Model-Centric Federated Machine Learning

AUTHORS, Institute xx, Country

Traditional Federated Machine Learning follows a server-domincated cooperation paradigm which narrows the application scenarios of federated learning and decreases the enthusiasm of data holders to participate.

CCS Concepts: • **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: datasets, neural networks, gaze detection, text tagging

ACM Reference Format:
Authors. 2018. Model-Centric Federated Machine Learning. *Proc. ACM Meas. Anal. Comput. Syst.* 37, 4, Article 111 (August 2018), 21 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

In recent years, the barriers to the development of Artificial Intelligence (AI) have been broken down with the rapid progress of ABC technologies in computing: AI, Big Data, and Cloud Computing, as well as the emergence of cost-effective specialized hardware [121] and software [54]. This has led to the world entering the third wave of AI development: Deep Learning [63]. The success of current data-driven AI relies on massive amounts of training data and follows a gather-and-analyze paradigm [134], which confronts with challenges of complying with rigorous data protection regulations such as OECD Privacy Guidelines [125] and General and Data Protection Regulation (GDPR) [128]. So although data-centric AI is now the mainstream, a novel model-centric distributed collaborative training framework called Federated Learning is gaining popularity in both academia and industry due to its advantages in complying with privacy regulations. So although data-centric AI is currently mainstream, Federated Learning (FL) [74], a novel model-centric distributed collaborative training framework, is gaining popularity in both academia and industry for its advantages in complying with privacy regulations [126].

According to the definitions of IEEE Standard for Federated Machine Learning (FML, aka FL) [119], *FL is a framework or system that enables multiple participants to collaboratively build and use machine learning models without disclosing the raw and private data owned by the participants while achieving good performance.* For example, a typical workflow of FL systems is that the entity with modeling demand (aka FL server) first deploys the FL services and initializes the model training task, and then distributing this task to participants with training data (aka FL clients) for modeling [12]. Based on this workflow pattern, many FL frameworks have been derived with specialized improvements in communication [60, 91, 136], optimizaiton [59, 71, 75], robustness [30, 67, 114] and privacy [13, 24, 38]. While these fascinating improvements greatly enhance the utility of FL, they all follow a task-based interaction paradigm, in which an FL server dominates the cooperation between FL participants. In this narrow interpretation of FL, the data owner is treated more like a worker than a collaborator and performs training primarily for the benefit of the server's goals. Due to the above defects, clients have little enthusiasm to participate, and the potential for redundant training also leads to low model reusability, further diminishing

Author's address: Authors, Institute xx, City, Country, @mail.com.

2476-1249/2018/8-ART111 $15.00
https://doi.org/XXXXXXX.XXXXXXX

the efficiency of the FL systems. This explains why current FL frameworks are more akin to private distributed modeling services rather than sustainable and privacy-preserving modeling platforms for everyone as expected.

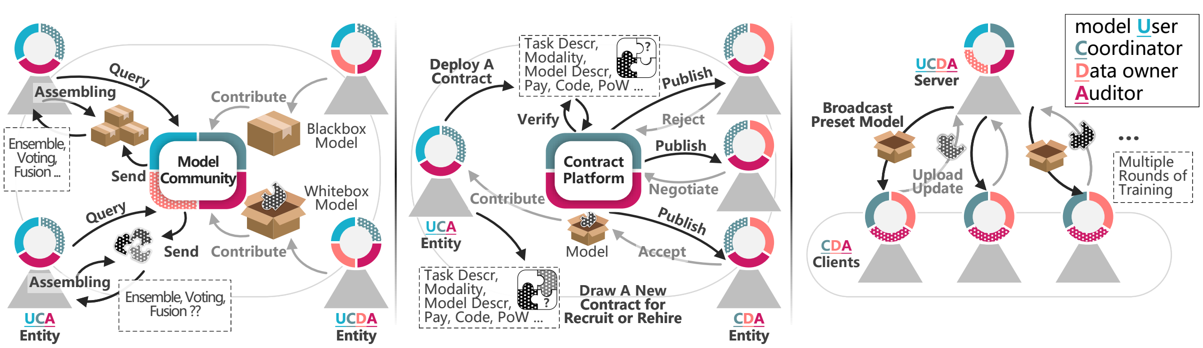
In this paper, we try to answer the question: **Can we establish a sustainable open FL platform based on a novel reciprocal cooperation framework?** Obviously, to answer this quesion, it is insufficient simply study the basic concepts of FL and investigate existing FL techniques. We also need to conduct a wide survey of potential techniques that can facilitate the construction of open FL platforms. To aid understanding, Fig. 1 provides a first glimpse of two novel FL cooperation frameworks we advocated:

- **Query-based FL.** It follows a loosely-coupled cooperation framework between entities (we use "entities" instead of "participants" to emphasizes equality), where any entity can freely upload their local models or retrieve models from the open repository named Model Community. There are many valuable challenges that can be explored, such as how to query for models, how to "assemble" the retrieved models, or how to transfer knowledge from these models (see Section 3).
- **Contract-based FL.** It follows a mutual choice cooperation framework, where each entity can deploy model training contracts with specialized requirements such as task modality, execution environment, model architecture and license. Meanwhile, entities holding data can choose whether to accept the contract. Research topics in this area include model pricing, model ownership verification and .... (see Section **??**)

It's worth noting that the definitions of the four roles (i.e., model user, coordinator, data owner, auditor) are adopted for compatibility with the IEEE standard [119], and our proposals are also within the scope of FML definitions. The diagram in Fig. 1(c) illustrates the workflow of traditional FL, where all FL clients are required to accept the training schedule from the FL server and perform multiple rounds of local training until the model converges. In contrast, the entities in query-based FL and contract-based are proactive in their participate. We believe that these reciprocal cooperation frameworks have the potential to expand the prevalence of FL and establish FL ecosystems.

1.1 Related Surveys

Federated learning has become a buzzword in various fields, leading to the emergence of numerous FL studies. These works can be classified into three primary categories: FL systems design, FL appllications and FL toolkits. Extensive surveys are available to summarized the advancement of federated learning, as shown in Table 1. The initial architectures and concepts for FL systems were summaried by Yang *et al.* [139]. They categorized



(a) Query-based FML (b) Contract-based FML (c) Traditional FML

Fig. 1. A schematic diagram of three cooperation frameworks of FL. (a) (b) are the proposed open FL platforms, (c) is the traditional FL platform. Four colors correspond to four roles in [119], and colors with grid lines indicate non-essential roles.

FL into horizontal FL, vertical FL and federated transfer learning based on the distribution characteristics of data, which are written in IEEE Standard 3652.1-2020 [119, 138]. Following this, an increasing number of surveys have emerged focusing on enhancing FL system design [7, 58, 72, 74, 146]. From the algorithmic perspective, personlized FL [62, 122] aims to learn personlized models for each client to address the challenge of statistical heterogeneity [88]. Besides, the privacy-perserving computing platforms and model aggregation protocols for FL systems also been widely studied and sumaried by [33, 84, 87, 141]. Furthermore, many advanced FL architectures had been proposed, such as asynchronous [136], decentralized and blockchain-based FL frameworks [93, 102, 154]. Given that federated learning technologies enable collaboration among distributed participants in model training and decision-making, this capability holds great promise in a wide range of application scenarios. For instance, multiple geogrphically distributed medical insitutions can enhace medication recommendation, drug-drug interaction prediction and medical image analysis in a collaborative manner without exchanging any sensitive data [8, 101, 109, 137]. The massive real-time data generated by IoT devices in smart cities [106, 150], industries [14], vehicles [29] has also sparked interest in exploring how FL technology can be used to deliver more advanced services such as intrusion detection, anomaly detection, fraud detection and network load prediction [5, 6, 39].

As summarized in Table 1, most surveys extensively discuss the challenges of efficiency, heterogeneity, privacy in FL systems design, with the surveys from blockchain fileds offering the most comprehensive review. However, except for a few blockchain-based FL studies, most of the above surveys just present the same story from slightly different angles or backgrounds, i.e a server sets the model training task and delegate it to data holders to complete. This *server-dominated* cooperation framework is a narrow implementation of the FL systems. Therefore, this survey aim to fill the gap by investigating and surveying the associated tenchnologies that support more open and inclusive cooperation frameworks in FL systems, where all entities, whether they own the data or not, can benefit from it. The challenges investigated in this survey are not listed in the Table 1, to the best of our knowledge, this is the first survey that focuses on the **cooperation frameworks** of FL. In the following section, we will differentiate this survey from other related concepts in the field of FL.

1.2 Distinction of Our Survey

This survey focuses on exploring the innovative cooperation frameworks in FL, which will involve some FL concepts such as decentralized FL, blockchain-based FL, few-shot FL, ML related platforms and services but goes beyond them. In this section, we will distinguish our survey by highlingting the similarities and differences between these related concepts.

1.2.1 FL Systems. Federated learning, with its nature advantages in privacy-preserving decision sharing, has garnered significant attention in both industry and academia, leading to the rapid development of federated learning systems. The earliest attempt at the large-scale FL system was by Google, where FL was used to improve next-word prediction [46] and query suggesion [140] for Gboard applications. Subsequently, many novel FL systems have emerged to adapt to diverse federated training scenarios, such as Horizontal FL (e.g. TFF [1], FedLab [145], Felicitas [148], IBM FL [86]), Vertical FL [135] or both (e.g. FATE [82], FedML [47], PaddleFL [89], Flower [11], FedTree [69], NVFLARE [112]). Despite these frameworks covering a wide range of application scenarios, they all follow the server-dominated cooperation mechanism. This business model restricts FL to function as a collaborative modeling software, rather than an open platform that provides FL services to the public.

Unlike the FL systems mentioned above, PySyft [156] developed by OpenMined depicts a novel FL cooperation frameworks which is closely realted to our focus. PySyft encourages data owners to share their data on a private domain server, which provides data management and privacy controls, as well as limited machine learning analysis APIs for third-party data scientists. Besides, a public network server will provide connections between data owners and data scientist, enabling datasets search and discovery for platform users. Recently, a new FL

Table 1. Summary of existing FL surveys, SYS denotes FL Systems Design, APP denotes FL Applications, SDC denotes Server-Dominated Cooperation frameworks.

