A Survey on Federated Learning for Resource-Constrained IoT Devices

Ahmed Imteaj, Urmish Thakker, Shiqiang Wang, *Member, IEEE,* Jian Li, *Member, IEEE,* and M. Hadi Amini, *Member, IEEE*

***Abstract*—Federated learning (FL) is a distributed machine learning strategy that generates a global model by learning from multiple decentralized edge clients. FL enables on-device training, keeping the client's local data private, and further, updating the global model based on the local model updates. While FL methods offer several advantages, including scalability and data privacy, they assume there are available computational resources at each edge-device/client. However, the Internet-of-Things (IoTs) enabled devices, e.g., robots, drone swarms, and low-cost computing devices (e.g., Raspberry Pi), may have limited processing ability, low bandwidth and power, or limited storage capacity. In this survey paper, we propose to answer this question: *how to train distributed machine learning models for resource-constrained IoT devices?* To this end, we first explore the existing studies on FL, relative assumptions for distributed implementation using IoT devices, and explore their drawbacks. We then discuss the implementation challenges and issues when applying FL to an IoT environment. We highlight an overview of FL and provide a comprehensive survey of the problem statements and emerging challenges, particularly during applying FL within heterogeneous IoT environments. Finally, we point out the future research directions for scientists and researchers who are interested in working at the intersection of FL and resource-constrained IoT environments.**

***Index Terms*—Federated Learning, resource-constrained IoT devices, global model, on-device training, local model, convergence.**

I. Introduction

In this section, we explain the motivation to conduct a comprehensive survey on FL for resource-constrained IoT devices, followed by recently published prior works, and differentiate how our proposed survey is necessary for the FL domain. After that, we discuss our contributions and the necessity of conducting this research. Finally, at the end of this section, we briefly highlight the organization of this paper.

Corresponding Author: M. Hadi Amini, Florida International University, Miami, FL 33199, moamini@fiu.edu

Ahmed Imteaj and M. Hadi Amini are with Knight Foundation School of Computing and Information Sciences, Florida International University, Miami, FL 33199, USA. They are also with the Sustainability, Optimization, and Learning for InterDependent networks laboratory (solid lab) at FIU.

Urmish Thakker is with Deep Learning Research, SambaNova Systems, USA.

Shiqiang Wang is with IBM T. J. Watson Research Center, Yorktown Heights, NY, USA.

Jian Li, Binghamton University, State University of New York, USA.

Manuscript received February 28, 2021.

A. Motivation

The ever-growing data collected/produced at edge devices is the result of billions of connected Internet-of-Things (IoTs) devices as every active IoT client extracts their observed data and pushes those data to the edge. The traditional machine learning (ML) approaches need to perform aggregation of that extracted data element on a data center or a single machine, and such a learning scheme is common in different AI-based giant companies such as Facebook and Google. Companies store all the data collected in their data center, where they train the respective ML model. To attain a better ML model under the conventional centralized approach, the users may need to compromise their privacy by sending private data to the data center. Such a model training strategy is privacy-intrusive, particularly when the clients need to address their personal or sensitive data to achieve a better training model.

Federated learning (FL) is such an approach that is capable of training a model, leveraging the private data of clients without ever sharing it with other entities. However, the client may possess a lack of resources to perform on-device computation and may fail to reach the target convergence within an expected time. Moreover, we may face some unique challenges that could not be observed in a traditional FL-based approach in terms of communication, computation, privacy, storage, power, and energy utilization, e.g., straggler issue, high energy consumption, handling dropped participants. This paper reveals the challenges of FL setting in such a situation and describes the impact of having such resource-constrained clients within a network by considering their practical constraints. To that end, we emphasize the open research issues in this area and enumerate numerous future directions.

B. Related works and Contributions

Numerous studies from a wide range of research disciplines, including databases, distributed systems, cryptography, machine learning, and data mining, explored FL methods from various perspectives. It is a prevailing goal to learn from the distributed dataset and simultaneously preserve privacy by not exposing the data. In 1982, a cryptographic mechanism was developed to apply on encrypted data [1]. The works of [2], [3], [4], [5], [6] are some of the early examples to discover knowledge from local data while maintaining privacy. To that end, the introduction of FL maintains privacy by storing client data only on-device, eliminates the dependency on a single server to generate prediction model by performing computation on client devices, and builds a smarter model by learning

from various client models. It is to be noted that any resource-constrained device could be a server in an IoT environment; therefore, it is not a good solution to consider such a device to store all the extracted data of the available clients and generate a model like conventional ML approach. Instead, the server can only be used to perform aggregation on the collected local models to generate an updated global model. In this paper, we focus on the deployment and implementation of FL in an IoT environment, where the IoT nodes are considered as clients with limited resources. These resources include computation power, communication bandwidth, memory, and battery power. The IoT clients may have different technical characteristics and available resources, and that is why all the clients can not be treated the same. The list of abbreviations that are used in this paper is listed in Table **I**.

Several detailed surveys on FL have already been conducted by assuming that all clients within the network are resource-unbounded. Li *et al.* [7] presented an overview of challenges, open problems, and issues associated with FL by considering the heterogeneity of devices; however, they assumed that all clients are resource-boundless. The authors of [8] focused on the categorization of FL settings while the authors in [9] presented the issues of FL in a wireless environment. Besides, a federated optimization-based framework is proposed in [10], which is constructed by addressing challenges related to both system and statistical heterogeneity. They mentioned that straggler client is responsible for increasing statistical heterogeneity which put adverse impact during convergence. By adding proximal terms during local training, they obtained faster convergence and were able to analyze the effect of heterogeneity. Another exciting paper [11] discussed FL from the perspective of mobile edge computing (MEC), including caching and communication mechanism at the edge, while a detailed survey is presented in [12] by analyzing the recent advancement and issues of FL.

There are a couple of survey papers available on FL systems, and we listed them in Table **II**. The papers in Table **II** are classified according to the area of FL and edge computing. FL survey papers [7], [8], [9], [10], [7], [12], [11] are mostly focused on FL settings, system design, and components, implementation challenges, or on recent advancements. On the other hand, edge computing surveys [13], [14], [15], [16], [17], [18], [19] are mainly conducted on edge computing infrastructure, applications including ML and AI, resource-management, wireless communication, and security and privacy issues. However, all these works considered only heterogeneity of systems or their statistical data, and did not discuss the challenges that would arise when the clients are resource-bounded. Throughout this paper, we point out the FL challenges while applying on a resource-constrained IoT environment, analyze the potential solutions towards those challenges, and reveal the future directions of this domain. This paper is mainly a critical survey on the previous works that identifies gaps in resource-constrained FL implementation. To the best of our knowledge, this paper is the first comprehensive survey on FL for resource-constrained IoT devices.

TABLE I
LIST OF ABBREVIATIONS USED IN THIS PAPER.

Abbreviation	Description
CM	Cryptographic Method
CNN	Convolutional Neural Network
CV	Computer Vision
DL	Deep Learning
DNN	Deep Neural Network
DP	Differential Privacy
DRL	Deep Reinforcement Learning
DT	Decision Tree
FedAvg	Federated Averaging
FL	Federated Learning
FLS	Federated Learning System
GAN	Generative Adversarial Network
IID	Independent and Identically Distributed
IoT	Internet of Things
LM	Linear Model
LSTM	Long Short Term Memory
MEC	Mobile Edge Computing
ML	Machine Learning
MLP	Multilayer Perceptron
NLP	Natural Language Processing
NN	Neural Network
RNN	Recurrent Neural Network
SGD	Stochastic Gradient Descent
SVM	Support Vector Machine
TFF	TensorFlow Federated
UE	User Equipment

C. Organization

The rest of this paper is organized as follows. In Section **II**, we present an overview and taxonomy of FL with a comprehensive list of existing studies. In Section **III**, we review distributed optimization and ML approaches. Section **IV** presents a detail analysis of the major challenges of FL while applying on resource-constrained devices, which is followed by Section **V**, where we discuss the potential solutions of those emerging challenges. After that, in Section **VI**, we present the existing FL applications, and in Section **VII**, we highlight the future research direction in FL-based IoT domain. Finally, in Section **VIII**, we conclude our paper.

II. AN OVERVIEW OF EXISTING STUDIES ON FEDERATED LEARNING MODELS

This section covers the definition of FL, a detailed description of the FL taxonomy, a brief highlight on the existing FL frameworks, and a comparison summary of the existing FL-based studies which are classified in terms of privacy maintenance, attack schemes, fairness, learning effectiveness, and resource utilization.

A. Definition of Federated Learning

Federated learning can be defined as a distributed machine learning approach where the clients train themselves locally without sharing their direct information to the server. By periodically updating a shared global model based on performing aggregation of each client model information, this approach trains each device to capture the global view [20]. A high-level architecture of FL process is presented in Fig. **1**. The FL process generally includes three steps:

TABLE II
COMPARING OUR PROPOSED SURVEY PAPER WITH EXISTING SELECTED SURVEYS ON FL AND MEC

Reference	Area	Published in	Year	No. of Times cited (as of 2/25/21)	Contribution	Considered FL for resource-constrained IoT?
[7]	FL	IEEE Signal Processing Magazine	2020	390	Tutorial on characteristics and implementation challenges of FL	No
[8]	FL	ACM TIST	2019	729	Discussed categorization of FL settings e.g. vertical, horizontal	No
[9]	FL	Arxiv	2019	76	Presented applications and issues of FL in wireless communications	No
[10]	FL	IEEE Communications Surveys & Tutorials	2020	197	Comprehensive survey on FL in mobile-edge computing	No
[11]	FL	IEEE Network	2019	227	Discussed on MEC, caching, and communication of FL	No
[12]	FL	Foundations and Trends® in Machine Learning	2021	456	Survey on recent advancements and open problems of FL	No
[13]	Edge Computing	IEEE	2019	289	Survey on AI for edge intelligence	No
[14]	Edge Computing	IEEE Internet of Things Journal	2017	834	Survey on edge computing infrastructure, applications, security and privacy issues	No
[15]	Edge Computing	International Journal of Machine Learning and Cybernetics	2018	54	Survey on ML applications for IoT	No
[16]	Edge Computing	IEEE Communications Surveys & Tutorials	2017	1804	Survey on resource-management in mobile edge computing and wireless communication	No
[17]	Edge Computing	IEEE Network	2018	662	Survey on DL for IoTs in MEC environment	No
[18]	Edge Computing	IEEE Access	2017	593	Survey on computation, caching, and communication strategies at mobile edge	No
[19]	Edge Computing	IEEE Communications Surveys & Tutorials	2017	1452	Survey on Computation offloading, resource-management and mobility management in edge computing	No

Step 1 (Initiate training task and global model): In the initial phase, the central server decides the task requirement and target application. A global model (W_G^0) is initialized and the server broadcasts that global model to the selected local clients that are known as participants.

Step 2 (Local model update): Each participant generates a model utilizing their local data. Upon receiving the global model W_G^t (where t denotes the t-th iteration), each client k updates its model parameters W_i^t for finding optimal parameters that minimizes the local loss function $F_k(W_k^t)$. The local optimal models are then shared with the FL server.

Step 3 (Global aggregation): After receiving the local models from the participants, the FL server performs aggregations and generates an updated global model (W_G^{t+1}). The latest global model is again shared with all the new participants.

Steps 2 and 3 are repeated until the central server reaches a convergence by minimizing the global loss function $F(W_G^t)$ which can be expressed as follows [21]:

$$\min_w f(w) = \sum_{k=1}^{N} P_k F_k(w)$$

where, N is the total number of available devices, $P_k(\geq 0)$ indicates the relative impact of each device k while satisfying $\sum_k P_k = 1$, and $F_k(w)$ is the expected prediction loss on a sample input of k^{th} device on parameter w. Each device k possesses n_k samples (where $n = \sum_k n_k$). thus, the relative impact of each local device can be expressed as $P_k = \frac{n_k}{n}$.

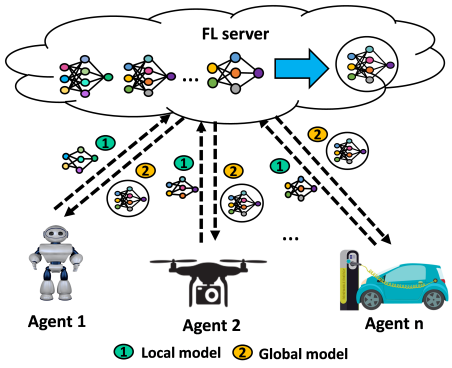


Fig. 1. Federated learning procedure considering N number of participants.

B. A Taxonomy of FL-based Systems

Federated learning system (FLS) can be categorized according to data sample, communication, prediction model, scale, privacy, and participation motivation (see Fig. **2**). In this segment, we discuss each individual categorization instance with proper examples.

1) Partitioning sample: While designing an FL model, we need to analyze the data distribution records by utilizing both the features and non-overlapped instances. We can categorize FL into **(a)** Horizontal FL, **(b)** Vertical FL, and **(c)** Hybrid FL based on the data samples distributed over networks and features space of those samples.

(a) Horizontal FL: Horizontal or sample-based FL have

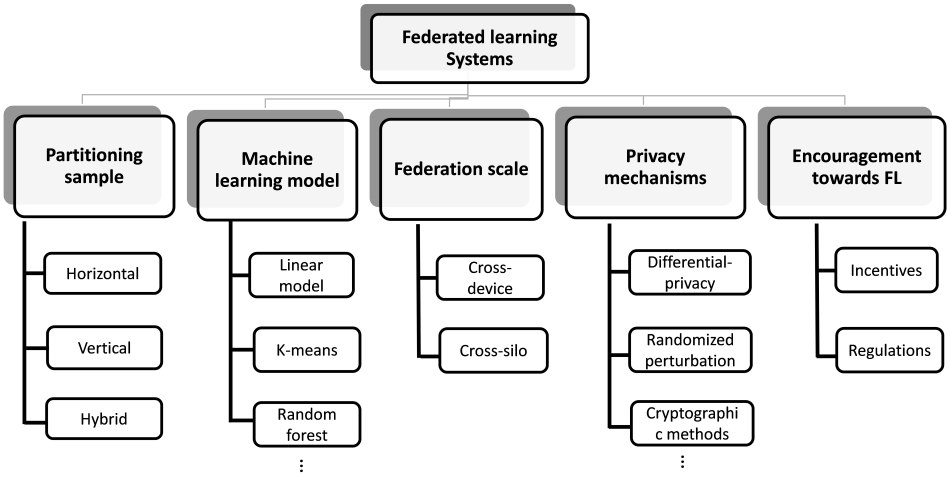


Fig. 2. A taxonomy of federated learning based systems.

different data samples, but they share the same feature space. In Fig. **3**, we can see that two client devices have a data sample that is generated using some similar applications, and each client device has an identical feature space. Each client generates a local model by utilizing the data samples and carry out the FL process. We can also consider horizontal FL from the perspective of real-life scenarios. Assume that two local superstores have different customers, thus, the user intersection set would be minimal. However, the business structure and policy of the two superstores may be similar, i.e., the feature spaces are aligned. In such a case, we can apply horizontal FL to perform the learning action. Most of the FL studies conform to the horizontal FL strategy, where the local participants train their model by sharing the same feature space, and a similar global model architecture is generated. Next-word prediction [22], wake-word detector [23], recommendation system [24] are some examples of horizontal FL.

