Grenze International Journal of Engineering and Technology, June Issue

Exploring the Landscape of Federated Learning: Review of Neoteric FL Algorithms

Shraddha Subhedar[1] and Deepa Parasar[2]
[1]Research Scholar, Amity School of Engineering and Technology, Amity University, Mumbai.
Email: shraddhasubhedar23@gmail.com
[2]Amity School of Engineering and Technology, Amity University, Mumbai.
Email: dparasar@mum.amity.edu

***Abstract*— Federated Learning also known as collaborative learning which employs a decentralized approach. Its features like security, privacy, and low cost of communication makes it popular in the industry. FL facilitates algorithms to get trained across multiple servers with no exchange of the actual data. It results in generating more robust models. This paper furnishes a comprehensive study of various FL algorithms applied in diverse domains as IOT, Secured Banking, Healthcare IOT, IIOT, Cloud based system etc. Objective of the paper is to provide a more detailed review of the FL algorithms in the recent literature.**

***Index Terms*— Federated learning, FTL, GAN, HFL, Non-IID and VFL.**

I. INTRODUCTION

Today, we are witnessing a swift growth of big data and artificial intelligence on a daily basis which resulted in generation of large amounts of data and models. Traditionally, data centres and cloud servers are used to place AI functions used for data learning and modelling [1], which incurs profound limitations causing the IoT data emission. Newly, to build the profound and privacy-enhanced IoT systems, the notion of federated learning (FL) has been put forward. FL is a decentralized collaborative AI strategy in which multiple nodes synchronize with a central server for data training with no sharing of actual data [2]. Distributed multiple devices can work collaboratively to show better performance [3]. As FL limits the attack surface only to the local device, it remarkably reduces the privacy and security threat of the cloud [4]. In this paper, we have discussed various FL algorithms applied in diverse domains such as IOT, Secured Banking, Healthcare IOT, Cloud based system etc. This paper aims to summarize the FL algorithms in recent years.

In 2016, Google coined the concept of Federated Learning. FL establishes a data sharing scheme between mobile terminals and servers to utilize data silos while effectively preserving user privacy [5]. Fig. 1 shows impactful features of Federated Learning Systems which makes it an exceptional extension to merge cross-organizational enterprise into a federal framework, thus constructing joint models for various entities, data from multiple sources, and multiple feature dimensions in an insightful way. Privacy preservation is the primary feature of FL as raw data never leaves the local node. Decentralization is employed as the training data is distributed across multiple devices or clients.

Devices connected to the network can participate in training asynchronously i.e. with no worry of global clock synchronization.

In FL systems, non-IID data implies non-Independently and Identically Distributed data refers to the scenario

Grenze ID: 01.GIJET.10.2.395

where the data on multiple nodes or clients is not uniformly distributed or follows different statistical patterns or properties. To address non-IID data issues, FL systems often adopt algorithms such as weighted aggregation or personalized learning. Local training is a feature of personalized learning.

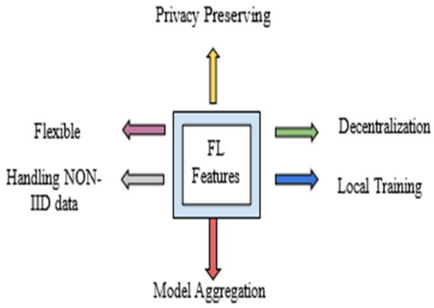

Fig. 1 Features of Federated Learning Systems

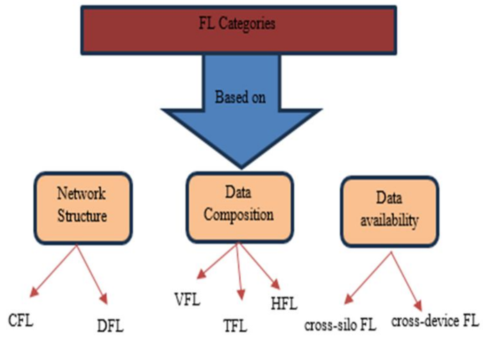

Fig. 2 Federated Learning Categorization

Federated learning can be categorized with respect to various factors as shown in Fig. 2 [6]. First factor is a Network design. Collaborative culture for learning can be built using Federated frameworks with distinct network topology. FL can be categorized into centralized FL and decentralized FL with respect to the underlying architecture. In CFL, a centralized server is connected to massive decentralized worker nodes. In DFL, there is no need for a centralized server. DFL has an aggregator which aggregates information from all the worker nodes and retains a global model over the network.