		Challenges					Contents		
Scenarios/Tasks	FL Surveys	Efficiency	Heterogeneity	Privacy	Incentive	Decentralized	SYS	APP	SDC
General	Yang *et al.* [139]	✓	✓	✓	✓	✓	✓	✓	✓
	Li *et al.* 2020 [74]	✓	✓	✓		✓	✓	✓	✓
	Zhang 2021*et al.* [146]	✓	✓	✓			✓	✓	✓
	Gupta *et al.* [43]	✓	✓	✓		✓	✓	✓	✓
	Xu *et al.* [136]	✓	✓	✓		✓	✓	✓	✓
	Li *et al.* 2021 [72]	✓	✓	✓	✓	✓	✓	✓	✓
	El *et al.* [33]			✓		✓	✓		✓
	Kulkarni *et al.* [62]	✓	✓				✓		✓
	Liu *et al.*[84]	✓		✓		✓	✓		✓
	Tan *et al.* [122]		✓				✓		✓
	Zhu *et al.* 2021 [153]		✓				✓		✓
	Ma *et al.* [88]	✓	✓	✓			✓		✓
	Aledhari *et al.* [7]	✓	✓				✓	✓	✓
	Kairouz *et al.* [58]	✓	✓	✓	✓	✓	✓	✓	✓
	AbdulRahman *et al.* [3]	✓	✓	✓	✓		✓	✓	✓
	Lim *et al.* [80]	✓	✓	✓	✓		✓	✓	✓
Healthcare	Xu *et al.* [137]	✓	✓	✓			✓	✓	✓
	Pfitzner *et al.*[101]	✓	✓	✓			✓	✓	✓
	Antunes *et al.* [8]		✓	✓				✓	✓
	Rieke *et al.* [109]		✓	✓		✓	✓	✓	✓
IoT	Zhang 2022*et al.* [150]	✓	✓				✓	✓	✓
	Boopalan *et al.* [14]	✓	✓	✓	✓	✓	✓	✓	✓
	Ramu *et al.* [106]	✓	✓	✓		✓	✓	✓	✓
	Du *et al.* [29]	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity	Agrawal *et al.* [5]	✓	✓	✓		✓	✓	✓	✓
	Alazab *et al.* [6]			✓			✓	✓	✓
	Ghimire *et al.* [39]	✓		✓			✓	✓	✓
Blockchain	Nguyen *et al.* [93]	✓	✓	✓	✓	✓	✓	✓	✓
	Qu *et al.* [102]	✓	✓	✓	✓	✓	✓	✓	✓
	Zhu *et al.* 2022 [154]	✓	✓	✓	✓	✓	✓	✓	✓

platform named PySyTFF[1] was announced. It integrates TFF and PySyft, allowing data scientists to train models under the coordination of TFF and the datasets provided by PySyft domain servers. However, even with inference controls of datasets, there is still a high security risk associated with exposing access to sensitive data on the Internet [35]. To preserve the privacy advantages of FL, in this survey, we aim to discuss an open and data-free FL platform under the scope of model-centric ML [85]. In such FL platform, every user is free to collaborate on the training of machine learning models while privacy is protected.

1.2.2 As-a-Service Business Model. In the current context of Software-as-a-Service (SaaS) [16], there are several as-a-service cloud computing frameworks that encapsulate ML tasks as services and provides unified APIs for upper layer applications. For example, Model-as-a-Service (MaaS) [36, 81, 110, 120, 157] and Machine-Learning-as-a-Service (MLaaS) [45, 48, 61, 68, 108] encapsulate model execution and model development as services. The original concept of MaaS [36, 110] was to provide re-usable and fine-grained user interfaces and visualization tools of domain-specific models (e.g wealther model, oil spill detection model) for environmental decision support

[1] https://blog.openmined.org/announcing-proof-of-concept-support-for-tff-in-pysyft-0-7/

systems. Subsequently, this concept has been extended to the field of recommendation systems [157] and deep learning based systems [81, 120]. However, in contrast to the focus of this survey, the aforementioned MaaS framework does not involve any user collaboration but solely provides model inference APIs to users.

As the architectures of deep neural networks (DNNs) become increasingly complex, training and maintaining DNNs become more and more challenging [44]. To address this issue, cloud service providers have introduced MLaaS, which offers an integrated development environment as a service for constructing and operationalizing ML workflows, aiming to reduce the computational resources required. MLaaS enables users to upload their data for training [48, 108, 151] or inference [45], freeing them from the responsibility of managing hardware resources and implementation. Most MLaaS providers adopt a pay-by-query business model, such as Google Vertex AI[2], Microsoft Azure Machine Learning[3] and ChatGPT[4]. However, privacy protection can be compromised when users upload data to perform inference and training in the cloud. Moverover, under this model, users are not given the ability to contribute their own models to the repository or collaborate with others to enhance the diversity of available models. While there are some ongoing efforts to offer privacy-preserving MLaaS services using techniques such as Isolated Execution Environment [45, 90] and Homomorphic Encryption [37, 48], it is worth noting that our focus is not solely on privacy. Rather, the FL framework we focus on emphasizes a collaborative framework where all entities involved have equal access to services and mutual benefits.

Recently, Kourtellis *et al.* [61] propose Federated Learning as a Service (FLaaS) that provides high-level and extensible APIs aim to enabling third-party applications to build collaborative, decentralized, privacy-preserving ML models. Jiang *te al.* [55] propose an open FL ecosystem for mobile devices, which shares a similar concept to FLaaS. However, those approach also follow the traditional server-dominated cooperation framework, which falls under the scope of previous FL surveys[58, 74, 139].

1.2.3 Dcentralized FL. ref: given the high scalability of modern edge computing networks, a single MEC server cannot manage to aggregate all updates offloaded from millions of devices. Therefore, there is an urgent need to develop a more decentralized FL approach without using a central server so as to solve security and scalability issues for enabling the next generation intelligent edge networks.

1.2.4 Blockchain-based FL.

1.2.5 Few-shot FL.

1.3 FAIR in FL

FAIR Data Principles: Findable, Accessible, Interoperable, Reusable.

2 BASIC CONCEPTS OF FEDERATED LEARNING

2.1 Definition

Federated Learning [91, 119] is a collaborative machine learning modeling paradigm that enables sharing and aggregation of knowledge from multiple sources while maintaining the confidentiality of source data. Generally, in terms of task organization, there are two kinds of entities in FL systems: the server and participant. The FL server can launche a federated training task and invites participants with sufficient training data and hardware resources to contribute their local modeling results for multi-source knowledge aggregation. In practice, FL systems can be divided into two categories based on application scenarios [58]:

- Cross-device FL. In this setting, the participants are numberous end devices with relatively small dataset size, such as mobiles, IoT sensors and wearable devices, the server is hosted in the cloud. Since there is low context correlation between the data of distributed end devices and less overlapping sample ids, this

[2] https://cloud.google.com/vertex-ai [3] https://azure.microsoft.com/products/machine-learning/ [4] https://chat.openai.com/chat

setting typically falls within the scope of horizontal FL. The cross-device FL applications include: Gboard input suggestion [46, 105, 140], e-commerce recommendation [95].

- Cross-silo FL. In this setting, the participants are orginizations or institutions with large amounts of well-maintained structured data, and the server is hosted by a trusted FL service providers such as FATE [82] and NVFLARE [112]. As participants can be different departments within an organization, the data silo owned by these departments can have a large overlap in sample space and less overlap in feature space, which falls within vertical FL. The applications of cross-silo FL include federated data analysis for radiomics [76, 77, 116], epidemiology [27] and EHR [17, 50].

The allocation to the server and participants in FL is dependent on the particular application context. Furthermore, FL entities can also serve multiple functional roles to support advanced features such as privacy enhancement [13, 38, 95], participant scheduling [2, 67], model verification [117, 124] and incentive mechanisms [143]. Recall that there are four roles defined in the FL standard [119]:

- Model User. The FL model users can request for FL modeling services and preset the targeted task, and then establish cooperation with participants who provide training data. This role can leverage the benefits of collaborative training to improve the preformance of its objective models.
- Coordinator. The FL coordinators are responsible for providing FL services to all FL entities. This role involves setting up communication channels with entities, initializing the execution environment of participants [45], scheduling the training and aggregation workflows for improve system efficiency, such as by alleviating the straggler effect [20, 65], optimizing data heterogeneity [2, 31] and compressing model transfer [60, 114]. Additionaly, the FL coordinator provides privacy control mechanisms [13, 33, 48] for model users and authorization verification for participants to maintain the security of FL systems. Furthermore, the coordinator can hold a validation dataset for evaluate the models contributed by participants or detect potential disturbances from Byzantine attacks [113].
- Data Owner. The FL data owners are knowledge contributors of FL systems, they collect and desentize raw data to maintain a local dataset for federated training. Although they have full authority of data processing and modeling, they cannot share the raw data due to privacy concerns. To address these concerns, de-identification [4] and differential privacy [32] techniques can be applied to meet privacy budgets as required by privacy policies.
- Auditor. The FL auditors are responsible for formulating privacy control policies and establishing supervisory mechanisms that ensure the training process is compliant with data protection regulations (e.g. HIPAA [4], GDPR([128])) and preventing potential privacy breaches for both model users and data owners. Especially in FL, the latent knowledge in models can potentially reveal the sensitive information of training data [56, 132, 155], making it crucial for auditors to scrutinize the model transmission [78, 133] and verify the ownership of models [117, 124].

Fig. 2 illustrates the typical architecture of FL systems, which as a distributed modeling toolkits consists of server part and client part. In general FL setting, the server part is the central aggregator installed in a trusted cloud environment, while the client part of software can operate in different operating environments of client devices. The server and clients are connected via Internet and typically with the help of Remote Procedure Call (RPC) interface for coordinating [1, 11, 47, 82, 148]. We use four colors to represent the four FL roles and the colors with grid lines indicate non-essential roles. For example, in Fig. 2, the UCDA server takes on the roles of model user, coordinator and audior in traditional FL. However, it is no necessary to hold training data or validation data, so the role of data owner is non-essential. To illustrate the workflow of traditional FL, we leverage the vanilla FL framework Federated Averaging (FedAvg) [12, 91] as an example.

First, the FL server pre-defines the objective modeling task and initializes the server process. Secondly, the coordinator in server-side specifies a preset global model and the operational parameters. Thirdly, the coordinator

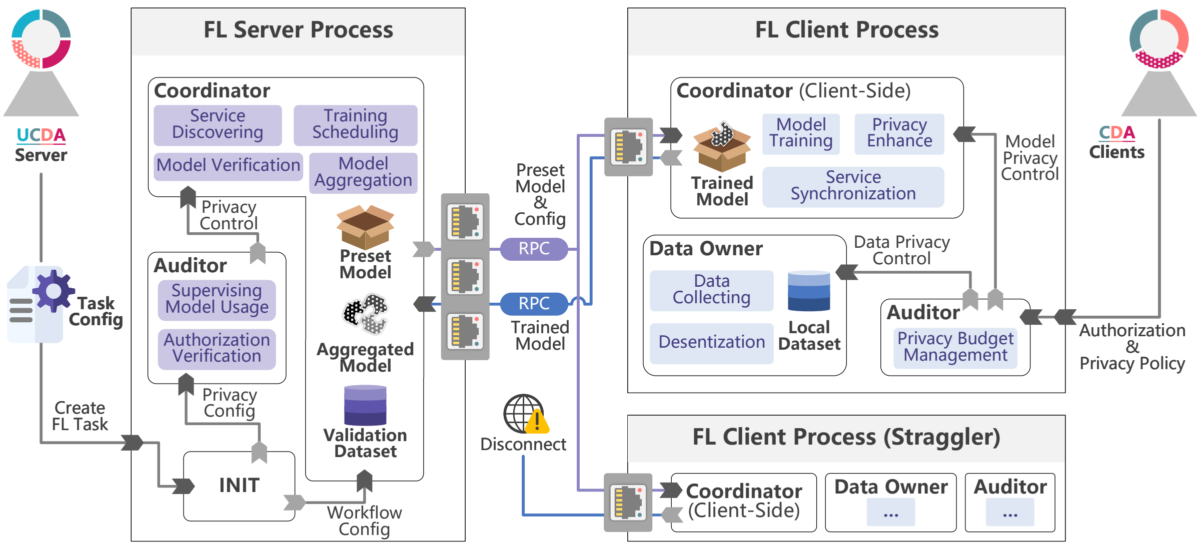


Fig. 2. An overview of traditional FL systems. (U: model User, C: Coordinator, D: Data owner, A: Auditor)

discovers the availability of clients' FL services, boardcasts the global model and training config to them. The training config contains bath size, local epoch round, optimizer parameters and so on. Then, the coordinator will wait for the trained results contributed by the coordinator in clients-side and drop those clients with network problems. Finally, the server aggregates the trained resultes received from various clients into the global model and begins a new round based on this aggregated global model. The aggregation strategy adopted in FedAvg is the weighted model parameters based on the size of local dataset, which means the global objective of FL can be regarded as a joint objective function of clients. By this way, the FL server can learn a generalized global model by jointly optimizing all local optimization objectives and incorporating the latent knowledge from the local models. Although the auditor component was not included in earlier FedAvg, it play an important role in the later business-ready FL frameworks [82, 112, 156].

