Cluster Computing (2026) 29:221
https://doi.org/10.1007/s10586-026-06028-6

A comprehensive survey on federated semi-supervised learning: applications, challenges, and future directions

Ahmet Alkılınç[1] · Feyza Yıldırım Okay[2] · İbrahim Kök[3] · Suat Özdemir[1]

Received: 10 March 2025 / Revised: 3 December 2025 / Accepted: 8 February 2026
© The Author(s) 2026

Abstract
Federated Learning (FL) is a decentralized method for collaboratively training a global machine learning model while preserving the privacy of user data. In recent years, its privacy-preserving and collaborative nature has attracted substantial interest among researchers. However, in real-world scenarios, it is often impractical to assume that all clients have fully labeled data, as acquiring large labeled datasets can be costly and requires expertise. To overcome this problem in FL, a new approach called Federated Semi-Supervised Learning (FSSL) is presented which aims to enhance the overall performance of the global model in FL by incorporating unlabeled data during model training. To provide a thorough examination of this area and to stimulate further research, we provide a systematic and comprehensive overview of recent studies using the FSSL method. We also discuss current challenges and open issues to provide researchers with directions for future research.

Keywords Federated semi-supervised learning · Federated learning · Machine learning · Unlabeled data

Abbreviations

AI	Artificial Intelligence
AE	Auto-Encoder
CNN	Convolutional Neural Networks
DDPG	Deep Deterministic Policy Gradient
DL	Deep Learning
DNN	Deep Neural Network
FATE	Federated AI Technology Enabler
FedAvg	Federated Averaging
FL	Federated Learning
FSSL	Federated Semi-Supervised Learning
FTL	Federated Transfer Learning
FCN	Fully Connected Layer
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
HAR	Human Activity Recognition
HFL	Horizontal Federated Learning
IID	Identical and Independently Distributed
IoT	Internet of Things
LSTM	Long Short-Term Memory
ML	Machine Learning
MIS	Medical Image Segmentation
MLP	Multilayer Perceptron
NLP	Natural Language Processing
NN	Neural Network
SSL	Semi-Supervised Learning
SER	Speech Emotion Recognition
TFF	TensorFlow Federated
TMI	Transportation Mode Identification
UAV	Unmanned Aerial Vehicle
VFL	Vertical Federated Learning

✉ Ahmet Alkılınç
ahmetalkilinc@cs.hacettepe.edu.tr

Feyza Yıldırım Okay
feyzaokay@gazi.edu.tr

İbrahim Kök
ikok@ankara.edu.tr

Suat Özdemir
ozdemir@cs.hacettepe.edu.tr

[1] Department of Computer Engineering, Hacettepe University, Ankara 06800, Turkey

[2] Department of Computer Engineering, Gazi University, Ankara 06570, Turkey

[3] Department of Artificial Intelligence and Data Engineering, Ankara University, Ankara 06100, Turkey

Published online: 30 March 2026

1 Introduction

In recent years, with the rapid proliferation of wireless networks, smart devices, personal mobile devices, and sensors, there has been a tremendous explosion in the volume of data produced on the edge. In order to obtain meaningful information within large volumes of data, it is necessary to analyze and process the data effectively. Traditional Machine Learning (ML) requires collecting distributed user data on a single central server and training the model centrally. However, transmitting such a substantial volume of data to a central server is both cumbersome and expensive. Also, devices like Internet of Things (IoT) devices that have limited battery and processing capacity cannot consistently transmit data to a central server. Moreover, in real-world scenarios, gathering distributed data on a central server is not feasible owing to concerns regarding data privacy and security. For example, data in healthcare institutions often contain private information about patients, and the leaking of data can jeopardize the privacy of patients. To prevent such situations, the security and privacy of users' data have become an important issue in recent years. The General Data Protection Regulation (GDPR) [1] protects the confidentiality and security of the personal information of users and also sets the rules for data sharing between organizations.

In order to deal with the above-mentioned challenges, Federated Learning (FL) has been proposed [2]. FL is an innovative method that allows multi-devices to collectively train a shared global ML model without requiring direct access and sharing of local user data. In 2016, Google introduced FL as an ML approach that satisfies the prerequisites for ensuring data privacy and security [3, 4]. The objective of FL is to develop an ML training model that has high predictive accuracy among multiple participants while complying with legal regulations and policies to protect personal data privacy [5]. The idea of FL based on data parallelism was initially introduced by McMahan et al. [2], who also put forth the Federated Averaging (FedAvg) algorithm. FedAvg is a decentralized ML approach that facilitates the collaborative training of a model by multiple devices while storing user data locally without sharing (Fig. 1).

Although FL shows great promise in protecting data privacy, its practical implementation in real-world applications poses numerous challenges [6]. Some of these challenges are the transmission cost of the parameters between the server and the devices, the heterogeneity of many local devices during the model training process, and the energy usage required for the local devices. Another important problem faced by FL is the non-independent and non-identical distribution of data (non-IID). Although the study [7] claims that FedAvg can handle non-IID data to a certain degree, several studies have shown that a decline in FL's model accuracy in non-IID or heterogeneous data is unavoidable [8]. Another major disadvantage of FedAvg is the high resource requirement to deploy and train models on IoT devices. However, IoT devices have limited memory, computation, and energy resources. In addition, the inadequacy and heterogeneity of the local data sample negatively affect the model's performance. Furthermore, most of the research on FL assumes that every client possess fully labeled data, which is unrealistic for real-world scenarios. Due to time and resource constraints, the training data on all clients are not fully labeled in reality. The scarcity of labeled data makes the development of an effective global model more challenging. For these reasons, utilizing unlabeled data to train the global model becomes an important challenge for FL [9].

To address the challenge of limited labeled data in FL, Federated Semi-Supervised Learning (FSSL) is proposed [10, 11]. FSSL aims to improve global model training by integrating unlabeled data inside federated supervised learning. To this end, different FSSL methods are suggested in the literature. Jeong et al. [10] developed naive combinations of FL and semi-supervised learning (SSL) techniques which incorporate an inter-client consistency loss and parameter decomposition on labeled and unlabeled data. Albaseer et al. [12] suggested FedSem, a method that utilizes real-time unlabeled data. FedSem includes two steps: in the first step, a global model is trained exclusively with labeled data, while in the second step, FedSem incorporates unlabeled data by employing the pseudo-labeling technique and the model developed in the initial stage to enhance the learning performance. Zhang et al. [13] proposed a new grouping-based model average technique to replace FedAvg method and improve convergence effectiveness. Itahara et al. [14] presented a distillation-based semi-supervised method that involves exchanging the outputs of local models between clients and training the unlabeled data using pseudo-labels.

There are different scenarios in FSSL, such as labels-at-server and labels-at-client [15]. In the labels-at-server scenario, all labeled data resides solely on the server, while unlabeled data is across the clients. On the other hand, in the label-at-client scenario, both labeled and unlabeled data are exclusively present on the clients and there is not any data in server [10]. In addition, there may be different scenarios where all labeled data resides on the clients while all unlabeled data resides on the server [16]. Itahara et al. [14] first distributed unlabeled data from the cloud to clients, followed by the application of FSSL utilizing hashed data from the clients. It is however one of the major disadvantages of this approach is that IoT devices suffer from limited storage, computing power, and energy resources. In addition, sending data from the cloud to clients incurs high communication costs and increases the computational load for resource-constrained clients. A higher resource capacity

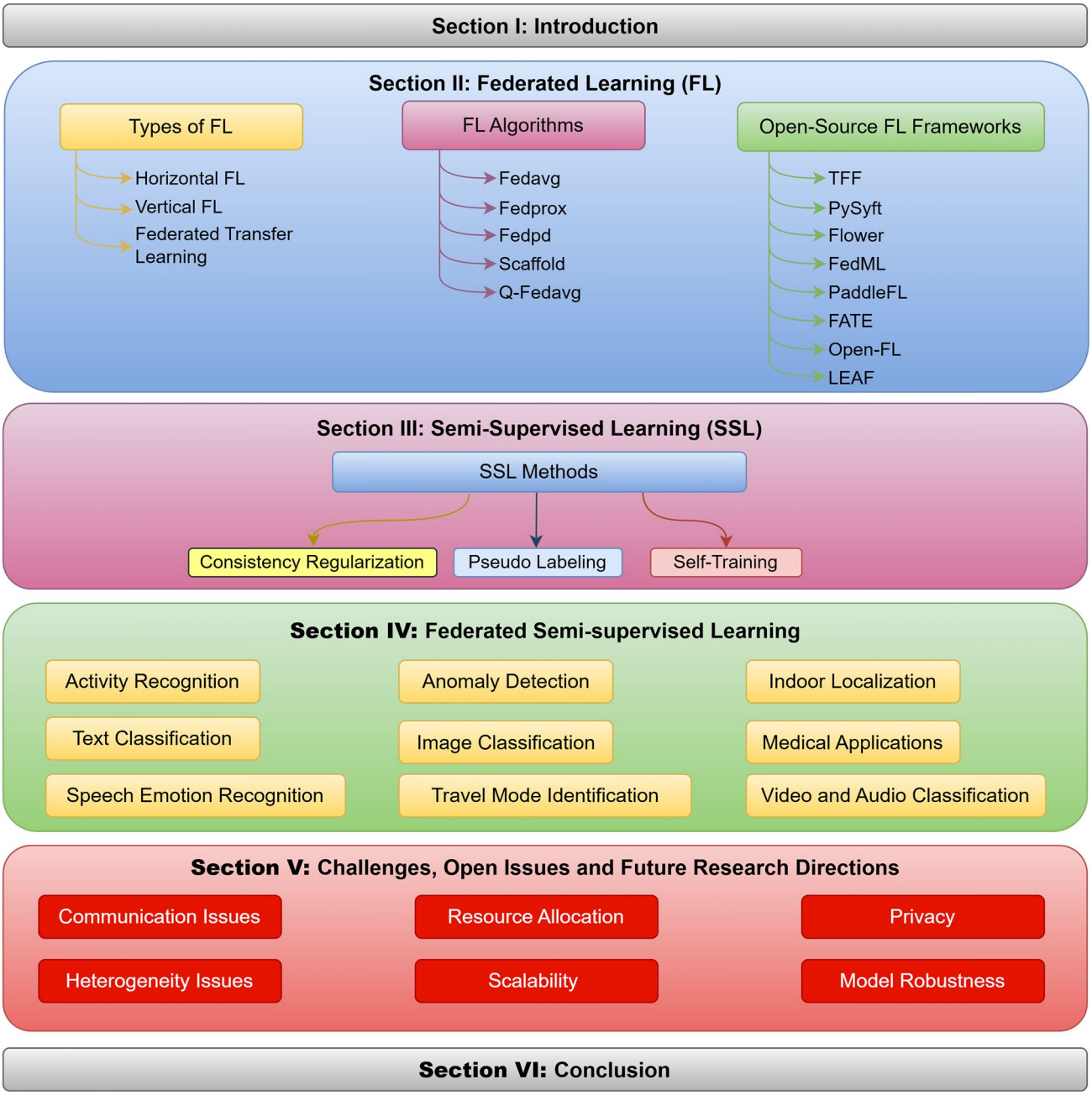


Fig. 1 The organization of the paper

is required to distribute and train data on these devices. In addition, each IoT device has a different capacity and computing power. Due to this heterogeneity of the devices, model performance and convergence speed are also negatively affected.

1.1 Motivation and contributions

FL has become a widely adopted paradigm for privacy-preserving collaborative model training, particularly in areas where data is not centralized due to privacy, security or legal constraints [2, 5]. However, the traditional supervised FL paradigm is based on the impractical assumption that client devices have completely labeled datasets. In practical FL applications, however, many clients participating in model training have only limited labeled data and a significant portion of local datasets remain unlabeled. Acquiring high-quality labels is often costly, domain-dependent and time-consuming. This discrepancy between abundant unlabeled data and scarce labeled data creates a performance bottleneck for traditional FL methods that rely solely on supervised learning. Therefore, FSSL has emerged as a

promising solution that integrates semi-supervised learning mechanisms into the federated environment to utilize unlabeled data as well as limited labeled data [10]. With the recent growth in interest in FSSL, research in the FSSL field has also increased significantly. This motivates the need for structured, comprehensive and systematic research on FSSL. Figure 2 displays the chronological sequence of FSSL approaches.

Several survey articles have contributed to the understanding of the concepts of FL [17–19] and SSL [20]. However, as summarized in Table 1, existing studies either focus very broadly on general FL systems or focus entirely on centralized SSL. This leaves a gap for a comprehensive analysis of FSSL, especially in terms of applications and emerging challenges. The research conducted in the FL domain provides comprehensive analyses of FL architectures, communication protocols and privacy mechanisms. However, it does not discuss how unlabeled data can be systematically used in FL or how SSL principles can be transferred to federated non-IID settings. Similarly, SSL-focused research only addresses class imbalance and label scarcity, but does not consider federative constraints such as statistical heterogeneity, communication constraints or decentralized optimization. Song et al. [21] presented a systematic review providing a fundamental overview of FSSL. In contrast, our study examines FSSL studies in different application areas in detail. Furthermore, our study provides a more comprehensive analysis by also examining recent studies conducted in FSSL in recent years. The primary contributions of this article are as below:

- To the best of our knowledge, there is no existing survey paper that explores and examines the studies in the field of FSSL in a detailed and systematic manner.
- We conduct a comprehensive review of recent studies utilizing FSSL methods, examining various approaches, architectures, and algorithms. Through this analysis, we present a thorough overview of the advancements in the field of FSSL.
- We address the challenges and open issues associated with implementing FSSL in real-world scenarios. We address these challenges to shed light on the areas requiring potential future research directions.

Figure 1 illustrates the structure of the survey. The paper is organized as follows. Section 2 presents the methodology of FL. Section 3 explains the SSL methods. In Section 4, we conduct a comprehensive review of current studies focusing on FSSL. Section 5 summarizes the challenges and potential future directions. Lastly, Section 6 provides a summary of the paper.

1.2 Research methodology

This research follows a systematic methodology to analyze the current state of the FSSL. This structured methodology aims to maintain the integrity of the research process and contributes to a deeper understanding of the FSSL. To ensure systematic, transparent and reproducible research on FSSL, we followed the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [22]. This process consisted of four structured stages: (i) identification, (ii) screening,

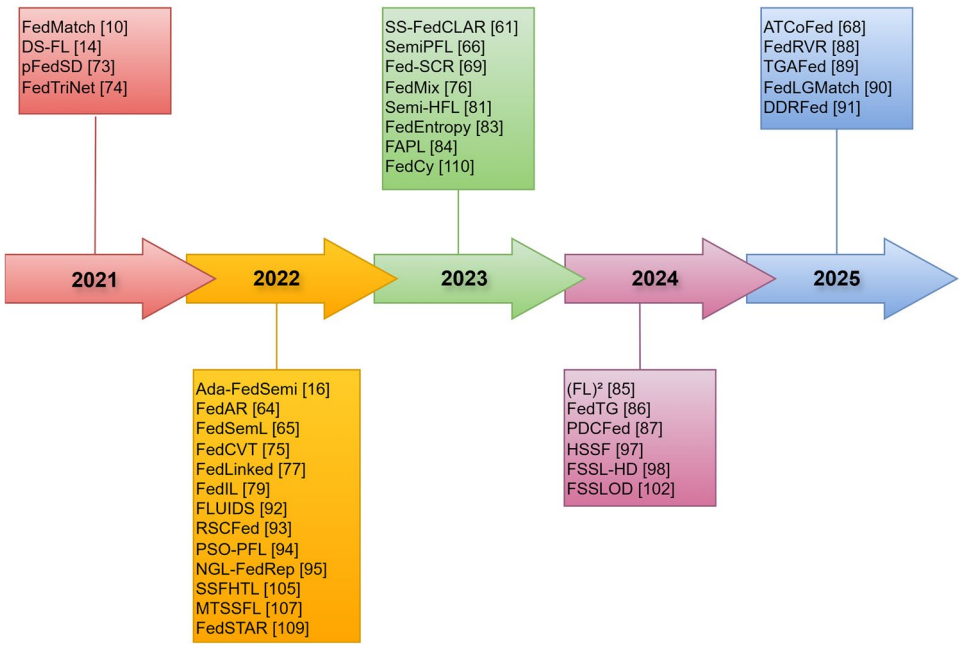


Fig. 2 Timeline evolution of FSSL

Table 1 Comparison of our survey with existing FL, SSL and FSSL surveys

Reference	Core focus	Overview of FL	Overview of SSL	Covers FSSL	Key differences
Zhang et al. (2021) [17]	General FL	✓	✗	✗	Provides comprehensive FL overview
Li et al. (2021) [18]	FL Systems & Privacy	✓	✗	✗	Focuses on FL architecture and privacy
Chaudhary et al. (2025) [19]	FL Paradigm	✓	✗	✗	Systematically provides a detailed overview of FL
de Oliveira et al. (2023) [20]	Class-Imbalance in SSL	✗	✓	✗	Focuses on SSL techniques for the class imbalance
Song et al. (2024) [21]	FSSL Overview	✓	✓	✓	Presented a systematic review providing a fundamental overview of FSSL
Our survey	FSSL & Applications	✓	✓	✓	Provides a detailed review and comparison of FSSL studies in different application areas and also examines more recent studies conducted in the field of FSSL

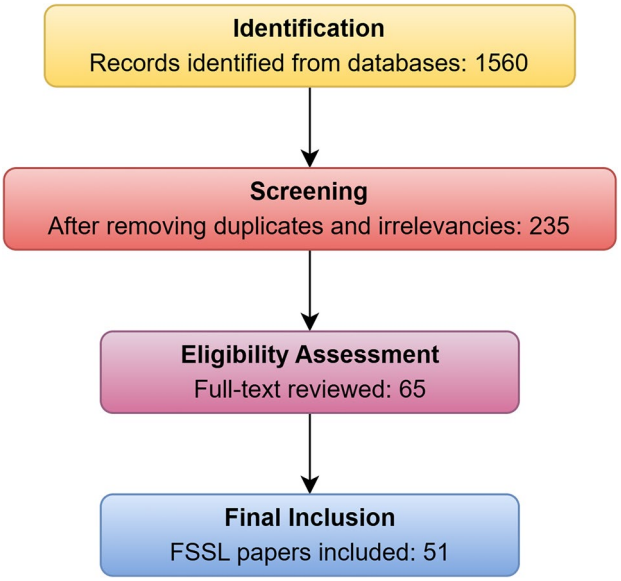


Fig. 3 Flow diagram the literature selection process

(iii) eligibility assessment and (iv) final inclusion. Figure 3 shows the literature selection process.

1.2.1 Identification

We conducted a comprehensive search across major scientific databases such as IEEE Xplore[1], ScienceDirect[2], ACM Digital Library[3], SpringerLink[4] and Scholar[5]. The search covered the years 2020-2025 and used keyword combinations such as "federated semi-supervised learning" and "federated learning with unlabeled data." A total of 1560 publications were identified at this stage.