Data Composition can be an impactful second factor to divide FL systems. According to how training data are spread out among the worker nodes as per the features and samples, FL split into three subcategories: HFL (horizontal federated learning), VFL (vertical federated learning) and FTL (federated transfer learning). VFL can be employed to enable federated learning where sample space is the same but different data features are used by nodes [7] whereas HFL is apt for sample-partitioned FL which means nodes in the network learn collaboratively by utilizing similar features but from non-identical samples.

FTL is inspired from transfer learning which actually transfers knowledge to the worker nodes with data scarcity problems. Usually, these nodes lack overlapping samples and feature samples. [8] [9]

Third factor to divide FL is data availability. Participant entities can distinguish FL either as a cross-silo FL or a cross device FL. Geo-distributed data nodes are Cross - silo FL nodes whereas Mobile or IoT devices are referred as cross device FL nodes.

Federated process shown in Fig. 3 is comprised of following key steps:

Local Update: Initially, the global model is received and based on it, model parameters are updated by local nodes by using local data and processing power.

Data generated by edge nodes will be non-IID which implies non-Independently and Identically Distributed data refers to the scenario where the data on multiple nodes or clients is not uniformly distributed or follows different statistical patterns or properties.

Participant selection: For training random participants will be selected. The global server will accept the gradients only from these selected participants.

Global Aggregation: server aggregates the parameters and updates the global model on every participant.

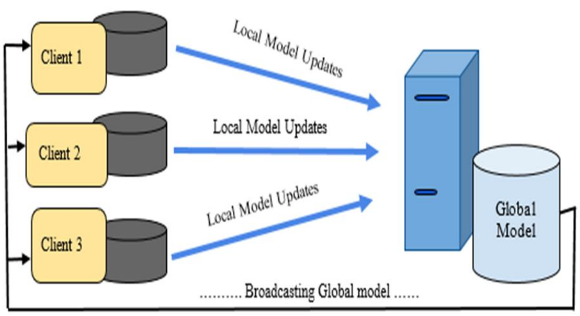

Fig. 3 FL process

II. Literature Review

In literature, a plethora of FL systems have been proposed. We present a meticulous study on various 10 FL algorithms along with their working domain such as communication, image segmentation, network classification and CPS i.e. Cyber Physical Systems.

In a paper entitled “SPinS-FL: Communication-Efficient Federated Subnetwork Learning ", an author Masayoshi Tsutsuihas et. al. [10] has proposed a solution to the bottleneck problem faced by the edge devices in low bandwidth traffic environments. This communication efficiency is enhanced by this. SPinS-FL is a new approach utilizing the Edge-Popup algorithm and the lottery ticket hypothesis. This algorithm forms a subnetwork. In this process, a score is designated to each randomly initialized weight and weights are accepted based on the score. The lottery ticket hypothesis is used to build a trained model where only a random seed value and a supermask are used with no storage of a large number of weights. This suits edge devices with limited memory capacity.

SPinS-FL stands for selectively pinned super-mask federated learning. Instead of communicating all the scores with the server, SPinS-FL only sends a few super masks and a set of scores of the weights around the boundary between selected and unselected in the subnetwork. It causes improvement in communication efficiency dramatically. In this paper, CIFAR-10 and CIFAR-100 datasets are used to experiment. Author has claimed that, in comparison with communicating all the scores, SPinS-FL reduced the traffic volume by up to 79.8%. Accuracy is also achieved by SPinS-FL which proves that it can serve as federated averaging method with less traffic cost.