However, in comparing FedAvg workflow described above with Fig. 2, it is easy to notice that the client part has been excluded. This is because we are elaborating from a server-side perspective, which is usual way FL is presented [18, 73, 91]. Actually, the underlying reason is that in traditional FL, the client-side process is tightly coupled with server-side process, and there is no alternative for clients other than to either accept or reject the training scheduling from the server wholesale. So the clients are not considered as an autonomous entities but rather work as subordinates to server. In this server-domianted cooperation framework, the benefits and autonomy of clients are compromised, which hinders their enthusiasm to participate in FL network and subsequently limits the applicability of FL. From this perspective, we summarize the limitations of traditional FL in the next section, which motivates us to explore more innovative sustainable FL cooperation frameworks.

2.2 Limitations of Traditional FL

Previous surveys [6, 58, 74, 93, 122, 139, 150, 154] has extensively discussed the challenges in FL systems from various aspects However, the cooperation mechanism of FL systems has been overlook because almost all mainsteam FL frameworks follow the FL prototype [91], which shape the form of current FL frameworks: a modeling software. We summarize three inherent limitations of traditional FL cooperation mechanism: (1) **Server-client Coupling**, (2) **Low Model Reusability**, (3) **Non-public**.

2.2.1 Server-client Coupling. The tightly-coupled server-client design is a major limitation of FL systems. From the perspective of FL service providers, adapting the programs to heterogeneous client hardware and software components, such as various operating and database systems, processor and storage architectures, communication protocols, eneragy constrains and data licenses, is a challenging task that significantly increases the complexity of the FL system.

On the other hand, the invasive software deploy mode compromises the integrity of client environments and expose them to new privacy risks. Specifically, the coordinator components (client-side) pushed by the server may not offer demanded privacy control mechanisms [18, 91, 145], or cause resource depletion on client-side [12, 23, 95], or even piggyback malicious executable codes [66]. So the auditor role of client is non-essential as depicted in Fig. 2, not only because the client maybe lacks a corresponding policy for FL training, but also because its privacy is not completely under its control. Likewise, the malicious clients can also exploit the vulnerability in the aggreagation strategy to currupt the FL tranining process [15, 34, 98, 113] or insert backdoors [10, 129]. In addition, the unstable network environment can drive clients to drop out from traning (i.e. straggler effect), thereby reducing system efficiency [98, 107]. Therefore, the server-client coupling design of traditional FL systems make them susceptible to unpredictable runtime environments, leading to system vulnerability and low reliability.

2.2.2 Low Model Reusability. The traditional FL scheduling follows a task-centric manner and erminates once the training reaches a preset number of rounds or meets traget metrics on global model set by FL server [12]. As a result, only FL server can guarantee having the latest global model after the task is terminated. This ad-hoc modeling paradigm results in low model reusability and transportability. For example, if a client who participated in the previous training turn wants to continue training, they can only start the task from scratch unless they have the up-to-date global model. Since only FL server is able to maintain the complete modeling trajectory, it is difficult for the client to roll back the training itself to eliminate the potential privacy risk. Furthermore, the non-deliverable scheduling mechanism of FL tasks also hinders inter-task model reuse, which leads to unnecessary wasted energy and time on participants that have been involved in similar tasks.

2.2.3 Non-public. As we mention in Sec. 1.2.1, except PySyft [156], the application scenarios of mainstream FL frameworks [1, 11, 18, 47, 82, 86, 112, 145] aim to provide private collaborative ML traning service, and there is no any accessible FL platform for the public. Although there have been real-world deployment practices of FL for the public with scales of millions [12] and billions [95], these have been carried out only by tech giants with a massive base of active users. For an individual user, there is no practical way to organize such a large-scale FL training network.

But in fact, due to the limitations in the cooperation mechanism mentioned above, data owners are not sufficiently motivated to participate in this server-take-all FL training even if it is public accessible. Therefore, the cornerstone of buliding a sustainable open FL platform is to establish a reciprocal FL cooperation framework, followed by corresponding mulit-source knowledge aggregation strategies, which we discuss in the following sections.

3 QUERY-BASED FEDERATED LEARNING

3.1 Overview

Let us continue by establish a sustainable open FL platform based on a query-based cooperation framework. An overview of this platform is presented in Fig. 3, the desin philosophy behind this framework is to break the coupling between FL server and clients. In the query-based FL systems, all traditional FL roles and components are maintained on an open model repository called Model Community. The Model Community privdes a one-stop

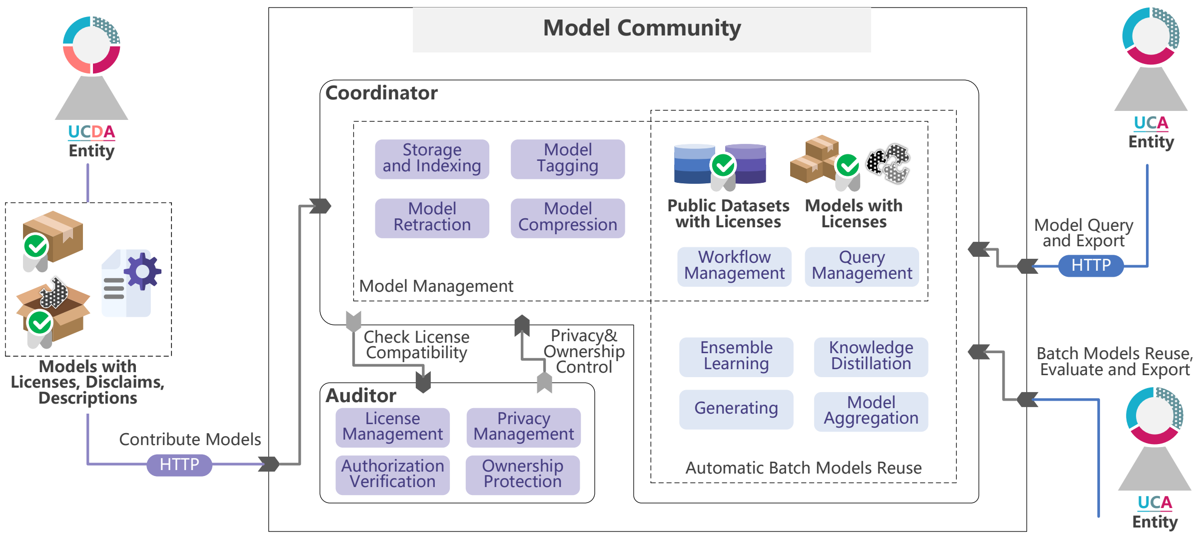


Fig. 3. An overview of query-based FL systems. (U: model User, C: Coordinator, D: Data owner, A: Auditor)

ML models redistribution and reuse service, including model indexing, automatic batch model reuse, license management, privacy control and so on. In addition to large-scale pretrained models like BERT [28], BLOOM [115] with great generalization abilities, we also encourage individuals to upload their task-specific models trained on limited domain data to boost the knowledge mining within models [142]. The derivatives of knowledge mining can learn representations from multiple domains, resulting in more promising performance that can be evaluated by platform users. Furthermore, the contributors can open models under applicable licenses, granting them distribution control and legal protection of their intellectual property. In summary, the properties of query-based FL are: (1) **Model Agnostic**, as there are no restrictions on the types and architectures of the models uploaded by users; (2) **Contactless**, as coomunication channels need not be maintained; (3) **Community-powered**, whereby sharing models enriches the entire community.

Actually, we aim to advocate a novel SaaS [16] ML platform with automatic model reuse integrated, which has potential to leverage the transportability of models to address previously unexplored ML problems. Due to the high computational demands of deep learning, current ML platforms primarily concentrate on computing, for example, MaaS, MLaaS, FLaaS provide ML models deployment and development services to handle user-specified tasks. (Section 1.2.2). On the other hand, there are several ML platforms provide open model search and download services. So, can we leverage leverage off-the-shelf open model platforms to build a query-based FL system? Unfortunately, these platforms are designed solely for sharing and are no suitable for more advanced functionalities such as model ensemble [52] and knowledge distillation [49], we will explain the reasons in the following section.

3.2 How to Query for Models

To establish a query-based FL platform, the first thing that comes to mind is how to query for models. Unlike traditional ML model sharing repositories that mainly query for a specific model by name, it requires an efficiency approach to export a batch of target models that ready for ensemble or distillation. We summaried the filter conditions of existing DNNs sharing repositories in Table. 2. The prevailing method for querying models involves

Table 2. Filter conditions and characteristics of DNNs repositories. ✓: Supported, ✗ : Unsupported, ! : Information provided but unsearchable, listed in descending order by number of models.

	DS Name	Model Architecture	Modality/Task	Tag	License	Input-Output	Batch Export	# of Models
Hugging Face[5]	✓	✓	✓	✓	✓	!	✗	133,641
Model Zoo[6]	✓	✓	✓	✓	✗	✗	✗	3,426
Tensorflow Hub[7]	✓	✓	✓	✓	!	!	✗	1,356
NVIDIA NGC[8]	!	✓	✓	✓	!	!	✗	527
OpenVINO[9]	!	✓	✓	✗	!	!	✓	278
Pytorch Hub[10]	!	✓	✗	✗	✗	!	✗	49

searching for the desired model by its name, datasets used, associated tasks. To illustrate, one might search for the model name GPT [103], models trained on the MNIST dataset [64], or models capable of performing image segmentation tasks. However, this model retrieval method requires the users have a strong priori knowledge in data science, thus raising the barrier for knowledge mining within models. For example, there is no effective way to acquire a batch of image classfication models that contains the knowledge of *lesser panda* for further distillation. A compromise solution is to manually search the schema of each dataset one-by-one and subsequently search for models trained on those datasets.