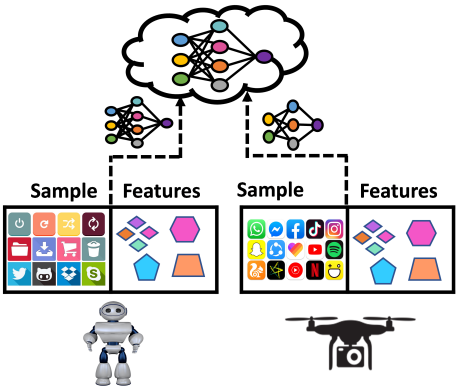


Fig. 3. Horizontal Federated Learning scenario.

(b) Vertical FL: In vertical or feature-based FL, the datasets share different sample spaces, but the sample IDs are the same (see Fig. **4**). For instance, consider a bank and a superstore in the same area. Most of their customers may be the same, but their business structure, i.e., the feature space, is different, and thus the user-space intersection is quite large. We can consider another example. Suppose we want to make a prediction model for product purchases based on user information, credit card rating, and purchasing history. In such a case, vertical FL can perform aggregation of these different features and collaboratively construct a prediction model. SecureBoost [25], FedBCD [26] are some of the examples of vertical FL.

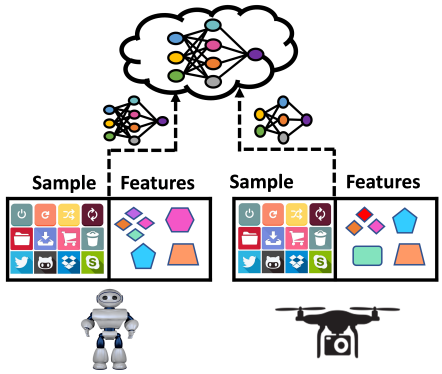


Fig. 4. Vertical Federated Learning scenario.

(c) Federated Transfer Learning (FTL): FTL [27] can be consideblack as the combination of both horizontal and vertical partitioning of data (see Fig. **5**). Horizontal and vertical FL would not be effective when two clients (A and B) have small overlapping data samples and feature space, and we need to learn all the sample labels of a client (e.g., client A). FTL is applicable in such scenarios where the data samples and feature spaces are both different in the two clients' datasets. In other words, FTL can be applied when the clients' local data can differ in terms of both data samples and feature space. For instance, a group of research labs wants to invent a COVID-19 vaccine, but their samples (e.g., testing samples may contain different coronavirus categories) and feature spaces (i.e., strategic plan, test results) may be dissimilar. Similarly, two different multinational companies located in different countries may have different customers (i.e., samples) as well as distinguishable rules and regulations (i.e., features). Due to geographical location difference of the two companies, the overlapping data sample would be

negligible, while due to different business types, there may be a very small intersection in the feature space. In such a case, FTL can be applied to handle variance in data sample and feature space while performing on-device learning. In FTL, an overlapping representation between two feature space of the clients are learned utilizing the small common data samples and each client obtains predictions for local samples using one-side features. Liu *et al.* [28] designed a framework that can learn a feature representation of multiple parties based on common instances.

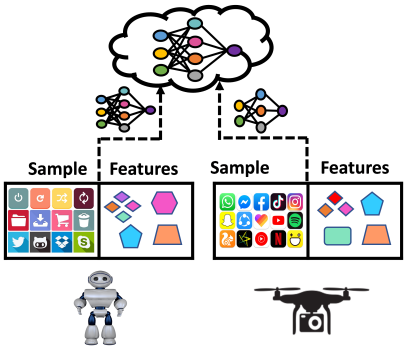


Fig. 5. Federated Transfer Learning (FTL) scenario.

2) Machine learning Model: The appropriate ML model needs to adapt based on the training objective. For instance, if we want to classify the objects from an image, we need to train the FL model using convolutional neural networks (CNN). Several existing studies develop ML models for FL settings. The most popular ML model that is used in FL is Federated Stochastic Gradient Descent (Fed-SGD) coupled with neural network (NN), e.g., image classification [20], word prediction [29], [22]. The decision tree (DT) is another popular and widely used ML method that is highly efficient for training models. In tree-based FL, a model is generated for training single or multiple decision trees. The authors in [30], [25] designed a gradient boosting decision trees (GBDTs) by considering both horizontal and vertical partitioned data schemes. Different linear models (e.g., linear regression and classification, logistic regression, support vector machine (SVM) [31], [32]) are convenient to handle. Such linear models are easier to learn than different complex models (e.g., DTs, NNs). In a nutshell, many FL applications and frameworks are proposed on FedSGD [20], [33], [21], [34]. SGD is basically a common optimization technique that can be applied in different models, including SVM, linear regression, and NN. To improve the model accuracy in a large-scale FLS and to cover the gap between FLS with state-of-the-art ML models, it is necessary to exploit the ML architecture for obtaining better FL training.

3) Federation scale: FLS can be divided into cross-silo and cross-device categories based on the scale of federation [12], [7]. This categorization is performed based on the number of clients and their data quantity.

Cross-device: In cross-device FL, the number of clients can be large, but each client has a limited size of data. Different smartphones or IoT devices can be considered as the clients of such a system, which could be millions or billions in number. Recently, Google has invented an FL-based keyboard suggestion [29] by training the model on-device of the user and aggregate the model information in the server. However, in such an approach, the clients may not be able to train themselves in a complex training environment because of resource scarcity. Thus, the server needs to be capable enough to process all the model information to generate a global training model.

Cross-silo: Cross-silo FL holds a relatively small number of clients, but they own a large amount of data. Typically, in cross-silo FL, the clients are data centers or different organizations. For instance, Amazon recommends products by training models using the collected data from hundreds of data centers, where each data center stores large amounts of data and configured with sufficient computational resources.

4) Encouragement towards FL: In real-world FL applications, the clients need encouragement or motivation to participate in the training phase and that can be carried out through regulations or incentives mechanism. For instance, Google FL keyboard suggestion [29] can not force the users to provide data, but they ensure better keyboard suggestions to the users who upload their data. Such incentives motivate the users to share information or performing on-device training.

C. Summary of Existing FL-based Studies

There have been several studies on FL due to its positive effect in terms of privacy preservation, resource utilization, and overall efficiency of the learning scheme [35]. We have extended the classification provided by [35] and presented a detailed summary of those studies in Table **III**.

We provide classification of the prior works based on two categories, i.e., FL algorithm (e.g., FedAvg [20]), and feature integration (e.g., blockchain-based FL [36]). We categorized each work according to their data partition scheme, i.e., vertical and horizontal, as discussed in Section II-B1. For the sake of simplicity, different model types, i.e., neural networks, linear models, and decision trees, are abbreviated as "NN", "LM" and "DT", respectively. We provide the model types in some cases, where the authors applied multiple ML strategies for their proposed approaches. For instance, the authors in [37] combined DP with multiparty computation to protect their system from inference threats and to generate high-quality models. We included all three model types (i.e., "NN", "LM" and "DT") for [37] as they validated their system using CNN, SVM, and DT. We also classified the existing studies based on their decision-making architecture. We realized that a major part of the existing approaches are based on server-centric design using trusted servers (e.g., [38]). However, such a server-centric decision-making architecture may face trust issues, particularly in a cross-silo FL setting. In order handle a cross-silo environment, one approach is to replace the central server while enabling each client to share their model parameters and maintaining a similar global model. Such strategies increase the computation cost and communication overhead as compared with the server-centric approaches. In Table **III**, we explore such studies (e.g., [39]) as "Client-

centric" in the "Decision-making" column. We also considered the privacy methods that are deployed in prior works and categorized them in three groups: cryptographic methods (CM), differential privacy (DP), and hashing based privacy. In CM, a cryptographic strategy is adapted to encrypt client data (e.g., tree boosting model [25]) during communication or data storage considering the security threat involved in the learning process. DP is another privacy-preserving strategy, where the patterns of groups within the dataset is shared while withholding raw data or information about any individual (e.g., [40]). Besides, some studies (e.g., [30]) considered a hashing-based privacy-preserving approach, where a hashing algorithm is applied on data to generate a hash that is used to verify data integrity. Finally, in the "Remark" column of Table **III**, we highlighted the main research directions (e.g., effectiveness, fairness, privacy, incentives) of the existing FL studies.

III. Distributed Learning and Optimization Algorithms

In this section, we discuss the areas of research related to distributed learning and optimization techniques. Even though the main focus of the paper is not in such domains, a brief highlight on these areas could motivate researchers to bring with a new or improved version of distributed learning setting or optimization techniques.

A. Federated Learning Algorithms

As we discussed earlier, after introducing FL by [20], several modified versions of the algorithms are proposed that can be effective in different circumstances. In this segment, we present some of the well-known and effective FL algorithms that would motivate researchers to introduce an improved version of FL.

1) Federated Averaging (FedAvg): FedAvg algorithm [20] performs training operation via a central server that propagates a shared global model w_t, where indicates t the communication round. However, each client orchestrates local optimization using the concept of SGD. This algorithm has five hyperparameters: a fraction of clients or, participants C that takes part in the training round, size of local mini-batch B, learning rate η, number of local epoch on the client-side before updating of the global model E, and a learning rate decay λ. The algorithm is presented in Algorithm 1. When the system starts, the global model parameter w_o is randomly initialized (line **1**). At each communication round of the server, a fraction of clients is selected (line **3**), and a random set of the client is chosen for the training phase (line **4**). Each client sends his/her local optimal model parameter, which is then aggregated onto the server (line **5-7**). The iteration period continues until a certain number of iterations, or if the update is small enough, or reaches a convergence.

2) Local Gradient Descent: Large-scale models are often constructed, and first-order techniques are applied to solve related problems as they scale well in terms of dimension and data size. One popular choice is to use the Local Gradient Descent approach, where the optimization process is divided into epochs. Each iteration initiates to perform averaging steps across available N devices. The rest of the other epoch does not involve any further communication. Each client device implements a fixed number of Gradient Descent (GD) steps (declares from the average model) using their local function independently in parallel [70]. See the details in Algorithm **2**.

Algorithm 1: Federated Averaging (FedAvg) [20]. The index of N clients are denoted by k; B represents the minibatch size of local client, E is the number of local epochs, n_k is the local examples of a client while n denotes the total data points, P_k stores a client data samples, and η represents the learning rate.

1 initialize w_o
2 for each round $t = 0, 1, 2, \dots$ do
3 $\quad c \leftarrow \max(\lfloor C \cdot N \rfloor, 1)$
4 $\quad R_t =$ random set of c clients
5 $\quad$ for each client $k \in R_t$ in parallel do
6 $\quad\quad w_{t+1}^k =$ UpdateFromClient (k, w_t)
7 $\quad w_{t+1} \leftarrow \sum_{k=1}^{N} \frac{n_k}{n} w_{t+1}^k$
8 **UpdateFromClient** (k, w) : // Run on client k
9 $\quad Batch \leftarrow$ (split P_k into batches of size B)
10 $\quad$ for each local epoch i from 1 to E do
11 $\quad\quad$ for batch $b \in Batch$ do
12 $\quad\quad\quad w \leftarrow w - \eta \nabla \ell(w; b)$
13 $\quad$ return w to server

Algorithm 2: Local Gradient Descent [70]. $\eta > 0$ represents the learning rate, and t_p denotes a particular communication time and g indicates fixed number of Gradient Descent (GD) steps.

1 Initialize vector w_0
2 Initialize $w_0^k = w_0$ for all $k \in [N] \overset{\text{def}}{=} \{1, 2, \dots, N\}$
3 for $t = 0, 1, 2, \dots$ do
4 $\quad$ for $k = 1, 2, \dots, N$ do
5 $\quad\quad w_{t+1}^k =$

$$\begin{cases} \frac{1}{N} \sum_{g=1}^{N} \left(w_t^g - \eta \nabla f_g \left(w_t^g \right) \right), & \text{if } t = t_p,\ p \in \{1, 2, \dots\} \\ w_t^k - \eta \nabla f_k \left(w_t^k \right), & \text{otherwise} \end{cases}$$

6 $\quad$ end for
7 end for

3) FedProx: In FL settings, the clients may need to perform a nonuniform amount of tasks that can handle the negative effect of system heterogeneity. Still, too many clients' updates can diverge the overall methods in the results of underlying heterogeneous data. The authors in [21] proposed an algorithm named *FedProx* that is particularly useful for resource-constrained FL-based IoT environment. They enable variable local updates from the participated devices by adding a proximal term within the local subproblems. The proximal term is useful in two aspects. First, it limits the client's local updates to address the statistical heterogeneity issue. Second, it helps incorporate a variant amount of clients to work safely. We summarize the technique in Algorithm **3**.

TABLE III
COMPARING THE EXISTING FEDERATED LEARNING LITERATURE.
NN: NEURAL NETWORKS, **DT**: DECISION TREE, **LM**: LINEAR MODEL, **DP**: DIFFERENTIAL PRIVACY, **CM**: CRYPTOGRAPHIC METHOD.