An author Zhixin Li, Zhihui Lu et. al. has proposed an algorithm AsyFed.[11] It implies Accelerated Federated Learning with Asynchronous Communication Mechanism. AsyFed addresses the straggler issue which is common in IoT devices as there is a huge diversity. [12] Innovativeness of this algorithm lies in model parameter storage which is done by using a gear layer among FL server and Client nodes.

The clients with identical training capacities will be dropped in the same layer to conduct synchronous training. Asynchronous communication takes place among global FL servers and these gears. To deal with the slow gear, authors have also proposed a T-step mechanism which can lower the weight. Using python processing library, threading library AsyFed is implemented on the flsim which is a FL simulation framework based on PyTorch. Process and lightweight thread in flism are used to simulate the gear and client device respectively. CNN is used to train the model. Results claim that in terms of CPU and NIC utilization as well as convergence speed, AsyFed can be preferred over FedAvg. Datasets used are MNIST and CIFAR-10 in IID and Non- IID sets. For performance analysis, results are compared with other FL methods such as FedAvg, TiFL,FedProx and K-center.

Decentralized approach in FL model provides high benefits in medical image analysis. [13] In the paper [14] “IOP-FL Inside and Outside model Personalization in FL” the inside model implies if at the time of model training, clients are seen and present whereas outside model implies unknown clients not present at the time of model training. Here, the global gradients are collected for common knowledge and the local gradients are collected for client-specific optimization. IOP-FL utilizes U-Net and the Adam optimizer. For the dataset, T2-weighted MRI images from 6 different sources and the optic disc and cup segmentation tasks with retinal fundus images from 4 different institutions are used. To evaluate model efficiency on both tasks, The common metric Dice score is used. Authors claim that this algorithm has the perspective of satisfying needs from different clients in parallel in practice.

The major challenges observed in business are uncertainty and endless competition. Establishing strong collaboration among business stakeholders can provide a strong base to face these challenges. To collect vision from various stakeholders and to profound decision-making FL can be served as a strong solution.[15] FedEE is proposed by Zhenzhen Xie, Yan Huang et. al. [16] which utilizes spatial-temporal graph structure data. It can be used as a solution for Extended Enterprise Collaboration for graph Learning. It helps to forcast prediction errors which is helpful for better decision making. For traffic forcasting, TCN (temporal convolutional network), GCN and GRU (gated recurrent unit) are used. Dataset used is collected by the performance measurement system in California named PeMS dataset which is a traffic speed dataset. For performance evaluation MAE, RMSE and loss parameters are used.

Resource heterogeneity is a high concern in a conventional FL, as clients may be unable to complete local training using the same local training hyper-parameters as their weak computational and communication competency. [17] Another algorithm we have referred is HELCHFL which stands for High-efficiency and low-cost hierarchical FL which suits in Heterogeneous MECC (Mobile-Edge Cloud Computing).[18] It enhances the efficiency of FL in terms of cost and training. HELCHFL consists of 3 parts. First is Hierarchical FL with High-Efficiency and Low-Cost. Second based on User Selection which employs Utility-Driven and Heterogeneity-Aware Heuristic approach and third is User’s selection to detect CPU Operating Frequencies. For hierarchical FL training, SqueezeNet ML model is used which is beneficial in terms of training communication cost. Both IID and Non-IID variation of data used from CIFAR-10 and Fashion-MNIST.

K-FL [19] is another FL method we have studied in this survey. Author claims that K-FL can train models with fewer communication rounds in a Non IID environment. The Kalman filter is used to predict accuracy. This accuracy is used to classify devices. LeNet-5 is used as a training model. Datasets used are MNIST, FMNIST and CIFAR-10.