1.2.2 Screening

After duplicate records are removed, the papers are screened according to the following

- Papers without peer review,
- White papers,
- Papers without a robust evaluation section,
- Papers published before 2020,
- Papers not directly related to FL, SSL and FSSL.

After screening, 235 papers remained.

[1] https://ieeexplore.ieee.org/
[2] https://www.sciencedirect.com/
[3] https://dl.acm.org/
[4] https://link.springer.com/
[5] https://scholar.google.com/

1.2.3 Eligibility assessment

Full-text articles are evaluated as follows:

- Relevance to FSSL,
- Technical contribution to federated optimization with unlabeled data,
- Clarity of problem formulation,
- Reproducibility and completeness of methodological description.

We excluded studies focusing solely on supervised FL, SSL without federated components or general privacy technologies. 65 articles proceeded to the final stage.

1.2.4 Final inclusion

Based on quality, relevance and completeness, we selected 51 papers that focus on FSSL and satisfy our selection criteria. These papers are classified in nine different domains as follows: 6 articles in Activity Recognition, 4 in Anomaly Detection, 21 in Image Classification, 1 in Indoor Localization, 7 in Medical Applications, 2 in Network Classification, 1 in Object Detection, 2 in Speech Emotion Recognition, 3 in Text Classification, 2 in Travel Mode Identification, and 2 in Video and Audio Classification. Additionally, we included several peer-reviewed FL and SSL surveys and foundational works for contextual completeness.

2 Federated learning

FL [2] is a decentralized method that is designed to train a global model collaboratively using distributed devices while maintaining the privacy of users' data. FL trains a globally shared data model, leveraging data from massively distributed devices while maintaining data privacy. The primary concept behind FL is to analyze data in a decentralized way to protect user privacy and ensure private user data remains on the client device and is not transmitted to the central server. Unlike traditional centralized ML training, in the FL algorithm, devices (called clients) perform model training, while the central server generates a global model by averaging the local parameters. Figure 4 shows the structures of ML and FL. A typical FL scenario basically involves the steps below: *i)* Initially, the central server selects a subsample of clients and distributes the global model to them. *ii)* After receiving the global model from the central server, the chosen clients engage in training the model using their individual private data. Subsequently, they transmit the updated models back to the central server. *iii)* Finally, the central server collects incoming local models and updates the global model by averaging it and redistributing it to the devices. The server and clients iteratively repeat this process until the model converges.

FL aims to train a global model $w \in \mathbb{R}^d$ by collaboratively leveraging decentralized data distributed across K clients. Each client k holds a private dataset. $D_k = \{(x_i^{(k)}, y_i^{(k)})\}_{i=1}^{n_k}$. The global optimization problem is defined as:

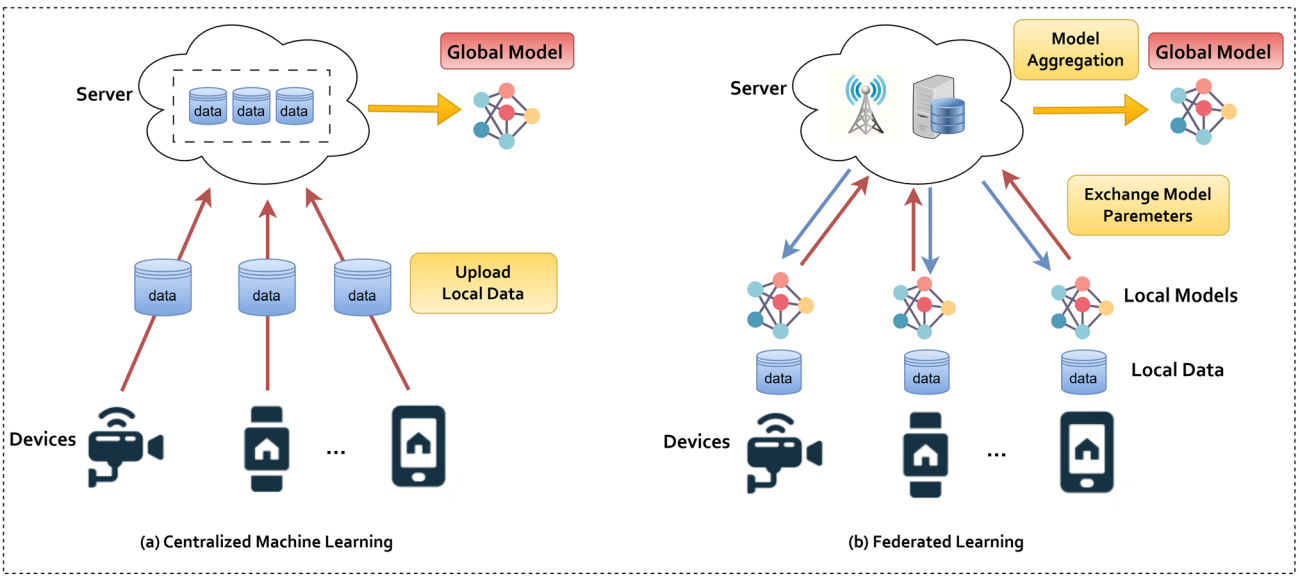


Fig. 4 The structure of (**a**) Centralized ML and (**b**) FL

$$\min_w F(w) = \min_w \sum_{k=1}^{K} \frac{n_k}{n} F_k(w), \quad n = \sum_{k=1}^{K} n_k, \tag{1}$$

where the local objective function is

$$F_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} \ell\big(f(x_i^{(k)}; w), y_i^{(k)}\big). \tag{2}$$

A common optimization procedure, such as FedAvg, performs E steps of stochastic gradient descent (SGD) on each client:

$$w_{t+1}^{(k)} = w_t^{(k)} - \eta \nabla F_k\big(w_t^{(k)}\big), \tag{3}$$

after which the server aggregates the updates:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{(k)}. \tag{4}$$

FL has several advantages over traditional ML methods. First, it enables the creation of models that can be trained on decentralized data, thereby enhancing privacy protection and minimizing the potential for data breaches. Second, it can be more efficient than traditional ML methods, as it eliminates the need to transfer large amounts of data to a central server. Finally, it exhibits greater resilience to data failures or disruptions, as the model can continue to learn even if some devices or servers are offline or unavailable. Although FL has made significant innovations and advances in security and privacy protection, it still faces some challenges such as communication cost, system heterogeneity, statistical heterogeneity, and data scarcity [23].

2.1 FL taxonomy

FL is commonly classified into three types based on data distribution: horizontal federated learning (HFL), vertical federated learning (VFL), and federated transfer learning (FTL) [6]. Figure 5 illustrates the types of FL.

2.1.1 Horizontal FL

HFL [17] is a type of FL where multiple devices or servers have similar data types and share a common goal. In HFL, data is partitioned horizontally, meaning each device or server keeps a subset of all-featured data records. HFL is practical when data is distributed among multiple clients and each party is not willing to share its data with other clients owing to privacy considerations. For example, a group of hospitals could collaborate on training a model to diagnose a particular disease, and each hospital could contribute its own patient data. By using HFL, clients can engage in collaborative ML model training using their respective local data, all while avoiding the need to share the actual data with one another. In HFL, individual devices or servers train the model by using their local data and transmit the updated parameters to the central server. The central server aggregates these parameters to construct a global model, which is subsequently returned to the devices or servers for further training. This iterative process continues till the global model achieves an acceptable level of accuracy.

2.1.2 Vertical FL

VFL [17] allows multiple parties to collaboratively train an ML model on vertically partitioned data, which refers to data that is distributed across different parties with different features or attributes. In VFL, different parties hold different subsets of the dataset features. Each party only has visibility to its own data while collaborating with other parties to collectively train a model on the combined data. For example, one server might hold data on patients' demographics, while another server might hold data on their medical history.

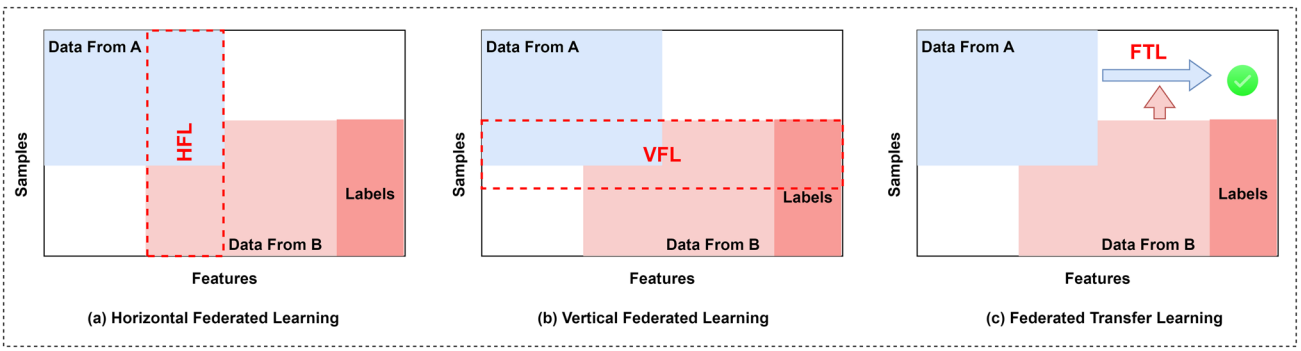


Fig. 5 Types of FL (**a**) HFL, (**b**) VFL, and (**c**) FTL

Servers collaborate to train a model that can predict disease outcomes based on both sets of traits. VFL can be especially valuable in situations where data privacy is a paramount concern, like in healthcare or finance, as it enables the creation of models that incorporate data from diverse sources while upholding the privacy of individual parties' data.

2.1.3 Federated transfer learning

FTL [24] is a type of FL where a pre-trained ML model is distributed to multiple devices or servers, and each device or server fine-tunes the model on its own local data. The fine-tuned models are then transmitted back to a central server, where they are combined to enhance the overall performance of the model. FTL is useful when the task of interest has similar characteristics across different devices or servers, and there is a pre-trained model available that can be used as a starting point. For example, let there is a group of hospitals, each of which has collected a large number of medical images. However, each hospital has a different mix of different types of medical images. One hospital may have many images of the lungs, while another may have many images of the heart. To train a robust image classification model across all hospitals' data, FTL can be used. By using FTL, the devices or servers can leverage the pre-trained model's knowledge while adapting it to their local data to achieve better performance.

2.2 FL algorithms

Numerous FL algorithms have been introduced in the literature [25]. This section lists some important FL algorithms and briefly discusses them.

2.2.1 Fedavg

McMahan et al. [2] introduced Federated averaging (FedAvg) as an iterative, privacy-preserving, efficient algorithm for FL. FedAvg is widely used as an FL algorithm. Despite its success, FedAvg faces several problems and challenges related to the heterogeneity of data and cannot fully resolve these issues.

2.2.2 Fedprox

The FedProx algorithm is a type of federated optimization technique that is regarded as a reparameterization of FedAvg [26]. By enabling each participating device to perform varying degrees of work and incorporating data from non-identical distributions, FedProx alleviates the heterogeneity issue in FL. In heterogeneous environments, FedProx shows considerably more precise and stable convergence than FedAvg, thereby improving overall test accuracy.

2.2.3 Fedpd

Zhang et al. [27] proposed Federated Primal-Dual (FedPD) that can be customized in different sub-variables. This algorithm offers methods capable of handling non-convex objective functions to achieve optimal optimization and communication complexity. In addition, this algorithm may be tailored adaptive to varying levels of non-IID data between agents.

2.2.4 Scaffold

Karimireddy et al. [28] presented the Stochastic Controlled Averaging algorithm (SCAFFOLD) which utilizes variance reduction to mitigate the negative impacts of heterogeneity. This algorithm converges in a reduced number of communication rounds and remains resilient to data heterogeneity. SCAFFOLD provides even faster convergence by exploiting similarity in client data.

2.2.5 Q-Fedavg

Li et al. [29] proposed q-Fair Federated Learning (q-FFL) to encourage a more equitable distribution of accuracy among devices on FL. This algorithm is inspired by the work on fair resource allocation for wireless networks. It minimizes the total re-weighted loss, hence devices with higher losses are given a higher relative weight.

2.3 Open-source FL frameworks

This section offers an overview of available open-source FL frameworks, which may be used for efficient testing and experimentation of new FL algorithms. Open-source FL frameworks provide a valuable resource for researchers and developers interested in constructing and deploying FL models. Table 2 provides an overview of the open-source FL frameworks.

2.3.1 TensorFlow federated (TFF)

It is a framework for building FL systems on a variety of devices such as mobile phones, IoT devices, and servers [30]. TFF is a widely-used deep learning framework that is an extension of TensorFlow. It extends its functionality to support FL. TFF provides a wide range of FL algorithms, including FedAvg, Federated SGD, and FL with Differential Privacy. These algorithms can be customized to meet the specific requirements of a particular use case. TFF supports

Table 2 Open-source FL frameworks

Framework	Developer	Language	ML framework	Privacy preservation	Communication optimization	Deployment	Scalability	Community support
TFF [30]	Google	Python	TensorFlow	Federated Averaging, Secure Aggregation	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	Moderate	High
PySyft [35]	OpenMined	Python	PyTorch	Federated Averaging, Differential Privacy, Homomorphic Encryption	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	Moderate	High
Flower [36]	Adap & University of Oxford	Python	PyTorch, TensorFlow, Scikit-Learn	Federated Averaging, Differential Privacy, Secure Aggregation	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	High	High
FedML [37]	UC Berkeley	Python	PyTorch, TensorFlow, Scikit-Learn	Federated Averaging, Differential Privacy, Secure Aggregation	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	Moderate	Medium
PaddleFL [38]	PaddlePaddle	Python	PaddlePaddle	Federated Averaging, Secure Aggregation	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	High	Low
FATE [39]	WeBank AI	Python	PyTorch, TensorFlow	Differential Privacy, Homomorphic Encryption, Secure Multi-party Computation	Compression, Quantization, Sparsification	Cloud, Edge	High	High
OpenFL [40]	Intel	Python	TensorFlow, PyTorch	Federated Averaging, Differential Privacy, Secure Aggregation	Compression, Quantization, Sparsification	Cloud, Edge, Mobile	High	Medium
LEAF [41]	University of Chicago	Python	PyTorch	Entropy-based Privacy	Compression, Sparsification	Cloud, Edge	High	Low

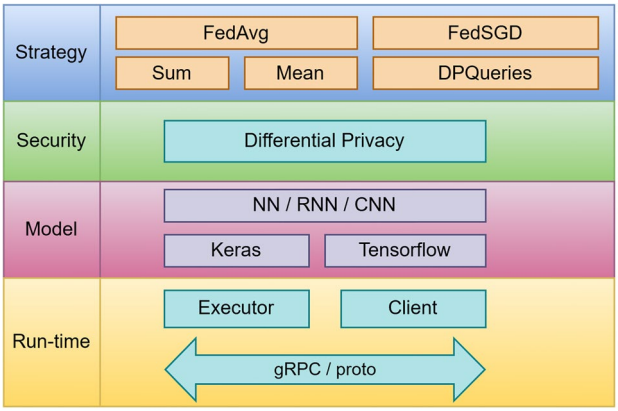


Fig. 6 Architecture of TFF [34]

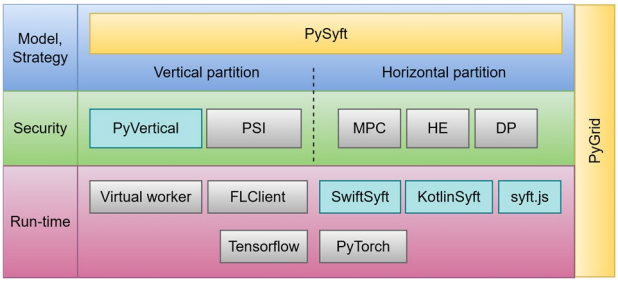


Fig. 7 Architecture of PySyft [34]

several privacy-preserving techniques, including Differential Privacy [31], Secure Aggregation [32], and Encrypted Computation [33]. These techniques contribute to safeguarding the privacy of user data throughout the FL process. TFF is a powerful framework for constructing FL systems that may be deployed across a diverse array of devices. The architecture of TFF is shown in Fig. 6.

2.3.2 PySyft

Developed by OpenMined, PySyft [35] is a framework that facilitates the implementation of FL utilizing PyTorch. It is designed to support FL and other privacy-preserving ML techniques. PySyft is constructed on PyTorch and offers a comprehensive suite of tools that enable secure and private computation over distributed data. PySyft provides a variety of features and techniques for FL, including differential privacy, secure aggregation, and homomorphic encryption. It also supports various types of FL, such as HFL and VFL. The architecture of PySyft is shown in Fig. 7.

2.3.3 Flower

It [36] is a framework that facilitates the implementation of FL using PyTorch, TensorFlow, and other ML frameworks. It was developed by the University of Oxford. It provides APIs for distributed learning, model selection, and secure aggregation. It is designed to simplify the process of building FL systems by providing a high-level programming interface and several pre-implemented algorithms. The framework facilitates the deployment of FL algorithms on devices like smartphones, tablets, and IoT devices. It provides a flexible and modular design, enabling researchers and developers to customize the system according to their specific needs. Also, it supports various types of FL, including HFL and VFL, as well as differential privacy and secure aggregation. Flower also provides several built-in optimization algorithms, such as FedAvg, Federated SGD, and Federated Momentum. Flower has a distinctive ability in supporting federated reinforcement learning, enabling the training of agents that interact with a dynamic environment in a decentralized manner.

2.3.4 FedML

FedML [37] is a research framework for FL developed by researchers from several universities, including Stanford, UC Berkeley, and Carnegie Mellon University. FedML provides a flexible and customizable architecture that enables researchers to easily experiment with different FL algorithms and configurations. The framework supports various types of FL, including HFL and VFL, as well as FTL and federated meta-learning. FedML focuses on benchmarking and reproducibility. The framework provides several pre-implemented benchmark datasets and evaluation metrics, as well as a set of reproducible experiments that can be easily run and compared across different algorithms and settings. FedML also provides a comprehensive set of optimization algorithms and communication protocols such as Federated Averaging, Secure Aggregation, and Federated Stochastic Gradient Descent. It also supports various privacy-preserving methods like differential privacy and FL with secure multi-party computation. The architecture of FedML is shown in Fig. 8.

2.3.5 PaddleFL

It [38] is an FL framework developed by PaddlePaddle. It supports heterogeneous devices, including mobile devices and IoT devices, as well as servers and clusters. PaddleFL also provides a comprehensive set of optimization algorithms and communication protocols, including FedAvg, Federated Proximal Gradient Descent, and Federated Stochastic Gradient Descent. The architecture of PaddleFL is shown in Fig. 9.