Additionally, as shown in Table. 2, most DNNs repositories are simply list the description of input/output (e.g., NVIDIA NGC, OpenVINO) or even just present the source codes (e.g., Tensorflow Hub, Pytorch Hub), This lack of unified convention for model input/ouput poses a challenge for query-based FL. Besides, most of DNNs repositories do not enable querying models by licenses, resulting in the cumbersome task of individually handling model licenses and ensuring compatibility among different licenses. Hence, it is imperative to reconsider the design of DNN repositories to enable quick identification of readily reusable models for model knowledge mining. We further suggest following filter conditions for query-based FL.

3.2.1 Data Description. Similar with the data heterogeous challenges in FL [70]. The local datasets of contributors have varing quality and contain intractable biases, imbalances and noisies that can be attributed to the natural characteristics of demographic or improper data collection mechanisms [27]. Besides, label errors pervasive even in open datasets [96]. So, in addition to searching for domain-specific datasets based on their data descriptions, we are also seeking such descriptions for the purpose of future traceability and debugging. The data description can consist of statistical analysis results or the visualization diagrams that used to profile the data distribution [77] and complementary provenance information.

3.2.2 Workflow and History. The process of building an ML model is iterative, involving repeated hyperparameter tuning and architecture exploration, resulting in abundant workflow and historical trajectory data. This information includes pipelines, model structures, hyperparameter values for pre-training and fine-tuning, test metrics, and results. These data can be useful in filtering models that meet specific requirements, such as those with data standardization in preprocessing or evaluated using mean average precision (mAP). Instead of manually saving and uploading the logs and configuration files, a more efficient method is to leverage ML workflow management tools [127], such as MLflow [11] and Neptune [12], to automatically track and store the ML workflow during model building process. Additionally, to ensure that the computational consumption of models is within budget, the Deep Learning Profiler [13] can be leveraged to generate a report that shows the FLOPS and bandwidth requirements.

[5] https://huggingface.co [6] https://modelzoo.co/ [7] https://tfhub.dev/ [8] https://catalog.ngc.nvidia.com/models
[9] https://docs.openvino.ai/latest/model_zoo.html [10] https://pytorch.org/hub/ [11] https://mlflow.org [12] https://neptune.ai
[13] https://docs.nvidia.com/deeplearning/frameworks/dlprof-user-guide/index.html

3.2.3 Software Dependency. ML models are software that depend on underlying ML libraries, so it is important to declare the dependencies of the model to analyze software compatibility between batches of models. For instance, resource-constrained devices may need to trim down the list of software-dependent libraries to meet limited storage space requirements [26]. In some cases, contributed models may rely on other models as dependencies. For example, Fast R-CNN [40] uses VGG16 [118] as its backbone. It is crucial to release this information for further model license compatibility analysis.

The aforementioned filter conditions provide comprehensive coverage of the ML modeling process. However, there are additional requirements depending on the reuse mechanisms of the model retrieval side. For example, FedAvg [91] aggregates the local models weights element-wise, which requires full access to the models. In contrast, MoE with a gating network [52] only ensembles a batch of model outputs, so the individual models can remain blackboxes in this scenario. So, in the context of software licenses or model licenses, the batch models reused by FedAvg should be released as source code, while those reused by MoE can be released as binary object code (static linking). The above distinction is critical for ensuring that model reuse results meet the legal framework, and this has been overlooked in traditional FL. We will expand on this topic in the following section.

3.3 How to Reuse Batch of Models

Once we have acquired a certain number of models that can contribute to the new target task, the next step is to reuse the knowledge of these pre-trained models, i.e., transfer their knowledge from source domain to the target domain [97]. However, before deciding on how to reuse the model, it is important to ensure that the necessary legal rights and permissions have been obtained. This may involve reviewing the terms and conditions of the licenses under which the models were originally released or obtaining permission from the original creators or copyright holders. Therefore, in this section, we will not focus on the technical details of how to reuse models, which is already covered by many related surveys, such as Transfer Learning [97], Ensemble Leanring [152], Domain Adaptation [131], Knowledge Distillation [130], Deep Generative Models [19] and Model Fusion [53]. Furthermore, the specific model reuse technique or techniques used is at the user's discretion, and the query-based FL platform we advocate is not bound or restricted to any particular model reuse algorithm. Innovatively, we study how to reuse batch of models, from the perspective of **legal compliance**.

The machine learning community benefits from the openness of ideas and code, and many high-impact ML conferences and journals encourage authors to publish their source code and dataset to research platforms like Papers With Code [14] and Code Ocean [15] to increase exposure and facilitate reproducibility. To restrict the use of ML techniques for unethical purposes (i.e. Deepfakes [92]) and protect the intellectual property (IP) of creators, models are typically published under a license agreed upon by the licensor. Here, we summary the licenses, granted rights, restrictions and enforcements for ML models posted on Hugging Face in Table. 3.

3.3.1 Model Licensing Forms. ML models are licensed in three main forms: as software (e.g. Apache, MIT, GPL), as a model (e.g. OpenRAIL), and as content/database (e.g. CC-BY, PDDL). The reason for the mixed use of licenses is the ambiguity in the dependency relationship between the code, model, and data. ML models can be released with reproducable code and be considered as a component of software. So many open software licenses are naturally deferred for licensing of models. The most popular license is Apache-2.0, which is a permissive open software license that allows the freedom to make derivative works. However, the model building process also relies on a massive amount of data [63] that may be licensed under different licenses, which can lead to license conflicts. A practical example is BERT [28], which was published under the Apache-2.0 license but pre-trained on English Wikipedia documents that are licensed under CC BY-SA 3.0. This changing of license violates the requirement of the CC BY-SA 3.0, which states that any contribution must be distributed under the **same license** as the original work.

[14] https://paperswithcode.com [15] https://codeocean.com

From the perspective of content and database licensing, some word embedding models, such as GloVe [100], compute vector representations of words based on licensed open linguistic resources. These representations can be regarded as a translation of corpus and fall under the license of the original linguistic resources. A more complex scenario arises when the model is fine-tuned with other data that has a different license, for example, fine-tune RoBERTa [83] (MIT license) with SQuAD2 [104] (CC BY 4.0). The resulting model can be interpreted as both derived works and combined works.

Not only limited to protecting the intellectual property and controlling the diffusion of ideas, but AI companies and researchers are also concerned about licensees using their models for unethical purposes [9, 57, 144], which is not restricted by traditional licenses based on the context of software and content. We can infer the concerns of the inventors of GPT-2 [103] about the unethical use of the model from its modified MIT license, which states, *We don't claim ownership of the content you create with GPT-2, so it is yours to do with as you please. We only ask that you use GPT-2 responsibly and clearly indicate your content was created using GPT-2.* However, such a statement lacks legal enforcement, and users may avoid accountability by convincing themselves that despite their efforts to minimize harm, they could not predict the AI artifact they generated would be used for harmful purposes. Besides, the original licensing frameworks (e.g. MIT, CC BY) for software and content are not well suited to the data-driven ML. Many ML operations, such as training, fine-tuning, inference, and distillation, are not explicitly defined in traditional software and content licenses, leaving a potential legal loophole for licensees.

To address the unique challenges and considerations surrounding the use and distribution of ML models, several specific licenses for ML models have been proposed. The CreativeML OpenRAIL-M license, proposed by Responsible AI [25], is the most popular model-specific license on Hugging Face and enables legally enforceable responsible use. By accepting this license, licensees must adhere to the use-based restrictions stated by the licensor, and these restrictions must also apply to derivative works. With a multitude of different model licenses available, it becomes a challenging and tedious task to reuse them in bulk. It is therefore imperative to establish guidelines for selecting a license for models that are ready for query-based FL.

3.3.2 Model License Choosing Preferences. In query-based FL, the model community automatically reuses models contributed by users, which raises unique concerns about licensing rights. Firstly, the license should allow the modification, combination and redistribution of the works and any derived works. Secondly, the sublicensing right can lubricate the republication of derived works resulting from knowledge mining. Thirdly, some licenses require the source of the derived works to be disclosed and prohibit their commercial use, which hinders model selling [22]. Lastly, some licenses are copyleft (denoted by * in Table. 3), which means the derivatives should be licensed under the same license or a compatible one, leading to potential license conflicts and license proliferation [41].

In summary, the

Another example is finetune the pretrained model RoBERTa [83] (MIT license) with SQuAD2 [104] licensed under CC-BY-4.0.

However, BERT [28] pretrained corpus using English Wikipedia document CC BY-SA 3.0 no compatible with Apache-2.0

difussion of ideas

The

Therefore, the focus of this section is how to reuse batch of models,

There are many efforts deal with model reuse.

Single Model Reuse

Batch Model Reuse

Model type?

Model heterogeneity?

Black box, White box, Mix?

Table 3. Licenses for ML models available on Hugging Face with a focus on their rights, restrictions and enforcements, grouped by free software licenses, AI model licenses, free content or database licenses in descending order of number of models (GPL, BSD, LGPL, CC licenses with unspecified versions are excluded, the similar revisions are merged). ✓: Permited or Required, ✗ : Not Permited or Not Required, **!** : Not Explicitly Permited, * : Copyleft License