In heterogeneous environments, an innovative federated approach called FEAT is provided which is mainly intended at privacy-protecting network traffic classification. [20] Federated Analytics approach is also another identity of FEAT which is designed to upgrade the accuracy by safeguarding privacy. FA performs local analytic tasks that can estimate traffic data skewness and select appropriate clients for FL model training. FEAT framework follows various steps like broadcasting a global model; training a local model to derive insights and patterns; uploading results on servers; skewness approximation; client's selection; and aggregating models. A convolutional neural network (CNN)-based multitask learning method is used for the local model training in each client [21]. Here, the core task performed is training local CNN models and estimating weight gradients during the process. These gradients make insightful weight parameters which are uploaded to the server. Skewness approximation is done by exploiting Hoeffding's inequality.[22] FA server sets low skewness as a selection parameter to finalize the client selection which will be contributing to model aggregation of FL. Finally, local model weight parameters are sent by the selected clients to the aggregator server and then local classification model is updated by broadcasting the aggregated global model parameters to the clients. Thompson Sampling is used to select Low Skewness Clients. Datasets used are QUIC and ISCX. The QUIC dataset is a Bidirectional network flow in CSV. The CESNET2 network is used to acquire the data. Realistic characteristics of network traffic originating from various web browsers, operating systems, mobile devices, and desktop machines are provided by this data source. ISCX is an Intrusion detection evaluation dataset which is distinguished in various groups such as Traffic, Chat, Web Browsing, Email, Streaming, File Transfer, VOIP, and P2P.

Another clustering-based model aggregation strategy is CluFL [23] which also employs weighted FL as proposed by Hanchi Shen, Jun Li et. al. It mainly focuses on non-IID data specially designed to address heterogeneity issues in FL. The proposed algorithm exerts spectral clustering in which differences of data distributions among clients are used as a prime factor to designate the aggregation weights. Then the CluFL is used as a base to derive a convergence bound by taking into consideration a practical non-convex setting in a neural network environment. Here, an author has claimed that convergence speed in the order of O (1/T) can be achieved by CluFL. For the clustering part, finding arbitrary shape class clusters was needed which is achieved by spectral clustering [20]. Spectral clustering is very effective for clustering of thinly distributed data availing a similarity matrix between data. Datasets used are Fashion MNIST and CIFAR-10. CluFL has achieved highest test accuracy 88% on Fashion MNIST dataset. Secondly, faster convergence speeds are also mentioned in the paper.

Trustworthy Federated Learning as a Service federated learning (FL) algorithm named TruFLaaS by Carlo Mazzocca, Nicolo Romandini et. al. [24] In this research paper, authors assert a promising ML paradigm - Federated Learning where on-premises data will not be outsourced but a global model will be trained by the participating nodes in collaborative fashion. However, FL set up and FL usage can incur extremely high cost as well as it can be a prolonged process. To restrain the cost overhead and to beat the learning curve of underlying technology, federated learning as a service (FLaaS) can be offered by service providers. It will also smoothen the adoption of FL in current world scenarios. Involvement of unknown participants can be one of the major concerns while designing an FLaaS architecture as it will cause hurdles to achieve trustworthiness among collaborators. TruFLaaS is Trustworthy federated learning as a service. It is an architecture employing blockchain technology. In the architecture of TruFLaaS, there is client interaction with the FLaaS offering service. Smart contracts in blockchain, validation set and DON are the architectural entities that help TrueFlaas in achieving trustworthiness. DON is a decentralized oracle network which acts as a middleware layer contributing in off-chain validation data delivery to the blockchain by maintaining security and reliability perseverance.[25] Oracles are mainly responsible for validation dataset provision to the smart contract. These validation datasets are managed by the service provider which are fed to the smart contract. A well-known baseline and widely accepted dataset [26] used in TruFLaaS is from NASA consisting of the working parameters of the Turbofan Jet Engine and it is mostly used for engine degradation modeling.

Today, many challenges are faced by Human Activity Recognition (HAR), such as scarcity of training data, computationally intensive learning, threat of sensitive information theft and lack of personalization in model design. In today's technological world we are witnessing integration of cyber-physical systems, Internet of Things (IoT) technologies, and social media technologies which are referred to as the CPSS (Cyber-Physical-Social Systems). It is observed that the CPSS suffers with two major issues: insufficiency in training data and insecurity in data sharing. The 2DFL framework is designed to cope with these issues during a secure distributed learning process.[27] In the proposed 2DFL framework by Xiaokang Zhou, Wei Liang et. al. [28] To address the constraint of heterogeneous data sharing across different devices, vertical federated learning is practiced in 2DFL. It effectively enhances a personalized HAR model while safeguarding privacy between nodes of different vendors. The other dimension in the 2DFL framework refers to horizontal federated learning. Here, the model accuracy is efficiently enhanced by aggregating local models with a similar feature space across multiple users. To average the model of all collaborating users with similar feature space, individual model parameters are encrypted and transmitted to the cloud server. This server is responsible for Averaging function.