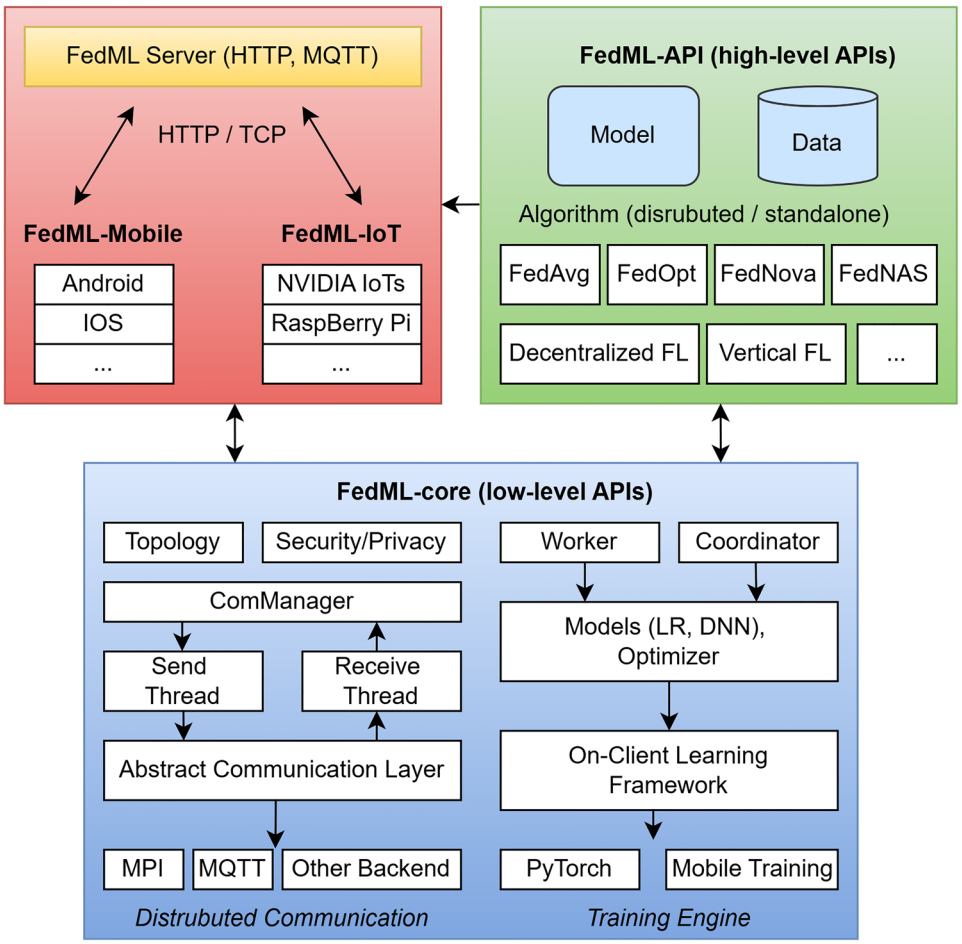


Fig. 8 Architecture of FedML [42]

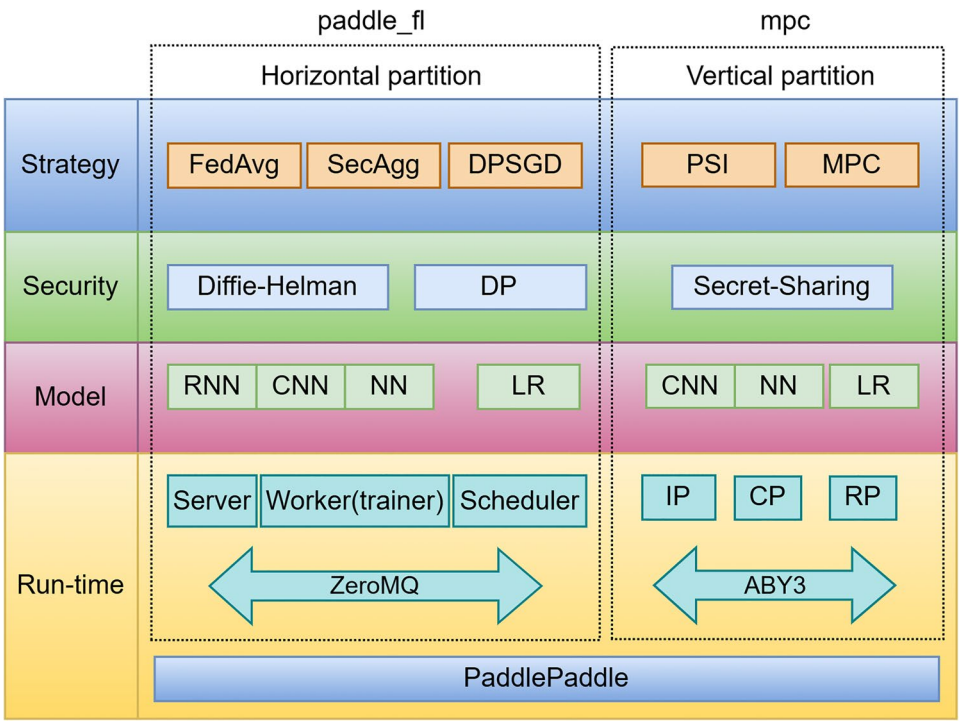


Fig. 9 Architecture of PaddleFL [34]

2.3.6 Federated AI Technology Enabler (FATE)

It [39] is an FL framework that supports a variety of FL scenarios, including HFL, VFL, FTL, and federated reinforcement learning. FATE also provides a comprehensive set of optimization algorithms and communication protocols, including Federated Stochastic Gradient Descent, FedAvg, and Federated Newton Method. The framework also supports various privacy protection methods like differential privacy, homomorphic encryption, and secure multi-party computation. The framework supports a variety of ML frameworks, including TensorFlow, PyTorch, and Scikit-learn. The framework also provides a RESTful API for model training and prediction. It is designed to be easy to deploy on various platforms, including cloud and edge devices. Also, it is actively maintained by a community of developers and researchers.

2.3.7 Open Federated Learning (Open-FL)

It [40] is an FL framework developed by IBM Research. Open-FL handles heterogeneous FL, which involves devices or nodes with varying computing capabilities and limitations. This allows developers to build FL applications that can work with a variety of devices, from smartphones to edge servers and cloud data centers. It supports dynamic resource allocation and workload balancing, which can help optimize training performance and resource utilization in FL applications.

2.3.8 LEAF

It [41] is an FL framework developed by NVIDIA. LEAF comprises a collection of benchmark datasets along with reference implementations for FL algorithms. It supports secure FL, where the participating devices or nodes can train models without revealing their data to other nodes or to the server. This is accomplished through the utilization of advanced cryptography methods, including homomorphic encryption and secure multi-party computation. LEAF provides benchmark datasets that are designed to simulate real-world applications like medical data and financial data, and are suitable for testing FL algorithms. LEAF is designed to be modular and extensible, so it can be easily integrated with other FL frameworks and algorithms.

3 Semi-supervised learning

SSL [43] is an ML method used to extract useful information from unlabeled data in a partially labeled or mostly unlabeled data set and enable the model to achieve better training performance. When there is a limited amount of labeled data, this learning method is particularly helpful in enhancing model performance. SSL provides a robust connection between supervised and unsupervised learning paradigms by utilizing structural knowledge in unlabeled samples to enhance model generalization. Formally, given a labeled dataset $D_l = \{(x_i, y_i)\}_{i=1}^{n_l}$ and an unlabeled dataset $D_u = \{x_j\}_{j=1}^{n_u}$ with $n_u \gg n_l$, the goal of SSL is to learn a predictive model $f(x)$ that minimizes the following objective:

$$\mathcal{L} = \mathcal{L}_{sup}(D_l) + \lambda \mathcal{L}_{unsup}(D_u) \tag{5}$$

where $\mathcal{L}_{sup}$ is the supervised loss on labeled examples, $\mathcal{L}_{unsup}$ is the unsupervised loss capturing the consistency or regularization term and λ is the balancing coefficient.

Different SSL methods are suggested in the literature. For instance, pseudo-labeling [44] makes predictions on unlabeled data using a model trained on labeled data and then uses predicted labels as "pseudo-labels" to train a new model.

Another effective method is to add a consistency regularization over training loss [45]. Consistency regularization involves training models by minimizing the discrepancy between stochastic outputs. UDA [46], MixMatch [47], ReMixMatch [48], and Fixmatch [49] are other SSL methods that combine many practical methods.

3.1 Assumptions of SSL

SSL performance relies on certain fundamental assumptions that define the relationship between the marginal data distribution $p(x)$ and the conditional label distribution $p(y|x)$. They define how information obtained from unlabeled data can guide model training and improve generalization ability when full supervision is not available.

3.1.1 Smoothness assumption

The smoothness assumption states that if two data points x_i and x_j are close to each other in the input space, then the corresponding labels y_i and y_j should also be similar. This is the supervised learning assumption but in SSL, the unlabeled data help define the high-density region. Formally, if the distance $\|x_i - x_j\|$ is small, the conditional probabilities should satisfy:

$$p(y_i|x_i) \approx p(y_j|x_j). \tag{6}$$

3.1.2 Cluster assumption

The cluster assumption implies that if data points are in the same cluster, they belong to the same class. In other words, it assumes that examples belonging to the same cluster are likely to share the same class label, while different clusters correspond to different classes. Let $\{C_k\}_{k=1}^{K}$ denote the clusters induced by the data distribution $p(x)$. Then, for samples $x_i, x_j \in C_k$:

$$p(y_i = y_j | x_i, x_j \in C_k) \approx 1, \tag{7}$$

and for samples in different clusters $C_k \neq C_l$:

$$p(y_i \neq y_j | x_i \in C_k, x_j \in C_l) \approx 1. \tag{8}$$

3.1.3 Low-density assumption

The low-density assumption is a more effective formulation of the cluster assumption. This assumption states that the decision boundary between classes should not pass through high-density regions and improves the cluster assumption by emphasizing that the decision boundary should pass through regions where the marginal data probability $p(x)$ is small.

3.1.4 Manifold assumption

The manifold assumption is a more general assumption and assumes that high-dimensional data does not fill the entire space, but rather lies on or near a low-dimensional manifold $\mathcal{M}$ embedded in the environment space $\mathbb{R}^d$. In other words, the probability density $p(x)$ is concentrated around $\mathcal{M}$, where $\dim(\mathcal{M}) \ll d$. Therefore, the learning of $f(x)$ can be effectively constrained to $\mathcal{M}$ instead of the entire input space. Mathematically, this can be formulated as:

$$p(x) \approx p_{\mathcal{M}}(x), \quad \text{where } x \in \mathcal{M}. \tag{9}$$

A smooth labeling function $f : \mathcal{M} \to \mathcal{Y}$ should satisfy:

$$\int_{\mathcal{M}} \|\nabla_{\mathcal{M}} f(x)\|^2 p_{\mathcal{M}}(x)\, d\mathcal{M} < \infty, \tag{10}$$

where $\nabla_{\mathcal{M}} f(x)$ is the gradient along the manifold.

3.2 SSL methods

There are many SSL algorithms in the literature [50] [51]. This section lists and discusses some of the most important SSL algorithms.

3.2.1 Consistency regularization

It is a popular SSL technique that attempts to enhance the performance of models trained on data that is both labeled and unlabeled. The fundamental concept underlying consistency regularization is that a model's predictions should be consistent across similar inputs. In this technique, consistency is enforced between the predictions of a model on different perturbations of the same input like adding Gaussian noise. The key objective of consistency regularization is to penalize the model for producing different outputs for similar inputs. This is achieved by incorporating a consistency term into the loss function, which measures dissimilarity among the model's predictions over two slightly perturbed versions of the same input. To generate the perturbations, small amounts of noise are typically added, or random transformations are applied to the input.

3.2.2 Pseudo-labeling

Consistency regularization has been used in different domains like object detection, natural language processing, and image classification. Sajjadi et al. [52] proposed stochastic transformations and perturbations (STP) that ensure consistency in the model's predictions on perturbations of the same input. STP uses stochastic data augmentation to generate perturbations, applies a perturbation to an input, computes the model's prediction, applies the same perturbation, and computes the prediction again, with the STP loss being the mean squared error between the two predictions. Laine et al. [53] proposed temporal ensembling that enhances the consistency of a model's predictions on unlabeled data over time. This approach involves training a model on labeled and unlabeled data, generating soft labels from a moving average of the model's predictions on unlabeled data, and using soft labels in order to train the model in the next iteration. The ensemble of model predictions from previous iterations is used as a regularizer to enhance the consistency of the model's predictions. Tarvainen et al. [54] introduced the Mean Teacher approach, which utilizes the predictions of a teacher model to regularize the predictions of a student model. Another popular method is Virtual Adversarial Training (VAT) [55], which introduces minor perturbations to the input data to maximize the difference in predictions made by the model under the perturbed input.

Pseudo labeling [44] aims to improve model performance by using the model predictions on unlabeled data to generate pseudo labels. These pseudo-labels are then combined with labeled data to train the model in a supervised manner. Essentially, pseudo-labeling harnesses the abundant unlabeled data typically available to enhance model performance, especially in scenarios where labeled data is scarce. The idea is that the predictions of the model on the unlabeled data can be used to assign labels to the data, which are then employed for supervised training of the model. However, it is important to note that pseudo-labeling can lead to overfitting if the quality of the pseudo-labeling is poor or the distribution of unlabeled and labeled data differs significantly. Hence, it is crucial to carefully evaluate the quality of pseudo labels and their potential effect on the overall model performance.

3.2.3 Self-training

Self-training [56] is an SSL approach that involves training a model on a limited set of labeled data and subsequently utilizing the trained model to generate predictions for unlabeled data. The highly confident predictions are then treated as labeled data and used to augment the training set. This iterative process continues until a stopping criterion is satisfied or the performance of the model on the validation set reaches a plateau. The main goal of self-training is to leverage the model's confidence in its predictions on unlabeled data to enhance its performance on the target task. Yarowsky [57] first introduced the self-training technique as a solution for word sense disambiguation in text documents. Since then, this approach has been applied in various fields with different modifications. Rosenberg et al. [58] showed the efficiency of self-training in object detection tasks. Dópido et al. [59] proposed a method for the classification of hyperspectral images, where they selected informative unlabeled samples based on domain knowledge and pseudo-labeled them using the predictions of the trained classifier. Xie et al. [60] presented a modification to the self-training technique called "Self-Training with Noisy Student" for image classification on the ImageNet dataset. The approach involves training a student model on labeled data, subsequently utilizing this model to generate pseudo-labels for unlabeled data. The student model is then augmented with noise during training to prevent overfitting and to create a more robust model, which is subsequently utilized as the teacher model in the next iteration to generate pseudo-labels.

4 Federated semi-supervised learning

FSSL is an innovative ML method that integrates the principles of FL and SSL. By utilizing FSSL, models can be trained on decentralized datasets that comprise both labeled and unlabeled data [10, 11]. This methodology is particularly valuable in scenarios where labeled data is scarce yet there is a significant volume of unlabeled data that can be utilized to enhance the model's accuracy. The FSSL structure is shown in Fig. 10. This section provides a comprehensive review of research on FSSL across diverse domains. The summary of recent studies according to the problem and key idea is given in Table 3. Also, these recent studies are summarized according to the data and methodology in Table 4.

4.1 Activity recognition

In activity recognition, FSSL provides an effective solution to problems like privacy preservation, uneven data distribution and system scalability. Using SSL under a federated

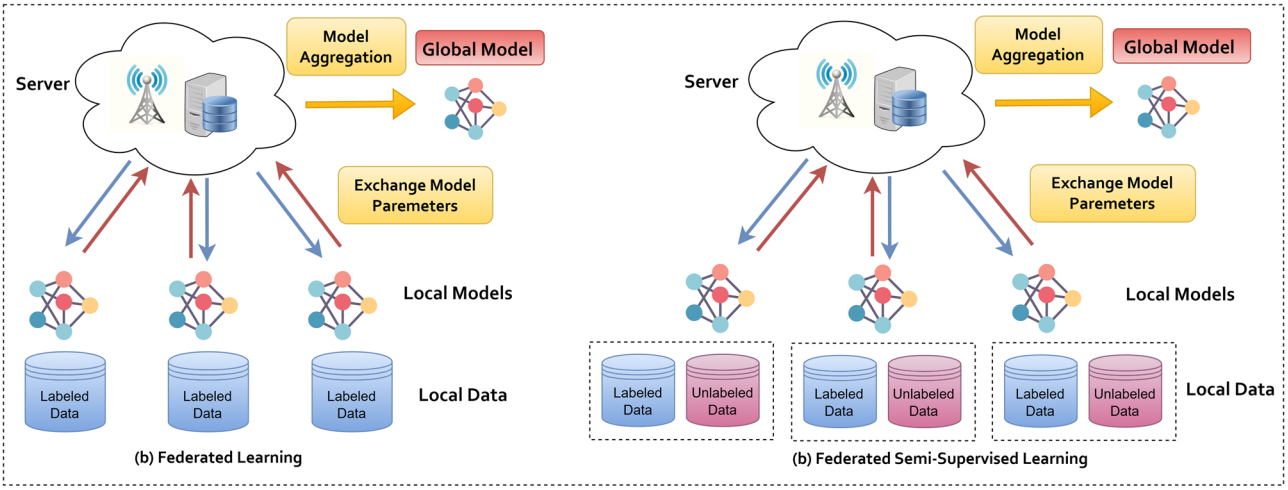


Fig. 10 The general structure of (**a**) FL and (**b**) FSSL

Table 3 Summary of recent FSSL studies according to problem and key idea

Domain	Ref	Year	Problem	Key idea
Activity Recognition	[61]	2023	Heterojen nature of HAR data and challenge of personalization in FL for HAR. Additionally, the lack of labeled data on each client can lead to reduced performance of federated clustering-based approaches.	Proposed a new approach for Personalized sensor-based HAR by combining Federated Clustering and SSL. This unique combination effectively addressed non-IID and scarcity of data problems which are commonly observed in federated HAR.
	[64]	2022	The data scarcity problem of HAR in which there are limited availability of labeled data and a huge amount of unlabeled data, and it is challenging to collect labeled data from multiple users due to privacy concerns.	Proposed a hybrid method for HAR called FedAR, which create a privacy-aware and scalable global activity model. FedAR uses active learning and label propagation and incorporates a transfer learning strategy.
	[65]	2022	The use of FSSL in smart cities, where the majority of the data gathered by IoT devices are unlabeled, and the wireless characteristics of the network edge impact the efficiency of the global model.	Proposed a solution to run FSSL over the edge of the wireless network in smart city applications, where a significant portion of the data collected is unlabeled.
	[66]	2023	The challenge of labeling massive sensor data generated in edge devices, as well as the difficulties of developing a global model which is a good fit for all users due to personal attributes and edge heterogeneity.	Presented an FL framework called SemiPFL, which supports edge users with limited labeled availability datasets and a huge amount of unlabeled data. The framework involves the training of a Hyper-network in the server to generate personalized AE for every user.
	[68]	2025	HAR systems often suffer from insufficient labeled data and strict privacy constraints, making it difficult to train reliable models on decentralized sensor data. Existing FSSL methods mostly rely on confidence thresholds, leading to low-quality pseudo-labels that degrade performance in real-world activity recognition.	ATCoFed presents an activity-aware FSSL framework that improves pseudo-label quality by validating predicted activity sequences using temporal models derived from LSTMs and reasoning methods derived from LLMs.
Anomaly Detection	[70]	2022	Traditional approaches to intrusion detection systems centralization of all data and labels leading to high bandwidth overhead, low incentives for devices to share private data the need for large computing and storage resources on the server side.	Proposed an FSSL model for intrusion detection systems using network softwarization, to improve network and service management on the edge-cloud environment.
	[92]	2022	Traditional intrusion detection systems rely on centralized models that require access to all data to detect anomalies. However, this raises privacy concerns and may not be practical for distributed networks.	Proposed FLUIDS that is an FL with SSL approach for an intrusion detection system that combines supervised and unsupervised learning in a collaborative way to better protect privacy, enhance training and extraction efficiencies, obtain higher accuracy, and be cheaper to deploy.
	[69]	2023	How to perform reliable anomaly detection in smart grids while preserving the security and privacy of the users' data.	Proposed an FSSL method for anomaly detection on smart grids. They used a generative network to learn the underlying distribution of normal data in a privacy-preserving way and then use this network to identify anomalies in a distributed and federated setting.
	[71]	2023	Concerns about privacy, efficiency, and latency in DL approaches, as well as the difficulty of obtaining labeled data.	Designed a novel FSSL method that takes advantage of labeled and unlabeled data in a federated manner for intrusion detection in Industry 4.0.
Image Classification	[10]	2021	The practical issue of FSSL is where clients in an FL setting have partially labeled or fully unlabeled data with is only available on the server.	Presented a new approach, named FedMatch, which enhances the combination of FL and SSL methods by introducing an inter-client consistency loss and parameter decomposition for separate learning on unlabeled and labeled data.
	[73]	2021	The challenges posed by heterogeneous data and models in FL.	Presented a new FL framework called pFedSD that improves communication efficiency and ensures privacy while allowing for personalized models.
	[14]	2021	The high communication costs that typically arise in FL due to model sizes.	Presented a distillation-based FSSL framework, called DS-FL which reduces communication costs without compromising model performance by exchanging the outputs of local models between mobile devices rather than exchanging model parameters as typically done.