Licenses	Modify / Merge	Redistribution	Sublicensing	Commercial Use	Patent Use	Trademark Use	State Changes	Disclose Source	Responsible-use Restrictions	License/Disclaim Preservation	# of Models	Licensed Materials / Remarks
Apache-2.0	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	23,519	BERT [28]
MIT	✓	✓	✓	✓	!	!	✗	✗	✗	✓	9,605	GPT-2 [103]
AFL-3.0	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	1,561	Italian-Legal-BERT [79]
*GPL-3.0	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	404	CKIP BERT Chinese
Artistic-2.0	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	331	Include original source
BSD-3-Clause&-Clear	✓	✓	✓	✓	!	!	✗	✗	✗	✓	209	CodeGen [94] / A MIT-style license
WTFPL-2.0	✓	✓	!	✓	!	!	✗	✗	✗	✗	131	A MIT-style permissive license
*AGPL-3.0	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	96	Distributed under AGPL only
Unlicense	✓	✓	!	✓	!	!	✗	✗	✗	✗	90	A MIT-style permissive license
BSL-1.0	✓	✓	✓	✓	!	!	✗	✗	✗	✓	60	A MIT-style permissive license
*GPL-2.0	✓	✓	✗	✓	!	!	✓	✓	✗	✓	34	Not compatible with GPL-3.0
BSD-2-Clause	✓	✓	✓	✓	!	!	✗	✗	✗	✓	34	A MIT-style permissive license
*LGPL-2.1&3.0	✓	✓	✗	✓	!	!	✓	✓	✗	✓	25	For software libraries
*OSL-3.0	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	22	Linking is not derivative work
ECL-2.0	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	12	For education communities
*MPL-2.0	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	9	State changes under MPL only
ISC	✓	✓	!	✓	!	!	✗	✗	✗	✓	8	MIT-style license w/o sublicense
Zlib	✓	✓	!	✓	!	!	✗	✗	✗	✓	8	Rename if modified
*Ms-PL	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	7	Weak copyleft license
*EPL-1.0&2.0	✓	✓	✓	✓	✓	!	✗	✓	✗	✓	6	Can link proprietary license code
NCSA	✓	✓	✓	✓	!	✗	✗	✗	✗	✓	4	Include full text of license
PostgreSQL	✓	✓	!	✓	!	!	✗	✗	✗	✓	2	A MIT-style license
OFL-1.1	✓	✓	✗	✓	!	!	✗	✗	✗	✓	2	For font software
*EUPL-1.1	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	1	License of EU covers SaaS
LPPL-1.3c	✓	✓	✓	✓	!	✗	✓	✓	✗	✓	1	Covering stewardship transfer
CreativeML-OpenRAIL-M	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	3,590	Stable Diffusions v1 [111]
OpenRAIL	>Responsible AI License template, w/o full text										2,393	ControlNet [147]
BigScience-BLOOM-RAIL-1.0	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	196	BLOOM [115]
BigScience-OpenRAIL-M	>Same as BigScience-BLOOM-RAIL-1.0										155	A general version of 1.0
OpenRAIL++	>Same as CreativeML-OpenRAIL-M										72	Stable Diffusion v2 [111]
OPT-175B	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	≈ 66	OPT LLM [149]
SEER	>Same as OPT-175B, ban on reverse-engineer										/	SEER Vision Model [42]
CC-BY-4.0&3.0&2.5&2.0	✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	1,740	RoBERTa-SQuAD2.0 [104]
*CC-BY-SA-4.0&3.0	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	590	LEGAL-BERT [21]
*CC-BY-NC-SA-4.0&3.0	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	556	LayoutLMv3 [51]
CC-BY-NC-4.0&3.0&2.0	✓	✓	✗	✗	✗	✗	✓	✗	✗	✓	499	GALACTICA [123]
CC0-1.0	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	165	BlueBERT [99]
CC-BY-NC-ND-4.0&3.0	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	21	NonCommercial, NoDerivatives
PDDL	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	16	Database-specific license
C-UDA	✓	✓	✓	✗	!	!	✗	✗	✓	✓	13	Data for computational use only
*LGPL-LR	✓	✓	✗	✓	!	!	✓	✓	✗	✓	12	LGPL for linguistic resources
*GFDL	>Same as GPL, a free document license										12	txtai-wikipedia
CC-BY-ND-4.0	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	11	Disallow making derivatives
ODC-By	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	7	Database license w/o sublicense
*ODbL	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	6	Automatic relicensing

With val?
Horizontal or Vertical?

Query syntax: Table. 2, data description, workflow metadata/history of ML pipeline (Scientific workflow management), model performance and profile (task-specific), software dependency, model use mode

CreativeML Open RAIL-M: we added use-based restrictions not permitting the use of the Model in very specific scenarios, in order for the licensor to be able to enforce the license in case potential misuses of the Model may occur.

3.4 How to Protect Models

ACKNOWLEDGMENTS

ACK.

REFERENCES

[1] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. 2016. Tensorflow: A system for large-scale machine learning. In *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*. 265–283.

[2] Sawsan AbdulRahman, Hanine Tout, Azzam Mourad, and Chamseddine Talhi. 2020. FedMCCS: multicriteria client selection model for optimal IoT federated learning. *IEEE Internet of Things Journal* 8, 6 (2020), 4723–4735.

[3] Sawsan AbdulRahman, Hanine Tout, Hakima Ould-Slimane, Azzam Mourad, Chamseddine Talhi, and Mohsen Guizani. 2020. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal* 8, 7 (2020), 5476–5497. https://doi.org/10.1109/JIOT.2020.3030072

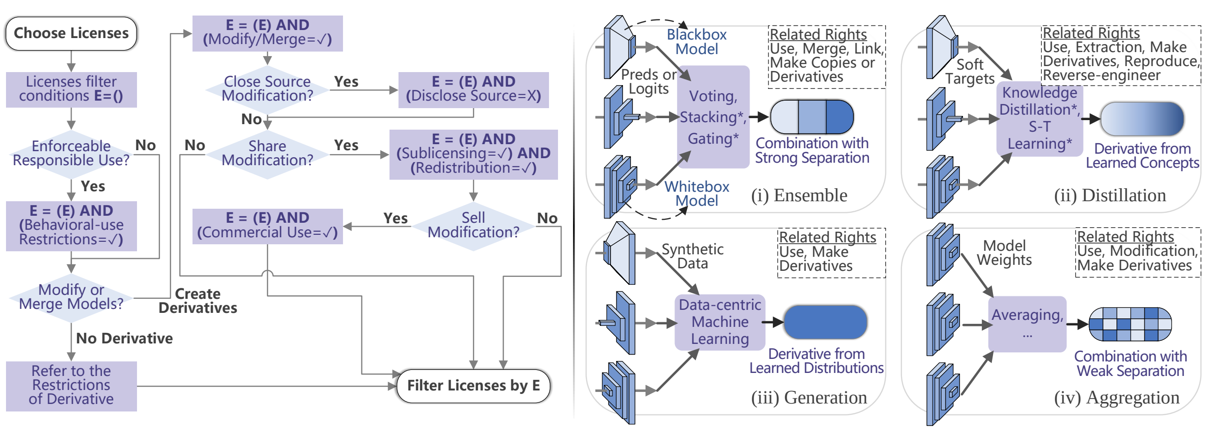
[4] Accountability Act. 1996. Health insurance portability and accountability act of 1996. *Public law* 104 (1996), 191.

[5] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2022. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications* (2022). https://doi.org/10.1016/j.comcom.2022.09.012

[6] Mamoun Alazab, Swarna Priya RM, M Parimala, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, and Quoc-Viet Pham. 2021. Federated learning for cybersecurity: concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics* 18, 5 (2021), 3501–3509. https://doi.org/10.1109/TII.2021.3119038

[7] Mohammed Aledhari, Rehma Razzak, Reza M Parizi, and Fahad Saeed. 2020. Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access* 8 (2020), 140699–140725. https://doi.org/10.1109/ACCESS.2020.3013541

[8] Rodolfo Stoffel Antunes, Cristiano André da Costa, Arne Küderle, Imrana Abdullahi Yari, and Björn Eskofier. 2022. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transactions on Intelligent Systems and Technology (TIST)* 13, 4 (2022), 1–23. https://doi.org/10.1145/3501813



(a) ML Model Licenses Choosing Flowchart

(b) ML Batch Models Reuse Mechanisms

Fig. 4. flowchart

[9] Edmond Awad, Sohan Dsouza, Richard Kim, Jonathan Schulz, Joseph Henrich, Azim Shariff, Jean-François Bonnefon, and Iyad Rahwan. 2018. The moral machine experiment. *Nature* 563, 7729 (2018), 59–64. https://doi.org/10.1038/s41586-018-0637-6

[10] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. 2020. How to backdoor federated learning. In *International Conference on Artificial Intelligence and Statistics*. PMLR, 2938–2948.

[11] Daniel J Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, Pedro PB de Gusmão, and Nicholas D Lane. 2020. Flower: A friendly federated learning research framework. *arXiv preprint arXiv:2007.14390* (2020).

[12] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konecny, Stefano Mazzocchi, H Brendan McMahan, et al. 2019. Towards Federated Learning at Scale: System Design. In *Proceedings of the 2nd SysML Conference*.

[13] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2017. Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 1175–1191.

[14] Parimala Boopalan, Swarna Priya Ramu, Quoc-Viet Pham, Kapal Dev, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, Thien Huynh-The, et al. 2022. Fusion of federated learning and industrial Internet of Things: A survey. *Computer Networks* (2022), 109048. https://doi.org/10.1016/j.comnet.2022.109048

[15] Nader Bouacida and Prasant Mohapatra. 2021. Vulnerabilities in federated learning. *IEEE Access* 9 (2021), 63229–63249. https://doi.org/10.1109/ACCESS.2021.3075203

[16] Pearl Brereton, David Budgen, Keith Bennnett, Malcolm Munro, Paul Layzell, Linda MaCaulay, David Griffiths, and Charles Stannett. 1999. The future of software. *Commun. ACM* 42, 12 (1999), 78–84. https://doi.org/10.1145/322796.322813

[17] Theodora S Brisimi, Ruidi Chen, Theofanie Mela, Alex Olshevsky, Ioannis Ch Paschalidis, and Wei Shi. 2018. Federated learning of predictive models from federated electronic health records. *International journal of medical informatics* 112 (2018), 59–67. https://doi.org/10.1016/j.ijmedinf.2018.01.007

[18] Sebastian Caldas, Peter Wu, Tian Li, Jakub Konečnỳ, H Brendan McMahan, Virginia Smith, and Ameet Talwalkar. 2018. Leaf: A benchmark for federated settings. *arXiv preprint arXiv:1812.01097* (2018).

[19] Hanqun Cao, Cheng Tan, Zhangyang Gao, Guangyong Chen, Pheng-Ann Heng, and Stan Z Li. 2022. A survey on generative diffusion model. *arXiv preprint arXiv:2209.02646* (2022).

[20] Zheng Chai, Ahsan Ali, Syed Zawad, Stacey Truex, Ali Anwar, Nathalie Baracaldo, Yi Zhou, Heiko Ludwig, Feng Yan, and Yue Cheng. 2020. Tifl: A tier-based federated learning system. In *Proceedings of the 29th international symposium on high-performance parallel and distributed computing*. 125–136. https://doi.org/10.1145/3369583.3392686

[21] Ilias Chalkidis, Manos Fergadiotis, Prodromos Malakasiotis, Nikolaos Aletras, and Ion Androutsopoulos. 2020. LEGAL-BERT: The Muppets straight out of Law School. In *Findings of the Association for Computational Linguistics: EMNLP 2020*. 2898–2904. https://doi.org/10.18653/v1/2020.findings-emnlp.261

[22] Lingjiao Chen, Paraschos Koutris, and Arun Kumar. 2019. Towards model-based pricing for machine learning in a data marketplace. In *Proceedings of the 2019 International Conference on Management of Data*. 1535–1552. https://doi.org/10.1145/3299869.3300078

[23] Yanjiao Chen, Baolin Zheng, Zihan Zhang, Qian Wang, Chao Shen, and Qian Zhang. 2020. Deep learning on mobile and embedded devices: State-of-the-art, challenges, and future directions. *ACM Computing Surveys (CSUR)* 53, 4 (2020), 1–37. https://doi.org/10.1145/3398209

[24] Kewei Cheng, Tao Fan, Yilun Jin, Yang Liu, Tianjian Chen, Dimitrios Papadopoulos, and Qiang Yang. 2021. Secureboost: A lossless federated learning framework. *IEEE Intelligent Systems* 36, 6 (2021), 87–98. https://doi.org/10.1109/MIS.2021.3082561

[25] Danish Contractor, Daniel McDuff, Julia Katherine Haines, Jenny Lee, Christopher Hines, Brent Hecht, Nicholas Vincent, and Hanlin Li. 2022. Behavioral use licensing for responsible AI. In *2022 ACM Conference on Fairness, Accountability, and Transparency*. 778–788. https://doi.org/10.1145/3531146.3533143

[26] Robert David, Jared Duke, Advait Jain, Vijay Janapa Reddi, Nat Jeffries, Jian Li, Nick Kreeger, Ian Nappier, Meghna Natraj, Tiezhen Wang, et al. 2021. Tensorflow lite micro: Embedded machine learning for tinyml systems. *Proceedings of Machine Learning and Systems* 3 (2021), 800–811.

