Federated Learning was used as an experimental method to solve the privacy problem for the first time in 2017[13] . Where the tensor factor model was used to analyze the apparent pattern of obtaining hidden Information from the data record in hospitals and health centres to maintain patient privacy. Use FL to predict the death rate of heart patients[14]. Used in COVID-19 identification [15,16,17,18,19,20,21] . The study presented within this article has the potential to facilitate comprehension of the technical efficacy of FL within the medical domain. Have been expected that FL for medical applications will see increasing publicity in the future.

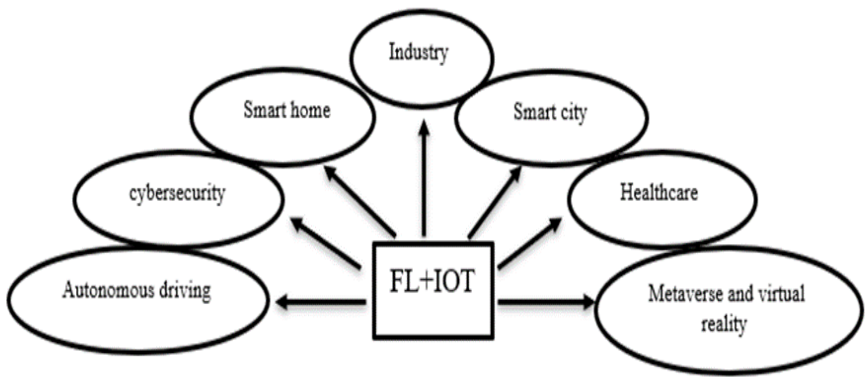

Figure 3: The applications of Federated Learning (FL).

3. Literature Review

Statistical analysis is undertaken on the sorts of articles as shown in Figure 4, by reading and analyzing FL-related articles. Because FL is a new study path, there are significant gaps in theory and implementation. As a result, many research papers have appeared on platforms like as arXiv, which does not require direct peer review, which is not surprising considering that FL is a relatively new study field that is widely utilized to build new technologies quickly. ArXiv/bioRxiv published 41% of the articles. The fact that 36% of the publications were published in conferences demonstrates FL's rapid development and new qualities. FL has produced more developed findings, as evidenced by the fact that 19% of the publications were published in journals. Theses and dissertation are accounted for 4% of the papers, demonstrating that FL has been thoroughly researched [23].

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

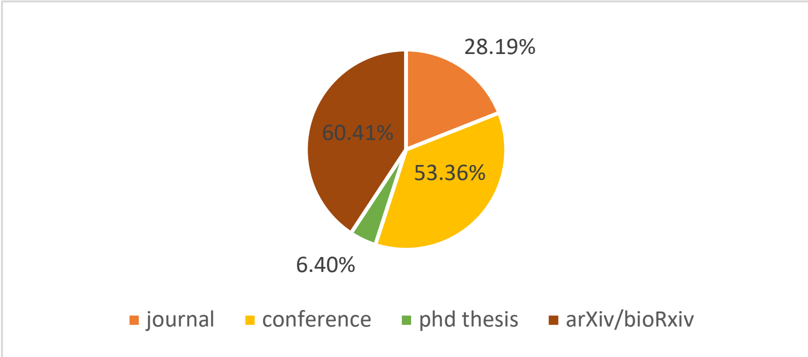

Figure 4: Article type

Machine learning is becoming increasingly important in various sectors, including natural language processing, Internet of Things (IoT), pattern recognition, machine vision and others. The implementation of the General Data Protection Regulation (GDPR) in 2016 by the European Union (EU) was a direct response to the increasing frequency of data leaks and privacy breaches in the context of widespread data usage and artificial intelligence. The European Union (EU) has stipulated a two-year period for member states to achieve full compliance with the General Data Protection Regulation (GDPR) within their respective jurisdictions. The General Data Protection Regulation (GDPR) was officially implemented on May 25, 2018.

In 2017, McMahan et al.[13] developed (FL) method to resolve the conflict between the machine learning training process and data privacy protection involving many data-shared samples. FL is based on sharing model parameters that can be combined into a single model.