Table 3 (continued)

Domain	Ref	Year	Problem	Key idea
	[74]	2021	The challenge of exploiting unlabeled data in FL, which is often present in real-world applications.	Proposed a new FSSL method called FedTriNet that aims to exploit unlabeled data for distributed data usage and privacy protection in FL. FedTriNet includes two learning steps: pre-training using labeled data with FedAvg and making use of unlabeled data to improve model learning.
	[75]	2022	Use of FSSL in applications affecting VFL performance where most aligned sample sets are small and most unaligned data is not used.	Proposed an FSSL approach called FedCVT to improve the effectiveness of VFL models with limited aligned instances.
	[16]	2022	How to utilize both on-device labeled data and unlabeled data in the cloud to improve model performances?	Presented the Ada-FedSemi system, which is an FSSL technology that utilizes both on- device labeled data and unlabeled data in the cloud to improve the DL models effectiveness. It proposes a novel online algorithm based on MAB to dynamically determine the participating fraction and confidence threshold during the training of federated models.
	[77]	2022	Problem of multitask learning in distributed environments where multiple participants try to improve their performance by collaborating but cannot share their own private dataset and model parameters due to business and privacy issues.	Proposed method named FedLinked that aims to solve the problem of multitask learning in distributed environments using federated, semi-supervised, and multi-task learning algorithms. FedLinked is a privacy-preserving solution method that targets semi-supervised multitask cross-silo issues.
	[79]	2022	The limitations of traditional FL methods that assume fully labeled data in user devices and slow training in proposed SSL methods, and problems of convergence in real network environments.	Presented FedIL, FSSL framework that addresses the limitations of FSSL methods in real network environments.
	[93]	2022	The issue of unequal credibility between models from fully-labeled, fully-unlabeled, or partially labeled clients in FL.	Presented an FL approach called RSCFed to address the issue of unequal reliability between models from fully- labeled, fully-unlabeled, or partially-labeled clients. They also introduced a novel distance-reweighted model aggregation method to improve the robustness of sub-consensus models.
	[80]	2023	The non-IID data between clients in FL affects the consistency between local update and the performance of global aggregation.	Presented a method called SDA-FL which addresses the non-IID data challenge in FL by sharing synthetic data.
	[76]	2023	The use of UAVs to collect labeled data for automatic image recognition raises data privacy and data availability concerns. Additionally, The number, features, and distribution of local data collected by UAVs using different camera modules in different environments exhibit substantial variations, resulting in statistical heterogeneity.	Presented a privacy-preserving FSSL framework (called FedMix) for UAV image recognition in the context of an aerial computing network infrastructure focused on the Internet of Drones.
	[78]	2023	The statistical heterogeneity of distributed data is a significant challenge to achieving robust performance and consistent convergence in FL and the limitation of existing model personalization methods which rely on fully labeled data.	Presented a new personalized SSL paradigm for FL that allows partially labeled or unlabeled clients to request labeling support from helper agents. The proposed method aims to address the issue of statistical heterogeneity in distributed data and achieve more stable convergence and robust performance in FL.
	[82]	2023	The challenge is to perform SSL in a federated setting, where clients have limited labeled data and do not wish to share their data with anyone else.	Presented FedProp that uses a manifold-based approach to estimate the data manifold jointly from the data of multiple clients and utilizes cross-client label propagation to compute pseudo-labels.
	[83]	2023	Lack of labeled data in FL that is costly to obtain and limits the performance of FL models.	Proposed a novel algorithm (called FedEntropy) that uses information entropy to optimize the training process and enhance the FSSL performance.
	[84]	2023	The non-IID data distributed in clients cause imbalanced model training because of the unequal learning impacts on different classes, resulting in unstable performance both across different classes and between different clients.	Presented a new method for FSSL that tackles the problem of imbalanced model training and fairness issues in federated settings.

Table 3 (continued)

Domain	Ref	Year	Problem	Key idea
	[85]	2024	FSSL is struggling with a performance gap due to multiple local training periods and confirmation bias which is exacerbated by the separation of labeled and unlabeled data.	Proposed$(FL)^2$which is a method using sharpness-aware consistency regularization, client-specific adaptive thresholding, and learning status-aware aggregation.
	[86]	2024	The challenge of relying on single pseudo labels, which limits model accuracy and information utilization for FL, under-labeled data and unlabeled data in edge computing.	Proposed FedTG that uses multiple high-probability pseudo labels from unlabeled data and excludes classifier updates during training.
	[87]	2024	FSSL faces challenges in handling non-IID data and balancing accuracy with communication efficiency.	Proposed PDCFed, a two-stage sampling method that achieving higher accuracy and communication efficiency on non-IID datasets.
	[88]	2025	FSSL approaches suffer from biased classifiers and skewed unlabeled clients due to reliance on data-level augmentation for prediction consistency and simplistic weighted average aggregation at the server.	Proposed a novel FSSL framework (FedRVR) that introduces versatile regularization at clients and a relation-guided directional aggregation strategy at the server.
	[89]	2025	FL faces challenges with partially labeled data due to high labeling costs and the need for additional annotation expertise and limits the use of large volumes of unlabeled data.	Proposed TGAFed which uses truncated Gaussian aggregation to weight unlabeled samples, optimize pseudo-label filtering and provide inter-client consistency loss.
	[90]	2025	In non-IID client data distributions, noisy and unreliable labels cause confirmation bias. This makes it difficult to effectively use unlabeled data in realistic federated environments where labeling is scarce.	Proposed new framework called FedLGMatch, which uses both global and local models to create cleaner pseudo labels and allows customer-specific information to guide the refinement of the pseudo labels.
	[91]	2025	FSSL struggles with limited labeled data and non-IID client distributions and existing pseudo-labeling methods ignore low-confidence samples and rely on fixed thresholds, leading to poor model performance.	DDRFed is proposed, which introduces a data generation strategy based on the diffusion model to reduce non-IID effects and uses dynamic class-balanced thresholds to adaptively use both high and low confidence examples.
Indoor Localization	[94]	2022	Fingerprint-based indoor localization is facing issues such as frequent data collection, privacy concerns, and personalized localization requirements of users. Most existing FL-based indoor localization works solely consider static data distribution.	Proposed a new method called PSO-PFL for fingerprint-based indoor localization that considers the personalized localization requirements of users and their dynamic data distribution. The method utilizes FL to overcome privacy concerns and efficiently utilize unlabeled data for improved accuracy.
Medical Applications	[95]	2022	The challenge of training effective ML models on sensitive electronic healthcare data which are rarely labeled and distributed across a network of healthcare institutions.	Proposed a dynamic neural graphs-based FL framework to tackle the challenge of training effective ML models for AI healthcare applications on sensitive electronic healthcare records.
	[96]	2022	Insufficient labeled data and privacy concerns in medical image segmentation.	Inroduced a novel FSSL framework for MIS, which leverages both labeled and unlabeled data from different hospitals without exposing raw data.
	[97]	2024	Medical image segmentation faces challenges such as privacy concerns, high annotation costs, and the need for local model personalization.	Proposed a Model-Heterogeneous Semi-Supervised Federated (HSSF) Learning framework that includes Regularity Condensation, Regularity Fusion, a Self-Assessment (SA) module, and a Reliable Pseudo-Label Generation (RPG) module to enhance personalization.
	[98]	2024	FSSL in IoT healthcare systems faces challenges due to heterogeneous data distributions and the scarcity of labeled data across devices.	Proposed a unified FSSL framework (FSSL-HD) that introduces a novel objective function, a loss-based aggregation mechanism, and dynamically adjusted confidence thresholds to enhance generalization, reduce inter-model discrepancies, and improve self-training capabilities.
	[99]	2025	The scarcity of labeled data and its distribution across clinical centers with privacy restrictions, coupled with the insufficient utilization of large amounts of heterogeneous unlabeled data, poses challenges in training accurate lung tumor segmentation models.	Developing a combined FSSL that utilizes self-supervised pre-training, refined pseudo-labeling and dynamic model aggregation methods to effectively utilize heterogeneous unlabeled clinical data for lung tumor segmentation.
Network Traffic Classification	[100]	2023	Protecting the privacy of users' traffic data and difficulty in obtaining labeled data.	Proposed a novel approach using FSSL for network traffic classification, which can help to protect users' privacy and overcome the challenge of obtaining labeled data.

Table 3 (continued)

Domain	Ref	Year	Problem	Key idea
	[101]	2024	Traffic classification faces challenges such as high data dependency, costly traffic labeling, and privacy concerns, particularly in smart home networks.	Proposed a FL-based framework for traffic classification that enhances privacy through local training, reduces labeling dependency using a semi-supervised AE model, and ensures explainability with XAI methods, achieving high performance with minimal data.
Object Detection	[102]	2024	FL faces challenges in object detection tasks in densely packed scenes due to limited labeled data and data distribution disparities	Proposed a framework (FSSLOD) that uses a teacher–student network with consistency loss for local SSL and an elastic update mechanism to address data distribution disparities.
Speech Emotion Recognition	[103]	2022	The limited availability of quality labeled data instance in SER applications and the privacy concerns associated with acquiring and transmitting speech data to remote cloud platforms.	Described an FSSL framework called Semi-FedSER for SER applications. The framework uses labeled and unlabeled data instances to handle the problem of limited labeled data instances in FL and protect user privacy.
	[104]	2022	Lack of privacy in existing centralized SER approaches, as well as the challenges of limited labeled data and non-IID distributions in training models.	Presented an FL approach for SER that is privacy-preserving and data-efficient, and utilizes both labeled and unlabeled data to train models.
Text Classification	[105]	2022	The challenge of heterogeneous data in FL, where data across different devices or institutions may be in different formats or distributions, making it difficult to train accurate and generalizable models	Inroduced an SSFHTL approach that leverages transfer learning techniques to learn shared representations from heterogeneous data available at different devices or institutions in FL.
	[106]	2023	How to reduce the spread of false and misleading information and data disclosure tasks on social media platforms that can be extremely harmful to individuals and society, and how to improve the generalization of the learning system in hyper-partisan classification while achieving high precision.	Proposed a novel FSSL framework based on self-ensembling to address the challenge of propagating false and misleading information on social media platforms. The framework utilizes stylometric and linguistic information of annotated journal articles and looks for hidden patterns in unlabeled data to denoise labels.
	[81]	2023	The proposed approach addresses the challenges of resource heterogeneity and lack of labeled data in FL.	Presented Semi-HFL, an FSSL method for heterogenous devices that splits the model into small sub-models utilizing early exit branches to accommodate different devices' resource needs.
Travel Mode Identification	[107]	2022	The key challenge in building intelligent transportation systems is privacy-preserving TMI. Existing TMI approaches heavily rely on labeled data, which is usually limited in real-world application	Described an FSSL framework called MTSSFL for privacy-preserving TMI. This framework enables correct and privacy-preserved crowdsourced TMI without relying on large labeled data.
	[108]	2022	The use of GPS trajectories for travel mode identification is hindered by concerns around user privacy, as such data can directly integrate sensitive information. Moreover, existing identification methods are inefficient and error-prone since they depend heavily on manual travel mode annotations.	Proposed an FSSL framework for accurately identifying travel modes from GPS trajectories without compromising users' privacy. It uses a CNN-GRU model and a pseudo-labeling method for clients and adopts grouping-based aggregation and data flipping augmentation to improve performance.
Video and Audio Classification	[109]	2022	Labeling audio data can be time-consuming and costly, leading to a problem that too much unlabeled data remains unexploited.	Presented method called FedSTAR, an SSL approach for audio models that combines self- training with FL to leverage on-device unlabeled data.
	[110]	2023	The effectiveness of DL techniques in surgery usually relies on training on various datasets from multiple medical institutions. However, sharing sensitive medical data is not always feasible, and data annotation can be time-consuming and require clinical expertise.	Proposed FedCy, an FSSL technique that integrates FL and self-supervised learning to improve performance in a surgical phase recognition task. The proposed method leverages temporal patterns in labeled data to guide unsupervised training on unlabeled data and learn task-specific features for phase recognition.

Table 4 Summary of recent FSSL studies according to data and methodology

Domain	Ref	Year	ML/DL Model(s)	SSL method	Data type	Dataset	Data distribution
Activity Recognition	[64]	2022	MLP, CNN	Label Propagation	Time-Series	MobiAct, WISDM	IID
	[65]	2022	DL	Pseudo-Labeling	Time-Series, Image	HAR, CIFAR-10, MNIST	IID, non-IID
	[61]	2023	DNN	Pseudo-Labeling Label Propagation	Time-Series	WISDM, MobiAct	IID, non-IID
	[67]	2023	AE, Bi-LSTM	Pseudo-Labeling	Time-Series	HAR-UCI, PAMAP2	IID
	[66]	2023	AE	-	Time-Series	Mobiact,WISDM,HAR-UCI, HHAR, PAMAP2,WESAD	IID
	[68]	2025	CNN, LSTM, LLM	Pseudo-Labeling	Time-Series	WISDM, PAMAP2, RealWorld	IID, non-IID
Anomaly Detection	[70]	2022	AE, NN	-	Numerical	UNSW-NB15	IID
	[92]	2022	AE, NN	-	Numerical	UNSW-NB15	IID
	[69]	2023	GANs	-	Numerical	Industrial Control System, Cyber Attack Datasets	IID, non-IID
	[71]	2023	AE, FCN	-	Numerical	SCADA	IID
Image Classification	[10]	2021	ResNet-9	Consistency Regularization	Image	CIFAR-10	IID, non-IID
	[14]	2021	CNN, LSTM	-	Image, Text	MNIST, Fashion-MNIST, IMDb, Reuters	IID, non-IID
	[74]	2021	CNN	Pseudo-Labeling	Image	MNIST, Fashion-MNIST, SVHN	IID, non-IID
	[75]	2022	DNN, CNN	Pseudo-Labeling	Image, Numerical	NUS-WIDE, Vehicle, CIFAR-10	IID
	[16]	2022	VGG9, CNN	Pseudo-Labeling	Image	CIFAR-10, SVHN	IID, non-IID
	[77]	2022	CNN	-	Image	CIFAR-10, SVHN	IID
	[79]	2022	ResNet9	Pseudo-Labeling	Image	MNIST, CIFAR-10, CIFAR-100	IID, non-IID
	[93]	2022	CNN	Consistency Regularization	Image	SVHN, CIFAR-100, ISIC2018	IID, non-IID
	[80]	2023	CNN, ResNet18	Pseudo-Labeling	Image	MNIST, Fashion-MNIST, CIFAR-10, SVHN, COVID- 19	IID, non-IID
	[76]	2023	ResNet9	Pseudo-Labeling Consistency Regularization	Image	CIFAR-10, Fashion-MNIST	IID, non-IID
	[78]	2023	ResNet9	Pseudo-Labeling	Image	CIFAR-10, Fashion-MNIST	IID, non-IID
	[82]	2023	CNN, ResNet-18	Label Propagation	Image	CIFAR-10	IID, non-IID
	[83]	2023	Resnet18, CNN	-	Image	Fashion-MNIST, CIFAR-10	IID
	[84]	2023	Resnet18, CNN	Pseudo-Labeling	Image	CIFAR-10, SVHN,COVID-19	IID, non-IID
	[85]	2024	WideResNet	Pseudo-Labeling Consistency Regularization	Image	CIFAR10, CIFAR100, SVHN	IID, non-IID
	[86]	2024	ResNet18	Pseudo-Labeling	Image	MNIST, CIFAR10, CIFAR100	IID
	[87]	2024	CNN	Pseudo-Labeling	Image	CIFAR-10, CIFAR-100, SVHN	IID, non-IID
	[88]	2025	CNN, ResNet18	Consistency Regularization	Image	CIFAR-10, CIFAR100, ISIC-2018	IID, non-IID
	[89]	2025	ResNet-9	Pseudo-Labeling Consistency Regularization	Image	CIFAR-10, CIFAR100, CINIC-10	IID, non-IID
	[90]	2025	Wide ResNet-28-2 Wide ResNet-28-8	Pseudo-Labeling	Image	SVHN, CIFAR-100, CIFAR-10	IID, non-IID
	[91]	2025	ResNet18	Pseudo-Labeling	Image	CIFAR-10, Fashion-MNIST	IID, non-IID
Indoor Localization	[94]	2022	DDPG	Pseudo-Labeling	Numerical	UJIndoorLoc	IID, non-IID

Table 4 (continued)