TABLE I. LITERATURE REVIEW SUMMARY

Algorithm	Summary
SPinS-FL	Edge-Popup-based FL used. It only sends a few super masks and a set of scores of the weights around the boundary between selected and unselected in the subnetwork.
AsyFed	In this research paper an author has named a gear-based asynchronous FL architecture as AsyFed. To store the model parameters, it adds a gear layer which acts as a mediator between the clients and the FL server. Similar training abilities clients are grouped into the same gear.
IOP-FL	It addresses performance issues due to heterogeneity in data. Prediction accuracy is optimized using a gradient based approach by accumulating local and global gradients.
FedEE	It utilizes spatial-temporal graph structure data. It can be used as a solution for Extended Enterprise Collaboration for graph Learning. It helps to forecast prediction errors which is helpful for better decision making. This framework plays a vital role in each enterprise to learn the insights of both spatial and temporal features found in an entity's data source. It supports more accurate decision-making by reducing the prediction error.
HELCHFL	This algorithm aims at improving efficiency and cost effectiveness in hierarchical FL which suits in Heterogeneous MECC (Mobile-Edge Cloud Computing). In this research paper SqueezeNet ML model is used for hierarchical FL training
K-FL	Focused on resolving the non-IID problems. Author claims that K-FL can train models with fewer communication rounds in a Non IID environment. The Kalman filter is used to predict accuracy. Performance gain by providing a specific model with low variance to the device.
FEAT	Author has designed the FEAT to upgrade the accuracy by safeguarding privacy. FA performs local analytic tasks that can estimate traffic data skewness and select appropriate clients for FL model training. Here, the core task performed is training local CNN models and estimating weight gradients during the process.
CluFL	This algorithm mainly works for clustering. CluFL is a weighted FL model aggregation technique for each client. It mainly focuses on data heterogeneity specially designed for non-IID data in FL. Author claims convergence speed in the order of O (1/T). Spectral clustering is also taken into account for the same.
TruFLaaS	Authors claim Federated Learning as a promising ML paradigm where participants collaboratively train a global model without outsourcing on-premises data. It is a blockchain-based architecture.
2D FL	2DFL framework is designed to cope with insufficiency in training data and insecurity in data sharing. Here 2 dimensions refers to Horizontal federated learning and vertical federated learning. It effectively enhances a personalized HAR model while safeguarding privacy between nodes of different vendors.

Table I shows a summary of all the papers we have studied.
Table II can be referred to understand different abbreviations used in this review paper.

TABLE II ABBREVIATIONS AND FULL FORMS

Sr. No.	Abbreviations	Full Forms
1	SPinS-FL	Selectively pinned super-mask federated learning.
2	AsyFed	It implies Accelerated Federated Learning

3	IOP-FL	Inside and Outside model Personalization in FL"
4	FedEE	A Federated Graph Learning Solution for Extended Enterprise Collaboration.
5	HELCHFL	High-efficiency and low-cost hierarchical FL.
6	K-FL	Kalman Filter-Based Clustering Federated Learning Method
7	FEAT	A Federated Approach for Privacy-Preserving Network Traffic Classification in Heterogeneous Environments.
8	CluFL	Cluster-driven Weighted FL Model Aggregation Strategy
9	TruFLaaS	Trustworthy Federated Learning as a Service federated learning (FL)
10	2DFL	2 dimentional federated learning

Table III shows List of datasets used by all researchers to evaluate all 10 algorithms we have studied in this survey paper. Authors have used multiple evaluation parameters to analyse performance of these algorithms with below mentioned datasets. The CIFAR-10 dataset is a well-established benchmark in the field of machine learning, the dataset is segmented into 10 distinct classes, each representing a different object. MNIST dataset contains a lot of handwritten digits. Members of the AI/ML/Data Science community love this dataset and use it as a benchmark to validate their algorithms. The CIFAR-100 dataset consists of 60000 32x32 colour images in 100 classes, with 600 images per class. The 100 classes in the CIFAR-100 are grouped into 20 super classes.