In 2018, B. Yan et al.[24] a study showcased the efficacy of a unique algorithm that leverages these weaknesses to substitute models. The program's performance was evaluated on prevalent Federated Learning tasks, including image classification and word prediction. The process of model replacement has been executed effectively.

in 2018, A. Hard et al. [25] proposed the next-word prediction model was put up. This model employs a variant of the Long Short-Term Memory (LSTM) recurrent neural network, specifically the Coupled Input and Forgets Gate (CIFG) architecture. To construct a predictive model, it is necessary to obtain a representative sample of the textual data that users often generate in the context of big data.

In 2018, T. Li et al. [26] saw the introduction of an approach known as FedProx, which aimed to tackle the issue of heterogeneity inside federated networks. FedProx is a method that involves re-parametrizing the FedAvg algorithm, specifically in the context of the Modified National Institute of Standards and Technology's dataset (MNIST).

In 2019, Y. M. Saputra et al. [27] proposed novel approaches using state-of-the-art machine learning techniques aiming at predicting energy demand for electric vehicle (EV) networks. These methods can learn and find the correlation of complex hidden features to improve prediction accuracy.

In 2020, C. He et al. [28], the concept of Federated Learning (FL) was redefined as FedGKT, which stands for Federated Group Knowledge Transfer, an algorithm designed for training in knowledge transfer among groups. The CIFAR-10, CIFAR-100, and CINIC-10 datasets are all data collections curated by the Canadian Institute for Advanced Research. It is widely recognized that augmenting the scale of a convolutional neural network (CNN), such as expanding its width, depth, and other relevant factors, leads to enhanced model accuracy.

In 2021, M. Malekzadeh et al. [29] proposed Dopamine, a system for training DNNs on distributed medical image datasets that combines (FL) with (DPSGD) differentially-private stochastic gradient descent and, when combined with very secure aggregation, achieves a good trade-off between differential privacy (DP) guarantee and DNN accuracy than other approaches. Using model averaging, Federated Learning allows hundreds or even millions of participants, some of whom will almost certainly be evil, to have direct control over the weights of the jointly learned model. A malicious participant can use this to insert a backdoor subtask into the joint model. Secure aggregation ensures that no one can spot abnormalities in participant submissions. Furthermore, Federated Learning is designed to benefit from non-identifiable local training data while maintaining privacy. This leads to a wide variety of models among participants, rendering anomaly detection ineffective in any case.

In 2021, Z. Xiong et al. [30] Federated learning (FL) has received considerable attention in the domain of Artificial Intelligence of Things (AIoT) due to its potential as a method for managing extensive data processing, ensuring privacy protection, and providing high-quality service . primarily concentrates on privacy-preserving Federated Learning (FL) in the context of independent and identically distributed (IID) data, without taking into account the implications of non-IID data. This study utilizes a distinctive methodology referred to as 2DP-FL in order to attain differential privacy through the introduction of noise during local model training and global model distribution.

In 2021, R. Kumar et al. [31] introduced a system that utilizes data collection from several sources, including hospitals equipped with diverse types of CT scanners. The system employs a global deep learning model, which is trained through blockchain-based Federated Learning techniques, while ensuring the preservation of the organization's identity. Federated Learning enables hospitals to maintain data privacy by exclusively sharing weights and gradients, while blockchain technology facilitates data distribution across multiple institutions. Federated Learning employs data encryption and decentralizes the training process across a network, facilitating the development of an improved model by leveraging up-to-date patient data.

In 2021 L. Qu et al [7] demonstrated the improved uniform learning on heterogeneous data due to the greater robustness of self-interest-based designs (e.g., transformers) against distribution modifications. Notably, it was carried out the first thorough experimental analysis of several neural architectures using a range of standardized algorithms, industry norms, and diverse data segmentations.

In 2022 X. Shang et al.[32] CReFF algorithm was proposed to solve one of the FL problems where heterogeneous data was handled by retraining a workbook with standardized learnable features on the server. An interesting fact revealed is that the biased classifier is The primary factor that leads to poor performance of the global FL model on heterogeneous and long-tail data.