Domain	Ref	Year	ML/DL Model(s)	SSL method	Data type	Dataset	Data distribution
Medical Applications	[95]	2022	LSTM	Graph-based	Numeric, Text	MIMIC-III	IID, non-IID
	[96]	2022	UNET, Resnet50	Consistency Learning	Image	ISIC2018, REFUGE	IID
	[112]	2023	ResNet-9	Pseudo-Labeling	Image	MIT-BIH	IID, non-IID
	[111]	2023	MobileNetV2	Pseudo-Labeling	Image	RIM-ONE-r3, Drishti-GS, NCI-ISBI, I2CVB	IID
	[97]	2024	ResNet18, ResNet34, ResNet101	Pseudo-Labeling	Image	Kvasir, CVC-ClinicDB, CVC-300, EndoTectETIS	IID, non-IID
	[98]	2024	CNN, ResNet18	Pseudo-Labeling	Image	Fashion-MNIST, SVHN, CIFAR-10, CIFAR100	non-IID
	[99]	2025	Vision Transformer	Pseudo-Labeling Consistency Regularization	Image	Lung1, Radio, MSD, GDPH, TMCUH, FAHZU, ZJCH	IID
Network Traffic Classification	[100]	2023	CNN	-	Numerical	QUIC dataset	IID
	[101]	2024	AE, CNN	-	Numerical	ISCX VPN2016	IID
Object Detection	[102]	2024	ResNet, R-CNN	Consistency Loss	Image	SKU-110K, RebarDSC	IID, non-IID
Speech Emotion Recognition	[103]	2022	MLP	Pseudo-Labeling	Speech	IEMOCAP, MSP-Improv	IID, non-IID
	[104]	2022	CNN	Pseudo-Labeling	Speech	IEMOCAP	IID, non-IID
Text Classification	[105]	2022	DNN	Pseudo-Labeling Label Propagation	Image, Text	IMDB, Handwritten, ALLAML	IID
	[106]	2023	BERT, LSTM	Pseudo-Labeling	Text	PAN-SemEval-Hyperpartisan- News-Detection-19	IID
	[81]	2023	CNN, RNN	Pseudo-Labeling	Image, Text	MNIST, CIFAR-10, MR, Shakespeare	IID, non-IID
Travel Mode Identification	[107]	2022	DNN	Pseudo-Labeling Consistency Updating	Time-Series	Geolife	IID, non-IID
	[108]	2022	CNN, GRU	Pseudo-Labeling	Time-Series	GeoLife	IID, non-IID
Video and Audio Classification	[109]	2022	CNN	Pseudo-Labeling	Speech	Ambient Context, Speech Commands,VoxForge	IID, non-IID
	[110]	2023	ResNet50, ImageNet	-	Video	MultiChole2022, Cholec80	IID

framework, activity recognition models can be trained in a decentralized manner, where clients use their locally collected data while sensitive information stays on-device. This enables the development of robust activity recognition systems without compromising user privacy. In order to leverage the benefits of federated clustering and SSL, Presotto et al. [61] introduced a new framework for Human Activity Recognition (HAR) called SS-FedCLAR. At SS-FedCLAR, each client combines active learning and label propagation techniques to generate pseudo labels for large volumes of unlabeled data. These labels are utilized to collaboratively train an FL Clustering model. The effectiveness of SS-FedCLAR was evaluated using the WISDM [62] and MobiAct [63] datasets. They achieved a similar accuracy rate to fully supervised FL methods and also proved their superiority over existing semi-supervised FL solutions. Presotto et al. [64] present FedAR that combines label propagation and active learning techniques to add annotations to unlabeled sensor data and uses FL to construct a privacy-aware model. The authors also incorporated transfer learning to refine the global model. The authors show that FedAR achieves an accuracy close to FL-supervised learning methods while addressing the problem of data scarcity in HAR. Albaseer et al. [65] presented FedSemL system over wireless network edges, taking into account the limitations of limited computation and communication resources, as well as the deadline. Their approach involves two phases to optimize the learning performance, training time, and energy consumption of FSSL. In the initial phase, they introduced a bisection-based algorithm that determines optimal transmission power and local processing speeds for newly labeled data. The subsequent phase comprises three algorithms that are designed to regulate local updates and the injection of samples that adhere to the deadline constraint. They presented novel algorithms specifically designed to handle confident pseudo-labeling for unlabeled data samples, which can effectively enhance model performance. Their approach utilizes strong data augmentation techniques in the training phase and switches to weaker data augmentation in the pseudo-labeling phase. They performed comprehensive simulation experiments to assess the effectiveness of their proposed algorithms in two important smart city applications: HAR and object detection. They utilized realistic Federated datasets under non-IID data distributions and tested various percentages of labeled data.

Tashakori et al. [66] introduced SemiPFL which is a framework designed to address the challenge of training models on edge devices that have limited labeled datasets and also a significant volume of unlabeled data. In the proposed approach, edge users work together to train a Hyper-network on the server, which generates personalized autoencoders for every user. Then, the server generates a set of base models for every user that they can combine locally using its own labeled dataset. The proposed solution performed well for users with limited labeled datasets. Gao et al. [67] presented an approach for personalized federated HAR using SSL. The approach addresses some of the challenges of FL: the scarcity of annotated data and the necessity of personalization due to data heterogeneity. In the proposed system, the clients perform unsupervised learning on autoencoders with unlabeled data to develop a general representation model, while the server performs supervised learning on a classifier using labeled data from volunteers. This is personalized for each client by pseudo-labeling, considering both trust and uncertainty. Extensive experiments on two HAR datasets demonstrate the efficacy of the proposed approach. Bukit et al. [68] introduced ATCoFed which is a sensor-based HAR framework. To overcome the challenges posed by limited labeled data and strict privacy requirements, it improves the pseudo-labeling process by incorporating temporal activity transition expectations. The framework uses both LSTMs and LLMs to evaluate and filter predicted activity sequences. This dual evaluator strategy produces more quality pseudo-labels and provides more robust and accurate HAR models. Experiments on benchmark HAR datasets show that ATCoFed outperforms existing FSSL methods while maintaining computational and communication efficiency.

4.2 Anomaly detection

FSSL offers an effective solution to challenges in anomaly detection: data privacy and distribution heterogeneity. Through this collaborative model, knowledge in diverse and heterogeneous data is aggregated to learn more robust and precise models of anomaly detection while preserving client confidentiality. Abdel-Basset et al. [69] proposed a privacy-preserving FSSL framework called Fed-SCR which is designed for detecting abnormal power data in fog-assisted smart grids. They addressed the challenge of performing reliable anomaly detection by prioritizing the privacy and security of the users' data. They suggested a semi-supervised generative network-based approach to learn the underlying distribution of normal data in a privacy-preserving way. Subsequently, they utilized this network to detect anomalies in a distributed and federated environment. The proposed approach combines both labeled and unlabeled data from multiple smart grid substations and uses an FL framework to collaboratively train the generative network. They also introduced a novel aggregation method named Federated Geometric Median Aggregation (Fed-GMA), which uses selective and periodic geometric-median-based aggregation to enhance the resilience of the Fed-SCR framework to noisy gradients while ensuring efficient communication.

Aouedi et al. [70] presented an FSSL model for addressing the limitations of traditional centralized approaches to intrusion detection systems. The proposed model combines FL and SSL, where clients train unsupervised models (AE) with unlabeled data, and the server trains a supervised model (NN) with labeled data. The proposed model utilized network software for automation and deployment and also maintained data confidentiality with minimal overhead and also demonstrated high accuracy and detection. In another study, Aouedi et al. [71] addressed the challenges of using DL approaches for intrusion detection in Industry 4.0 due to privacy, efficiency, and latency concerns and also highlighted the difficulty of obtaining labeled data for DL approaches, which need a lot of data to train effectively. In order to overcome this issue, the authors proposed an FSSL scheme that leverages labeled and unlabeled data. The proposed scheme uses an AE to learn representative features on each device using local unlabeled data, which are then aggregated into a global AE model using FL. Subsequently, the global model is trained using publicly available labeled data. The proposed approach ensures privacy, and high classification performance, works with limited labeled data, and has low communication overhead. They validated the effectiveness of their proposed approach by conducting experiments on industrial datasets. Naeem et al. [72] proposed a federated learning supported semi-supervised active learning (FL-SSAL) framework to address privacy concerns and the problem of limited labeled data in distributed 6G networks. The FL-SSAL framework combines FL, SSL and active learning techniques to improve intrusion detection accuracy while reducing communication overhead and labeling costs. The method selects the most informative examples for annotation using entropy-based active learning and exploits unlabeled data in a semi-supervised approach. Experimental evaluations show that FL-SSAL improves intrusion detection accuracy and reduces communication overhead compared to baseline schemes.

4.3 Image classification

In image classification, FSSL effectively addresses challenges such as limited labeled data, privacy restrictions and inherent distribution of data across a large number of user devices. In recent years, substantial progress has been made in FSSL for image classification, with researchers proposing new techniques, algorithms and architectures specific to this environment. Jeong et al. [10] introduced a method called Federated Matching (FedMatch) which improves the existing FL and SSL approaches. FedMatch uses inter-client consistency loss and parameter decomposition to facilitate disjoint learning on labeled and unlabeled data in two essential scenarios of FSSL: labels-at-server and labels-at-client. They conducted experiments to validate their method, showing that it outperforms local SSL and baselines which naively combine FL with SSL. In another research, Itahara et al. [14] presented a new approach to FL called Distillation-based Semi-supervised FL (DS-FL) which reduces communication costs and enhances model performance. Instead of exchanging model parameters like in typical FL frameworks, DS-FL facilitates the exchange of local model outputs among mobile devices. These outputs are then used to label an open dataset and produce an additional labeled dataset. The local models are subsequently trained using this new dataset. They also proposed an entropy reduction averaging method to prevent ambiguity and training convergence issues caused by heterogeneity among devices' datasets. Their experiments demonstrated a substantial reduction in communication costs with the implementation of DS-FL while maintaining similar or higher classification accuracy compared to FL benchmarks. To enhance communication efficiencies and protect the privacy of participants' model architectures, Li et al. [73] proposed a framework called personalized FL with semi-supervised distillation (pFedSD). The proposed method utilizes an adaptive aggregation technique to diminish the impact of poor-quality model predictions and transmits predicted class distributions instead of model parameters. The predicted class distribution is then returned to clients for local training to get a personalized model. Through experiments on various datasets, the researchers showed that the proposed framework surpasses the performance of the latest federated distillation algorithms. Research [74] presented a new FSSL technique called FedTriNet to leverage unlabeled data in FL. FedTriNet is composed of two steps: In the first step, the model is pre-trained using labeled data through FedAvg. In the second step, unlabeled data is utilized to generate high-quality pseudo labels that are subsequently incorporated into the training set. The authors demonstrated that their approach outperformed existing techniques on three publicly available datasets, both under IID and non-IID settings.

In order to improve the efficiency of the VFL models with a limited amount of aligned instances, Kang et al. [75] introduced Federated Cross-view Training (FedCVT) as an approach to address the limitations of VFL when the set of aligned samples is small, leaving a significant portion of non-aligned data unused. FedCVT addresses this issue by predicting pseudo-labels for unlabeled samples, estimating representations for missing features, and expanding the training set. It trains three classifiers jointly based on different views of the expanded training set, resulting in improved performance of the VFL model. Notably, the proposed approach preserves data privacy as it does not need the sharing of original data and model parameters. Experiment results show that FedCVT outperforms vanilla VFL

which only uses aligned samples. Research [16] discussed a system called Ada-FedSemi, which leverages FSSL techniques to enhance the effectiveness of DL model. The system combines labeled data from on-device sources with unlabeled data from cloud sources to enhance accuracy of the global model. The proposed approach utilizes a multi-armed bandit (MAB) based algorithm to dynamically identify the participation rate of clients and the trust threshold during model training. Through extensive experiments, Ada-FedSemi demonstrates improved test accuracy compared to baseline methods, while saving up to 48% training costs. In the domain of IoT, Zhang et al. [76] discussed the use of Unmanned Aerial Vehicle (UAV) swarms for automatic image recognition. However, sharing ground-truth-labeled data among UAVs for training such models presents challenges related to data privacy and data availability. To mitigate this problem, the authors proposed an FSSL framework called Federated Mixing (FedMix), which uses a model parameter mixing strategy to combine federated and SSL methods. They also proposed an aggregation rule that considers the frequency of client participation in training to handle statistical heterogeneity. Their empirical findings demonstrate that the suggested method surpasses existing baselines and exhibits robustness to varying levels of non-IID client data.

Kádár et al. [77] discussed the problem of multitask learning in distributed environments where multiple participants aim to enhance their performance through collaboration while preserving the privacy of datasets and model parameters. The authors introduced FedLinked, a privacy-preserving method that combines FL, multitask learning, and SSL to address cross-silo problems with limited labeled data. The method involves regularizing representation learning based on the cross-utility of participating clients. In their evaluation, the authors compared FedLinked to FedAvg and non-cooperating client-based solutions in multitasking scenarios for image classification. The experimental results demonstrated that FedLinked is better than other methods regarding accuracy and convergence speed. Shi et al. [78] discussed the challenge of statistical heterogeneity in FL and the limitation of existing model personalization methods that rely on fully labeled data. The proposed solution is a personalized SSL paradigm that enables clients with partially labeled or unlabeled data to obtain labeling assistance from other data-relevant clients, known as helper agents. The method incorporates an ambiguity-based data-relationship metric to provide reliable pseudo labels and a helper choice protocol to optimize communication efficiency. Experimental results showcased the superiority of the proposed method over existing approaches in highly heterogeneous settings with partially labeled data. Yang et al. [79] addressed the limitations of traditional FL methods that assume fully labeled data on user devices, and the problems of slow training and convergence of methods proposed in the literature. They introduced an FSSL framework called Federated Incremental Learning (FedIL), which is specifically designed for edge computing. It introduces a group-based asynchronous training algorithm that allows more clients to participate simultaneously, thus accelerating model training with provable convergence. The performance superiority of FedIL was demonstrated through track-driven simulations and the development of a prototype system. To tackle the challenge of non-IID data in FL, Li et al. [80] introduced a new FL framework called Synthetic Data Aided Federated Learning (SDA-FL). The proposed framework includes a local GAN pre-training of each client to produce differentially private synthetic data. These synthetic data samples are then used to construct a global shared synthetic dataset on the parameter server. The framework also includes an iterative pseudo-labeling mechanism to produce confident pseudo-labels for the synthetic dataset. They experimentally demonstrated that using a synthetic dataset with confident pseudo-labels improves consistency between local updates and benefits global aggregation.

Zhong et al. [81] described a novel FL method called Random Sampling Consensus Federated Learning (RSCFed). The proposed method addresses the problem of varying reliability between fully-unlabeled, fully-labeled, and partially labeled clients. RSCFed achieves consensus by distilling multiple sub-consensus models through random sub-sampling across clients, rather than directly aggregating local models. To improve the robustness of sub-consensus models, the authors introduced a distance-reweighted model aggregation method. Research [82] introduced FedProp which is a novel method for SSL in a federated setting. FedProp simultaneously predicts the data manifold using data from multiple clients and uses cross-client label propagation to calculate pseudo-labels. The method utilizes secure Hamming distance computation and secure aggregation protocols to protect data privacy. The authors showed that FedProp outperforms previous FSSL methods and complements consistency-based approaches. Also, they demonstrated that combining both methods can lead to further accuracy gains. Qian et al. [83] introduced a new method to enhance the performances of FSSL utilizing information entropy. The authors introduced the FedEntropy algorithm, which utilizes information entropy to calculate the loss function for both labeled and unlabeled data simultaneously. The proposed method includes an adaptive proportional adjustment algorithm based on inverse trigonometric functions, which dynamically determines the ratio between the loss of labeled and unlabeled data. By utilizing labeled data for parameter updates and unlabeled data for model regularization, the method aims to improve the generalization

performance of the model. They evaluated FedEntropy on several benchmark datasets and compared its performance to existing FSSL algorithms. Their experimental findings demonstrate that FedEntropy surpasses existing algorithms in terms of performance while maintaining the privacy and security of the client's data. In another research, Wei et al. [84] addressed the problem of imbalanced model training in FSSL owing to the non-IID data in the clients. The authors introduced a balanced FSSL approach incorporating the fairness-aware pseudo-labeling (FAPL) strategy to address fairness concerns. Their method ensures a balanced distribution of unlabeled data samples for model training and establishes personalized local constraints for each client to facilitate local pseudo-labeling.

Lee et al. [85] proposed $(\mathrm{FL})^2$ to solve the performance problem in FSSL caused by confirmation bias and the separation of labeled and unlabeled data. The method uses sharpness-sensitive consistency regularization to improve the training of unlabeled clients (clients with completely unlabeled local data) and carefully selects instances for regularization rather than applying it to the entire pseudo-labeling loss. The approach also includes client-specific adaptive thresholding and learning state-sensitive aggregation to tailor the training process to the progress of each client. Wang et al. [86] proposed a new FSSL method called FedTG for image classification in edge computing. The approach addresses the issues of unlabeled data for edge nodes that reduce the accuracy of the model. The proposed FedTG provides better information extraction and reduces errors by using multiple high-probability pseudo-labels from unlabeled data instead of relying on a single pseudo-label. Experiments show that FedTG is efficient in improving the accuracy of traditional FL models. Zhu et al. [87] introduced PDCFed, a two-stage sampling method that evaluates sample reliability using predicted distribution changes and data augmentation to address challenges in FSSL, especially non-ID data and communication inefficiency. The proposed approach evaluates sample reliability based on weak augmentation predictions and uses a Gaussian function to adjust the predicted distribution changes for less reliable samples. PDCFed includes an entropy penalty term to improve model generalization after unsupervised training loss. Experimental results show that the proposed method shows superior performance compared to existing methods on non-IID datasets and significantly improves communication efficiency. Yang et al. [88] addressed limitations in existing FSSL approaches such as biased classifiers and skewed unlabeled clients caused by over-reliance on data-level augmentation and simple aggregation methods. They introduced a new FSSL framework, namely FedRVR which incorporates multi-directional regularization at clients and a relation-driven directional aggregation strategy at the server. This approach leverages pairwise model relationships to improve global model quality and enhance local training consistency. Zhu et al. [89] addressed the problem of partially labeled data caused by high labeling costs in FL. They proposed TGAFed that uses truncated Gaussian aggregation to weight unlabeled instances, optimize pseudo-label filtering, and provide inter-client consistency loss. This approach improves pseudo-label usage and global model performance through local and global quantity-quality factors.