Approach	Category	Data partition	Model type	Decision-making	Privacy	Remark
FedAvg [20]	FL-based Algorithms	Horizontal	NN*	Server-centric	–	SGD-based
Residual FL [41]			LM*			
Agnostic FL [38]			NN, LM			
FL SVRG [42]			LM			
FedProx [21]			–			
FedBCD [26]		Vertical	NN			
Bayesian FL [43]		Horizontal				NN-specialized
FedMA [34]						
Tree-based FL [39]			DT*	Client-centric	DP*	DT-specialized
SimFL [30]					Hashing	
FedXGB [44]				Server-centric	CM*	
FedForest [45]						
SecureBoost [25]		Vertical				
Ridge Regression FL [32]		Horizontal	LM			LM-specialized
PPRR Linear Regression FL [46]						
Linear Regression FL [47]		Vertical				
Logistic Regression FL [31]		Horizontal				
Federated MTL [48]					–	Multi-task learning
Federated Meta-Learning [24]			NN			Meta-learning
Personalized FedAvg [49]						
Lifelong FL [50]						Reinforcement learning
FedNAS [51]						Efficiency improvement
Structure and sketched updates [33]	Functionality Upgrade					Efficiency improvement
Multi-Objective optimization FL [52]						
Federated distillation [53]						
FL STC [54]						
Client-Side DP FL [40]					DP	Privacy guarantees
FedSel [55]						
FL Language Models [56]						
Federated Extra-Trees [57]			LM			
FL Scalar DP[58]			LM, NN			
Secure Aggregation FL [59]			NN		CM	
SPC+DP FL [37]			LM, DT, NN		CM, DP	
Backdoor FL [60]			NN		–	Attacks
Adversarial Lens FL [61]						
Distributed Backdoor [62]						
Fair-allocation FL [63]			LM, NN			Fairness
FedCoin [64]			LM			Incentives
Blockchained FL [36]						
Contract Theory FL [65]						
Client Selection FL [66]			NN			Edge computing
Adaptive FL [67]			LM, NN			
LEAF [68]	Benchmark		–	–		benchmark
Revocable FRF [69]						

Algorithm 3: FedProx [21].

for $t = 0, \dots$ do
  Server randomly chooses a subset R_t of N devices (each client k is chosen with probability P_k)
  Server sends latest global model w_t to all chosen clients
  Each device $k \in R_t$ finds a w_{t+1}^k where, $w_{t+1}^k \approx \arg\min_w h_k(w; w_t) = F_k(w) + \frac{\mu}{2} \|w - w^t\|^2$
  Each device $k \in R_t$ sends w_{t+1}^k back to the server
  Server aggregation, $w_{t+1} = \frac{1}{N} \sum_{k \in R_t} w_{t+1}^k$
end for

4) q-FedAvg: Though the state-of-the-art FedAvg significantly accelerates the convergence speed [20], it fails to allocate client resources fairly (performs uniform allocation of resources). The allocation of resources is significantly crucial when we consider resource-constrained devices for the FL process. With this motivation, the authors in [63] proposed q-FedAvg algorithm that can impose fairness based on the clients' contributions. In q-FedAvg algorithm, for a given cost functions F_k and parameter $q > 0$ (which is the fairness amount we wish to impose), the FL objective is defined as:

$$\min_w f_q(w) = \sum_{k=1}^{m} \frac{p_k}{q+1} F_k^{q+1}(w),$$

where $F_k^{q+1}(\cdot)$ denotes $(q+1)$ as a power of $F_k(\cdot)$. Here, q is a parameter that tunes the amount of fairness we wish to impose. When $q > 0$, it prevents the execution of local SGD. To solve the issues of the local updating approach, particularly while allocating resources, the authors in [63] proposed a heuristic

solution by replacing gradient with the client's local updates obtained by running SGD on each local device. The algorithm is depicted in Algorithm **4.**

Algorithm 4: q-FedAvg [63]

for $t = 0, 1, 2, \cdots$ do
  Server randomly selects a subset R_t of N devices (each client k is chosen with probability P_k)
  Server sends latest global model w_t to all chosen clients
  Each chosen client device k updates w_t by performing SGD for E epochs with η to obtain $\bar{w}_{t+1}^k$
  Each selected client k computes:
    $\Delta w_t^k = L\left(w_t - \bar{w}_{t+1}^k\right)$
    $\Delta_t^k = F_k^q\left(w_t\right)\Delta w_t^k$
    $h_t^k = qF_{q-1}^k\left(w_t\right)\left\|\Delta w_t^k\right\|^2 + LF_q^k\left(w_t\right)$
  Each selected client k sends his/her parameters Δ_t^k and h_t^k to the server
  Server update: $w_{t+1} = w_t - \frac{\sum_{k\in S_t}\Delta_t^k}{\sum_{k\in S_t}h_t^k}$
end for

B. Distributed Learning

As discussed in Section **II**, the central server of the FL process orchestrates the learning process by managing the contributions of its clients. Thus, it can be considered as a single point of failure (see Fig. **6(b)**). Though large organizations and companies may afford to place a powerful, robust, and secure central server to carry out the training process, all types of sectors can not adapt that [71]. Besides, some clients within the network can slow down the overall process [72], [73]. The main idea of fully distributed and decentralized learning is peer-to-peer communications of the clients that eliminates the central server (see Fig. **6(c)**). In contrast, on-device training without learning from a server or its peers is shown in (see Fig. **6(a)**). In these figures, the communication topology looks like a connected graph, where each node represents a client, and the line between two nodes specifies a communication channel. In a distributed learning mechanism, each round corresponds to a local update by the clients and information exchange with peers. Though we do not have any global model or state as in standard FL, still, we can design the process such that all clients reach a global solution through local models. The local models can be converged through on-device training and learning from their peers [12]. Fully decentralized SGD and other optimization algorithms are recently getting popular for scalability in large-scale systems [74] and decentralization of networks devices [71], [75], [76], [77], [78], [79], [80], [81], [82]. Note that even in the decentralized distributed setting, a central authority may need that will be in charge of setting up system configuration, learning tasks, hyper-parameters, algorithm selection, or resolve system failure. A degree of trust needs to establish among the clients to replace the central authority. Alternatively, such decisions can be made by a leader client, through a collaborative consensus scheme [83], [56], [59].

C. Distributed and Federated Optimization

The early trend of distributed optimization was naive distributed variants of corresponding serial algorithms, which is often inefficient in terms of communication. The second trend is to design communication-efficient algorithms. The idea is to perform a lot of local computation that is further followed by a communication round. Such technique is useful in practice and Distributed Approximate Newton (DANE) [84], CoCoA [85], DiSCO [86] are some of the examples of such distributed optimization techniques. In distributed optimization, the data-centers possess huge data with relatively few devices. Later on, federated optimization is introduced to protect privacy in a better way. In that concept, the users keep their data private and provide the computational power of resources. Consequently, the data points are relatively smaller, the number of devices is huge, and data patterns vary on different devices.

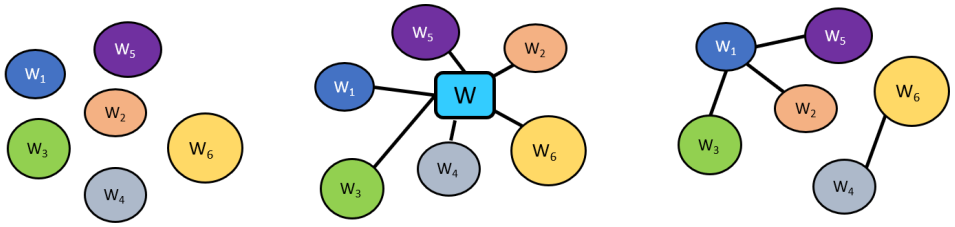
There have been various methods to deal with distributed online optimization and distributed learning, including Stochastic Variance Reduced Gradient (SVRG) [87], [88], DANE [84] that is particularly for distributed optimization, naive Federated SVRG and Federated SVRG (FSVRG). The desirable properties while designing an algorithm for unbalanced, non-IID, and massively distributed can be stated as follows [33]:

1) An algorithm stays there in case it is initialized to the optimal solution.
2) In case a single node possesses all data, the algorithm should converge in $\mathcal{O}(1)$ communication rounds.
3) If all available features within the system occur on a single node, then the problem can be decomposed, and the algorithm is supposed to converge in $\mathcal{O}(1)$ rounds of communication.
4) If we assume that each node has an identical dataset, then the algorithm converges in $\mathcal{O}(1)$ communication rounds.

Property **(1)** is valuable for any optimization setting whereas properties **(2)** and **(3)** are applicable in federated optimization systems (e.g. unbalanced, non-IID, massively distributed). To the end, property **(4)** is an extreme case, particularly for a distributed optimization setting where we have a large number of IID data per device.

IV. Learning on Resource-Constrained Devices

Before discussing the challenges associated with resource-constrained devices, it is essential to understand the definition of on-device learning of edge devices clearly. We can define an edge device as a resource-constrained entity with limited computational power, storage capacity, transmission range, and battery [89]. We consider an object as an edge device if it cannot be integrated with additional resources, i.e., the device resources can not be increased or decreased. For instance, a workstation cannot be considered as an edge device as we can integrate additional resources within that device. However, a manufactured robot can be considered as an edge device since we cannot directly incorporate any more support to the robot's capability. If we look at our today's IoT world, then we can see the use of resource-constrained devices in every aspect, from monitoring the environment to controlling human life.



(a) Learn model on device, not learn from peers.

(b) Learn through global model and on-device model.

(c) Learn model on device and from peers.

Fig. 6. Different modeling approaches in federated networks. Depending on properties of the data, network, and application of interest, one may choose to (a) learn separate models for each device, (b) fit a single global model to all devices, or (c) learn related but distinct models in the network.

Within such an IoT environment, edge devices are utilized as they are smaller in size and are more transportable. Different kinds of robots, drones, and smartphones can be considered as edge devices possessing limited resources that communicate remotely. To attain optimal service performance from such IoT components, we need to train those edge devices that prevent them from being stragglers during the learning process. Those devices should be trained with diversified sample environments to perform accurate prediction in a various of testing data. It is not feasible to train those edge devices with a large dataset due to their limited resource availability. In this section, we discuss the potential challenges we may face while considering such resource-bounded IoT nodes in the FL environment.

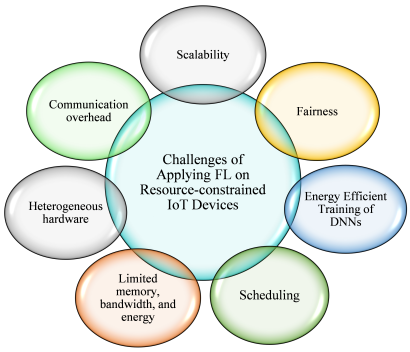


Fig. 7. Core challenges of FL considering resource-constrained IoT devices.

A. Communication Overhead

Communication overhead is considered one of the major challenges in an FL-based IoT environment. The communication cost mainly increases due to the large sizes of data passing during the process and the iterative and non-optimized approach of conducting communication between the server and the clients. This problem becomes adverse when clients possess insufficient resources. For instance, if a client possesses limited bandwidth, then the client would not be able to communicate with the FL server effectively during model training. Similarly, if a client has weak processing capability, then performing an assigned local computational task would be infeasible for that client. Further, there could be large data across the network that could produce a large model size, and eventually, the resource-constrained clients would struggle in dealing with such a large model. To carry-out efficient training in a large data network, the client models need to be compressed so that the clients do not have to waste extra resources in training a large model. If a majority of the FL clients are resource-constrained, then the FL process requires more server-client interaction to reach a target convergence, and the clients would not be able to afford such a high communication cost. While frequent FL server-client interaction can reduce convergence time, recurrent communication can encounter high costs. Therefore, it is required to design an effective optimization technique that can handle the trade-off between communication overhead and resource utilization of an FL setting. The authors in [90] analyzed the trade-offs of communication and resource expense; however, they did not address the complexity of the clients' local model solutions.

B. Heterogeneous Hardware

The training phase of FL can run on multiple devices which may belong to various generations of products. Such product variation creates a network that consists of heterogeneous devices with a discrepancy in computational ability, memory size, or battery life. Therefore, the training period may vary significantly across clients, and it is not effective to consider all participants with the same scale. To achieve optimal results in training, FL needs to be aware of heterogeneous hardware configurations [7]. The proficient and trusted clients need to be selected in the training phase considering system requirements. After selecting suitable clients, it may be possible that a model fails to send its local model due to connection error or out of a battery issue (see Fig. **8**). However, due to system requirements (e.g. memory, bandwidth), most of the clients may not be able to be a part of the training round. Besides, it is possible that the majority of proficient clients go out of networks, and we may end up with a few clients that do not satisfy system requirements. Thus, carrying out the FL training process in such a situation is challenging.

C. Limited Memory and Energy Budget

In Section IV-B, we discuss heterogeneous hardware challenges, and in this segment, we describe the memory availability and energy budget issue across heterogeneous FL clients. Any FL client may have a very limited memory size, or a client having a larger memory size may not have space. Besides, the FL clients may have a preset energy budget,

which may not fulfill the system requirements during the training process. While limited computational ability takes more processing time, memory shortage leads to over-flooding of the device. Such situations encounter extra communication overhead and degrade the system performance. Hard *et al.* [22]

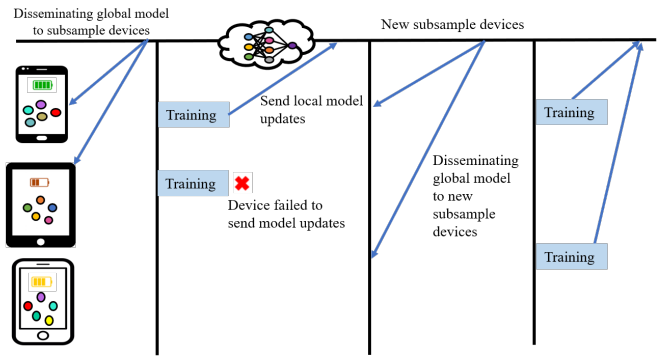


Fig. 8. Systems heterogeneity scenario in Federated Learning.

pointed out the necessary hardware requirement, including the required memory size and processing ability during their implementation of next-word prediction on the keyboard. They mentioned that to simulate their application, the device should have a minimum of 2 GB of free memory, whereas many IoT devices hardly possess even free megabytes of memory. Considering such memory constraints, the authors in [91] proposed an approach of distributing shards of data across FL clients to attain the target model swiftly. In their approach, they selected proficient clients who possessed a greater memory size, energy budget, higher bandwidth, and processing capability. However, they did not discuss the memory management and data handling for FL clients with limited available memory. We can manage such memory limitation by storing limited sizes of data, and in case of memory shortage, data aggregation technique can be applied to avoid memory outburst. The authors in [92], [93], [67], [94] analyzed hardware limitation challenges in the implementation of FL by considering Raspberry Pi and other types of resource-limited clients. They studied the feasibility of implementing FL on resource-constrained edge devices but did not cover the way of leveraging optimal memory requirement and quantifying energy budget throughout the FL process.