In 2022 Luca.A et al. [33] investigated the generalization of federated domains. The objective is to develop a model through Federated Learning that generalizes both in-domain (ID) and out-of-domain (OOD) information, with each client owning a proprietary dataset. A client that has not taken part in the federated training process possesses an out-of-domain dataset. The in-domain datasets are the private ones used by the participating clients during training. Federated Learning and Domain Generalization (DG) are bridged in this situation. Inspired by the success of data augmentation in DG, have been demonstrated how data augmentation might improve generalization and convergence by mitigating the non-iidness in FL from a causal standpoint

In 2023, Chen.k et al. [34] Work was presented to solve the problem of complete heterogeneity in standardized learning where model heterogeneity, data heterogeneity and computational heterogeneity were addressed. Three approaches called synthetic data generation, knowledge distillation and opportunistic computation were introduced to produce a new method called FHFL.

In 2023 Z. Liu et al.[35] The Federated Contrastive Learning (FedCL) method has been proposed, based on the combination of standardized learning and contrastive learning to solve the problem of data heterogeneity in hospitals. The basic idea of contrastive learning is to reduce the distance between the features of a pair of samples from the same class, and to increase the distance between the features of a pair of samples from different classes.

4. Training Process in Federated Learning

The primary concept underlying Federated Learning is decentralized learning, wherein the data owner refrains from transmitting their data to a central computer [36]. The process of training a machine learning model consists of the following steps: The learning model constructed by the server is contingent upon the specific network type being employed. Subsequently, the model undergoes instruction on the server. This task can be accomplished by utilizing data obtained from a company that possesses a cloud infrastructure containing the requisite data or by first employing zero values as a substitute. The trained model is distributed by the server to the appropriate clients. The requisite data must be provided to the server in advance. Every each client imparts its knowledge to the local model it possesses by utilizing its own data, so generating a novel model. Subsequently, this new model is transmitted to the server. Thus effectively creating a new main model. However, one-time training is not enough, so the process must be repeated more than once until the model becomes good, and the new model is considered an initial model for the second attempt see Figure 5.

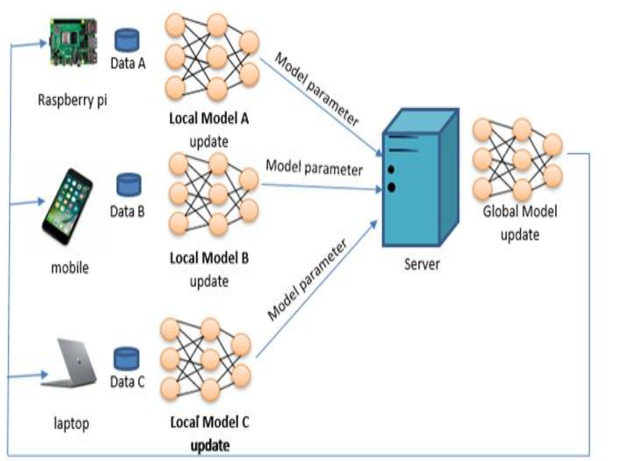

Figure 5: Training process in Federated Learning (FL)

After several attempts, the smart machine shows a sign of intelligence. Thus, a smart machine was created while maintaining the data privacy used in the learning process, as each client trained the model locally and shared only the change in the weights that are the model's parameters without sharing the basic data. The other important thing solved using FL is to create a global model and use data from more than one place to create this model and thus collaboratively share data from more than one source while maintaining privacy. FL is used in circumstances where data is:

• Massively distributed: important data is held by many clients (up to millions) scattered over the world [37].

• Non-IID: Data acquired by different participating clients comes from distinct distributions and is not disseminated independently and uniformly (ID)[38].

• Unbalanced: Some clients may have many data samples, while others may have one[39].

Because these data are heterogeneous, they reduce the accuracy of the normal model used in the Federated Learning technique. Therefore, have been must shed light on this problem and propose new models that overcome the problem of the difference in data distributed to different clients.

5. Challenge in Federated Learning

There are several open challenges in FL, among which are seeking to improve the hyperparameter to maintain specificity and improving the accuracy of the model:

- The high cost of communication: Communication is considered one of the critical issues in the Federal Learning Network, in addition to protecting data privacy during the communication process between the server and the client [40].
- Heterogeneity of the system refers to the difference between local devices, where each device differs in terms of operating frequencies (CPU cycles per second), and each device differs with backup power[26].
- Privacy protection: When opposed to centralized machine learning, the FL training method allows the data to be stored locally, which increases privacy protection. On the other hand, communicating model updates throughout the training process can divulge sensitive information to a third party or a central server. So, recent technologies aim to improve Federated Learning's privacy [41].
- Data (Statistical) heterogeneity refers to the difference in the distribution of the local data set among the participants[42]. The method of calculating the global model with the traditional FL uses the average process to produce the global model without paying attention to the heterogeneity of the data to address this problem .