[27] Ittai Dayan, Holger R Roth, Aoxiao Zhong, Ahmed Harouni, Amilcare Gentili, Anas Z Abidin, Andrew Liu, Anthony Beardsworth Costa, Bradford J Wood, Chien-Sung Tsai, et al. 2021. Federated learning for predicting clinical outcomes in patients with COVID-19. *Nature medicine* 27, 10 (2021), 1735–1743. https://doi.org/10.1038/s41591-021-01506-3

[28] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2018. BERT: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805* (2018).

[29] Zhaoyang Du, Celimuge Wu, Tsutomu Yoshinaga, Kok-Lim Alvin Yau, Yusheng Ji, and Jie Li. 2020. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society* 1 (2020), 45–61. https://doi.org/10.1109/OJCS.2020.2992630

[30] Moming Duan, Duo Liu, Xianzhang Chen, Renping Liu, Yujuan Tan, and Liang Liang. 2020. Self-balancing federated learning with global imbalanced data in mobile systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 32, 1 (2020), 59–71.

[31] Moming Duan, Duo Liu, Xianzhang Chen, Yujuan Tan, Jinting Ren, Lei Qiao, and Liang Liang. 2019. Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications. In *Proceedings of the IEEE 37th International Conference on Computer Design (ICCD)*. IEEE, 246–254.

[32] Cynthia Dwork. 2006. Differential privacy. In *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*. Springer, 1–12. https://doi.org/10.1007/11787006_1

[33] Ahmed El Ouadrhiri and Ahmed Abdelhadi. 2022. Differential privacy for deep and federated learning: A survey. *IEEE Access* 10 (2022), 22359–22380. https://doi.org/10.1109/ACCESS.2022.3151670

[34] Minghong Fang, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong. 2020. Local model poisoning attacks to byzantine-robust federated learning. In *Proceedings of the 29th USENIX Conference on Security Symposium*. 1623–1640.

[35] Attlee M Gamundani and Lucas M Nekare. 2018. A review of new trends in cyber attacks: A zoom into distributed database systems. In *2018 IST-Africa Week Conference (IST-Africa)*. IEEE, Page–1.

[36] Gary N Geller and Woody Turner. 2007. The model web: a concept for ecological forecasting. In *2007 IEEE International Geoscience and Remote Sensing Symposium*. IEEE, 2469–2472. https://doi.org/10.1109/IGARSS.2007.4423343

[37] Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing (STOC)*. 169–178. https://doi.org/10.1145/1536414.1536440

[38] Robin C Geyer, Tassilo Klein, and Moin Nabi. 2017. Differentially private federated learning: A client level perspective. *arXiv preprint arXiv:1712.07557* (2017).

[39] Bimal Ghimire and Danda B Rawat. 2022. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal* (2022). https://doi.org/10.1109/JIOT.2022.3150363

[40] Ross Girshick. 2015. Fast r-cnn. In *Proceedings of the IEEE international conference on computer vision*. 1440–1448.

[41] Robert W Gomulkiewicz. 2009. Open Source License Proliferation: Helpful Diversity or Hopeless Confusion? *Washington University Journal of Law & Policy* 30, 1 (2009).

[42] Priya Goyal, Quentin Duval, Isaac Seessel, Mathilde Caron, Mannat Singh, Ishan Misra, Levent Sagun, Armand Joulin, and Piotr Bojanowski. 2022. Vision models are more robust and fair when pretrained on uncurated images without supervision. *arXiv preprint arXiv:2202.08360* (2022).

[43] Ruchi Gupta and Tanweer Alam. 2022. Survey on federated-learning approaches in distributed environment. *Wireless Personal Communications* 125, 2 (2022), 1631–1652. https://doi.org/10.1007/s11277-022-09624-y

[44] Xu Han, Zhengyan Zhang, Ning Ding, Yuxian Gu, Xiao Liu, Yuqi Huo, Jiezhong Qiu, Yuan Yao, Ao Zhang, Liang Zhang, et al. 2021. Pre-trained models: Past, present and future. *AI Open* 2 (2021), 225–250. https://doi.org/10.1016/j.aiopen.2021.08.002

[45] Lucjan Hanzlik, Yang Zhang, Kathrin Grosse, Ahmed Salem, Maximilian Augustin, Michael Backes, and Mario Fritz. 2021. Mlcapsule: Guarded offline deployment of machine learning as a service. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 3300–3309.

[46] Andrew Hard, Kanishka Rao, Rajiv Mathews, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. 2018. Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604* (2018).

[47] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, et al. 2020. FedML: A research library and benchmark for federated machine learning. In *NeurIPS 2020 Workshop on Scalability, Privacy, and Security in Federated Learning*.

[48] Ehsan Hesamifard, Hassan Takabi, Mehdi Ghasemi, and Rebecca N Wright. 2018. Privacy-preserving machine learning as a service. *Proc. Priv. Enhancing Technol.* 2018, 3 (2018), 123–142. https://doi.org/10.1515/popets-2018-0024

[49] Geoffrey Hinton, Oriol Vinyals, and Jeffrey Dean. 2014. Distilling the Knowledge in a Neural Network. In *NIPS Deep Learning and Representation Learning Workshop*.

[50] Li Huang, Andrew L Shea, Huining Qian, Aditya Masurkar, Hao Deng, and Dianbo Liu. 2019. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. *Journal of biomedical informatics* 99 (2019), 103291. https://doi.org/10.1016/j.jbi.2019.103291

[51] Yupan Huang, Tengchao Lv, Lei Cui, Yutong Lu, and Furu Wei. 2022. Layoutlmv3: Pre-training for document ai with unified text and image masking. In *Proceedings of the 30th ACM International Conference on Multimedia*. 4083–4091. https://doi.org/10.1145/3503161.3548112

[52] Robert A Jacobs, Michael I Jordan, Steven J Nowlan, and Geoffrey E Hinton. 1991. Adaptive mixtures of local experts. *Neural computation* 3, 1 (1991), 79–87. https://doi.org/10.1162/neco.1991.3.1.79

[53] Shaoxiong Ji, Teemu Saravirta, Shirui Pan, Guodong Long, and Anwar Walid. 2021. Emerging trends in federated learning: From model fusion to federated x learning. *arXiv preprint arXiv:2102.12920* (2021).

[54] Yangqing Jia, Evan Shelhamer, Jeff Donahue, Sergey Karayev, Jonathan Long, Ross Girshick, Sergio Guadarrama, and Trevor Darrell. 2014. Caffe: Convolutional architecture for fast feature embedding. In *Proceedings of the 22nd ACM international conference on Multimedia*. 675–678. https://doi.org/10.1145/2647868.2654889

[55] Xiaopeng Jiang, Han Hu, Thinh On, Phung Lai, Vijaya Datta Mayyuri, An Chen, Devu M Shila, Adriaan Larmuseau, Ruoming Jin, Cristian Borcea, et al. 2022. FLSys: Toward an Open Ecosystem for Federated Learning Mobile Apps. *IEEE Transactions on Mobile Computing* (2022). https://doi.org/10.1109/TMC.2022.3223578

[56] Xiao Jin, Pin-Yu Chen, Chia-Yi Hsu, Chia-Mu Yu, and Tianyi Chen. 2021. CAFE: Catastrophic data leakage in vertical federated learning. *Advances in Neural Information Processing Systems (NeurIPS)* 34 (2021), 994–1006.

[57] Anna Jobin, Marcello Ienca, and Effy Vayena. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1, 9 (2019), 389–399. https://doi.org/10.1038/s42256-019-0088-2

[58] Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. 2021. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning* 14, 1–2 (2021), 1–210. https://doi.org/10.1561/2200000083

[59] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. 2020. Scaffold: Stochastic controlled averaging for federated learning. In *International Conference on Machine Learning*. PMLR, 5132–5143.

[60] Jakub Konečnỳ, H Brendan McMahan, Felix X Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. 2016. Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492* (2016).

[61] Nicolas Kourtellis, Kleomenis Katevas, and Diego Perino. 2020. FLaaS: Federated learning as a service. In *Proceedings of the 1st workshop on distributed machine learning*. 7–13. https://doi.org/10.1145/3426745.3431337

[62] Viraj Kulkarni, Milind Kulkarni, and Aniruddha Pant. 2020. Survey of personalization techniques for federated learning. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 794–797. https://doi.org/10.1109/WorldS450073.2020.9210355

[63] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. 2015. Deep learning. *nature* 521, 7553 (2015), 436.

[64] Yann LeCun, Corinna Cortes, and CJ Burges. 2010. MNIST handwritten digit database. *ATT Labs [Online]. Available: http://yann. lecun. com/exdb/mnist* 2 (2010).

[65] Li Li, Moming Duan, Duo Liu, Yu Zhang, Ao Ren, Xianzhang Chen, Yujuan Tan, and Chengliang Wang. 2021. FedSAE: A Novel Self-Adaptive Federated Learning Framework in Heterogeneous Systems. *arXiv preprint arXiv:2104.07515* (2021).

[66] Li Li, Daoyuan Li, Tegawendé F Bissyandé, Jacques Klein, Yves Le Traon, David Lo, and Lorenzo Cavallaro. 2017. Understanding android app piggybacking: A systematic study of malicious code grafting. *IEEE Transactions on Information Forensics and Security* 12, 6 (2017), 1269–1284. https://doi.org/10.1109/TIFS.2017.2656460

[67] Li Li, Duo Liu, Moming Duan, Yu Zhang, Ao Ren, Xianzhang Chen, Yujuan Tan, and Chengliang Wang. 2022. Federated learning with workload-aware client scheduling in heterogeneous systems. *Neural Networks* 154 (2022), 560–573. https://doi.org/10.1016/j.neunet.2022.07.030

[68] Li Erran Li, Eric Chen, Jeremy Hermann, Pusheng Zhang, and Luming Wang. 2017. Scaling machine learning as a service. In *International Conference on Predictive Applications and APIs*. PMLR, 14–29.

[69] Qinbin Li, Yanzheng Cai, Yuxuan Han, Ching Man Yung, Tianyuan Fu, and Bingsheng He. 2022. FedTree: A Fast, Effective, and Secure Tree-based Federated Learning System. https://github.com/Xtra-Computing/FedTree/blob/main/FedTree_draft_paper.pdf.

[70] Qinbin Li, Yiqun Diao, Quan Chen, and Bingsheng He. 2021. Federated learning on non-iid data silos: An experimental study. *arXiv preprint arXiv:2102.02079* (2021).