D. Scheduling

Existing federation optimization techniques can be classified into synchronous and asynchronous training. The authors in [42], [33], [20], [95] focused on analyzing federated optimization that considers synchronous communication during training between the FL server and clients. In every training round, a subset of clients is triggered to perform a task. However, device or network issues can compel some clients to be unresponsive in the process, and the server needs to wait until getting a response from sufficient clients. Otherwise, the server drops that epoch as time-out and proceeds on to the next iteration. On the contrary, asynchronous optimization enables FL participants to directly send gradients to the FL server after every local update that is excluded in synchronous FL optimization. Asynchronous training [96] is applied in some recent works because of its faster convergence when communication latency is comparatively higher and heterogeneous across the clients. The authors in [97], [98], [99] analyzed asynchronous FL training with provable convergence by combining it with federated optimization. We present the synchronous and asynchronous FL behaviors in Fig. **9**.

In an FL process, it is indispensable to set the training phase of the participants, which is called scheduling. Scheduling is explicitly important when there exists resource-constrained IoT devices within the networks, and frequent interaction with the server costs more resources. Optimized scheduling can play a vital role in minimizing energy consumption as well as utilizing less bandwidth. Scheduling should be carried out in such a manner so that there remains less possibility of possessing old data by the participants. It is possible that some participants can generate local models utilizing their old data repeatedly while skipping new data [95]. Such a situation can lead to resource-wastage without bringing any variations or improvements in the model. Besides, any participant can collect data by using a malicious application, and recognizing such harmful application data can be a challenge as it needs extra resources. Moreover, improper scheduling can lead to slow learning or straggler issues, which is considered as one of the reasons of a performance bottleneck, particularly for a resource-constrained FL-based IoT environment. By straggler clients, we mean the IoT devices that fail to respond within a specified period while the other clients react to the server successfully. Due to the slow response, the server needs to wait for the straggler client model, resulting in a delay in performing aggregation of the model parameters in synchronizing FL. If the number of such straggler clients is high, then the overall model convergence would be at stake [100], [101]. Besides, in the conventional FL approach, the straggler clients are simply dropped [102]. However, if a significant portion of the clients is straggler, and we drop all of them, then the model quality would be extremely low [94]. Therefore, it is challenging to leverage a proper scheduling and guarantee model convergence even when a major portion of the clients are stragglers.

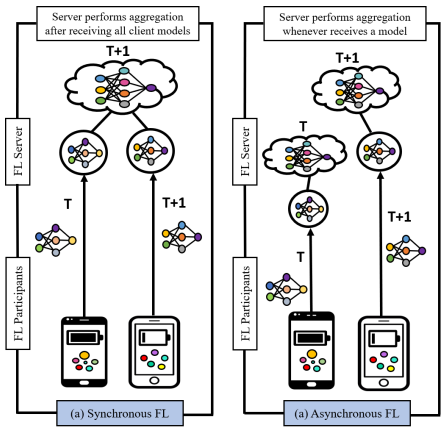


Fig. 9. Difference between a synchronous and asynchronous FL.

E. Energy Efficient Training of DNNs

Deep neural networks (DNNs) are applied in various artificial intelligence and deep learning-based applications where the sample dataset is large. A lot of edge applications are now using DNN based algorithms [103], [104] and there is an increasing focus on making DNN inference efficient on edge devices [105], [106]. Additionally, FL requires edge devices to perform on-device training. However, training DNNs requires high computation capability, large memory and energy availability, and most of the IoT clients may lack such system configurations. Wu *et al.* [107] proposed an approach to reduce the cost of training and inference by using lower-bitwidth integers for both stages of the application. Jiang *et al.* proposed an efficient learning technique using pruned models, while the authors in [108] proposed a strategy to generate a high-quality ML model through on-device model output, parameters, and data aggregation. Another interesting approach to training high capacity models having fewer parameters is discussed in [23]. Specifically, in case the size and features of the training dataset is huge, we need to devise energy-efficient training on resource-constrained clients, perhaps a challenging approach.

The memory requirement of the training phase of DNN has been an issue that is well studied for training on large GPU and CPU server clusters. Training on edge devices can benefit by adapting techniques that have served well in managing this problem in the server context like efficient gradient checkpointing [109], tensor rematerialization [110] and recompute [111]. The authors in [112] proposed another way to reduce the memory required for on-device training by introducing a lite residual module that can be adapted to new data. By only changing this lightweight module and keeping the other parameters constant, they reduce the memory requirement of the training process.

Another factor that can cost extra energy resources during training is mislabeled or unlabeled training data, particularly when the size of the dataset is large. The existing FL-based applications consider that all extracted data are appropriately labeled. Nevertheless, this assumption can be disproved if the collected data is mislabeled via security holes or unlabeled due to a network connection error. Mislabeled data would generate a wayward model that eventually affects the global model update. In case we have unlabeled data, it costs extra resources to put labels, and that would be crucial for resource-constrained IoT settings. Gu *et al.* [113] proposed a framework to identify the mislabeled data which are injected through data poisoning attacks. Using representation-based fingerprints, they detect the malicious or compromised participant's data label while coming across erroneous predictions during runtime. Tuor *et al.* [114] proposed a method of finding and ignoring irrelevant data (possibly due to mislabelling) from FL. To come up with a solution of unlabeled data, the authors in [115] proposed a strategy to make labeling of unlabeled data through applying collaborative learning with the neighbor clients. Implementing the same procedure for resource-constrained clients would be challenging in real-time as it needs additional resources.

F. Fairness in Federated Learning

Fairness in the FL process means the distribution of client resources in an equitable manner. We can think of the global model as a resource, which is responsible for serving the client devices. However, the service that each user receives needs to be fair, i.e., the resource allocation and accuracy distribution across the client devices are unprejudiced. A minimax optimization framework named Agnostic FL [38] is developed, which can optimize the target distribution of the centralized model and is formed as a mixture of participated client distributions. However, their proposed approach is applied only at small scales. The authors in [63] used a α-fairness metric and proposed a q-Fair FL to ensure fair accuracy distribution. Their proposed strategy can tune resource distribution by considering the desired amount of fairness. A collaborative fair FL framework is proposed in [116], which utilizes client reputation and compels them to converge to different models. They achieved fairness without degrading predictive performance. In [117], an FL-based client selection process is investigated to minimize clients' model exchange time that guarantees long-term, flexible fairness in the presence of rigid system constraints. However, they could not figure out a way to quantify how the fairness factor would impact the convergence speed and final target accuracy.

Moreover, some recent works on the optimization of resource allocation with incentive mechanisms for the FL process can be found in [118], [117], [119], [120], [121], [122]. The authors in [118] designed an incentive-based FL model via a Stackelberg game for motivating client participation in the learning process. With the motivation of addressing issues related to costs and mismatch between client's contributions and receiving incentives, the authors in [117], [123] proposed a payoff-sharing scheme named Federated Learning Incentivizer (FLI). Their proposed scheme can dynamically distribute a given budget among data owners by ensuring maximization of collective utility and minimization of inequality, considering the received rewards and waiting time for receiving those rewards. A trust and incentive-based FL model is designed in [120], where they proposed to add local computation results of the clients using the concept of blockchain consensus to establish a public auditable and decentralized FL ecosystem. In their model, honest clients can receive incentives while malicious clients are punished heavily in terms of payoffs. Besides, the authors in [121] proposed a strategy of estimating the contributions of each client in an FL process and provide incentives accordingly, reducing the communication and computation overhead. Similarly, the authors in [122] designed a client contribution-based incentive method for FL but using the concept of Vickrey-Clarke-Groves (VCG) mechanism.

After analyzing the above-mentioned FL-fairness strategy, we can conclude that any client within an FL-IoT environment may have resource scarcity. Therefore, designing a fair resource allocation and distribution scheme is necessary to reduce communication overhead, computation power and to achieve higher accuracy. We need to check clients' activities, resource status, and contributions towards model convergence to ensure fairness in FL resource allocation.

G. Scalability of Federated Learning

In a realistic FL-based IoT environment, we may observe a large number of IoT devices that are heterogeneous in nature and possess limited resources. In such a situation, FL training can be executed through effective client selection and optimal resource utilization. The authors in [124] developed a framework via joint learning and establishing wireless communication among the FL clients. They discussed that the FL process can be hampered due to packet errors or the unavailability of wireless resources (e.g., limited wireless bandwidth). Considering the factors, they formulate an optimization problem considering joint learning, resource block allocation, and effective user selection with a goal of minimizing FL loss function. They derive a closed-form expression for FL convergence by considering the effect of the wireless channel. Their proposed framework ensures scalability and sparsification. The authors in [66] design a client selection protocol, using FL edge server. Their proposed model can manage the communication resources between the FL server and the clients, choosing clients based on their resource conditions. Besides, an activity and resource-aware FL model is presented in [125]. They proposed a strategy of examining client's resources and assigning trust scores to clients as per their contributions towards model convergence. On the basis of sufficient resources and a higher trust score, they only select a subset of eligible clients for the training round from a large number of available clients. Their proposed model ensures scalability, robustness, and sparsification of the FL process. The authors in [126] proposed a selective client model aggregation-based FL framework for vehicular edge computing. Instead of a random selection of FL clients, they leverage a technique of selecting clients based on contract theory. Moreover, a tri-layer lightweight FL framework is proposed in [127] that is capable to handle a large number of clients and their huge data streams across the networks. They shrink large model size through pruning mechanism, select clients based on their resource status and previous activities, handle divergent local model update, and also allow a variable local model update. Their proposed framework ensures scalability, quantization, robustness, and sparsification.

H. Privacy Issues

In federated settings, we keep the raw data of each client on-device due to privacy concerns. However, it is possible to leak sensitive information [128], [129], [58], [130] through sharing model update during the training process. For instance, the authors in [129] presented that sensitive patterns (e.g., credit card numbers) can be extracted from a user-trained model based on recurrent neural networks. In the case of having sensitive datasets distributed across several data owners, privacy can be preserved via Secure Multiparty Computation (SMC) or Secure Function Evaluation (SFE). The protocol outcome enables multiple data owners to collaboratively agree to generate a function without leaking any information [131], [132], [133]. Though several privacy definitions for FL are stated in [40], [134], [58], [135], [136], [129], [137], [138], [56], [139], we can classify them as global and local privacy. In the global privacy setting, the server is assumed to be trusted, and local model updates are private. In local privacy, individual local model updates are generated on the client-side and aggregated on the server. In Table **IV**, we show key ideas of some existing FL-based privacy-preserving approaches. However, due to the presence of resource-constrained devices, the existing privacy-preserving FL algorithms may not be suitable for running on those devices. Thus, beyond ensuring rigorous privacy guarantees, novel methods need to be designed that are communication-efficient, computationally cheap, and capable of handling dropped participants.

V. Potential Solutions of Emerging Challenges in Deploying Federated Learning Algorithms on Resource-Constrained IoT Devices

In the previous section, we explored the implementation challenges of the FL process during on-device training with resource-scarce devices. A clear direction towards possible solutions for those emerging challenges can be effective in future research of this domain. This section describes the existing works and possible solutions of emerging challenges during training of resource-constrained devices in an FL environment.

A. Deploying Existing Algorithms to Reduce Communication Overhead

We explored a couple of key approaches that aim to reduce communication costs and can be classified into three categories: decentralized training, model compression, and importance-based updating. The integration of such strategies can be useful to overcome the trade-offs and shortcomings in this area. Haddadpour *et al.* [91] proposed an approach to infuse redundancy among the clients to bring diversity and reach convergence taking less communication round. Chen *et al.* [124] also designed a framework of joint-learning by considering the effect of wireless factors on participants in the FL scenario. Some of these methods adapted model compression strategies, but those methods may deteriorate model accuracy and encounter high computational costs. Such trade-offs are empirical, i.e., we need to conduct several local training rounds to find an optimal number of iterations before making a communication. FL method can be more scalable if we can apply effective optimization techniques that are formalized theoretically, and implemented and tested empirically. Apart from compressing the model size, FL approaches can be motivated by MEC paradigms and their applications. For instance, the authors in [147] considered an intermediate model aggregator for reducing instances during device-cloud communication. However, their model costs more time to converge when the number of clients or edge servers increased. The situation becomes adverse when there exists non-IID data across the network. Through multi-task learning [48], such a statistical challenge can be handled. Moreover, FL models can be exploited to efficiently utilize the storage and computing power for facilitating efficient FL.

To reduce communication overhead, the authors in [148], [149] discussed infusing redundancy among the client dataset to reach convergence with fewer communication rounds. In

TABLE IV
EXISTING FL-BASED PRIVACY PRESERVING APPROACHES.

Approaches	Ref.	Key ideas
Client-side DP	[40]	Adapting dynamic DP-preserving technique during decentralized training.
mGAN-AI	[140]	Designed a framework by incorporating GAN with multi-task discriminator to differentiate category, and client identity within input samples.
No-Peek	[141]	A survey on differentially private FL-based privacy-preserving techniques.
Hybrid FL	[37]	Combine SMC with DP to obtain stronger privacy and produce a model with high accuracy.
NbAFL	[142]	Designed a framework based on DP to add artificial noises at the client side before performing model aggregation, and analyze algorithms and performance of DP in FL.
PEFL	[143]	Presented a privacy-enhanced FL framework to protect local model update in presence of an untrusted server using Paillier homomorphic cryptosystem.
Wireless DP	[144]	Analyzed how superposition properties of wireless can be beneficial for privacy.
Fog FL	[145]	Enabled IoT data to satisfy ε-DP to prevent data and model attacks.
TEE FL	[146]	Based on Trusted Execution Environment (TEE), designed a training-integrity protocol that can preserve privacy and ensures integrity in deep learning processes.

Fig. **10**, we see that a particular data collection point $\mathcal{L}_1$ is used by two clients $\mathcal{D}_1$ and $\mathcal{D}_4$. Similarly, other data collection points i.e., $\mathcal{L}_2$, $\mathcal{L}_3$ and $\mathcal{L}_4$ are utilized by $\mathcal{D}_1$ and $\mathcal{D}_2$, $\mathcal{D}_2$ and $\mathcal{D}_3$, and $\mathcal{D}_3$ and $\mathcal{D}_4$, respectively. This setting leads to infusing redundant data samples among the client devices. According to

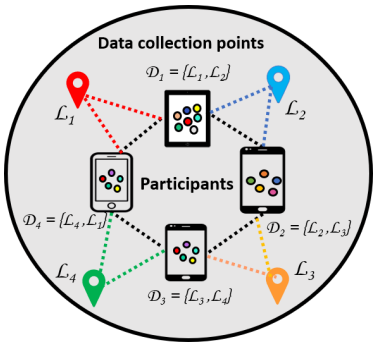


Fig. 10. Infusing data redundancy through overlapping data collection.