One of the new challenges in Federated Learning is the problem of not distributing data symmetrically across devices in the network when learning the global model. The first method used in the process of compiling the parameter is Fedavg. However, they found that this method diverges scientifically because the results are considered based on the assumption that each local analyzer is a copy From the same random process. To understand the federal learning settings and its dealing with statistically heterogeneous data, Fedprox was proposed. This method makes a simple modification to the previous method to help ensure convergence in theory and practice. Then the researchers developed these methods and worked to solve and improve the results when dealing with heterogeneous data. They suggested several The methods are as shown in table (1).

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

Table1: Review about methods that are suggested to solve data heterogeneity.

Ref.	Proposed method	Description	Dataset	Accuracy
[32]	CReFF	Classifier Re-training with Federated Features	CIFAR-10-LT CIFAR-100-LT	92%
[38]	HarmoFL	Solve data Heterogeneous challenges	Medical Images	95.48%
[43]	HADFL	Heterogeneity-aware Decentralized FL Framework	ResNet-18 vgg-16	91%
[44]	FEDGEN	Federated Distillation via Generative Learning	MNIST EMNIST CELEBA	73%
[45]	FedProto	Federated Prototype Learning	MNIST FEMNIST CIFAR10	92%
[46]	VIT-FL	Federated Learning with Vision Transformers	Retina dataset CIFAR-10	94.4%
[47]	Novel comprehensive methodology	The present study outlines a comprehensive methodology for conducting smart device sampling with data offloading in the context of Federated Learning (FL).	MNIST F-MNIST	85%
[31]	Normalization	method for dealing with various types of CT scanners	CT scanner COVID-19	98.86%
[48]	LoAdaBoost	IID and non-IID intensive care data are less computationally complex.	MIMIC-III eICU data 90 clients,	79%
[44]	FAug FD	Federated augmentation Federated distribution	MNIST	95% 98%

Table 1. shows an overview of past work that tried to solve the problem of heterogeneity, especially the problem of data heterogeneity, which is seen as more difficult because it can slow down the convergence in the global model and make it less accurate. Since the problem of data heterogeneity is an important challenge in Federated earning technology, have been proposed to find a solution to the problem of data heterogeneity between clients in terms of type, as researchers have not yet addressed this problem to the extent of our work. my suggesting is using a hybrid model to train this different type of data in addition to using data augmentation technology to reduce data heterogeneity and thus improve the results.

6. Conclusion

Federated learning is one of the new artificial intelligence technologies that has been suggested as a way to solve the problems of Machine Learning by training a global model and keeping data private. In this project, have been gaved an overview of Federated Learning and the different kinds of it, as well as a literature study of past work, the problems they faced, and the most important problems that will need to be solved in the future. To train the system, there is a proposal for a Federal Learning model that uses different kinds of data and gadgets. The goal of this paper is to give a review of Federated Learning and show the problem of different types of data and devices used in local training. This includes improving the performance of model training while keeping privacy high and using this system in a healthcare application.

References

[1] O. Simeone, Federated Learning. 2023. doi: 10.1017/9781009072205.019.

[2] M. Y. Topaloglu, E. M. Morrell, S. Rajendran, and U. Topaloglu, "In the Pursuit of Privacy: The Promises and Predicaments of Federated Learning in Healthcare," Front. Artif. Intell., vol. 4, no. October, pp. 1–10, 2021, doi: 10.3389/frai.2021.746497.

[3] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, 2019, doi: 10.1145/3298981.

[4] R. Razavi-far, B. Wang, and M. E. Taylor, Federated and Transfer Learning, vol. 27. 2023. [Online]. Available: https://link.springer.com/10.1007/978-3-031-11748-0

[5] H. Liu, X. Zhang, X. Shen, and H. Sun, "A Federated Learning Framework for Smart Grids: Securing Power Traces in Collaborative Learning," pp. 1–9, 2021, [Online]. Available: http://arxiv.org/abs/2103.11870

[6] P. Boobalan et al., "Fusion of Federated Learning and Industrial Internet of Things: A survey," Comput. Networks, vol. 212, pp. 1–24, 2022, doi: 10.1016/j.comnet.2022.109048.