TABLE III DATASETS LIST

Algorithm	Evaluated dataset
SPinS-FL	CIFAR-10, CIFAR-100
AsyFed	MNIST, CIFAR-10
IOP-FL	T2-weighted MRI images from 6 different sources and the optic disc and cup segmentation tasks with retinal fundus images from 4 different institutions.
FedEE	With provision by performance measurement system in California, PeMS dataset is used which is a traffic speed dataset.
HELCHFL	CIFAR-10, Fashion-MNIST
K-FL	LeNet-5 as the training model and the MNIST, FMNIST and CIFAR-10.
FEAT	QUIC and ISCX. QUIC dataset is a Bidirectional network flow in CSV. ISCX is an Intrusion detection evaluation dataset which is distinguished in various groups such as Traffic, Chat, Web Browsing, Email, Streaming, File Transfer, VOIP, and P2P.
CluFL	Fashion MNIST, CIFAR-10

III. CONCLUSION

When we look at ML/DL and Federated Learning shoulder to shoulder, both differ mainly in data labelling features. ML/DL requires data labelling which makes it highly expensive and time consuming. In FL, there is no such a requirement so it can serve as a cost effective and time saving solution. In model training of ML methods, data accumulation is done at the central server which enormously sources communication overhead which is not in the case of FL. This additional data transfer slows down the model. Another dominant concern about centralization of data is it compromises client data privacy. As client data is transferred to and fro centralized servers, crucial data is prone to threat. By taking everything in account, we can assent the prominence of Federated Learning.

We have studied various FL algorithms applied in diverse domains such as IOT, Secured Banking, Healthcare IOT, Cloud based system etc. We have also discussed the various datasets used by researchers to test the performance of various proposed algorithms. This survey can be served as a helping hand to the scholars who have the prospect of research in Federated Learning.

REFERENCES

[1] M. Aledhari et al. "FL: a survey on enabling technologies, protocols, and applications", IEEEAccess Multidisciplinary open access journal, version August 12, 2020.

[2] K. M. J. Rahman et al. "Challenges, applications and design aspects of FL: survey", IEEEAccess Multidisciplinary open access journal, version September 15, 2021.

[3] Sawsan Abdul Rahman, Hanine Tout et. al, A survey on federated Learning: The Journey from Centralized to Distributed On-Site Learning and Beyond, IEEE Internet Of Things Journal, Vol. 8, No. 7, April 2021.

[4] Yao Chen,Yijie Gui et. al. "Federated learning attacks and defenses: a survey", IEEE International Conference on Big Data (Big Data) 2022'.

[5] A Survey on Securing Federated Learning: Analysis of Applications, Attacks, Challenges, and Trends, Helio n. Cunha Neto, Jernej Hribar, Ivana Dusparic, IEEE Access, Open access Journal, May 2023.

[6] Junpeng Zhang et. al., A survey on security and privacy threats to federated learning, 2021 International Conference on Networking and Network Applications (NaNA), IEEE 2021.

[7] R. Nock, S. Hardy, W. Henecka, H. Ivey-Law, J. Nabaglo, G. Patrini, G. Smith, and B. Thorne, "The impact of record linkage on learning from feature partitioned data," in International Conference on Machine Learning. PMLR, 2021.

[8] D. Gao, Y. Liu, A. Huang, C. Ju, H. Yu, and Q. Yang, "Privacy- preserving heterogeneous federated transfer learning," in 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019.

[9] S. Sharma, C. Xing, Y. Liu, and Y. Kang, "Secure and efficient federated transfer learning," in 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019.

[10] SPinS-FL: Communication-Efficient Federated Subnetwork Learning, Masayoshi Tsutsui et. al. IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023.