[33], [150], a novel approach is proposed to share compressed sizes of message and carry out the reduced number of communication rounds to attain the target model. With the same motivation, the authors in [151] applied lossy compression and federated dropout to train a smaller subset of local clients and reduce client-to-server interaction and local computation (see Fig. **11**). Though frequent communication may accelerate convergence, recurrent interaction incurs more communication costs. Every time a client interacts with the server, it has to compromise its resources. To handle the limited resources of the clients, a resource-optimization algorithm is necessary to consider such a trade-off. In this regard, the authors in [90], [152], [153], [26], [154], [155], [156] studied the relation between communication cost and effective resource utilization, though they did not discuss the complications of the local problem's solution. Wang *et al.* [67] presented a distributed control algorithm for minimizing the training loss under a given resource budget. Besides, the authors in [11] designed a framework to exchange learning parameters of the clients through the collaboration for generating better local training models. Hence, this reduces communication overhead and ensures both system and application level improvement, which generates additional energy cost. A detailed discussion on the trade-offs between FL training period and energy requirement cost can be seen in [157], [115], [158], [159]. They minimized the weighted sum of the training completion period and energy consumption, applying an iterative algorithm. In the case of delay-sensitive scenarios, they adjusted the weights so that FL participants would expend more energy to achieve time minimization.

However, most of the studies that we discussed do not consider the heterogeneity of client resources. Due to such heterogeneity, some of the approaches can not be adapted in such a resource-constrained FL-based IoT environment. For instance, the key idea of [20] was to allow for more computation on the mobile-edge side, e.g., by conducting more local updates before interacting with the server. Such an application requires processing power, which may not be feasible for IoT clients with weak-processing units. Finally, the resource-limitations may cause a straggler effect.

B. Convergence Guarantee in Asynchronous FL

In Section IV-D, we highlighted the difference between synchronous and asynchronous communication. Most of the existing FL approaches are implemented on the concept of synchronous FL, where the global model aggregation depends on the receiving of all the local model parameters of the participants. Previous works obtained fast convergence in such synchronous FL procedures, as they assumed all participants have sufficient resources (e.g., computation, bandwidth, memory). In consequence, even the slowest participant does not affect much the overall accuracy; and eventually, the model convergences. On the other hand, in asynchronous FL, the server performs aggregation whenever a model is received and may include a participant in the middle of the training phase. This approach enables scalability within the system and reduces the straggler impact, but cannot guarantee convergence. In Table **V**, we point out the key ideas of different asynchronous FL-based approaches. Sprague *et al.* [160] analyzed the issues of ensuring convergence of asynchronous FL but did not present a solution to overcome such issues. The authors in [97] proposed asynchronous federated optimization, [160], [161] discussed on the asynchronous FL for geospatial applications, [162], [163], [164] proposed a DP-based asynchronous FL strategy for MEC, and [165] presented a blockchain-based secure data sharing strategy for asynchronous FL. Still, none of these

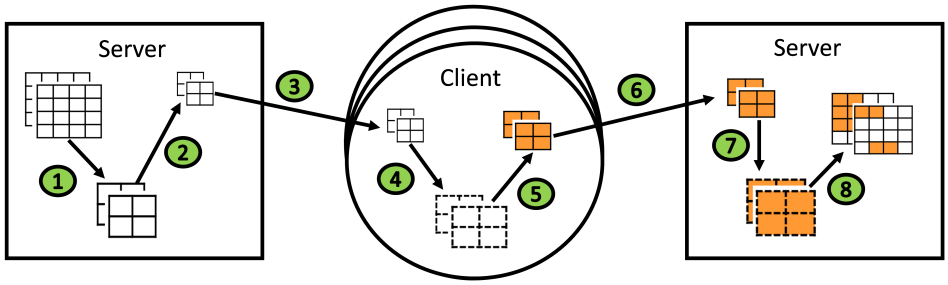


Fig. 11. Reducing size of the model by (1) generating a sub-model applying Federated Dropout, (2) lossily compressing the obtained resulting object which is passed to the client, who (4) applies decompression and trains that using its own local data, and (5) again compresses the update which is sent back to network server. There it is (7) again decompressed and finally, (8) aggregated to be a part of the global model.

works guarantee convergence during asynchronous FL communication of resource-constrained clients. Thus, formulating a method to ensure convergence in asynchronous FL can be a new research direction.

C. Quantification of Statistical Heterogeneity

FL training becomes complicated when the training data across devices are not identical in terms of data modeling and convergence behavior of the training process. Several ML works focused on the designing of statistical heterogeneity via meta-learning [169], [170], multi-task learning [171], [172], which are further extended to FL settings [48], [24], [173], [174], [175], [176]. For instance, an optimization framework MOCHA [48] allows for personalization through multi-task learning; however it considers convex objectives and is limited to its ability while scaling to massive networks. The authors in [174] modeled a Bayesian network by performing variational inference during learning. Though their proposed approach can handle both convex and non-convex models, it encounters high cost while generalizing to large federated networks. Besides, the authors in [175] aimed to identify cyclic patterns within data samples, while a detailed analysis of transfer learning strategy for personalization during FL can be seen in [173]. While the client data tend to be heterogeneous in terms of the number of samples, dataset structure, and format in a non-IID setting, all existing works on FL adjust the statistical heterogeneity after the training phase begins. It impacts the training quality, and the lack of proper quantification of such heterogeneity can cause poor training performance. A local dissimilarity approach is proposed [177] to quantify statistical sample variation, where the resource-quantification starts after the training starts. The authors in [178] proposed a centralized approach of handling heterogeneity of FL model training but did not consider specific support and analysis for statistical heterogeneity. Li et al. [21] proposed a reparametrization of the FedAvg [20] algorithm that can scale up divergent model updates and guarantees convergence while learning over statistical heterogeneous networks. However, they did not quantify the level of statistical heterogeneity while selecting clients during training or performing model aggregation.

D. Data Cleaning and Handling False Data Injection

In a real-world FL-based IoT environment, the IoT clients generate their models based on their extracted data. In a conventional FL-based IoT approach, there is no intermediate stage to refine the sensor data, which may cause a falsified local model with an erroneous update that eventually misleads the global model aggregation. As the number of such false data injected clients increases, the model accuracy reduces at the same phase. In time, it brings down the chance of reaching convergence. Bagdasaryan *et al.* [60] proposed a backdoor FL to identify malicious attacks during federated aggregation. They developed a train-and-scale scheme to restrict anomaly detectors from looking at the client's model weights or accuracy during FL tasks. The authors in [179] explained the vulnerability of sybil attacks in the FL process. They proposed a defense mechanism that can identify poisoning sybils by analyzing the diversity of FL clients during model training. However, none of them considered real-time false-data injection onto the IoT clients, which needs further research.

E. Reducing Energy Consumption and On-device Training

In line with our previous discussion, the clients of the IoT domain may possess a weak-processing unit. Therefore, it is challenging to conduct inference, training on devices, and executing timely interaction with the server through an energy-efficient communication scheme. However, on-device training causes two problems. First, the generated on-device model size needs to be small enough so that it fits within the device memory and still captures most of the data complexity to compute an effective model. The on-device inference problems are solved in [180] and [181], but the on-device training issues are not expounded. Second, the system can require high computational and storage availability for on-device training than these IoT clients can provide. Section IV-E presented some approaches suitable for specialized neumorphic or field-programmable gate array (FPGA) hardware or miss the combative constraints observed in the FL-IoT domain. Figuring out the solution to this dual problem is paramount. A potential direction can be found in [182]. They proposed an IoT-based network architecture to enable creating high-capacity client models with 15-38x fewer parameters compared to the conventional model experienced for such applications. Kumar *et al.* [180] proposed a tree-based approach to predict 2KB RAM IoT devices, e.g., Arduino Uno board that possessed 8-bit ATmega328P microcontroller without any floating-point support, and 32 KB size of the read-only flash. Their proposed algorithm attains standard prediction accuracy by constructing

TABLE V
ASYNCHRONOUS FEDERATED LEARNING BASED APPROACHES.

Approaches	Ref.	Key ideas
ASO-fed	[166]	Edge devices train themselves through online learning and server performs aggregation by dynamic learning step size and exponential moving average.
TWAFL	[167]	Apply synchronous learning technique on client participants and temporally weighted aggregation on the local client models.
FedAsync	[97]	Optimize a scheduler for selecting client for training phase periodically.
Blockchain Asynch	[168]	Designed a blockchain-based asynchronous FL communication in internet of vehicles
FedAsynch Geo	[160]	Applied the federated asynchronous approach in geospatial applications and analyzed the performance and difference with synchronous aggregation technique.
FedAsynch DP	[162]	Adapted differential privacy for a secure and robust asynchronous FL based scheme.
SAFA	[163]	Semi-asynchronous FL to avoid problems regarding synchronous and asynchronous FL for attaining less communication overhead.

a tree model that shrinks the model size and reduces prediction costs. They learned a sparse tree with high-powered nodes, carrying out the tree's learning process through sparsely projecting data within a low-dimensional space, and collaboratively learning all projection parameters and trees. Investigating such architecture to enable learning within the resource-constrained FL environments is an unexplored domain.

As we discussed, FL needs on-device training; therefore, any research that can enable energy-efficient execution of ML algorithms can help FL in turn. If we consider resource-constrained nodes for an IoT environment, then prolonging battery-power life duration is a challenge. Due to repeated interactions with the server, the battery charge can be reduced significantly. Minimizing the depreciation of battery power while interacting with the server is challenging. [180] developed a tree-based algorithm for making a prediction on resource-constrained IoT devices (i.e., Arduino) that possess only 2KB RAM. Still, they did not perform the training operation on resource-constrained IoT nodes. [183] designed a kNN-based algorithm that works on resource-scarce IoT nodes ($\leq$ 32kB RAM and 16MHz processor) to predict through supervised learning, but the edge devices are not trained locally. Therefore, it is essential to design an improved version of the FL algorithm that can handle small computational power as well as storage to train IoT nodes on edges, and how we can manage the energy consumption of client nodes during the training phase is also an open issue. An exciting direction in this front are dynamic computation technologies. Dynamic computation techniques activate only a part of the neural network for an input. This can help achieve both efficient training and inference as only a part of the neural network is updated for each input. There are many different ways one can introduce dynamic computation to a neural network. The techniques can be divided intothree broad categories - dynamic channel pruning (DCP), dynamic layer skipping (DLS), dynamic spatial gating (DSG), Dynamic Layer Skipping (DLS) and Mixture of Experts (MoE). DSG techniques ([184], [185]) identify spatial regions in the OFM that are deemed important and focus their attention only on those parts of the OFM. DCP techniques identify channels in the OFM that are deemed unimportant and skip computations for those channels ([186], [187]). DLS techniques are more specific to ResNet style architecture with skip connections or RNN based models ([188], [189]). Finally, MoE is based on the idea that instead of using a single large neural network to process an input data, multiple domain experts can be used to process the input. Based on the input, the results from the domain experts can be given more weight. The routing to the experts is done via a predictor network. By gating experts that are deemed unimportant for the input, one can achieve faster computation [190]. DCP techniques can be viewed as a specific instantiation of the techniques in this domain.

Beyond algorithm innovations, there has been a surge of work in the domain of design of software and hardware that executes ML algorithms efficiently. Here, efficiency refers to any or all of reduced energy consumption, faster runtime, and smaller memory footprint. The works in this area can be categorized in the domain of novel instructions for executing ML in CPU [191], [192], design of specialized accelerators [193], [194], [195], optimized software library [196], [197], development of new memory technologies [198] and near data processing to enable large storage using smaller energy budget [199]. However, the vast majority of these works are focused on the efficient inference of ML algorithms. A lot of these optimizations could be tailored to enable suitable training. Thus, further research in understanding the training algorithms of ML and how they execute on hardware can help tailor these solutions to solve this issue. The work described above modifies traditional hardware to make them amenable to machine learning. In traditional hardware, the unit responsible for processing information (processing unit) is separated from the unit responsible for storing data (memory). The instructions and data are fetched from memory and executed in the processing unit. This is called the von Neumann architecture. Apart from this, there is an entire body of works in the domain of neuromorphic computing [200], [201] dedicated to replicating the extreme power efficiency of the human brain by developing new hardware that mimics its synaptic structure. The main difference with traditional hardware lies in the non von Neumann architecture of these hardware as the processing and memory elements are not separate. We refer the readers to [200] to get a better overview of this field. FL can also benefit from edge units built using this neuromorphic hardware that can enable efficient on-device learning.

F. Managing Dropped Participants

Internet availability and network connection power are crucial, particularly while applying FL in an IoT environment.

Any FL-IoT participant may go out of network in the middle of the training phase or during the interaction with the server due to mobility, bandwidth shortage, lack of transmission power, or out of battery life. Most of the recent works considered that all FL participants maintain a continuous connection with the server and cannot drop connection in the middle. In the real-world FL-IoT environment, such a scenario is not feasible, and any participant may go offline due to out-of-resources. Dropping off a significant portion of the participants would fail to generate an effective global model. It is difficult to understand whether a client gives a slow response because of the network issue or resource-shortage. Figuring out the potential problem may help us act according to the problem scenario. The authors in [92] presented a solution to handle straggler clients by acknowledging their resource utilization (i.e., computation power) after each local update. They formed a predictive model by analyzing the client's resource utilization and adjusting local computation accordingly. Another strategy is to perform asynchronous training, i.e., updating the global model whenever it receives a model update from any of the participated clients [67], [167]. Moreover, a recently invented FL framework, FedProx [202] can handle heterogeneity in federated networks. FedProx allows a partial amount of work from each client device through a re-parameterization of the conventional FedAvg algorithm. However, when most of the clients within the network perform a low amount of partial works, their approach may take longer to reach convergence. The authors in [127] proposed activity and resource-aware FL strategy that can handle straggler issues by examining resource status, labeling clients with trust values in accordance to their contributions towards model convergence, and accepting variable works from the participated clients. However, further research needs to be conducted to optimize hyperparameters while enabling variable or partial works from the clients.