[7] I. Dayan et al., "Federated learning for predicting clinical outcomes in patients with COVID-19," Nat. Med., vol. 27, no. 10, pp. 1735–1743, 2021, doi: 10.1038/s41591-021-01506-3.

[8] X. Li, Z. Qu, B. Tang, and Z. Lu, "FedLGA: Toward System-Heterogeneity of Federated Learning via Local Gradient Approximation," IEEE Trans. Cybern., vol. 14, no. 8, pp. 1–24, 2023, doi: 10.1109/TCYB.2023.3247365.

[9] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," Med. Image Anal., vol. 65, 2020, doi: 10.1016/j.media.2020.101765.

[10] P. Pinyoanuntapong, P. Janakaraj, P. Wang, M. Lee, and C. Chen, "FedAir: Towards Multi-hop Federated Learning Over-The-Air," IEEE Work. Signal Process. Adv. Wirel. Commun. SPAWC, vol. 2020-May, pp. 0–4, 2020, doi: 10.1109/SPAWC48557.2020.9154266.

[11] B. P. L. Lau et al., "A survey of data fusion in smart city applications," Inf. Fusion, vol. 52, no. January, pp. 357–374, 2019, doi: 10.1016/j.inffus.2019.05.004.

[12] T. Hiessl, S. Rezapour Lakani, J. Kemnitz, D. Schall, and S. Schulte, "Cohort-based federated learning services for industrial collaboration on the edge," J. Parallel Distrib. Comput., vol. 167, pp. 64–76, 2022, doi: 10.1016/j.jpdc.2022.04.021.

[13] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," Proc. 20th Int. Conf. Artif. Intell. Stat. AISTATS 2017, vol. 54, 2017.

[14] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated Electronic Health Records," Int. J. Med. Inform., vol. 112, no. September 2017, pp. 59–67, 2018, doi: 10.1016/j.ijmedinf.2018.01.007.

[15] S. Ghafouri-Fard et al., "Effects of host genetic variations on response to, susceptibility and severity of respiratory infections," Biomed. Pharmacother., vol. 128, no. April, 2020, doi: 10.1016/j.biopha.2020.110296.

[16] M. Heidari Nia et al., "Association of polymorphisms in tumor necrosis factors with SARS-CoV-2 infection and mortality rate: A case-control study and in silico analyses," J. Med. Virol., vol. 94, no. 4, pp. 1502–1512, 2022, doi: 10.1002/jmv.27477.

[17] K. Suryamohan et al., "Human ACE2 receptor polymorphisms and altered susceptibility to SARS-CoV-2," Commun. Biol., vol. 4, no. 1, 2021, doi: 10.1038/s42003-021-02030-3.

[18] A. B. Engin, E. D. Engin, and A. Engin, “Two important controversial risk factors in SARS-CoV-2 infection: Obesity and smoking,” Environ. Toxicol. Pharmacol., vol. 78, no. May, p. 103411, 2020, doi: 10.1016/j.etap.2020.103411.

[19] E. W. Fakhouri, S. J. Peterson, J. Kothari, R. Alex, J. I. Shapiro, and N. G. Abraham, “Genetic polymorphisms complicate covid-19 therapy: Pivotal role of ho-1 in cytokine storm,” Antioxidants, vol. 9, no. 7, pp. 1–23, 2020, doi: 10.3390/antiox9070636.

[20] D. Yang et al., “Federated semi-supervised learning for COVID region segmentation in chest CT using multi-national data from China, Italy, Japan,” Med. Image Anal., vol. 70, p. 101992, 2021, doi: 10.1016/j.media.2021.101992.

[21] A. Tufan, A. Avanoğlu Güler, and M. Matucci-Cerinic, “Covid-19, immune system response, hyperinflammation and repurposinantirheumatic drugs,” Turkish J. Med. Sci., vol. 50, no. SI-1, pp. 620–632, 2020, doi: 10.3906/sag-2004-168.

[22] M. Pandey, S. Pandey, and A. Kumar, “Introduction to Federated Learning,” EAI/Springer Innov. Commun. Comput., pp. 1–17, 2022, doi: 10.1007/978-3-030-85559-8_1.

[23] R. O. Ogundokun, S. Misra, R. Maskeliunas, and R. Damasevicius, “A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology,” Inf., vol. 13, no. 5, 2022, doi: 10.3390/info13050263.