[71] Qinbin Li, Bingsheng He, and Dawn Song. 2021. Model-contrastive federated learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 10713–10722.

[72] Qinbin Li, Zeyi Wen, Zhaomin Wu, Sixu Hu, Naibo Wang, Yuan Li, Xu Liu, and Bingsheng He. 2021. A survey on federated learning systems: vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering (TKDE)* (2021). https://doi.org/10.1109/TKDE.2021.3124599

[73] Tian Li, Shengyuan Hu, Ahmad Beirami, and Virginia Smith. 2020. Ditto: Fair and robust federated learning through personalization. *arXiv preprint arXiv:2012.04221* (2020).

[74] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine* 37, 3 (2020), 50–60.

[75] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. 2020. Federated optimization in heterogeneous networks. In *Proceedings of the 3rd SysML Conference*.

[76] Wenqi Li, Fausto Milletarì, Daguang Xu, Nicola Rieke, Jonny Hancox, Wentao Zhu, Maximilian Baust, Yan Cheng, Sébastien Ourselin, M Jorge Cardoso, et al. 2019. Privacy-preserving federated brain tumour segmentation. In *Machine Learning in Medical Imaging: 10th International Workshop, MLMI 2019, Held in Conjunction with MICCAI 2019, Shenzhen, China, October 13, 2019, Proceedings 10*. Springer, 133–141. https://doi.org/10.1007/978-3-030-32692-0_16

[77] Xiaoxiao Li, Yufeng Gu, Nicha Dvornek, Lawrence H Staib, Pamela Ventola, and James S Duncan. 2020. Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results. *Medical Image Analysis* 65 (2020), 101765. https://doi.org/10.1016/j.media.2020.101765

[78] Zhuohang Li, Jiaxin Zhang, Luyang Liu, and Jian Liu. 2022. Auditing privacy defenses in federated learning via generative gradient leakage. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 10132–10142.
[79] Daniele Licari and Giovanni Comandè. 2022. ITALIAN-LEGAL-BERT: A Pre-trained Transformer Language Model for Italian Law. In *Companion Proceedings of the 23rd International Conference on Knowledge Engineering and Knowledge Management (CEUR Workshop Proceedings, Vol. 3256)*. CEUR, Bozen-Bolzano, Italy.
[80] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. 2020. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 22, 3 (2020), 2031–2063. https://doi.org/10.1109/COMST.2020.2986024
[81] Hao Liu, Qian Gao, Jiang Li, Xiaochao Liao, Hao Xiong, Guangxing Chen, Wenlin Wang, Guobao Yang, Zhiwei Zha, Daxiang Dong, et al. 2021. Jizhi: A fast and cost-effective model-as-a-service system for web-scale online inference at baidu. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*. Association for Computing Machinery, New York, NY, USA, 3289–3298. https://doi.org/10.1145/3447548.3467146
[82] Yang Liu, Tao Fan, Tianjian Chen, Qian Xu, and Qiang Yang. 2021. FATE: An industrial grade platform for collaborative learning with data protection. *The Journal of Machine Learning Research* 22, 1 (2021), 10320–10325.
[83] Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. 2019. RoBERTa: A robustly optimized bert pretraining approach. *arXiv preprint arXiv:1907.11692* (2019).
[84] Ziyao Liu, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao. 2022. Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data (TBD)* (2022), 1–20. https://doi.org/10.1109/TBDATA.2022.3190835
[85] Yihang Lou, Ling-Yu Duan, Yong Luo, Ziqian Chen, Tongliang Liu, Shiqi Wang, and Wen Gao. 2020. Towards efficient front-end visual sensing for digital retina: A model-centric paradigm. *IEEE Transactions on Multimedia* 22, 11 (2020), 3002–3013. https://doi.org/10.1109/TMM.2020.2966885
[86] Heiko Ludwig, Nathalie Baracaldo, Gegi Thomas, Yi Zhou, Ali Anwar, Shashank Rajamoni, Yuya Ong, Jayaram Radhakrishnan, Ashish Verma, Mathieu Sinn, et al. 2020. IBM Federated Learning: an Enterprise Framework White Paper V0. 1. *arXiv preprint arXiv:2007.10987* (2020).
[87] Lingjuan Lyu, Han Yu, and Qiang Yang. 2020. Threats to federated learning: A survey. *arXiv preprint arXiv:2003.02133* (2020).
[88] Xiaodong Ma, Jia Zhu, Zhihao Lin, Shanxuan Chen, and Yangjie Qin. 2022. A state-of-the-art survey on solving non-IID data in Federated Learning. *Future Generation Computer Systems* 135 (2022), 244–258. https://doi.org/10.1016/j.future.2022.05.003
[89] Yanjun Ma, Dianhai Yu, Tian Wu, and Haifeng Wang. 2019. PaddlePaddle: An open-source deep learning platform from industrial practice. *Frontiers of Data and Domputing* 1, 1 (2019), 105–115. https://doi.org/10.11871/jfdc.issn.2096.742X.2019.01.011
[90] Frank McKeen, Ilya Alexandrovich, Ittai Anati, Dror Caspi, Simon Johnson, Rebekah Leslie-Hurd, and Carlos Rozas. 2016. Intel® software guard extensions (Intel® SGX) support for dynamic memory management inside an enclave. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*. 1–9. https://doi.org/10.1145/2948618.2954331
[91] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. 2017. Communication-Efficient Learning of Deep Networks from Decentralized Data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. 1273–1282.
[92] Yisroel Mirsky and Wenke Lee. 2021. The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–41. https://doi.org/10.1145/3425780
[93] Dinh C Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H Vincent Poor. 2021. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal* 8, 16 (2021), 12806–12825. https://doi.org/10.1109/JIOT.2021.3072611
[94] Erik Nijkamp, Bo Pang, Hiroaki Hayashi, Lifu Tu, Huan Wang, Yingbo Zhou, Silvio Savarese, and Caiming Xiong. 2022. A conversational paradigm for program synthesis. *arXiv e-prints* (2022), arXiv–2203.
[95] Chaoyue Niu, Fan Wu, Shaojie Tang, Lifeng Hua, Rongfei Jia, Chengfei Lv, Zhihua Wu, and Guihai Chen. 2020. Billion-scale federated learning on mobile clients: A submodel design with tunable privacy. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.
[96] Curtis G Northcutt, Anish Athalye, and Jonas Mueller. 2021. Pervasive Label Errors in Test Sets Destabilize Machine Learning Benchmarks. In *Proceedings of the 35th International Conference on Neural Information Processing Systems Datasets and Benchmarks Track (Round 1)*.
[97] Sinno Jialin Pan and Qiang Yang. 2009. A survey on transfer learning. *IEEE Transactions on knowledge and data engineering (TKDE)* 22, 10 (2009), 1345–1359.
[98] Jungwuk Park, Dong-Jun Han, Minseok Choi, and Jaekyun Moon. 2021. Sageflow: Robust federated learning against both stragglers and adversaries. *Advances in neural information processing systems (NeurIPS)* 34 (2021), 840–851.
[99] Yifan Peng, Shankai Yan, and Zhiyong Lu. 2019. Transfer Learning in Biomedical Natural Language Processing: An Evaluation of BERT and ELMo on Ten Benchmarking Datasets. In *Proceedings of the 18th BioNLP Workshop and Shared Task*. 58–65. https://doi.org/10.18653/v1/W19-5006

[100] Jeffrey Pennington, Richard Socher, and Christopher D Manning. 2014. Glove: Global vectors for word representation. In *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*. 1532–1543. https://doi.org/10.3115/v1/D14-1162

[101] Bjarne Pfitzner, Nico Steckhan, and Bert Arnrich. 2021. Federated learning in a medical context: A systematic literature review. *ACM Transactions on Internet Technology (TOIT)* 21, 2 (2021), 1–31. https://doi.org/10.1145/3412357

[102] Youyang Qu, Md Palash Uddin, Chenquan Gan, Yong Xiang, Longxiang Gao, and John Yearwood. 2022. Blockchain-enabled federated learning: A survey. *ACM Computing Surveys (CSUR)* 55, 4 (2022), 1–35. https://doi.org/10.1145/3524104

[103] Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, Ilya Sutskever, et al. 2019. Language models are unsupervised multitask learners. *OpenAI blog* 1, 8 (2019), 9.

[104] Pranav Rajpurkar, Jian Zhang, Konstantin Lopyrev, and Percy Liang. 2016. SQuAD: 100,000+ Questions for Machine Comprehension of Text. In *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing*. 2383–2392. https://doi.org/10.18653/v1/D16-1264

[105] Swaroop Ramaswamy, Rajiv Mathews, Kanishka Rao, and Françoise Beaufays. 2019. Federated learning for emoji prediction in a mobile keyboard. *arXiv preprint arXiv:1906.04329* (2019).

[106] Swarna Priya Ramu, Parimala Boopalan, Quoc-Viet Pham, Praveen Kumar Reddy Maddikunta, Thien Huynh-The, Mamoun Alazab, Thanh Thi Nguyen, and Thippa Reddy Gadekallu. 2022. Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustainable Cities and Society* 79 (2022), 103663. https://doi.org/10.1016/j.scs.2021.103663

[107] Amirhossein Reisizadeh, Hossein Taheri, Aryan Mokhtari, Hamed Hassani, and Ramtin Pedarsani. 2019. Robust and communication-efficient collaborative learning. *Advances in Neural Information Processing Systems (NeurIPS)* 32 (2019).

[108] Mauro Ribeiro, Katarina Grolinger, and Miriam AM Capretz. 2015. MLaaS: Machine learning as a service. In *2015 IEEE 14th international conference on machine learning and applications (ICMLA)*. IEEE, 896–902. https://doi.org/10.1109/ICMLA.2015.152

[109] Nicola Rieke, Jonny Hancox, Wenqi Li, Fausto Milletari, Holger R Roth, Shadi Albarqouni, Spyridon Bakas, Mathieu N Galtier, Bennett A Landman, Klaus Maier-Hein, et al. 2020. The future of digital health with federated learning. *NPJ digital medicine* 3, 1 (2020), 119. https://doi.org/10.1038/s41746-020-00323-1

[110] Dumitru Roman, Sven Schade, Arne-Jørgen Berre, Nils Rune Bodsberg, and J Langlois. 2009. Model as a Service (MaaS). In *AGILE Workshop-Grid Technologies for Geospatial Applications*.

[111] Robin Rombach, Andreas Blattmann, Dominik Lorenz, Patrick Esser, and Björn Ommer. 2022. High-resolution image synthesis with latent diffusion models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 10684–10695.

[112] Holger R Roth, Yan Cheng, Yuhong Wen, Isaac Yang, Ziyue Xu, Yuan-Ting Hsieh, Kristopher Kersten, Ahmed Harouni, Can Zhao, Kevin Lu, et al. 2022. NVIDIA FLARE: Federated Learning from Simulation to Real-World. (2022).

[113] Felix Sattler, Klaus-Robert Müller, Thomas Wiegand, and Wojciech Samek. 2020. On the Byzantine Robustness of Clustered Federated Learning. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 8861–8865.