G. Privacy Preservation

The existing FL approaches aim to improve privacy by adapting classical cryptographic protocols and algorithms such as DP, SMC. An FL-based SMC protocol is proposed in [95] to protect client model updates. Through this method, the server cannot see the local update parameter but can still extract some information by observing the aggregated results after each round. However, this approach encounters a high communication cost, which is not feasible for a resource-constrained FL-IoT environment. The authors in [40], [56], [203] applied DP to FL to achieve a global DP, but the hyperparameters of these approaches affect the communication and model accuracy. An adaptive gradient clipping technique is presented in [204] to handle this issue. In [58], a modified version of local privacy is designed to limit the power of adversaries that guarantees more robust privacy than global privacy and results in better model accuracy. Another interesting approach to a DP mechanism based on meta-learning is proposed in [137] that can be used in FL through personalization. Besides, DP can be coupled with model compression strategies to reduce communication overhead and attain an improved version of privacy simultaneously [7], [136]. Further, some prior works [205], [206], [207], [208] proposed mechanisms to preserve privacy in a blockchain-enabled FL-based IoT environment. However, most of these approaches did not consider the heterogeneous resources of clients. They did not analyze the feasibility of applying a robust privacy-preserving algorithm that can be adapted without a straggler effect. Further research needs to be conducted to obtain maximum privacy benefits for resource-constrained heterogeneous FL-based IoT environment.

VI. Applications of Federated Learning

FL fits best in applications where we need to deal with sensitive information, and therefore, on-device training is more important than passing local data to the server. Most of the existing FL applications are based on labeled data collected from clients or user activities (e.g. type URLs or keyboard, click button). In this section, we discuss some existing FL applications to better understand the real-world impact of FL.

A. Resource-Sufficient Federated Learning Application

Recommendation System: A recommendation system can be compared to an information filtering scheme that tries to predict user preference or rating for an item. In the conventional recommendation system, user preference or rating would be shared with other users, and privacy is not maintained in many cases. Instead of sharing such private data, the authors in [24] proposed a federated meta-learning framework through which each local client shares his/her algorithm rather than his/her data or local model. In particular, federated meta-learning is useful when the model size is large; therefore, sharing algorithm is more flexible than sharing a model.

Next-word Prediction: A popular ML-based application is next-word prediction where a model is constructed that can predict what the next probable word would be. Such a centralized ML application may transfer private user data (e.g. SMS, URLs) to the server and may leak any sensitive information about the user. From that motivation, an on-device distributed ML-based framework is designed by [22], which is inspired by the FedAvg algorithm. They trained each participant locally and obtained a higher recall than the conventional approach. In this way, FL helps a user make predictions by learning his/her typing behavior and indirectly reading the user's mind.

Keyword Spotting: Wake-word detector applications are prevalent nowadays. For instance, Amazon's 'Hey Alexa' wake-word detector is used to play different songs, or execute different commands, while Google's wake-word detector 'Hey Google' is used for different purposes including driving e.g. to get direction on a map. However, most of those applications are based on the cloud-based system and pass user data to the server. Unlike this, an embedded speech model is proposed [23], where they used a wake-word detector 'Hey Snips' to recognize user's voice. They used a crowd-sourced dataset and applied the FL strategy by keeping user information private.

Relevant Content Suggestions for On-Device Keyboard: Google has recently implemented a virtual keyboard application named Gboard, where they applied the FL strategy to suggest relevant content [29]. It works on user-click or

TABLE VI
LIST OF EXISTING FEDERATED LEARNING APPLICATIONS.

Approach	Category	Data partition	Model type	Decision-making	Remark
MDLdroid [209]	Applications	Horizontal	NN	Server-centric	Reinforcement learning
FedNER [210]					
FedRec [211]					
In-edge AI [11]					
FCF [212]			LM		Collaborative filter
FedMF [213]					Matrix factorization
FL Next-Word Prediction [22]			NN		Natural language processing
FL Emoji-Prediction [69]					
FL OOV [214]					
Gboard [29]			LM		Linear regression
FL RBHS [215]			LM		SVM

ignores situations that are stored in training cache and value is added when related contents are suggested. Based on user-click, the information is stored in the cache and feeds into the on-device training process. In this work, inference and training are performed on-device. Only the model updated parameters are shared with the server, while globally trained models are deployed on each client.

B. Resource-Constrained Federated Learning Application

Smart Robotics: A lifelong reinforcement FL framework for mobile robots is proposed in [50]. They designed an architecture to enhance navigation systems of mobile robots to learn efficiently from prior knowledge and adapt to a new environment effectively. They used two types of transfer learning for fast adaptation of the mobile robots within a new environment. Their proposed system is scalable but lacks security, privacy, robustness, and sparsification.

Smart Object Detection: The authors in [216] designed an approach of optimizing object detection by considering Kullback- Leibler divergence (KLD) during measurement of weights divergence of client's local models. They adapted the Abnormal Weight Suppression technique to reduce the effects of weight divergence that may be caused by unbalanced and non-IID data.

Smart Healthcare: In healthcare services, the FL-based IoT concept can be extremely effective to preserve the privacy of sensitive medical data. The IoT devices can be useful to generate data streams of patient's status, and FL can be used to undertake early precautions or treatment utilizing the historical data. The authors in [217] developed an FL framework for smart healthcare by applying the FL mechanism, and reduced computation load of IoT devices during training. Their proposed approach also took the edge of communication overhead during interaction of FL server and IoT devices. However, their developed framework does not guarantee convergence, and is incapable of performing a successful learning process in presence of malfunction or edge/cloud server failure.

On-device Ranking: Another application of FL is to rank a search result. For instance, if we query something in our device, an automated search result appeared. This is done by making an expensive call to the server. To reduce such cost, implementation of on-device training to generate a ranking of search results is proposed in [95], which is particularly useful for resource-constrained devices. By observing the user's selected item from a ranked list, their system puts a label whenever a user interacts with the ranking feature. In this way, user preference is not revealed to anyone, and communication overhead is reduced by a significant margin.

Anomaly Detection: An autonomous self-learning scheme is proposed in [218] to identify compromised devices within IoT networks. Relying on unlabeled crowdsource data and depending on the device-type-specific behavior profiles, their proposed system can learn anomaly detection model without requiring any labeled data or human intervention to operate. They apply the FL strategy to aggregate behavior profiles for effective intrusion detection.

Resource-efficient Training of UAV-enabled IoT Devices: A particle swarm-based air quality monitoring framework is proposed in [57]. Their proposed system enables energy-efficient lightweight model training of Unmanned Aerial Vehicles (UAVs) using aerial haze images and predicts Air Quality Index (AQI) while preserving privacy. To sense ground systems, they proposed a Graph CNN-based Long Short-Term Memory (LSTM) model for obtaining accurate and real-time AQI inference. Besides, the authors in [219] addressed the issue of reducing latency and improving the energy efficiency of UAV-enabled IoT devices by optimizing battery resources and wireless bandwidth. They employed a deep deterministic policy gradient (DDPG) strategy to evaluate their system cost.

In Table **VI**, we present a detailed summary of some existing FL applications.

VII. FUTURE DIRECTIONS FOR FEDERATED LEARNING ALGORITHMS CONSIDERING RESOURCE-CONSTRAINED IOT DEVICES

As we discussed, FL is a recently invented distributed ML technique that can be considered as an emerging research area. After examining the core challenges of FL process while applying on resource-constrained IoT devices in Section IV, and analyzing some potential solutions of those emerging challenging in Section V, we point-out potential future directions

in FL-based IoT environments. In this section, we highlight the future directions of this domain.

• In an FL-based IoT environment, it can be experienced that some clients possess more data (e.g., due to frequent use of a particular application, or having a greater memory size) compared to other clients within the underlying IoT network setting. Such a discrepancy in the number of data samples, particularly due to heterogeneous memory size and availability, leads to massive deviation in terms of training periods from participant-to-participant. The non-uniform data distribution raises issues in generating the representation of the population distribution of any client dataset. Handling such disparity within **local training dataset** needs further research.

• To ensure convergence for asynchronous learning in a Non-IID setting with a presence of resource-constrained devices, loss functions of the **non-convex problem** (i.e., an objective function that has multiple feasible regions, and each region has multiple locally optimal points) need to be considered, and supportive algorithms should be proposed.

• In an FL system, we may need to choose a cluster head that would be responsible for passing the aggregated model parameter to the server for **energy efficiency**. The cluster head can collect client model parameters from its region in a synchronized fashion, while the central server can receive those locally aggregated models through a synchronous or asynchronous manner. Here, the leader can act as an intermediate aggregator and can avoid straggler nodes. It can marginally reduce power consumption as well as can minimize bandwidth requirements of the FL system, which could be effective for resource-constrained FL-based IoT environment. However, the leader node needs to be proficient to conduct swift operations and should be trustworthy to avoid false data injection.

• A **device-centric automatic wake-up mechanism** can be useful in determining the optimal period to carry out interaction with the server. Such an approach can reduce unnecessary communication with the server and avoid sending a model update when the client's local data does not change much. Besides, the automatic wake-up mechanism may help the resource-constrained devices to reserve energy, which could be utilized in further training.

• **Client mobility** can drastically change the overall system behavior. A network may hold a large number of active clients before the training starts, and after some period, most of them could go out of network. As a result, some areas may own a large number of clients, while some other regions may not be able to generate a feasible model due to a lack of active clients. Therefore, how to handle the mobility issues of the IoT devices and ensure successful federated model training is a potential research direction.

• During FL process, we may observe **statistical heterogeneity** among the client data. Such heterogeneity compels the clients to perform more interactions with the server, or with its neighbor nodes. The existing works did quantification of such statistical heterogeneity after initiating the training, which may cost extra resources and may have crucial impact on local training of the resource-constrained devices. Extensive research needs to be conducted to quantify the statistical heterogeneity even before the initialization of FL training to avoid idiosyncratic situations due to data sample variations.

• **Effective incentives mechanism design** is essential to encourage FL clients to share their model information. Some incentives or regulations schemes are implemented in blockchain [220], [221], [222], and some incentive mechanisms are proposed for high-quality federated data [223], [224]. Still, more extensive research needs to be conducted on incentives mechanism design to upgrade the effectiveness of FL. An example of such design is how game-theory models can be adapted in FLS or, in addition to the accuracy, what new benefit can be provided to the user to encourage them for joining in FL training. Besides, as the FL participants can be resource-bounded, or the participants can be business competitors, it is mandatory to design a strategy that divides the overall earnings to ensure the long-term engagement of the participants. Further, more focus needs to be placed on how to defend against adversarial attacks that try to collect the majority of the incentives.

• A **lightweight blockchain** framework for FL-IoT setting needs to be designed that can ensure robustness, enhance privacy and security while interacting with the server or neighbor clients. Blockchain can prevent model parameters or algorithm temperament and verify the model update and exchange. Some blockchain paradigm for on-device training is discussed in [36], [225], but they designed that framework without considering the challenges of the weak-processing unit and limited memory of IoT devices. Further research needs to be conducted on designing miner selection, block mining, consensus algorithm, validating a chain, atomicity, and blockchain interoperability, especially for FL with resource-constrained IoT clients.

• The FL structure leads us to think about integrating **trust model** to avoid adversarial clients during training. Selecting a client based on only resource availability would lead us to choose a malicious client. However, we can design a trust-based model based on the client's previous contribution to learning within the network and interacting with other clients. Typically, it is assumed that the server is trustworthy, and we can use the server to generate the trust model by analyzing the behavior of the clients. The incentive mechanism can be designed based on the generated trust model, and this may open us a new research direction.

VIII. Conclusion

This paper presented a comprehensive survey on federated learning algorithms and analyzed the implementation challenges while performing on-device training. We particularly emphasized the issues of FL process while considering resource-constrained IoT devices as FL clients. Firstly, we presented a highlight over FL algorithms that can enable efficient and scalable model training in edge devices. Then, we presented an overview of FL taxonomy and analyzed the existing papers to distinguish our contribution as compared with prior surveys. We discussed distributed learning and optimization techniques and explained various aspects of distributed algorithms for decision-making purposes. We analyzed the challenges during the on-device learning of resource-constrained devices and discussed existing feasible solutions.

After analyzing the challenges, we described the emerging challenges of FL implementation in resource-constrained IoT devices, which needs extensive further research. Afterwards, we explored the existing FL applications to provide a better understanding of the FL role in real-world applications. Finally, we listed the potential future directions of deploying FL within resource-constrained heterogeneous IoT environment.

REFERENCES

[1] Andrew C Yao. Protocols for secure computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)*, pages 160–164. IEEE, 1982.

[2] Rakesh Agrawal and Ramakrishnan Srikant. Privacy-preserving data mining. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, pages 439–450, 2000.

[3] Roberto J Bayardo and Rakesh Agrawal. Data privacy through optimal k-anonymization. In *21st International conference on data engineering (ICDE'05)*, pages 217–228. IEEE, 2005.

[4] Jaideep Vaidya, Hwanjo Yu, and Xiaoqian Jiang. Privacy-preserving svm classification. *Knowledge and Information Systems*, 14(2):161–178, 2008.

[5] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences*, 60(3):592–629, 2000.

[6] Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, and Tarek Abdelzaher. Pda: Privacy-preserving data aggregation in wireless sensor networks. In *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pages 2045–2053. IEEE, 2007.

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

[8] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):12, 2019.

[9] Solmaz Niknam, Harpreet S Dhillon, and Jeffery H Reed. Federated learning for wireless communications: Motivation, opportunities and challenges. *arXiv preprint arXiv:1908.06847*, 2019.

[10] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2020.

[11] Xiaofei Wang, Yiwen Han, Chenyang Wang, Qiyang Zhao, Xu Chen, and Min Chen. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. *IEEE Network*, 33(5):156–165, 2019.

[12] Peter Kairouz, H Brendan McMahan, et al. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1–2):1–210, 2021.

[13] Zhi Zhou et al. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proc. of the IEEE*, 107(8):1738–1762, 2019.

[14] Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie. Mobile edge computing: A survey. *IEEE Internet of Things Journal*, 5(1):450–465, 2017.

[15] Laizhong Cui, Shu Yang, et al. A survey on application of machine learning for internet of things. *J. M. L. Cybernetics*, 9(8):1399–1417, 2018.

[16] Yuyi Mao, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B Letaief. A survey on mobile edge computing: The communication perspective. *IEEE Communications Surveys & Tutorials*, 19(4):2322–2358, 2017.