[11] AsyFed: Accelerated Federated Learning with Asynchronous Communication Mechanism, Zhixin Li, Chunpu Huang, Keke Gai, Zhihui Lu, Jie Wu et.al, IEEE Internet of things journal, vol. 10, no. 10, 15 May 2023

[12] W. Wu, L. He, W. Lin, R. Mao, C. Maple, and S. A. Jarvis, "SAFA: A semi-asynchronous protocol for fast federated learning with low overhead," IEEE Trans. Comput., vol. 70, May 2021.

[13] Q. Liu, H. Yang, Q. Dou, and P.-A. Heng, "Federated semi-supervised medical image classification via inter-client relation matching," in Proc. MICCAI. Cham, Switzerland: Springer, 2021.

[14] IOP-FL: Inside-Outside Personalization for Federated Medical Image Segmentation, Meirui Jiang, Hongzheng Yang, Chen Cheng, Qi Dou, IEEE Transactions on medical imaging, vol. 42, no. 7, July 2023

[15] P. Sun et al., "Pain-Fl: Personalized privacy-preserving incentive for federated learning," IEEE J. Sel. Areas Commun., vol. 39, no. 12 Dec. 2021. [Online]. Available: https://doi.org/10.1109/

[16] FedEE: A Federated Graph Learning Solution for Extended Enterprise Collaboration, Zhenzhen Xie, Dongxiao Yu, Reza M. Parizi, Yanwei Zheng, IEEE Transactions on Industrial Informatics, Vol. 19, No. 7, July 2023

[17] Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," IEEE Internet Things J., vol. 9, no. 1, Jan. 2022.

[18] Optimizing Training Efficiency and Cost of Hierarchical Federated Learning in Heterogeneous Mobile-Edge Cloud Computing, Yangguang Cui, Kun Cao, Junlong Zhou, Tongquan Wei, IEEE Transactions on Computer Aided Design of Integrated Circuits And Systems, Vol. 42, No. 5, May 2023.

[19] K-FL: Kalman Filter-Based Clustering Federated Learning Method, Hyungbin Kim, Byungchan Kim, Yongho Kim, Cheolwoo You, Ieee Access Journal, April 2023

[20] FEAT: A Federated Approach for Privacy-Preserving Network Traffic Classification in Heterogeneous Environments, Yingya Guo, Dan Wang, IEEE Internet Of Things Journal, Vol. 10, No. 2, 15 January 2023

[21] CluFL: Cluster-driven Weighted FL Model Aggregation Strategy, Hanchi Shen, Jun Li et. al. 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS)

[22] TruFLaaS: Trustworthy Federated Learning as a Service, Carlo Mazzocca, Nicolo Romandini et. al. Journal of Latex Class Files, Vol. 14, No. 8, August 2021.

[23] Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives, Pengrui Liu†, Xiangrui Xu† and Wei Wang* Springer 2022

[24] A survey on security and privacy threats to federated learning Junpeng Zhang, Mengqian Li, Shuiguang Zeng, Bin Xie, Dongmei Zhao1 IEEE 2021

[25] Recent Advances on Federated Learning for Cyber Security and Cybersecurity for Federated Learning for Internet of Things Bimal Ghimire, Graduate Student Member, IEEE, and Danda B. Rawat, Senior Member, IEEE 2022.

[26] Federated learning: Applications, challenges and future directions, International Journal of Hybrid Intelligent Systems 18 (2022) 19–35 19 DOI 10.3233/HIS-220006, IOS Press.
[27] A federated learning algorithm using parallel-ensemble method on non-IID datasets, Haoran Yu1 · Chang Wu1 · Haixin Yu1, Xuelin Wei, Siyan Liu Ying Zhang, May 2023.
[28] A split-federated learning and edge-cloud based efficiency and privacy-preserving large-scale item recommendation model, Jiangcheng Qin, Xueyuan Zhang, Baisong Liu and Jiangbo Qian, Journal of Cloud Computing: Advances, Systems and Applications, Research Open Access, Springer 2023.