Zhao et al. [90] proposed FedLGMatch to address the limitations of existing FSSL methods, which typically rely solely on a global model for pseudo-label generation. Because local client data can be largely non-IID, solely using global pseudo-labeling often introduces noise and validation bias. FedLGMatch uses both local and global models to provide cleaner pseudo-labels personalized to the data distribution of each client. It enhances the stability and quality of labels by incorporating locally trained models from previous rounds into the pseudo-labeling process. Wang et al. [91] proposed DDRFed, a new FSSL framework that aimed to solve two important problems in FSSL: the scarcity of labeled data and non-IID data across clients. Unlike typical pseudo-labeling methods which use fixed confidence thresholds and exclude low-confidence samples, DDRFed introduces a client-side propagation model to generate data consistent with the global distribution and mitigate non-IID issues. It also uses dynamic class balance thresholds to better utilize both high- and low-confidence samples and applies residual class negative learning to extract useful information from uncertain samples.

4.4 Indoor localization

FSSL provides a promising solution for addressing privacy challenges in indoor localization systems, where location data are often highly sensitive. Moreover, the ability to incorporate large amounts of unlabeled data allows FSSL-based models to achieve better accuracy and resilience. Wu et al. [94] introduced an FL approach for fingerprint-based indoor localization. The objective of their work is to overcome challenges related to frequent data collection and privacy concerns. The authors observed that existing FL-based indoor localization studies often overlook users' specific localization preferences and requirements. To address this, they proposed Prediction-based Semi-supervised Online Personalized Federated Learning (PSO-PFL) approach, which considers two common indoor localization cases which have different data distributions and user mobility. In Scenario I, online SSL is used with personalization to improve localization performance. In Scenario II, the main objective is to offer localization services to highly mobile

users. To accomplish this, a prediction-based client selection strategy is employed. The experimental results demonstrated that the PSO-PFL approach outperformed centralized training and FedAvg methods in terms of personalization accuracy. Additionally, the approach shows that efficiently utilized unlabeled data to enhance performance.

4.5 Medical applications

In AI-based medical applications, strict privacy regulations and fragmented, largely unlabeled data make centralized model training difficult. FSSL offers a viable solution by enabling decentralized learning, allowing institutions to contribute to a shared model without exposing raw patient data. Thakur et al. [95] proposed a framework to build an effective ML model for AI healthcare applications. The framework is based on dynamic neural graphs and extends the Reptile meta-learning algorithm to a federated setting, where electronic healthcare records are distributed across a network of institutions. The proposed framework incorporates unlabeled examples in the supervised training setup, using a dynamic variant of neural graph learning to establish a neighborhood of a labeled example utilizing local graphs constructed over batches of training instances. The framework which operates in a semi-supervised manner was evaluated on the MIMIC-III dataset. The experimental results demonstrated its efficiency in single and multi-task scenarios, considering data decentralization restrictions. Wen et al. [96] discussed the challenges of medical image segmentation (MIS), as it requires large amounts of labeled data that may contain sensitive information. FL is proposed as a solution for collaborative model training without exposing raw data; however, previous FL works for MIS have only focused on fully supervised scenarios. Therefore, the authors introduced a novel FSSL framework for MIS that effectively utilizes labeled and unlabeled data from multiple hospitals. The proposed framework enhances the mean teacher mechanism by incorporating cross-client ensemble and model-wise self-ensembling modules. To evaluate its performance, the method is applied to two publicly available medical image datasets. The results demonstrate the effectiveness of the proposed FSSL method in leveraging unlabeled data to improve model performance and outperform existing FSSL approaches for MIS. Qiu et al. [111] proposed an FSSL method that uses a pseudo-labeling strategy to address the problems associated with limited labeled data in medical image segmentation. This method uses a federated pseudo-labeling strategy that exploits information from labeled clients to generate pseudo-labels for unlabeled clients and also reduces annotation gaps and provides a cost-effective solution for medical image analysis. The effectiveness of the presented method is demonstrated on fundus image and prostate MRI segmentation tasks. Ying et al. [112] presented FedECG which is a new FSSL framework for predicting electrocardiogram (ECG) abnormalities. This approach addresses the problems of non-IID data in ECG monitoring, the scarcity of labeled data, as well as privacy concerns. FedECG leverages a preprocessing module, a ResNet-9 based model, pseudo-labeling and data augmentation techniques to improve prediction accuracy. In addition, they developed a model aggregation algorithm to improve convergence in FL. Experimental results show that FedECG achieves 94.8% accuracy when only 50% of the data is labeled.

Ma et al. [97] presented a Model-Heterogeneous Semi-Supervised Federated (HSSF) Learning framework for medical image segmentation that addresses challenges such as data sensitivity, privacy concerns and expensive annotations. The framework includes Regularity Densification and Regularity Fusion to enable personalization across sites while transferring selective knowledge. It uses a Self-Assessment (SA) module and a Trusted Pseudo Label Generation (RPG) module for real-time trust building to reduce annotation overhead and effectively use unlabeled data. Li et al. proposed [98] FSSL-HD which is a unified framework designed for heterogeneous IoT health systems with limited labeled data. This framework addresses the challenges in IoT health devices with heterogeneous data distributions and limited labels. The proposed method includes a novel objective function for unlabeled devices, a loss-based aggregation mechanism to enhance knowledge distillation, multiple iterations for labeled devices to improve performance and dynamically adjusted confidence thresholds. Li et al. presented [99] a FSSL framework for lung tumor segmentation which effectively addresses privacy constraints and limited labeled data in clinical settings. This method first performs unified self-supervised pre-training on completely unlabeled sites using masked image modeling, then fine-tunes segmentation models using a pseudo-supervision refinement strategy that reduces label noise and stabilizes training. Additionally, a dynamic model aggregation mechanism is introduced to improve global model robustness under heterogeneous data distributions.

4.6 Network traffic classification

Jin et al. [100] introduced a new approach for network traffic classification using FSSL. The proposed approach uses unlabeled data on the client side and labeled data on the server side to train a global classification model. Additionally, the approach uses two traffic subflow sampling methods for data preprocessing. The experimental results on the QUIC dataset show that the proposed approach achieves high accuracy while protecting users' privacy and requiring

minimal labeled data. The proposed approach can be used for network traffic classification in scenarios where privacy and lack of labeled data are a concern. Wang et al. [101] presented a novel approach based on FSSL for network traffic classification in smart home networks. The authors address the main challenges in AI-based traffic classification, including data privacy concerns and the high cost of labeling traffic data. The proposed framework utilizes FL at end-home gateways to protect user privacy while providing local training and inference. In this framework, a DPI-based labeling method is used that preserves data privacy at the end-home gateways. Furthermore, an AE-based semi-supervised model is developed to reduce the need for labeled data and an XAI-based method is applied to improve the explainability of the model.

4.7 Object detection

Zhao et al. [102] proposed a new FSSL framework named FSSLOD for object detection in dense scenes where limited labeled data and data distribution disparities hinder performance. The framework uses a client-side teacher-student network for local SSL and utilizes a consistency loss to align the outputs of both networks. In addition, the model includes an elastic update mechanism to address data distribution issues which prevents under-trained knowledge from being incorporated into the shared model.

4.8 Speech emotion recognition

FSSL has been a promising approach to overcome data scarcity and data privacy issues in speech emotion recognition. With FSSL methods, training models can be collaboratively trained in a decentralized manner without sharing data. In this field, different works have been performed in speech emotion recognition. Feng et al. [103] proposed an FSSL framework called Semi-FedSER. The framework utilizes labeled and unlabeled data instances to tackle the issue of limited labeled data in FL. The authors demonstrated that the proposed framework can achieve effective speech-emotion recognition (SER) performance even in scenarios where the local label rate is low. Overall, they presented a promising solution to address privacy concerns while improving the performance of SER applications using FL. Tsouvalas et al. [104] introduced a novel approach for SER which combines SSL with FL to overcome the problem of limited labeled data and privacy concerns in traditional centralized approaches. The proposed approach is the first federated SER method that uses self-training learning with FL to take advantage of labeled and unlabeled on-device data. The authors showed that their method is able to learn generalizable SER models even with low data label availability and non-IID distributions.

4.9 Text classification

In text classification, FSSL can be used to develop global models by exploiting unlabeled data and preserving privacy. With this method, it is possible to train text classification models in a decentralized way without clients sharing data. Ahmed et al. [106] proposed a novel FSSL scheme based on self-ensembling which uses linguistic and stylometric features from annotated news articles and unlabeled data to denoise labels for hyper-partisan text classification. The authors proposed a method that incorporates various techniques to improve the learning system's performance in text classification tasks. These techniques include temporal context extraction for semantic vector representation, extraction of relevant boundary elements from unlabeled text for active learning, and reduction of data annotation tasks while enhancing generalization. To address heterogeneous data in FL, Feng et al. [105] presented a semi-supervised federated heterogeneous transfer learning (SSFHTL) approach. This approach uses transfer learning to learn shared representations from data available at different devices, guiding the model training process in a semi-supervised manner. The proposed approach has a shared feature extractor, a task-specific classifier, and a transfer learning module. It outperformed traditional FL approaches on heterogeneous data, in experiments with text and image data. Zhong et al. [81] proposed Semi-HFL which is an FSSL approach that divides the model into small submodels using early exit branches to accommodate different devices' resource requirements. The approach introduced semi-supervised techniques for training, which involves supervised learning on server and unsupervised learning on clients by leveraging the clients' unlabeled data.

4.10 Travel mode identification

FSSL offers an effective solution to address privacy concerns and labeled data scarcity in travel mode identification. FSSL preserves sensitive information while allowing the development of accurate and robust travel mode classification models. Zhang et al. [107] introduced a novel approach called mean teacher semi-supervised federated learning (MTSSFL) for privacy-preserving Transportation Mode Identification (TMI). This approach leverages crowdsourcing as a data source and aims to achieve accurate and privacy-preserved TMI without relying on a large amount of labeled data. MTSSFL incorporates consistency updating which involves incorporating the global model in the gradient updates of local models that only have access to

unlabeled data. This technique enhances the training of the local models. Furthermore, a secure parameter aggregation mechanism called mean-teacher-averaging is devised to further boost the global model's TMI performance without requiring extra training. Zhu et al. [108] proposed an FSSL framework to correctly identify the modes of travel without preserving client privacy. This framework uses CNN-GRU model to extract travel modes from GPS trajectories. The authors also incorporated a pseudo-labeling method for clients to assign pseudo-labels to their local unlabeled datasets. Additionally, they implemented grouping-based aggregation and data-flipping augmentation techniques to enhance performance and convergence.

4.11 Video and audio classification

FSSL provides an effective approach to tackle data privacy and labeled data scarcity in video and audio classification. This decentralized learning paradigm allows models to be trained collaboratively without sharing raw data, enabling researchers to preserve privacy while leveraging both labeled and unlabeled datasets to improve model performance. Kassem et al. [110] introduced a method called FedCy, which is an FSSL approach that uses a combination of FL and self-supervised learning to improve the performance of surgical phase recognition. This method is designed to address the challenges of training DL models for surgical phase recognition since medical data is highly sensitive and the need for various datasets from multiple medical institutions. FedCy combines labeled and unlabeled video data from multiple institutions and leverages temporal patterns in the labeled data to guide unsupervised training on the unlabeled data. Tsouvalas et al. [109] introduced FedSTAR which is an SSL approach for audio models that leverages FL and self-training to make use of on-device unlabeled data. The main idea behind this method is to improve the generalization of audio recognition models by using large-scale unlabeled data on user devices. The authors showed that pre-training models using self-supervision techniques can significantly enhance convergence during training.

5 Challenges, open issues and future research directions

FSSL is a promising approach for training effective ML models while maintaining data privacy, particularly in scenarios where labeled data is scarce. However, as in the case of FL [5] [25] [17], there are similar challenges that need to be addressed in FSSL. This chapter examines the main challenges faced in FSSL and suggests potential solutions to address these obstacles for future research. Firstly, communication poses a challenge to FSSL, arising when dealing with a large number of devices and the requirement to transmit and receive model updates. Secondly, resource allocation between devices with varying computational, processing, and storage capacities poses another challenge. Privacy is a crucial concern in FSSL, requiring careful handling of sensitive data. Moreover, the heterogeneity of devices and data introduces discrepancies in performance and accuracy. Table 5 shows a summary of challenges and possible future directions. The main challenges faced by FSSL are shown in Fig. 11.

5.1 Communication

In FSSL, the model undergoes training on data distributed among multiple clients, with model parameters being exchanged between the central server and the clients. However, this process introduces a significant communication overhead due to frequent device communication. Consequently, issues such as latency, network congestion, and high energy consumption arise, making communication a major challenge in FSSL. Additionally, communication between clients can result in inconsistent model updates [5, 113].

Several strategies can be employed to address these challenges and achieve efficient communication in FSSL. Firstly, the number of communication rounds in model updates can be reduced, or the size of transmitted data can be minimized [3]. This can be achieved through the utilization of data compression methods to decrease the size of transmitted data. Secondly, developing algorithms that optimize model updates can help in reducing the total number of communication rounds [114, 115]. It is also possible to adjust model updates based on their effectiveness and importance. Furthermore, leveraging edge and fog computing architectures can accelerate the communication of model updates between devices and the central server [116]. By utilizing these distributed computing frameworks, the proximity of devices to the server can be leveraged, reducing communication latency and enhancing overall efficiency in FSSL.

5.2 Resource allocation

The resource allocation problem presents a significant challenge in FSSL. Since FSSL involves model training on distributed devices with varying computational capabilities and data sizes, optimizing resource allocation is crucial to achieve an efficient and effective model. However, the devices involved in training may have diverse memory capacities, processing power, and bandwidth, which make optimal resource allocation across devices more complex. Moreover, imbalanced resource allocation can lead to

Table 5 FSSL challenges and potential future directions

FSSL challenges	Related problems	Potential future directions
Communication	- High communication overhead due to frequent communication between devices - Communication between clients can lead to inconsistent model updates	- Reducing the number of communication rounds - Reducing the transmitted data size - Cloud and fog computing structures
Resource Allocation	- Model training on distributed devices with different computational capabilities and data sizes - Imbalanced resource allocation	- Resource allocation algorithms - Task scheduling algorithms
Privacy	- Model training takes place on decentralized data owned by multiple devices. - Collecting model updates from various devices	- Differential privacy - Homomorphic encryption
Heterogeneity	- Diversity of participating devices (system heterogeneity) and data distributions (statistical heterogeneity) - Network heterogeneity with varying bandwidth, latency and reliability	- Adaptive learning methods - Personalized model training - Transfer learning techniques
Scalability	- Large number of clients with different data distributions, computational capacities and network conditions	- Hierarchical FL architecture - Adaptive client selection - Model compression techniques
Model robustness	- Sensitivity of the framework to data noise, adversarial attacks and biased updates from clients - Non-IID data distributions	- Robust aggregation techniques - Noise-tolerant pseudo-labeling
Confirmation Bias	- Locally generated pseudo-labels may be biased due to Non-IID distributions, creating a feedback loop that propagates errors and degrades the global model.	- Quality-aware aggregation - Client-side agreement scores - Server-side bias mitigation
Unaligned and Unlabeled Multimodal Data	- Multimodal data is unevenly distributed and often unaligned across clients, making cross-modal consistency and relationship learning difficult.	- Federated cross-modal alignment - Cross-modal contrastive learning
Imbalance between Labeled and Unlabeled Data Distribution	- Clients have heterogeneous amounts of labeled and unlabeled data, causing biased convergence and disruption in global optimization.	- Adaptive and context-aware aggregation

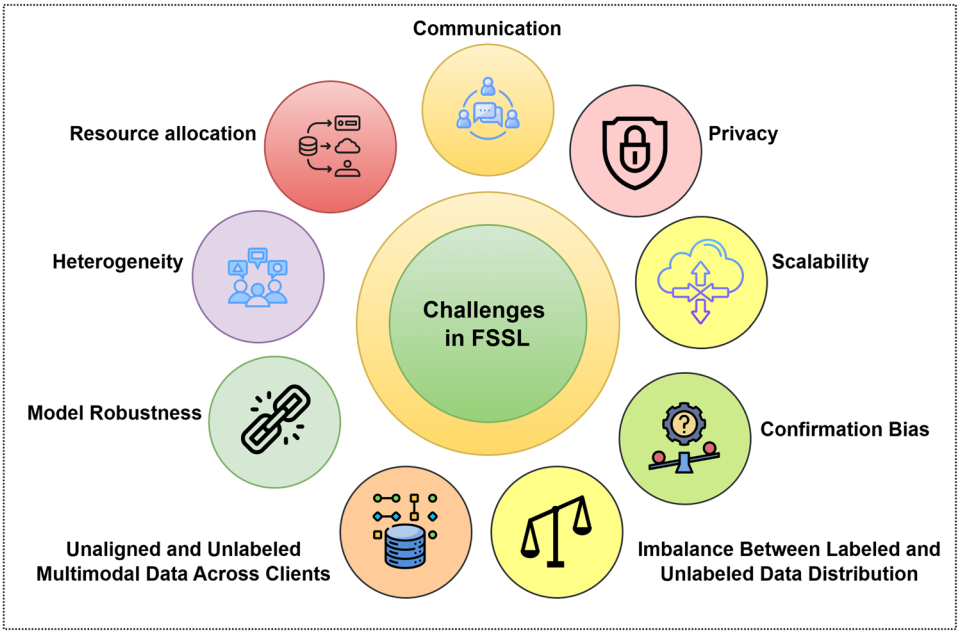


Fig. 11 FSSL challenges

degraded model performance, slow convergence, and inefficient resource utilization [5].

A promising solution to solve these problems is to develop resource allocation algorithms that consider the heterogeneous nature of the devices and the characteristics of the data distributed among them [29]. These algorithms dynamically allocate resources based on each device's capacity and the data they possess which results in more efficient and effective model training in FSSL. Another approach is to devise task scheduling algorithms that efficiently plan tasks across devices, balancing the workload and optimizing resource utilization [117]. Hence, tasks can be assigned appropriately based on device capabilities, minimizing idle time. Dynamic and adaptive resource allocation ensures reduced model learning time and faster convergence.

5.3 Privacy

In FSSL, ensuring privacy protection is a critical challenge. While FSSL achieves data security by conducting model training without sharing raw data, preserving the confidentiality of sensitive information becomes more challenging as training occurs on decentralized data owned by multiple devices. The distributed nature of the data introduces vulnerabilities, thereby raising concerns about unauthorized access and data breaches. Additionally, the collection of model updates from various devices while maintaining confidentiality adds complexity and increases the computational burden in FSSL [17, 113].

To ensure data privacy in FSSL, methods like homomorphic encryption and differential privacy can be employed [31, 118]. These methods aim to protect sensitive information; however, they may require additional computational and communication resources. Therefore, for future research, it is crucial to develop methods that effectively preserve confidentiality while also considering resource utilization.

5.4 Heterogeneity

The heterogeneity problem in FSSL stems from the diversity of participating devices (system heterogeneity) and data distributions (statistical heterogeneity) in a decentralized learning environment. FSSL presents additional complexities by combining the challenges of both FL and SSL. It involves multiple devices with different characteristics and constraints. These devices may have different hardware configurations (e.g., CPU, GPU, memory capacity), communication and computing capabilities, and battery life. The heterogeneity of these devices can have a negative impact on their computation and communication abilities, thereby influencing the overall performance of the FSSL system [23].