[17] He Li, Kaoru Ota, et al. Learning iot in edge: Deep learning for the internet of things with edge computing. *IEEE network*, 32(1):96–101, 2018.

[18] Shuo Wang, Xing Zhang, Yan Zhang, Lin Wang, Juwo Yang, and Wenbo Wang. A survey on mobile edge networks: Convergence of computing, caching and communications. *IEEE Access*, 5:6757–6779, 2017.

[19] Pavel Mach and Zdenek Becvar. Mobile edge computing: A survey on architecture and computation offloading. *IEEE Communications Surveys & Tutorials*, 19(3):1628–1656, 2017.

[20] H Brendan McMahan, Eider Moore, et al. Communication-efficient learning of deep networks from decentralized data. *arXiv:1602.05629*, 2016.

[21] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks, 2018.

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

[23] David Leroy, Alice Coucke, Thibaut Lavril, Thibault Gisselbrecht, and Joseph Dureau. Federated learning for keyword spotting. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 6341–6345. IEEE, 2019.

[24] Fei Chen, Zhenhua Dong, Zhenguo Li, and Xiuqiang He. Federated meta-learning for recommendation. *arXiv preprint arXiv:1802.07876*, 2018.

[25] Kewei Cheng, Tao Fan, Yilun Jin, Yang Liu, Tianjian Chen, and Qiang Yang. Secureboost: A lossless federated learning framework. *arXiv preprint arXiv:1901.08755*, 2019.

[26] Yang Liu, Yan Kang, Xinwei Zhang, Liping Li, Yong Cheng, Tianjian Chen, Mingyi Hong, and Qiang Yang. A communication efficient vertical federated learning framework. *arXiv preprint arXiv:1912.11187*, 2019.

[27] Sinno Jialin Pan and Qiang Yang. A survey on transfer learning. *IEEE Transactions on knowledge and data engineering*, 22(10):1345–1359, 2009.

[28] Yang Liu, Tianjian Chen, and Qiang Yang. Secure federated transfer learning. *arXiv preprint arXiv:1812.03337*, 2018.

[29] Timothy Yang, Galen Andrew, et al. Applied federated learning: Improving google keyboard query suggestions. *arXiv:1812.02903*, 2018.

[30] Qinbin Li, Zeyi Wen, and Bingsheng He. Practical federated gradient boosting decision trees. *arXiv preprint arXiv:1911.04206*, 2019.

[31] Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Richard Nock, Giorgio Patrini, Guillaume Smith, and Brian Thorne. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *arXiv preprint arXiv:1711.10677*, 2017.

[32] Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, and Nina Taft. Privacy-preserving ridge regression on hundreds of millions of records. In *2013 IEEE Symposium on Security and Privacy*, pages 334–348. IEEE, 2013.

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

[34] Hongyi Wang, Mikhail Yurochkin, Yuekai Sun, Dimitris Papailiopoulos, and Yasaman Khazaeni. Federated learning with matched averaging. *arXiv preprint arXiv:2002.06440*, 2020.

[35] Qinbin Li, Zeyi Wen, and Bingsheng He. Federated learning systems: Vision, hype and reality for data privacy and protection. *arXiv preprint arXiv:1907.09693*, 2019.

[36] Hyesung Kim, Jihong Park, et al. Blockchained on-device federated learning. *IEEE Communications Letters*, 2019.

[37] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, pages 1–11, 2019.

[38] Mehryar Mohri, Gary Sivek, and Ananda Theertha Suresh. Agnostic federated learning. *arXiv preprint arXiv:1902.00146*, 2019.

[39] Lingchen Zhao, Lihao Ni, Shengshan Hu, Yaniiao Chen, Pan Zhou, Fu Xiao, and Libing Wu. Inprivate digging: Enabling tree-based distributed data mining with differential privacy. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 2087–2095. IEEE, 2018.

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

[41] Alekh Agarwal, John Langford, and Chen-Yu Wei. Federated residual learning, 2020.

[42] Jakub Konečnỳ, Brendan McMahan, and Daniel Ramage. Federated optimization: Distributed optimization beyond the datacenter. *arXiv preprint arXiv:1511.03575*, 2015.

[43] Mikhail Yurochkin, Mayank Agarwal, Soumya Ghosh, Kristjan Greenewald, Trong Nghia Hoang, and Yasaman Khazaeni. Bayesian

nonparametric federated learning of neural networks. *arXiv preprint arXiv:1905.12022*, 2019.

[44] Yang Liu, Zhuo Ma, Ximeng Liu, Siqi Ma, Surya Nepal, and Robert Deng. Boosting privately: Privacy-preserving federated extreme boosting for mobile crowdsensing. *arXiv preprint arXiv:1907.10218*, 2019.

[45] Yang Liu, Yingting Liu, Zhijie Liu, Junbo Zhang, Chuishi Meng, and Yu Zheng. Federated forest. *arXiv preprint arXiv:1905.10053*, 2019.

[46] Yi-Ruei Chen, Amir Rezapour, and Wen-Guey Tzeng. Privacy-preserving ridge regression on distributed data. *Information Sciences*, 451:34–49, 2018.

[47] Ashish P Sanil, Alan F Karr, Xiaodong Lin, and Jerome P Reiter. Privacy preserving regression modelling via distributed computation. In *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 677–682, 2004.

[48] Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, and Ameet S Talwalkar. Federated multi-task learning. In *Advances in Neural Information Processing Systems*, pages 4424–4434, 2017.

[49] Yihan Jiang, Jakub Konečnỳ, Keith Rush, and Sreeram Kannan. Improving federated learning personalization via model agnostic meta learning. *arXiv preprint arXiv:1909.12488*, 2019.

[50] Boyi Liu, Lujia Wang, and Ming Liu. Lifelong federated reinforcement learning: a learning architecture for navigation in cloud robotic systems. *IEEE Robotics and Automation Letters*, 4(4):4555–4562, 2019.

[51] Chaoyang He, Murali Annavaram, and Salman Avestimehr. Fednas: Federated deep learning via neural architecture search, 2020.

[52] Hangyu Zhu and Yaochu Jin. Multi-objective evolutionary federated learning. *IEEE transactions on neural networks and learning systems*, 2019.

[53] Eunjeong Jeong, Seungeun Oh, Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. Communication-efficient on-device machine learning: Federated distillation and augmentation under non-iid private data. *arXiv preprint arXiv:1811.11479*, 2018.

[54] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek. Robust and communication-efficient federated learning from non-iid data. *IEEE transactions on neural networks and learning systems*, 2019.

[55] Ruixuan Liu, Yang Cao, Masatoshi Yoshikawa, and Hong Chen. Fedsel: Federated sgd under local differential privacy with top-k dimension selection, 2020.

[56] H Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. Learning differentially private recurrent language models. *arXiv preprint arXiv:1710.06963*, 2017.

[57] Yi Liu, Jiangtian Nie, Xuandi Li, Syed Hassan Ahmed, Wei Yang Bryan Lim, and Chunyan Miao. Federated learning in the sky: Aerial-ground air quality sensing framework with uav swarms. *IEEE Internet of Things Journal*, 2020.

[58] Abhishek Bhowmick, John Duchi, Julien Freudiger, Gaurav Kapoor, and Ryan Rogers. Protection against reconstruction and its applications in private federated learning. *arXiv preprint arXiv:1812.00984*, 2018.

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

[60] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. *arXiv preprint arXiv:1807.00459*, 2018.

[61] Arjun Nitin Bhagoji, Supriyo Chakraborty, Prateek Mittal, and Seraphin Calo. Analyzing federated learning through an adversarial lens. *arXiv preprint arXiv:1811.12470*, 2018.

[62] Chulin Xie, Keli Huang, Pin-Yu Chen, and Bo Li. Dba: Distributed backdoor attacks against federated learning. In *International Conference on Learning Representations*, 2019.

[63] Tian Li, Maziar Sanjabi, and Virginia Smith. Fair resource allocation in federated learning. *arXiv preprint arXiv:1905.10497*, 2019.

[64] Yuan Liu, Shuai Sun, Zhengpeng Ai, Shuangfeng Zhang, Zelei Liu, and Han Yu. Fedcoin: A peer-to-peer payment system for federated learning, 2020.

[65] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 6(6):10700–10714, 2019.

[66] Takayuki Nishio and Ryo Yonetani. Client selection for federated learning with heterogeneous resources in mobile edge. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2019.

[67] Shiqiang Wang, Tiffany Tuor, Theodoros Salonidis, Kin K Leung, Christian Makaya, Ting He, and Kevin Chan. Adaptive federated learning in resource constrained edge computing systems. *IEEE Journal on Selected Areas in Communications*, 37(6):1205–1221, 2019.

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

[69] Swaroop Ramaswamy, Rajiv Mathews, Kanishka Rao, and Françoise Beaufays. Federated learning for emoji prediction in a mobile keyboard, 2019.

[70] Ahmed Khaled, Konstantin Mishchenko, and Peter Richtárik. First analysis of local gd on heterogeneous data, 2019.

[71] Paul Vanhaesebrouck, Aurélien Bellet, and Marc Tommasi. Decentralized collaborative learning of personalized models over networks. 2017.

[72] Xiangru Lian, Ce Zhang, Huan Zhang, Cho-Jui Hsieh, Wei Zhang, and Ji Liu. Can decentralized algorithms outperform centralized algorithms? a case study for decentralized parallel stochastic gradient descent. In *Advances in Neural Information Processing Systems*, pages 5330–5340, 2017.

[73] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konečný, Stefano Mazzocchi, H. Brendan McMahan, Timon Van Overveldt, David Petrou, Daniel Ramage, and Jason Roselander. Towards federated learning at scale: System design, 2019.

[74] Mahmoud Assran, Nicolas Loizou, Nicolas Ballas, and Michael Rabbat. Stochastic gradient push for distributed deep learning. *arXiv preprint arXiv:1811.10792*, 2018.

[75] Igor Colin, Aurélien Bellet, Joseph Salmon, and Stéphan Clémençon. Gossip dual averaging for decentralized optimization of pairwise functions. *arXiv preprint arXiv:1606.02421*, 2016.

[76] Hanlin Tang, Xiangru Lian, Ming Yan, Ce Zhang, and Ji Liu. d^2: Decentralized training over decentralized data. In *International Conference on Machine Learning*, pages 4848–4856, 2018.

[77] Anastasia Koloskova, Sebastian U Stich, and Martin Jaggi. Decentralized stochastic optimization and gossip algorithms with compressed communication. *arXiv preprint arXiv:1902.00340*, 2019.

[78] Aurélien Bellet, Rachid Guerraoui, Mahsa Taziki, and Marc Tommasi. Personalized and private peer-to-peer machine learning. *arXiv preprint arXiv:1705.08435*, 2017.

[79] Anis Elgabli, Jihong Park, Amrit S Bedi, Mehdi Bennis, and Vaneet Aggarwal. Gadmm: Fast and communication efficient framework for distributed machine learning. *arXiv preprint arXiv:1909.00047*, 2019.

[80] Anusha Lalitha, Osman Cihan Kilinc, Tara Javidi, and Farinaz Koushanfar. Peer-to-peer federated learning on graphs. *arXiv preprint arXiv:1901.11173*, 2019.

[81] Tim Kraska, Ameet Talwalkar, John C Duchi, Rean Griffith, Michael J Franklin, and Michael I Jordan. Mlbase: A distributed machine-learning system. In *Cidr*, volume 1, pages 2–1, 2013.

[82] Mu Li, David G Andersen, Alexander J Smola, and Kai Yu. Communication efficient distributed machine learning with the parameter server. In *Advances in Neural Information Processing Systems*, pages 19–27, 2014.

[83] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[84] Ohad Shamir, Nati Srebro, and Tong Zhang. Communication-efficient distributed optimization using an approximate newton-type method. In *International conference on machine learning*, pages 1000–1008, 2014.

[85] Martin Jaggi, Virginia Smith, Martin Takác, Jonathan Terhorst, Sanjay Krishnan, Thomas Hofmann, and Michael I Jordan. Communication-efficient distributed dual coordinate ascent. In *Advances in neural information processing systems*, pages 3068–3076, 2014.

[86] Yuchen Zhang and Lin Xiao. Disco: Communication-efficient distributed optimization of self-concordant empirical loss. 2015.

[87] Rie Johnson and Tong Zhang. Accelerating stochastic gradient descent using predictive variance reduction. In *Advances in neural information processing systems*, pages 315–323, 2013.

[88] Jakub Konečnỳ and Peter Richtárik. Semi-stochastic gradient descent methods. *arXiv preprint arXiv:1312.1666*, 2013.

[89] Sauptik Dhar, Junyao Guo, Jiayi Liu, Samarth Tripathi, Unmesh Kurup, and Mohak Shah. On-device machine learning: An algorithms and learning theory perspective. *arXiv preprint arXiv:1911.00623*, 2019.

[90] Chenxin Ma, Jakub Konečnỳ, Martin Jaggi, Virginia Smith, Michael I Jordan, Peter Richtárik, and Martin Takáč. Distributed optimization with arbitrary local solvers. *Optimization Methods and Software*, 32(4):813–848, 2017.

[91] Farzin Haddadpour, Mohammad Mahdi Kamani, et al. Trading redundancy for communication: Speeding up distributed sgd for non-convex optimization. In *ICML*, 2019.

[92] Anirban Das and Thomas Brunschwiler. Privacy is what we care about: Experimental investigation of federated learning on edge devices. *arXiv preprint arXiv:1911.04559*, 2019.

[93] Yuang Jiang, Shiqiang Wang, Bong Jun Ko, Wei-Han Lee, and Leandros Tassiulas. Model pruning enables efficient federated learning on edge devices. *arXiv preprint arXiv:1909.12326*, 2019.

[94] Zirui Xu, Zhao Yang, et al. Elfish: Resource-aware federated learning on heterogeneous edge devices. *arXiv:1912.01684*, 2019.

[95] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konecny, Stefano Mazzocchi, H Brendan McMahan, et al. Towards federated learning at scale: System design. *arXiv preprint arXiv:1902.01046*, 2019.

[96] Martin Zinkevich, John Langford, and Alex J Smola. Slow learners are fast. In *Advances in neural information processing systems*, pages 2331–2339, 2009.

[97] Cong Xie, Sanmi Koyejo, and Indranil Gupta. Asynchronous federated optimization. *arXiv preprint arXiv:1903.03934*, 2019.