[24] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, “How To Backdoor Federated Learning,” 2018, [Online]. Available: http://arxiv.org/abs/1807.00459

[25] A. Hard et al., “Federated Learning for Mobile Keyboard Prediction,” 2018, [Online]. Available: http://arxiv.org/abs/1811.03604

[26] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated Optimization in Heterogeneous Networks,” 2018, [Online]. Available: http://arxiv.org/abs/1812.06127

[27] Y. M. Saputra, Di. T. Hoang, Di. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, “Energy demand prediction with federated learning for electric vehicle networks,” 2019 IEEE Glob. Commun. Conf. GLOBECOM 2019 - Proc., no. January 2021, 2019, doi: 10.1109/GLOBECOM38437.2019.9013587.

[28] C. He, M. Annavaram, and S. Avestimehr, “Group knowledge transfer: Federated learning of large CNNs at the edge,” Adv. Neural Inf. Process. Syst., vol. 2020-Decem, no. NeurIPS, 2020.

[29] M. Malekzadeh, B. Hasircioglu, N. Mital, K. Katarya, M. E. Ozfatura, and D. Gündüz, “Dopamine: Differentially Private Federated Learning on Medical Data,” no. 677854, 2021, [Online]. Available: http://arxiv.org/abs/2101.11693

[30] Z. Xiong, Z. Cai, D. Takabi, and W. Li, “Privacy Threat and Defense for Federated Learning with Non-i.i.d. Data in AIoT,” IEEE Trans. Ind. Informatics, vol. 14, no. 8, 2021, doi: 10.1109/TII.2021.3073925.

[31] R. Kumar et al., “Blockchain-Federated-Learning and Deep Learning Models for COVID-19 Detection Using CT Imaging,” IEEE Sens. J., vol. 21, no. 14, pp. 16301–16314, 2021, doi: 10.1109/JSEN.2021.3076767.

[32] X. Shang, Y. Lu, G. Huang, and H. Wang, “Federated Learning on Heterogeneous and Long-Tailed Data via Classifier Re-Training with Federated Features,” pp. 2218–2224, 2022, doi: 10.24963/ijcai.2022/308.

[33] A. B. de Luca, G. Zhang, X. Chen, and Y. Yu, “Mitigating Data Heterogeneity in Federated Learning with Data Augmentation,” pp. 1–18, 2022, [Online]. Available: http://arxiv.org/abs/2206.09979

[34] K. Chen et al., “Privacy preserving federated learning for full heterogeneity,” ISA Trans., no. xxxx, 2023, doi: 10.1016/j.isatra.2023.04.020.

[35] Z. Liu, F. Wu, Y. Wang, M. Yang, and X. Pan, “FedCL: Federated contrastive learning for multi-center medical image classification,” Pattern Recognit., vol. 143, 2023, doi: 10.1016/j.patcog.2023.109739.

[36] Y. Zhan, J. Zhang, Z. Hong, L. Wu, P. Li, and S. Guo, “A Survey of Incentive Mechanism Design for Federated Learning,” IEEE Trans. Emerg. Top. Comput., vol. 10, no. 2, pp. 1035–1044, 2022, doi: 10.1109/TETC.2021.3063517.

[37] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, “Federated learning for internet of things: Recent advances, taxonomy, and open challenges,” IEEE Commun. Surv. Tutorials, vol. 23, no. 3, pp. 1759–1799, 2021, doi: 10.1109/COMST.2021.3090430.

[38] M. Jiang, Z. Wang, and Q. Dou, “HarmoFL: Harmonizing Local and Global Drifts in Federated Learning on Heterogeneous Medical Images,” 2021, [Online]. Available: http://arxiv.org/abs/2112.10775

[39] V. D. Nguyen, S. K. Sharma, T. X. Vu, S. Chatzinotas, and B. Ottersten, “Efficient Federated Learning Algorithm for Resource Allocation in Wireless IoT Networks,” IEEE Internet Things J., vol. 8, no. 5, pp. 3394–3409, 2021, doi: 10.1109/JIOT.2020.3022534.

[40] H. Zhang and L. Hanzo, “Federated Learning Assisted Multi-UAV Networks,” IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 14104–14109, 2020, doi: 10.1109/TVT.2020.3028011.