Furthermore, FSSL systems operate over networks that may exhibit diverse distinct characteristics such as varying bandwidth, latency, and reliability. This network heterogeneity can affect the communication cost and accuracy of the FSSL system. Another aspect of heterogeneity is statistical heterogeneity which refers to the differences in data distributions among devices involved in the training process. This heterogeneity may arise due to various factors like device types, data collection methods, and geographic location of devices. In the FSSL environment, numerous edge devices store data that may exhibit non-IID (Independent and Identically Distributed) characteristics [119]. Such

data contradicts the IID data assumption used in distributed optimization problems. This can cause complexity in problem modeling, analysis and optimization, and experimental evaluation of solutions. Statistical heterogeneity poses a significant challenge in FSSL as it can affect the generalization and accuracy of ML models.

Dealing with the heterogeneity problem in FSSL necessitates the development of methods capable of handling the diversity between devices and data distributions. Adaptive learning methods [120] offer one such technique by allowing model parameters to adapt based on device heterogeneity. Personalized models tailored to each device's specific requirements and capabilities can also be employed, rather than relying on a one-size-fits-all approach [113]. Additionally, transfer learning techniques [121] can be leveraged to transfer knowledge from devices with diverse data or better capabilities to devices with limited resources. This involves transferring pre-trained models or fine-tuning features from one device to another, which mitigates the impact of heterogeneity. Another crucial technique involves designing data selection strategies [122] based on criteria such as data quality, similarity, or diversity. By employing such methods, the training data becomes more representative of the overall data distribution, aiding in overcoming the challenges posed by statistical heterogeneity.

5.5 Scalability

Scalability is a critical challenge for FSSL. This is especially true when applied to large-scale real-world scenarios involving a large number of clients with different data distributions, computational capacities and network conditions [123]. As the number of clients increases, so does the communication overhead and computational complexity. Resource-constrained clients such as IoT devices, mobile phones, etc. are more affected by these problems due to their limited bandwidth and hardware capabilities [5].

To overcome these challenges in FSSL, it is important to develop architectures such as hierarchical federated architectures that group clients locally and thus reduce communication costs [124]. In addition, adaptive client selection strategies based on data quality and resource availability can both maintain model integrity and ensure efficient participation [125]. Moreover, lightweight communication protocols and model compression techniques can reduce bandwidth constraints. These developments can contribute to extending the applicability of FSSL to large-scale, resource-diverse environments.

5.6 Model robustness

Ensuring model robustness in FSSL is a significant challenge due to the sensitivity of the framework to data noise, adversarial attacks and biased updates from clients. Non-IID data distributions increase these vulnerabilities, as the pseudo-labels produced by semi-supervised methods can be unreliable or noisy [126]. This leads to model drift and poor generalization. Besides, adversarial clients can inject poisoned data or manipulate updates in order to decrease the performance of the global model.

Overcoming these challenges requires the development of advanced robust aggregation techniques based on anomaly detection to reduce the impact of malicious or low-quality updates [127]. Also, noise-tolerant pseudo-labeling methods including uncertainty estimation [128] or confidence filtering [129] can improve the reliability of the learning process. Future research should focus on mechanisms for adaptively identifying and responding to anomalies in real time to maintain resiliency for FSSL in adversarial environments.

5.7 Confirmation bias

The effectiveness of FSSL largely depends on the quality of locally generated pseudo-labels. Although pseudo-labeling is the base of many SSL methods, its reliability significantly decreases in federated environments where unlabeled data usually exhibits non-IID features. A local model trained on a skewed class distribution naturally generates biased pseudo labels for locally unlabeled data. Including these biased labels in the training process generates a feedback loop known as confirmation bias where the model reinforces its own prediction errors. When these biased local updates are combined, they can propagate errors across communication rounds and degrade the global model's performance.

Future research should go beyond standard averaging algorithms for global consistency and focus on methods such as quality-aware aggregation [130]. Additionally, client-side agreement scores used to filter unreliable pseudo-labels, server-side bias mitigation models that align client distributions and pseudo-label merging approaches that account for uncertainty can reduce bias and enable global updates to better represent the underlying data distribution.

5.8 Unaligned and unlabeled multimodal data across clients

Modern federated systems include more multimodal data, such as text, image, audio or sensor streams from various devices. However, this data is often distributed unevenly among clients and may be inconsistent. One client may

only hold unlabeled data, while another may only hold unstructured text logs. Standard SSL consistency techniques which assume a consistent single view input domain will fail when the structural relationship between these modalities is unknown or the data is not temporally aligned across clients. This also makes learning cross-modal relationships difficult in FSSL.

In order to address this challenge, federated cross-modal alignment [131] and cross-modal contrastive learning [132] approaches can facilitate meaningful learning from inconsistent data. Future research should explore methods for aligning representations from different modalities in a common latent space without paired raw data needing to coexist on the same device.

5.9 Imbalance between labeled and unlabeled data distribution

The non-uniform distribution of labeled and unlabeled data among clients is a challenge in FSSL. In many real-world scenarios, some clients have a small amount of labeled data, while others have a large amount of unlabeled data and some may contain only unlabeled data. This heterogeneity disrupts the global optimization process and can also lead to biased model convergence dominated by clients with noisy or low-quality unlabeled data.

To address this issue, designing adaptive and context-aware aggregation [133] mechanisms can be a promising approach for future research. Instead of weighting client updates only based on dataset size, future approaches should consider the reliability of pseudo-labels, the entropy of predictions and the temporal consistency of local updates.

6 Conclusion

As FSSL methods evolve, they provide clients with a solution to the problem of scarce labeled data and enable collaborative ML model building without compromising privacy. FSSL achieves model updates while prioritizing data security and privacy without the need for data sharing. In addition, it leverages unlabeled data for model training, resulting in the construction of more robust ML models. Because of these attributes, FSSL has recently received considerable attention from the research community. Motivated by the rapid growth of this field, this survey provides a comprehensive and systematic analysis of FSSL. In addition to reviewing the fundamental principles of FL and SSL, we present detailed reviews and organized summaries of research involving the use of FSSL methods in various domains. Unlike previous FL or SSL research, our work focuses specifically on their intersection, presenting FSSL studies structurally and systematically. Finally, we identify the current challenges facing FSSL and highlight potential directions for future research.

Author contributions Ahmet Alkılınç: Conceptualization, Methodology, Software, Visualization, Writing – original draft, Writing – review & editing. Feyza Yıldırım Okay: Conceptualization, Methodology, Writing – review & editing. İbrahim Kök: Conceptualization, Methodology, Writing – review & editing. Suat Özdemir: Supervision, Writing – review & editing.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Albrecht, J.P.: How the gdpr will change the world. European Data Protection Law Review **2**, 287 (2016)
2. McMahan, B., Moore, E., Ramage, D., Hampson, S., Arcas, B.A.: Communication-efficient learning of deep networks from decentralized data. In: Artificial Intelligence and Statistics, 1273–1282 (2017). PMLR
3. Konecný, J., McMahan, H.B., Ramage, D., Richtárik, P.: Federated Optimization: Distributed Machine Learning for On-Device Intelligence (2016)
4. Konecný, J., McMahan, H.B., Yu, F.X., Richtárik, P., Suresh, A.T., Bacon, D.: Federated Learning: Strategies for Improving Communication Efficiency (2017)
5. Lim, W.Y.B., Luong, N.C., Hoang, D.T., Jiao, Y., Liang, Y.-C., Yang, Q., Niyato, D., Miao, C.: Federated learning in mobile edge networks: A comprehensive survey. IEEE communications surveys & tutorials **22**(3), 2031–2063 (2020)
6. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST) **10**(2), 1–19 (2019). https://doi.org/10.1145/3298981
7. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 13–16 (2012)

8. Zhao, Y., Li, M., Lai, L., Suda, N., Civin, D., Chandra, V.: Federated learning with non-iid data (2018)
9. Ji, S., Tan, Y., Saravirta, T., Yang, Z., Liu, Y., Vasankari, L., Pan, S., Long, G., Walid, A.: Emerging trends in federated learning: From model fusion to federated x learning. International Journal of Machine Learning and Cybernetics, 1–22 (2024)
10. Jeong, W., Yoon, J., Yang, E., Hwang, S.J.: Federated semi-supervised learning with inter-client consistency & disjoint learning. In: International Conference on Learning Representations (2021)
11. Jin, Y., Wei, X., Liu, Y., Yang, Q.: Towards Utilizing Unlabeled Data in Federated Learning: A Survey and Prospective (2020)
12. Albaseer, A., Ciftler, B.S., Abdallah, M., Al-Fuqaha, A.: Exploiting unlabeled data in smart cities using federated edge learning. In: 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 1666–1671. IEEE (2020). https://doi.org/10.1109/IWCMC48107.2020.9148475
13. Zhang, Z., Yang, Y., Yao, Z., Yan, Y., Gonzalez, J.E., Ramchandran, K., Mahoney, M.W.: Improving semi-supervised federated learning by reducing the gradient diversity of models. In: 2021 IEEE International Conference on Big Data (Big Data), pp. 1214–1225. IEEE (2021). https://doi.org/10.1109/BigData52589.2021.9671693.
14. Itahara, S., Nishio, T., Koda, Y., Morikura, M., Yamamoto, K.: Distillation-based semi-supervised federated learning for communication-efficient collaborative training with non-iid private data. IEEE Trans. Mob. Comput. **22**(1), 191–205 (2021)
15. Long, Z., Che, L., Wang, Y., Ye, M., Luo, J., Wu, J., Xiao, H., Ma, F.: FedSiam: Towards Adaptive Federated Semi-Supervised Learning (2021)
16. Wang, L., Xu, Y., Xu, H., Liu, J., Wang, Z., Huang, L.: Enhancing federated learning with in-cloud unlabeled data. In: 2022 IEEE 38th International Conference on Data Engineering (ICDE), 136–149 (2022). https://doi.org/10.1109/ICDE53745.2022.00015
17. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., Gao, Y.: A survey on federated learning. Knowledge-Based Systems **216**, 106775 (2021)
18. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., He, B.: A survey on federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Trans. Knowl. Data Eng. **35**(4), 3347–3366 (2021)
19. Chaudhary, R.K., Kumar, R., Saxena, N.: A systematic review on federated learning system: a new paradigm to machine learning. Knowl. Inf. Syst. **67**(2), 1811–1914 (2025)
20. Oliveira, W.D.G., Berton, L.: A systematic review for class-imbalance in semi-supervised learning. Artificial Intelligence Review **56**(Suppl 2), 2349–2382 (2023)
21. Song, Z., Yang, X., Zhang, Y., Fu, X., Xu, Z., King, I.: A systematic survey on federated semi-supervised learning. In: IJCAI **16**, 18 (2024)
22. Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G.: Preferred reporting items for systematic reviews and meta-analyses: The prisma statement. Int. J. Surg. **8**(5), 336–341 (2010). https://doi.org/10.1016/j.ijsu.2010.02.007
23. Li, T., Sahu, A.K., Talwalkar, A., Smith, V.: Federated learning: Challenges, methods, and future directions. IEEE Signal Process. Mag. **37**(3), 50–60 (2020). https://doi.org/10.1109/MSP.2020.2975749
24. Liu, Y., Kang, Y., Xing, C., Chen, T., Yang, Q.: A secure federated transfer learning framework. IEEE Intell. Syst. **35**(4), 70–82 (2020). https://doi.org/10.1109/MIS.2020.2988525
25. Aledhari, M., Razzak, R., Parizi, R.M., Saeed, F.: Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access **8**, 140699–140725 (2020). https://doi.org/10.1109/ACCESS.2020.3013541
26. Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A., Smith, V.: Federated optimization in heterogeneous networks. Proceedings of Machine learning and systems **2**, 429–450 (2020)
27. Zhang, X., Hong, M., Dhople, S., Yin, W., Liu, Y.: Fedpd: A federated learning framework with adaptivity to non-iid data. IEEE Trans. Signal Process. **69**, 6055–6070 (2021). https://doi.org/10.1109/TSP.2021.3115952
28. Karimireddy, S.P., Kale, S., Mohri, M., Reddi, S., Stich, S., Suresh, A.T.: Scaffold: Stochastic controlled averaging for federated learning. In: International Conference on Machine Learning, pp. 5132–5143. PMLR (2020).
29. Li, T., Sanjabi, M., Beirami, A., Smith, V.: Fair Resource Allocation in Federated Learning (2020)
30. Tensorflow: Tensorflow federated: Machine learning on decentralized data. Accessed on April, 2023 (2023). https://www.tensorflow.org/federated
31. Dwork, C.: Differential privacy. In: Automata. Languages and Programming, pp. 1–12. Springer, Berlin, Heidelberg (2006)
32. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., Seth, K.: Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1175–1191 (2017)
33. Fletcher, C.W., Dijk, M.v., Devadas, S.: A secure processor architecture for encrypted computation on untrusted programs. In: Proceedings of the Seventh ACM Workshop on Scalable Trusted Computing, 3–8 (2012). https://doi.org/10.1145/2382536.2382540
34. Kholod, I., Yanaki, E., Fomichev, D., Shalugin, E., Novikova, E., Filippov, E., Nordlund, M.: Open-source federated learning frameworks for iot: A comparative review and analysis. Sensors **21**(1), 167 (2021)
35. Openmined: Pysyft. Accessed on April, 2023 (2023). https://blog.openmined.org/tag/pysyft/
36. Flower: Flower. Accessed on April, 2023 (2023). https://flower.dev/
37. Fedml: Fedml. Accessed on April, 2023 (2023). https://www.fedml.ai/
38. PaddleFL: PaddleFL. Accessed on April, 2023 (2023). https://github.com/PaddlePaddle/PaddleFL
39. Fate: Fate. Accessed on April, 2023 (2023). https://fate.fedai.org
40. OpenFL: OpenFL. Accessed on April, 2023 (2023). https://www.openfl.org/
41. Caldas, S., Duddu, S.M.K., Wu, P., Li, T., Konecný, J., McMahan, H.B., Smith, V., Talwalkar, A.: Leaf: A benchmark for federated settings. In: Workshop on Federated Learning for Data Privacy and Confidentiality (2019)
42. He, C., Li, S., So, J., Zeng, X., Zhang, M., Wang, H., Wang, X., Vepakomma, P., Singh, A., Qiu, H., Zhu, X., Wang, J., Shen, L., Zhao, P., Kang, Y., Liu, Y., Raskar, R., Yang, Q., Annavaram, M., Avestimehr, S.: FedML: A Research Library and Benchmark for Federated Machine Learning (2020)
43. Zhu, X.J.: Semi-supervised learning literature survey. Technical report, University of Wisconsin-Madison Department of Computer Sciences (2005)
44. Lee, D.-H., et al.: Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks. In: Workshop on Challenges in Representation Learning, ICML, vol. 3, p. 896. Atlanta (2013).
45. Rasmus, A., Berglund, M., Honkala, M., Valpola, H., Raiko, T.: Semi-supervised learning with ladder networks. In: Advances in Neural Information Processing Systems, vol. 28 (2015). https://proceedings.neurips.cc/paper_files/paper/2015/file/378a063b8fdb1db941e34f4bde584c7d-Paper.pdf
46. Xie, Q., Dai, Z., Hovy, E., Luong, M.-T., Le, Q.V.: Unsupervised data augmentation for consistency training. In: Proceedings of the