[114] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek. 2019. Robust and communication-efficient federated learning from non-iid data. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)* 31, 9 (2019), 3400–3413. https://doi.org/10.1109/TNNLS.2019.2944481

[115] Teven Le Scao, Angela Fan, Christopher Akiki, Ellie Pavlick, Suzana Ilić, Daniel Hesslow, Roman Castagné, Alexandra Sasha Luccioni, François Yvon, Matthias Gallé, et al. 2022. BLOOM: A 176b-parameter open-access multilingual language model. *arXiv preprint arXiv:2211.05100* (2022).

[116] Jonas Scherer, Marco Nolden, Jens Kleesiek, Jasmin Metzger, Klaus Kades, Verena Schneider, Michael Bach, Oliver Sedlaczek, Andreas M Bucher, Thomas J Vogl, et al. 2020. Joint imaging platform for federated clinical data analytics. *JCO clinical cancer informatics* 4 (2020), 1027–1038. https://doi.org/10.1200/CCI.20.00045

[117] Shuo Shao, Wenyuan Yang, Hanlin Gu, Jian Lou, Zhan Qin, Lixin Fan, Qiang Yang, and Kui Ren. 2022. FedTracker: Furnishing Ownership Verification and Traceability for Federated Learning Model. *arXiv preprint arXiv:2211.07160* (2022).

[118] Karen Simonyan and Andrew Zisserman. 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).

[119] IEEE Computer Society. 2021. IEEE Guide for Architectural Framework and Application of Federated Machine Learning. *IEEE Std 3652.1-2020* (2021), 1–69. https://doi.org/10.1109/IEEESTD.2021.9382202

[120] Tianxiang Sun, Yunfan Shao, Hong Qian, Xuanjing Huang, and Xipeng Qiu. 2022. Black-box tuning for language-model-as-a-service. In *Proceedings of the 39th International Conference on Machine Learning (ICML)*. PMLR, 20841–20855.

[121] Vivienne Sze, Yu-Hsin Chen, Tien-Ju Yang, and Joel S Emer. 2017. Efficient processing of deep neural networks: A tutorial and survey. *Proc. IEEE* 105, 12 (2017), 2295–2329. https://doi.org/10.1109/JPROC.2017.2761740

[122] Alysa Ziying Tan, Han Yu, Lizhen Cui, and Qiang Yang. 2022. Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)* (2022), 1–17. https://doi.org/10.1109/TNNLS.2022.3160699

[123] Ross Taylor, Marcin Kardas, Guillem Cucurull, Thomas Scialom, Anthony Hartshorn, Elvis Saravia, Andrew Poulton, Viktor Kerkez, and Robert Stojnic. 2022. GALACTICA: A large language model for science. *arXiv preprint arXiv:2211.09085* (2022).

[124] Buse GA Tekgul, Yuxi Xia, Samuel Marchal, and N Asokan. 2021. WAFFLE: Watermarking in federated learning. In *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 310–320. https://doi.org/10.1109/SRDS53918.2021.00038
[125] Omer Tene. 2011. Privacy: The new generations. *International data privacy law* 1, 1 (2011), 15–27. https://doi.org/10.1093/idpl/ipq003
[126] Nguyen Truong, Kai Sun, Siyao Wang, Florian Guitton, and YiKe Guo. 2021. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Computers & Security* 110 (2021), 102402. https://doi.org/10.1016/j.cose.2021.10240
[127] Manasi Vartak, Harihar Subramanyam, Wei-En Lee, Srinidhi Viswanathan, Saadiyah Husnoo, Samuel Madden, and Matei Zaharia. 2016. ModelDB: a system for machine learning model management. In *Proceedings of the Workshop on Human-In-the-Loop Data Analytics*. 1–3. https://doi.org/10.1145/2939502.2939516
[128] Paul Voigt and Axel Von dem Bussche. 2017. The EU general data protection regulation (GDPR): A Practical Guide. *Springer International Publishing* (2017). https://doi.org/10.1007/978-3-319-57959-7
[129] Hongyi Wang, Kartik Sreenivasan, Shashank Rajput, Harit Vishwakarma, Saurabh Agarwal, Jy-yong Sohn, Kangwook Lee, and Dimitris Papailiopoulos. 2020. Attack of the tails: Yes, you really can backdoor federated learning. *Advances in Neural Information Processing Systems (NeurIPS)* 33 (2020), 16070–16084.
[130] Lin Wang and Kuk-Jin Yoon. 2021. Knowledge distillation and student-teacher learning for visual intelligence: A review and new outlooks. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 44, 6 (2021), 3048–3068. https://doi.org/10.1109/TPAMI.2021.3055564
[131] Mei Wang and Weihong Deng. 2018. Deep visual domain adaptation: A survey. *Neurocomputing* 312 (2018), 135–153. https://doi.org/10.1016/j.neucom.2018.05.083
[132] Zhibo Wang, Mengkai Song, Zhifei Zhang, Yang Song, Qian Wang, and Hairong Qi. 2019. Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning. In *Proceedings of the 2019 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2512–2520.
[133] Wenqi Wei, Ling Liu, Yanzhao Wut, Gong Su, and Arun Iyengar. 2021. Gradient-leakage resilient federated learning. In *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 797–807. https://doi.org/10.1109/ICDCS51616.2021.00081
[134] Steven Euijong Whang, Yuji Roh, Hwanjun Song, and Jae-Gil Lee. 2023. Data collection and quality challenges in deep learning: A data-centric ai perspective. *The VLDB Journal* (2023), 1–23. https://doi.org/10.1007/s00778-022-00775-9
[135] Zhaomin Wu, Qinbin Li, and Bingsheng He. 2022. Practical vertical federated learning with unsupervised representation learning. *IEEE Transactions on Big Data* (2022). https://doi.org/10.1109/TBDATA.2022.3180117
[136] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao. 2021. Asynchronous federated learning on heterogeneous devices: A survey. *arXiv preprint arXiv:2109.04269* (2021).
[137] Jie Xu, Benjamin S Glicksberg, Chang Su, Peter Walker, Jiang Bian, and Fei Wang. 2021. Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research* 5 (2021), 1–19. https://doi.org/10.1007/s41666-020-00082-4
[138] Qiang Yang, Lixin Fan, Richard Tong, and Angelica Lv. 2021. IEEE Federated Machine Learning. *IEEE Federated Machine Learning - White Paper* (2021), 1–18.
[139] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* 10, 2 (2019), 1–19. https://doi.org/10.1145/3298981
[140] Timothy Yang, Galen Andrew, Hubert Eichner, Haicheng Sun, Wei Li, Nicholas Kong, Daniel Ramage, and Françoise Beaufays. 2018. Applied federated learning: Improving google keyboard query suggestions. *arXiv preprint arXiv:1812.02903* (2018).
[141] Xuefei Yin, Yanming Zhu, and Jiankun Hu. 2021. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)* 54, 6 (2021), 1–36. https://doi.org/10.1145/3460427
[142] Shan You, Chang Xu, Fei Wang, and Changshui Zhang. 2021. Workshop on Model Mining. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*. 4177–4178. https://doi.org/10.1145/3447548.3469471
[143] Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang. 2020. A fairness-aware incentive scheme for federated learning. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. 393–399. https://doi.org/10.1145/3375627.3375840
[144] Rafael Yuste, Sara Goering, Blaise Agüera y Arcas, Guoqiang Bi, Jose M Carmena, Adrian Carter, Joseph J Fins, Phoebe Friesen, Jack Gallant, Jane E Huggins, et al. 2017. Four ethical priorities for neurotechnologies and AI. *Nature* 551, 7679 (2017), 159–163. https://doi.org/10.1038/551159a
[145] Dun Zeng, Siqi Liang, Xiangjing Hu, Hui Wang, and Zenglin Xu. 2021. Fedlab: A flexible federated learning framework. *arXiv preprint arXiv:2107.11621* (2021).
[146] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, and Yuan Gao. 2021. A survey on federated learning. *Knowledge-Based Systems (KBS)* 216 (2021), 106775. https://doi.org/10.1016/j.knosys.2021.106775
[147] Lvmin Zhang and Maneesh Agrawala. 2023. Adding conditional control to text-to-image diffusion models. *arXiv preprint arXiv:2302.05543* (2023).
[148] Qi Zhang, Tiancheng Wu, Peichen Zhou, Shan Zhou, Yuan Yang, and Xiulang Jin. 2022. Felicitas: Federated Learning in Distributed Cross Device Collaborative Frameworks. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 4502–4509. https://doi.org/10.1145/3534678.3539039

[149] Susan Zhang, Stephen Roller, Naman Goyal, Mikel Artetxe, Moya Chen, Shuohui Chen, Christopher Dewan, Mona Diab, Xian Li, Xi Victoria Lin, et al. 2022. Opt: Open pre-trained transformer language models. *arXiv preprint arXiv:2205.01068* (2022).

[150] Tuo Zhang, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari, and A Salman Avestimehr. 2022. Federated learning for the internet of things: applications, challenges, and opportunities. *IEEE Internet of Things Magazine* 5, 1 (2022), 24–29. https://doi.org/10.1109/IOTM.004.2100182

[151] Lingchen Zhao, Qian Wang, Cong Wang, Qi Li, Chao Shen, and Bo Feng. 2021. Veriml: Enabling integrity assurances and fair payments for machine learning as a service. *IEEE Transactions on Parallel and Distributed Systems* 32, 10 (2021), 2524–2540. https://doi.org/10.1109/TPDS.2021.3068195

[152] Zhi-Hua Zhou. 2012. *Ensemble methods: foundations and algorithms*. CRC press.

[153] Hangyu Zhu, Jinjin Xu, Shiqing Liu, and Yaochu Jin. 2021. Federated learning on non-IID data: A survey. *Neurocomputing* 465 (2021), 371–390. https://doi.org/10.1016/j.neucom.2021.07.098

[154] Juncen Zhu, Jiannong Cao, Divya Saxena, Shan Jiang, and Houda Ferradi. 2022. Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)* (2022). https://doi.org/10.1145/3570953

[155] Ligeng Zhu, Zhijian Liu, and Song Han. 2019. Deep leakage from gradients. *Advances in Neural Information Processing Systems (NeurIPS)* 32 (2019).

[156] Alexander Ziller, Andrew Trask, Antonio Lopardo, Benjamin Szymkow, Bobby Wagner, Emma Bluemke, Jean-Mickael Nounahon, Jonathan Passerat-Palmbach, Kritika Prakash, Nick Rose, et al. 2021. PySyft: A library for easy federated learning. *Federated Learning Systems: Towards Next-Generation AI* (2021), 111–139. https://doi.org/10.1007/978-3-030-70604-3_5

[157] Guobing Zou, Bofeng Zhang, Jianxing Zheng, Yinsheng Li, and Jianhua Ma. 2012. MaaS: Model as a service in cloud computing and Cyber-I space. In *2012 IEEE 12th International Conference on Computer and Information Technology*. IEEE, 1125–1130. https://doi.org/10.1109/CIT.2012.228

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009