[41] M. Habib, R. Mohamed, M. Gaber, and T. N. Ai, Federated Learning Systems : Towards Next-Generation AI. 2021. [Online]. Available: http://www.springer.com/series/7092

[42] A. Majeed, X. Zhang, and S. O. Hwang, “Applications and Challenges of Federated Learning Paradigm in the Big Data Era with Special Emphasis on COVID-19,” Big Data Cogn. Comput., vol. 6, no. 4, 2022, doi: 10.3390/bdcc6040127.

[43] J. Cao, Z. Lian, W. Liu, Z. Zhu, and C. Ji, “HADFL: Heterogeneity-aware Decentralized Federated Learning Framework,” Proc. - Des. Autom. Conf., vol. 2021-Decem, pp. 1–6, 2021, doi: 10.1109/DAC18074.2021.9586101.

[44] E. Jeong, S. Oh, H. Kim, J. Park, M. Bennis, and S.-L. Kim, “Communication-Efficient On-Device Machine Learning: Federated Distillation and Augmentation under Non-IID Private Data,” no. Nips, 2018, [Online]. Available: http://arxiv.org/abs/1811.11479

[45] Y. Tan et al., “FedProto: Federated Prototype Learning across Heterogeneous Clients,” 2021, [Online]. Available: http://arxiv.org/abs/2105.00243

[46] L. Qu et al., “Rethinking Architecture Design for Tackling Data Heterogeneity in Federated Learning,” 2021, [Online]. Available: http://arxiv.org/abs/2106.06047

[47] M. Aqib, R. Mehmood, A. Alzahrani, I. Katib, A. Albeshri, and S. M. Altowaijri, Smarter traffic prediction using big data, in-memory computing, deep learning and gpus, vol. 19, no. 9. 2019. doi: 10.3390/s19092206.

[48] L. Huang, Y. Yin, Z. Fu, S. Zhang, H. Deng, and D. Liu, “LoadaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data,” PLoS One, vol. 15, no. 4, pp. 1–16, 2020, doi: 10.1371/journal.pone.0230706.

ARTICLE

JOURNAL`S UNIVERSITY OF BABYLON FOR ENGINEERING SCIENCES (JUBES)

مـــجلــة جـــــامعة بــــــابــل للعلـــــوم الهندسية

Vol. 32, No. 2. \ 2024 ISSN: 2616 - 9916

مراجعة الأدبيات للتعلم الموحد في مختلف التطبيقات والتحديات والاتجاهات البحثية الناشئة

طيبة سعد محمد[1], هلال الليباوي[2]

[1&2]قسم هندسة الكهرباء, كلية الهندسة, جامعة بابل, بابل, العراق

Email: [1]sth.tiba.mohammed@student.uobabylon.edu.iq ,

[2] eng.hilal_al-libawy@uobabylon.edu.iq

الخلاصة

التعلم الموحد (FL) هو تقنية ناشئة تم استخدامها مؤخرا بشكل تعاوني مع مناهج التعلم الآلي. لقد كان المفتاح لحل فعال للمشكلة العالمية الرئيسية المتمثلة في حماية البيانات الحساسة. يتم تدريب البيانات محليا داخل العملاء ، ويجمع الخادم النماذج المدربة من العملاء ويتم إنشاء النموذج العالمي الموحد. لقد تم استخدامها في العديد من التطبيقات ، لا سيما في التطبيقات التي تتطلب حماية البيانات ، مثل التطبيقات الطبية التي تكون بياناتها محمية قانونا. تناقش هذه الورقة تطبيقات التعلم الموحدة التي لا تزال في مهدها بسبب التحديات العديدة التي تواجه الباحثين. تم تحديد أحدث التطورات في التعلم الموحد والمجالات المفتوحة للباحثين لتطوير هذه التكنولوجيا. وقد خلص الباحثون إلى أن أهم مجال يسعى الباحثون إلى تطويره هو تحسين النموذج العالمي. تم توضيح الأسباب والتحديات الرئيسية التي تؤثر على جودة النماذج العالمية. وأخيرا، تم تقديم بعض المقترحات لتحسين تكنولوجيا التعلم الموحد.

الكلمات الدالة : التعلم الفيدرالي ،إنترنت الأشياء الطبية ، البيانات غير المتجانسة ، الخادم