34th International Conference on Neural Information Processing Systems. NIPS '20. Curran Associates Inc., Red Hook, NY, USA (2020)
47. Berthelot, D., Carlini, N., Goodfellow, I., Oliver, A., Papernot, N., Raffel, C.: MixMatch: a holistic approach to semi-supervised learning. Curran Associates Inc., Red Hook, NY, USA (2019)
48. Berthelot, D., Carlini, N., Cubuk, E.D., Kurakin, A., Sohn, K., Zhang, H., Raffel, C.: Remixmatch: Semi-supervised learning with distribution matching and augmentation anchoring. In: International Conference on Learning Representations (2020). https://openreview.net/forum?id=HklkeR4KPB
49. Sohn, K., Berthelot, D., Carlini, N., Zhang, Z., Zhang, H., Raffel, C.A., Cubuk, E.D., Kurakin, A., Li, C.-L.: Fixmatch: Simplifying semi-supervised learning with consistency and confidence. In: Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M.F., Lin, H. (eds.) Advances in Neural Information Processing Systems, vol. 33, pp. 596–608 (2020). https://proceedings.neurips.cc/paper_files/paper/2020/file/06964dce9addb1c5cb5d6e3d9838f733-Paper.pdf
50. Pise, N.N., Kulkarni, P.: A survey of semi-supervised learning methods. In: 2008 International Conference on Computational Intelligence and Security **2**, 30–34. IEEE (2008). https://doi.org/10.1109/CIS.2008.204.
51. Van Engelen, J.E., Hoos, H.H.: A survey on semi-supervised learning. Mach. Learn. **109**(2), 373–440 (2020)
52. Sajjadi, M., Javanmardi, M., Tasdizen, T.: Regularization with stochastic transformations and perturbations for deep semi-supervised learning. In: Advances in Neural Information Processing Systems, vol. 29 (2016). https://proceedings.neurips.cc/paper_files/paper/2016/file/30ef30b64204a3088a26bc2e6ecf7602-Paper.pdf
53. Laine, S., Aila, T.: Temporal ensembling for semi-supervised learning. In: International Conference on Learning Representations (2017)
54. Tarvainen, A., Valpola, H.: Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results. In: Guyon, I., Luxburg, U.V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., Garnett, R. (eds.) Advances in Neural Information Processing Systems, vol. 30 (2017). https://proceedings.neurips.cc/paper_files/paper/2017/file/68053af2923e00204c3ca7c6a3150cf7-Paper.pdf
55. Miyato, T., Maeda, S.-I., Koyama, M., Ishii, S.: Virtual adversarial training: A regularization method for supervised and semi-supervised learning. IEEE Trans. Pattern Anal. Mach. Intell. **41**(8), 1979–1993 (2019)
56. Triguero, I., García, S., Herrera, F.: Self-labeled techniques for semi-supervised learning: taxonomy, software and empirical study. Knowl. Inf. Syst. **42**(8), 245–284 (2015)
57. Yarowsky, D.: Unsupervised word sense disambiguation rivaling supervised methods. In: In 33rd Annual Meeting of the Association for Computational Linguistics, 189–196 (1995). https://aclanthology.org/P95-1026.pdf
58. Rosenberg, C., Hebert, M., Schneiderman, H.: Semi-supervised self-training of object detection models. In: Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05) - Volume 1 - Volume 01. WACV-MOTION '05, pp. 29–36. IEEE Computer Society, USA (2005). DOI: 10.1109/ACVMOT.2005.107
59. Dópido, I., Li, J., Marpu, P.R., Plaza, A., Bioucas Dias, J.M., Benediktsson, J.A.: Semisupervised self-learning for hyperspectral image classification. IEEE Transactions on Geoscience and Remote Sensing **51**(7), 4032–4044 (2013). https://doi.org/10.1109/tgrs.2012.2228275
60. Xie, Q., Luong, M.-T., Hovy, E., Le, Q.V.: Self-training with noisy student improves imagenet classification. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020)
61. Presotto, R., Civitarese, G., Bettini, C.: Federated clustering and semi-supervised learning: A new partnership for personalized human activity recognition. Pervasive Mob. Comput. **88**, 101726 (2023). https://doi.org/10.1016/j.pmcj.2022.101726
62. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Activity recognition using cell phone accelerometers. ACM SIGKDD Explorations Newsletter **12**(2), 74–82 (2011)
63. Vavoulas, G., Chatzaki, C., Malliotakis, T., Pediaditis, M., Tsiknakis, M.: The mobiact dataset: Recognition of activities of daily living using smartphones. In: Proceedings of the International Conference on Information and Communication Technologies for Ageing Well and e-Health - Volume 1: ICT4AWE, (ICT4AGEINGWELL 2016), 143–151 (2016). https://doi.org/10.5220/0005792401430151
64. Presotto, R., Civitarese, G., Bettini, C.: Semi-supervised and personalized federated activity recognition based on active learning and label propagation. Pers. Ubiquit. Comput. **26**(5), 1281–1298 (2022). https://doi.org/10.1007/s00779-022-01688-8
65. Albaseer, A., Abdallah, M., Al-Fuqaha, A., Erbad, A., Dobre, O.A.: Semi-supervised federated learning over heterogeneous wireless iot edge networks: Framework and algorithms. IEEE Internet Things J. **9**(24), 25626–25642 (2022). https://doi.org/10.1109/JIOT.2022.3194833
66. Tashakori, A., Zhang, W., Jane Wang, Z., Servati, P.: Semipfl: Personalized semi-supervised federated learning framework for edge intelligence. IEEE Internet Things J. **10**(10), 9161–9176 (2023). https://doi.org/10.1109/JIOT.2022.3233599
67. Gao, L., Konomi, S.: Personalized federated human activity recognition through semi-supervised learning and enhanced representation. In: Adjunct Proceedings of the 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing & the 2023 ACM International Symposium on Wearable Computing, 463–468 (2023). https://doi.org/10.1145/3594739.3610739
68. Bukit, T.A., Pillado, E.P.B., Yahya, B.N., Lee, S.-L.: Activity transitions for semi-supervised federated learning in sensor-based human activity recognition. Applied Soft Computing **184**, 113793 (2025). https://doi.org/10.1016/j.asoc.2025.113793
69. Abdel-Basset, M., Moustafa, N., Hawash, H.: Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach. IEEE Transactions on Industrial Informatics **19**(1), 995–1005 (2023). https://doi.org/10.1109/TII.2022.3165869
70. Aouedi, O., Piamrat, K., Muller, G., Singh, K.: Intrusion detection for softwarized networks with semi-supervised federated learning. In: ICC 2022 - IEEE International Conference on Communications, 5244–5249 (2022). https://doi.org/10.1109/ICC45855.2022.9839042
71. Aouedi, O., Piamrat, K., Muller, G., Singh, K.: Federated semisupervised learning for attack detection in industrial internet of things. IEEE Trans. Industr. Inf. **19**(1), 286–295 (2023). https://doi.org/10.1109/TII.2022.3156642
72. Naeem, F., Ali, M., Kaddoum, G.: Federated-learning-empowered semi-supervised active learning framework for intrusion detection in zsm. IEEE Commun. Mag. **61**(2), 88–94 (2023). https://doi.org/10.1109/MCOM.001.2200533
73. Li, X., Gong, Y., Liang, Y., Wang, L.-E.: Personalized federated learning with semisupervised distillation. Security and Communication Networks **2021**(1), 3259108 (2021). https://doi.org/10.1155/2021/3259108
74. Che, L., Long, Z., Wang, J., Wang, Y., Xiao, H., Ma, F.: Fedtrinet: A pseudo labeling method with three players for federated semi-supervised learning. In: 2021 IEEE International Conference on Big Data (Big Data), pp. 715–724 (2021). https://doi.org/10.1109/BigData52589.2021.9671374

75. Kang, Y., Liu, Y., Liang, X.: Fedcvt: Semi-supervised vertical federated learning with cross-view training. ACM Trans. Intell. Syst. Technol. (2022). https://doi.org/10.1145/3510031
76. Zhang, Z., Ma, S., Yang, Z., Xiong, Z., Kang, J., Wu, Y., Zhang, K., Niyato, D.: Robust semisupervised federated learning for images automatic recognition in internet of drones. IEEE Internet of Things Journal **10**(7), 5733–5746 (2023). https://doi.org/10.1109/JIOT.2022.3151945
77. Kádár, A., Hadházi, D.: Fedlinked: A client-wise distilled representation based semi-supervised collaborative multitask learning scheme. In: 2022 International Joint Conference on Neural Networks (IJCNN), 1–8 (2022). https://doi.org/10.1109/IJCNN55064.2022.9892034
78. Shi, Y., Chen, S., Zhang, H.: Uncertainty minimization for personalized federated semi-supervised learning. IEEE Transactions on Network Science and Engineering **10**(2), 1060–1073 (2023). https://doi.org/10.1109/TNSE.2022.3226574
79. Yang, N., Yuan, D., Zhang, Y., Deng, Y., Bao, W.: Asynchronous semi-supervised federated learning with provable convergence in edge computing. IEEE Network **36**(5), 136–143 (2022). https://doi.org/10.1109/MNET.001.2200223
80. Li, Z., Shao, J., Mao, Y., Wang, J.H., Zhang, J.: Federated learning with gan-based data synthesis for non-iid clients. In: Trustworthy Federated Learning, pp. 17–32. Springer, Cham (2023)
81. Zhong, Z., Wang, J., Bao, W., Zhou, J., Zhu, X., Zhang, X.: Semi-hfl: semi-supervised federated learning for heterogeneous devices. Complex & Intelligent Systems **9**(2), 1995–2017 (2023)
82. Scott, J., Yeo, M., Lampert, C.H.: Cross-client label propagation for transductive and semi-supervised federated learning. Transactions on Machine Learning Research (2023)
83. Qian, D., Cui, Y., Fu, Y., Liu, F., Wei, T.: Fedentropy: Information-entropy-aided training optimization of semi-supervised federated learning. J. Syst. Architect. **137**, 102851 (2023). https://doi.org/10.1016/j.sysarc.2023.102851
84. Wei, X.-X., Huang, H.: Balanced federated semisupervised learning with fairness-aware pseudo-labeling. IEEE Transactions on Neural Networks and Learning Systems **35**(7), 9395–9407 (2023). https://doi.org/10.1109/TNNLS.2022.3233093
85. Lee, S., Le, T.-L.V., Shin, J., Lee, S.-J.: (fl) 2: Overcoming few labels in federated semi-supervised learning. In Advances in Neural Information Processing Systems **37**, 43693–43714 (2024)
86. Wang, J., Pei, X., Wang, R., Zhang, F., Chen, T.: Federated semi-supervised learning with tolerant guidance and powerful classifier in edge scenarios. Inf. Sci. **662**, 120201 (2024). https://doi.org/10.1016/j.ins.2024.120201
87. Zhu, S., Ma, X., Sun, G.: Two-stage sampling with predicted distribution changes in federated semi-supervised learning. Knowl.-Based Syst. **295**, 111822 (2024). https://doi.org/10.1016/j.knosys.2024.111822
88. Yang, Q., Chen, Z., Peng, Z., Yuan, Y.: Relation-guided versatile regularization for federated semi-supervised learning. International Journal of Computer Vision (2025). https://doi.org/10.1007/s11263-024-02330-1
89. Zhu, S., Wang, Y., Sun, G.: Federated semi-supervised learning based on truncated gaussian aggregation. J. Supercomput **81**(1), 1–22 (2025)
90. Zhao, Q., Chu, J., Li, Z., Huang, W., Luo, Z., Li, T.: Fedlgmatch: Federated semi-supervised learning via joint local and global pseudo labeling. Knowl.-Based Syst. **320**, 113642 (2025). https://doi.org/10.1016/j.knosys.2025.113642
91. Wang, Z., Liu, Y., Liang, G., Zhong, C., Yang, F.: Dynamic class-balanced threshold federated semi-supervised learning by exploring diffusion model and all unlabeled data. Futur. Gener. Comput. Syst. **170**, 107820 (2025). https://doi.org/10.1016/j.future.2025.107820
92. Aouedi, O., Piamrat, K., Muller, G., Singh, K.: Fluids: Federated learning with semi-supervised approach for intrusion detection system. In: 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), 523–524 (2022). https://doi.org/10.1109/CCNC49033.2022.9700632
93. Liang, X., Lin, Y., Fu, H., Zhu, L., Li, X.: Rscfed: Random sampling consensus federated semi-supervised learning. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 10154–10163 (2022)
94. Wu, Z., Wu, X., Long, Y.: Prediction based semi-supervised online personalized federated learning for indoor localization. IEEE Sens. J. **22**(11), 10640–10654 (2022). https://doi.org/10.1109/JSEN.2022.3165042
95. Thakur, A., Sharma, P., Clifton, D.A.: Dynamic neural graphs based federated reptile for semi-supervised multi-tasking in healthcare applications. IEEE J. Biomed. Health Inform **26**(4), 1761–1772 (2022). https://doi.org/10.1109/JBHI.2021.3134835
96. Wen, T., Zhao, S., Zhang, R.: Federated semi-supervised learning through a combination of self and cross model ensembling. In: 2022 International Joint Conference on Neural Networks (IJCNN), pp. 1–8 (2022). https://doi.org/10.1109/IJCNN55064.2022.9892834
97. Ma, Y., Wang, J., Yang, J., Wang, L.: Model-heterogeneous semi-supervised federated learning for medical image segmentation. IEEE Trans. Med. Imaging **43**(5), 1804–1815 (2024). https://doi.org/10.1109/TMI.2023.3348982
98. Li, B., Gao, W., Xie, J., Li, H., Gong, M.: A unified framework for federated semi-supervised learning in heterogeneous iot healthcare systems. IEEE Internet of Things Journal **11**(24), 41110–41123 (2024). https://doi.org/10.1109/jiot.2024.3457230
99. Li, W., Pan, X., Zhang, Z., Wu, G., Ye, G., Wee, L., Dekker, A., Han, C., Shi, L., Liu, Z., Liu, Z., Shi, Z.: Data-efficient federated semi-supervised learning framework via pseudo supervision refinement strategy for lung tumor segmentation. Biomed. Signal Process. Control **107**, 107793 (2025). https://doi.org/10.1016/j.bspc.2025.107793
100. Jin, Z., Liang, Z., He, M., Peng, Y., Xue, H., Wang, Y.: A federated semi-supervised learning approach for network traffic classification. International Journal of Network Management **33**(3), 2222 (2023)
101. Wang, Z., Li, Z., Fu, M., Ye, Y., Wang, P.: Network traffic classification based on federated semi-supervised learning. Journal of Systems Architecture **149**, 103091 (2024). https://doi.org/10.1016/j.sysarc.2024.103091
102. Zhao, C., Gao, Z., Bao, S., Xiao, K.: Toward industrial densely packed object detection: A federated semi-supervised learning approach. IEEE Internet Things J. **11**(22), 37340–37350 (2024). https://doi.org/10.1109/JIOT.2024.3443112
103. Feng, T., Narayanan, S.: Semi-fedser: Semi-supervised learning for speech emotion recognition on federated learning using multiview pseudo-labeling. In: Interspeech 2022, 5050–5054 (2022). https://doi.org/10.21437/interspeech.2022-141
104. Tsouvalas, V., Ozcelebi, T., Meratnia, N.: Privacy-preserving speech emotion recognition through semi-supervised federated learning. In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops), 359–364 (2022). https://doi.org/10.1109/PerComWorkshops53856.2022.9767445
105. Feng, S., Li, B., Yu, H., Liu, Y., Yang, Q.: Semi-supervised federated heterogeneous transfer learning. Knowl.-Based Syst. **252**, 109384 (2022). https://doi.org/10.1016/j.knosys.2022.109384
106. Ahmed, U., Lin, J.-W., Srivastava, G.: Temporal positional lexicon expansion for federated learning based on hyperpatism detection. Expert Systems **40**(5), 13183 (2023). https://doi.org/10.1111/exsy.13183

107. Zhang, C., Zhu, Y., Markos, C., Yu, S., Yu, J.J.Q.: Toward crowdsourced transportation mode identification: A semisupervised federated learning approach. IEEE Internet Things J. **9**(14), 11868–11882 (2022). https://doi.org/10.1109/JIOT.2021.3132056
108. Zhu, Y., Liu, Y., Yu, J.J.Q., Yuan, X.: Semi-supervised federated learning for travel mode identification from gps trajectories. IEEE Transactions on Intelligent Transportation Systems **23**(3), 2380–2391 (2022). https://doi.org/10.1109/TITS.2021.3092015
109. Tsouvalas, V., Saeed, A., Ozcelebi, T.: Federated self-training for semi-supervised audio recognition. ACM Trans. Embed. Comput. Syst. (2022). https://doi.org/10.1145/3520128
110. Kassem, H., Alapatt, D., Mascagni, P., Karargyris, A., Padoy, N.: Federated cycling (fedcy): Semi-supervised federated learning of surgical phases. IEEE Trans. Med. Imaging **42**(7), 1920–1931 (2023). https://doi.org/10.1109/TMI.2022.3222126
111. Qiu, L., Cheng, J., Gao, H., Xiong, W., Ren, H.: Federated semi-supervised learning for medical image segmentation via pseudo-label denoising. IEEE J. Biomed. Health Inform. **27**(10), 4672–4683 (2023). https://doi.org/10.1109/JBHI.2023.3274498
112. Ying, Z., Zhang, G., Pan, Z., Chu, C., Liu, X.: Fedecg: A federated semi-supervised learning framework for electrocardiogram abnormalities prediction. Journal of King Saud University-Computer and Information Sciences **35**(6), 101568 (2023)
113. Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., Zhang, W.: A survey on federated learning: challenges and applications. International Journal of Machine Learning and Cybernetics **14**(2), 513–535 (2023). https://doi.org/10.1007/s13042-022-01647-y
114. Paragliola, G., Coronato, A.: Definition of a novel federated learning approach to reduce communication costs. Expert Systems with Applications **189**, 116109 (2022). https://doi.org/10.1016/j.eswa.2021.116109
115. WANG, L., WANG, W., LI, B.: Cmfl: Mitigating communication overhead for federated learning. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 954–964 (2019). https://doi.org/10.1109/ICDCS.2019.00099
116. Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., Kong, J., Jue, J.P.: All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture **98**, 289–330 (2019). https://doi.org/10.1016/j.sysarc.2019.02.009
117. Lima Pilla, L.: Optimal task assignment for heterogeneous federated learning devices. In: 2021 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 661–670 (2021). https://doi.org/10.1109/IPDPS49936.2021.00074
118. Phong, L.T., Aono, Y., Hayashi, T., Wang, L., Moriai, S.: Privacy-preserving deep learning via additively homomorphic encryption. IEEE Transactions on Information Forensics and Security **13**(5), 1333–1345 (2018). https://doi.org/10.1109/TIFS.2017.2787987
119. Zhu, H., Xu, J., Liu, S., Jin, Y.: Federated learning on non-iid data: A survey. Neurocomputing **465**, 371–390 (2021). https://doi.org/10.1016/j.neucom.2021.07.098
120. Paramythis, A., Loidl-Reisinger, S.: Adaptive learning environments and e-learning standards. In: In Second European Conference on E-learning, vol. 1, pp. 369–379. ECEL (2003).
121. Torrey, L., Shavlik, J.: Transfer learning. In: Handbook of Research on Machine Learning Applications and Trends: Algorithms, Methods, and Techniques, pp. 242–264. (2010)
122. Ma, X., Zhu, J., Lin, Z., Chen, S., Qin, Y.: A state-of-the-art survey on solving non-iid data in federated learning. Futur. Gener. Comput. Syst. **135**, 244–258 (2022)
123. Khan, L.U., Saad, W., Han, Z., Hossain, E., Hong, C.S.: Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Communications Surveys & Tutorials **23**(3), 1759–1799 (2021). https://doi.org/10.1109/COMST.2021.3090430
124. Abad, M.S.H., Ozfatura, E., GUndUz, D., Ercetin, O.: Hierarchical federated learning across heterogeneous cellular networks. In: ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 8866–8870 (2020). https://doi.org/10.1109/ICASSP40776.2020.9054634
125. Zhang, H., Xie, Z., Zarei, R., Wu, T., Chen, K.: Adaptive client selection in resource constrained federated learning systems: A deep reinforcement learning approach. IEEE Access **9**, 98423–98432 (2021). https://doi.org/10.1109/ACCESS.2021.3095915
126. Kim, S., Shin, W., Jang, S., Song, H., Yun, S.-Y.: Fedrn: Exploiting k-reliable neighbors towards robust federated learning. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management, 972–981 (2022). https://doi.org/10.1145/3511808.3557322
127. Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., Piccialli, F.: Model aggregation techniques in federated learning: A comprehensive survey. Futur. Gener. Comput. Syst. **150**, 272–293 (2024)
128. Rizve, M.N., Duarte, K., Rawat, Y.S., Shah, M.: In Defense of Pseudo-Labeling: An Uncertainty-Aware Pseudo-label Selection Framework for Semi-Supervised Learning (2021)
129. Northcutt, C., Jiang, L., Chuang, I.: Confident learning: Estimating uncertainty in dataset labels. Journal of Artificial Intelligence Research **70**, 1373–1411 (2021)
130. Deng, Y., Lyu, F., Ren, J., Chen, Y.-C., Yang, P., Zhou, Y., Zhang, Y.: Improving federated learning with quality-aware user incentive and auto-weighted model aggregation. IEEE Trans. Parallel Distrib. Syst. **33**(12), 4515–4529 (2022). https://doi.org/10.1109/TPDS.2022.3195207
131. Huang, W., Wang, D., Ouyang, X., Wan, J., Liu, J., Li, T.: Multimodal federated learning: Concept, methods, applications and future directions. Information Fusion **112**, 102576 (2024). https://doi.org/10.1016/j.inffus.2024.102576
132. Zolfaghari, M., Zhu, Y., Gehler, P., Brox, T.: Crossclr: Cross-modal contrastive learning for multi-modal video representations. In: Proceedings of the IEEE/CVF International Conference on Computer Vision, 1450–1459 (2021)
133. Abbas, Q., Malik, K.M., Saudagar, A.K.J., Khan, M.B.: Context-aggregator: An approach of loss- and class imbalance-aware aggregation in federated learning. Comput. Biol. Med. **163**, 107167 (2023). https://doi.org/10.1016/j.compbiomed.2023.107167

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.