[98] Shuxin Zheng, Qi Meng, Taifeng Wang, Wei Chen, Nenghai Yu, Zhi-Ming Ma, and Tie-Yan Liu. Asynchronous stochastic gradient descent with delay compensation. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 4120–4129. JMLR. org, 2017.

[99] Xiangru Lian, Wei Zhang, Ce Zhang, and Ji Liu. Asynchronous decentralized parallel stochastic gradient descent. *arXiv preprint arXiv:1710.06952*, 2017.

[100] Zheng Chai, Hannan Fayyaz, Zeshan Fayyaz, Ali Anwar, Yi Zhou, Nathalie Baracaldo, Heiko Ludwig, and Yue Cheng. Towards taming the resource and data heterogeneity in federated learning. In *2019 {USENIX} Conference on Operational Machine Learning (OpML 19)*, pages 19–21, 2019.

[101] Sukjong Ha, Jingjing Zhang, Osvaldo Simeone, and Joonhyuk Kang. Coded federated computing in wireless networks with straggling devices and imperfect csi. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2649–2653. IEEE, 2019.

[102] Ahmed Imteaj, Urmish Thakker, Shiqiang Wang, Jian Li, and M. Hadi Amini. Federated learning for resource-constrained iot devices: Panoramas and state-of-the-art, 2020.

[103] Andy Zhou, Rikky Muller, and Jan Rabaey. Memory-efficient, limb position-aware hand gesture recognition using hyperdimensional computing, 2021.

[104] Colby R. Banbury, Vijay Janapa Reddi, Max Lam, William Fu, Amin Fazel, Jeremy Holleman, Xinyuan Huang, Robert Hurtado, David Kanter, Anton Lokhmotov, David Patterson, Danilo Pau, Jae sun Seo, Jeff Sieracki, Urmish Thakker, Marian Verhelst, and Poonam Yadav. Benchmarking tinyml systems: Challenges and direction, 2021.

[105] Colby Banbury, Chuteng Zhou, Igor Fedorov, Ramon Matas Navarro, Urmish Thakker, Dibakar Gope, Vijay Janapa Reddi, Matthew Mattina, and Paul N. Whatmough. Micronets: Neural network architectures for deploying tinyml applications on commodity microcontrollers, 2021.

[106] Han Cai, Chuang Gan, Tianzhe Wang, Zhekai Zhang, and Song Han. Once-for-all: Train one network and specialize it for efficient deployment. In *International Conference on Learning Representations*, 2020.

[107] Shuang Wu, Guoqi Li, Feng Chen, and Luping Shi. Training and inference with integers in deep neural networks. *arXiv preprint arXiv:1802.04680*, 2018.

[108] Jihong Park, Shiqiang Wang, Anis Elgabli, Seungeun Oh, Eunjeong Jeong, Han Cha, Hyesung Kim, Seong-Lyun Kim, and Mehdi Bennis. Distilling on-device intelligence at the network edge. *arXiv preprint arXiv:1908.05895*, 2019.

[109] Nimit Sharad Sohoni, Christopher Richard Aberger, Megan Leszczynski, Jian Zhang, and Christopher Ré. Low-memory neural network training: A technical report. *CoRR*, abs/1904.10631, 2019.

[110] Paras Jain, Ajay Jain, Aniruddha Nrusimha, Amir Gholami, Pieter Abbeel, Joseph Gonzalez, Kurt Keutzer, and Ion Stoica. Checkmate: Breaking the memory wall with optimal tensor rematerialization. In I. Dhillon, D. Papailiopoulos, and V. Sze, editors, *Proceedings of Machine Learning and Systems*, volume 2, pages 497–511, 2020.

[111] Tianqi Chen, Bing Xu, Chiyuan Zhang, and Carlos Guestrin. Training deep nets with sublinear memory cost. *CoRR*, abs/1604.06174, 2016.

[112] Han Cai, Chuang Gan, Ligeng Zhu, and Song Han. Tinytl: Reduce memory, not parameters for efficient on-device learning, 2021.

[113] Zhongshu Gu, Hani Jamjoom, et al. Reaching data confidentiality and model accountability on the caltrain. In *IEEE DSN*, 2019.

[114] Tiffany Tuor, Shiqiang Wang, Bong Jun Ko, Changchang Liu, and Kin K Leung. Overcoming noisy and irrelevant data in federated learning. In *25th International Conference on Pattern Recognition (ICPR)*, 2020. Accepted.

[115] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. Federated learning in mobile edge networks: A comprehensive survey. *arXiv preprint arXiv:1909.11875*, 2019.

[116] Lingjuan Lyu, Xinyi Xu, and Qian Wang. Collaborative fairness in federated learning. *arXiv preprint arXiv:2008.12161*, 2020.

[117] Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang. A fairness-aware incentive scheme for federated learning. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pages 393–399, 2020.

[118] Latif U Khan, Shashi Raj Pandey, Nguyen H Tran, Walid Saad, Zhu Han, Minh NH Nguyen, and Choong Seon Hong. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Communications Magazine*, 58(10):88–93, 2020.

[119] Yang Liu and Jiaheng Wei. Incentives for federated learning: a hypothesis elicitation approach. *arXiv preprint arXiv:2007.10596*, 2020.

[120] Xianglin Bao, Cheng Su, Yan Xiong, Wenchao Huang, and Yifei Hu. Flchain: A blockchain for auditable federated learning with trust and incentive. In *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*, pages 151–159. IEEE, 2019.

[121] Takayuki Nishio, Ryoichi Shinkuma, and Narayan B Mandayam. Estimation of individual device contributions for incentivizing federated learning. *arXiv preprint arXiv:2009.09371*, 2020.

[122] Mingshu Cong, Han Yu, Xi Weng, Jiabao Qu, Yang Liu, and Siu Ming Yiu. A vcg-based fair incentive mechanism for federated learning. *arXiv preprint arXiv:2008.06680*, 2020.

[123] Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang. A sustainable incentive scheme for federated learning. *IEEE Intelligent Systems*, 2020.

[124] Mingzhe Chen, Zhaohui Yang, Walid Saad, Changchuan Yin, H Vincent Poor, and Shuguang Cui. A joint learning and communications framework for federated learning over wireless networks. *arXiv preprint arXiv:1909.07972*, 2019.

[125] Ahmed Imteaj and M Hadi Amini. Fedar: Activity and resource-aware federated learning model for distributed mobile robots. *arXiv preprint arXiv:2101.03705*.

[126] Dongdong Ye, Rong Yu, Miao Pan, and Zhu Han. Federated learning in vehicular edge computing: A selective model aggregation approach. *IEEE Access*, 8:23920–23935, 2020.

[127] Ahmed Imteaj and M Hadi Amini. Fedparl: Client activity and resource-oriented lightweight federated learning model for resource-constrained heterogeneous iot environment. *Frontiers in Communications and Networks*, 2:10, 2021.

[128] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. Exploiting unintended feature leakage in collaborative learning. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 691–706. IEEE, 2019.

[129] Nicholas Carlini, Chang Liu, Jernej Kos, Úlfar Erlingsson, and Dawn Song. The secret sharer: Measuring unintended neural network memorization & extracting secrets. *arXiv preprint arXiv:1802.08232*, 2018.

[130] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1322–1333, 2015.

[131] M Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M Songhori, Thomas Schneider, and Farinaz Koushanfar. Chameleon: A hybrid secure computation framework for machine learning applications. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 707–721, 2018.

[132] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of cryptology*, 1(1):65–75, 1988.

[133] Neel Guha, Ameet Talwlkar, et al. One-shot federated learning. *arXiv:1902.11175*, 2019.

[134] Meng Hao, Hongwei Li, Xizhao Luo, Guowen Xu, Haomiao Yang, and Sen Liu. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, 2019.

[135] Milad Nasr, Reza Shokri, and Amir Houmansadr. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 739–753. IEEE, 2019.

[136] Naman Agarwal, Ananda Theertha Suresh, Felix Xinnan X Yu, Sanjiv Kumar, and Brendan McMahan. cpsgd: Communication-efficient and differentially-private distributed sgd. In *Advances in Neural Information Processing Systems*, pages 7564–7575, 2018.

[137] Jeffrey Li, Mikhail Khodak, Sebastian Caldas, and Ameet Talwalkar. Differentially private meta-learning. *arXiv preprint arXiv:1909.05830*, 2019.

[138] Wenqi Li, Fausto Milletarì, Daguang Xu, Nicola Rieke, Jonny Hancox, Wentao Zhu, Maximilian Baust, Yan Cheng, Sébastien Ourselin, M Jorge Cardoso, et al. Privacy-preserving federated brain tumour segmentation. In *International Workshop on Machine Learning in Medical Imaging*, pages 133–141. Springer, 2019.

[139] Badih Ghazi, Rasmus Pagh, and Ameya Velingker. Scalable and differentially private distributed aggregation in the shuffled model. *arXiv preprint arXiv:1906.08320*, 2019.

[140] Zhibo Wang, Mengkai Song, Zhifei Zhang, Yang Song, Qian Wang, and Hairong Qi. Beyond inferring class representatives: User-level privacy leakage from federated learning. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 2512–2520. IEEE, 2019.

[141] Praneeth Vepakomma, Tristan Swedish, Ramesh Raskar, Otkrist Gupta, and Abhimanyu Dubey. No peek: A survey of private distributed deep learning. *arXiv preprint arXiv:1812.03288*, 2018.

[142] Kang Wei, Jun Li, Ming Ding, Chuan Ma, Howard H Yang, Farhad Farokhi, Shi Jin, Tony QS Quek, and H Vincent Poor. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 2020.

[143] Jiale Zhang, Bing Chen, Shui Yu, and Hai Deng. Pefl: A privacy-enhanced federated learning scheme for big data analytics. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[144] Mohamed Seif, Ravi Tandon, and Ming Li. Wireless federated learning with local differential privacy. *arXiv preprint arXiv:2002.05151*, 2020.

[145] Chunyi Zhou, Anmin Fu, Shui Yu, Wei Yang, Huaqun Wang, and Yuqing Zhang. Privacy-preserving federated learning in fog computing. *IEEE Internet of Things Journal*, 2020.

[146] Yu Chen, Fang Luo, Tong Li, Tao Xiang, Zheli Liu, and Jin Li. A training-integrity privacy-preserving federated learning scheme with trusted execution environment. *Information Sciences*, 522:69–79, 2020.

[147] Lumin Liu, Jun Zhang, SH Song, and Khaled B Letaief. Edge-assisted hierarchical federated learning with non-iid data. *arXiv preprint arXiv:1905.06641*, 2019.

[148] Ahmed Imteaj and M Hadi Amini. Distributed sensing using smart end-user devices: pathway to federated learning for autonomous iot. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 1156–1161. IEEE, 2019.

[149] Yuxuan Sun, Sheng Zhou, and Deniz Gündüz. Energy-aware analog aggregation for federated learning with redundant data. *arXiv preprint arXiv:1911.00188*, 2019.

[150] Pengchao Han, Shiqiang Wang, and Kin K Leung. Adaptive gradient sparsification for efficient federated learning: An online learning approach. In *IEEE ICDCS*, 2020.

[151] Sebastian Caldas, Jakub Konečny, H Brendan McMahan, and Ameet Talwalkar. Expanding the reach of federated learning by reducing client resource requirements. *arXiv preprint arXiv:1812.07210*, 2018.

[152] Haifeng Sun, Shiqi Li, F Richard Yu, Qi Qi, Jingyu Wang, and Jianxin Liao. Toward communication-efficient federated learning in the internet of things with edge computing. *IEEE Internet of Things Journal*, 7(11):11053–11067, 2020.

[153] Yi Liu, Sahil Garg, Jiangtian Nie, Yang Zhang, Zehui Xiong, Jiawen Kang, and M Shamim Hossain. Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 2020.

[154] Canh T Dinh, Nguyen H Tran, and Tuan Dung Nguyen. Personalized federated learning with moreau envelopes. *arXiv preprint arXiv:2006.08848*, 2020.

[155] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet of Things Journal*, 2020.

[156] Alireza Fallah, Aryan Mokhtari, and Asuman Ozdaglar. Personalized federated learning: A meta-learning approach. *arXiv preprint arXiv:2002.07948*, 2020.

[157] Zhaohui Yang, Mingzhe Chen, Walid Saad, Choong Seon Hong, and Mohammad Shikh-Bahaei. Energy efficient federated learning over wireless communication networks. *arXiv preprint arXiv:1911.02417*, 2019.

[158] Kai Yang, Tao Jiang, Yuanming Shi, and Zhi Ding. Federated learning via over-the-air computation. *IEEE Transactions on Wireless Communications*, 19(3):2022–2035, 2020.

[159] Nguyen H Tran, Wei Bao, Albert Zomaya, Nguyen Minh NH, and Choong Seon Hong. Federated learning over wireless networks: Optimization model design and analysis. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 1387–1395. IEEE, 2019.

[160] Michael R Sprague, Amir Jalalirad, et al. Asynchronous federated learning for geospatial applications. In *ECML-PKDD*, 2018.

[161] Catalin Capota, Moritz Neun, Lyman Do, and Michael Kopp. Asynchronous federated learning for geospatial applications. In *ECML PKDD 2018 Workshops: DMLE 2018 and IoTStream 2018, Dublin, Ireland, September 10–14, 2018, Revised Selected Papers*, volume 967, page 21. Springer, 2019.

[162] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. *IEEE Transactions on Industrial Informatics*, 2019.

[163] Wentai Wu, Ligang He, Weiwei Lin, Stephen Jarvis, et al. Safa: a semi-asynchronous protocol for fast federated learning with low overhead. *arXiv preprint arXiv:1910.01355*, 2019.

[164] Yanan Li, Shusen Yang, Xuebin Ren, and Cong Zhao. Asynchronous federated learning with differential privacy for edge intelligence. *arXiv preprint arXiv:1912.07902*, 2019.

[165] Yan Zhang, Yunlong Lu, Xiaohong Huang, Ke Zhang, and Sabita Maharjan. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 2020.

[166] Yujing Chen, Yue Ning, and Huzefa Rangwala. Asynchronous online federated learning for edge devices. *arXiv preprint arXiv:1911.02134*, 2019.

[167] Yang Chen, Xiaoyan Sun, and Yaochu Jin. Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation. *IEEE Transactions on Neural Networks and Learning Systems*, 2019.

[168] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 69(4):4298–4311, 2020.

[169] Ricardo Vilalta and Youssef Drissi. A perspective view and survey of meta-learning. *Artificial intelligence review*, 18(2):77–95, 2002.

[170] Sebastian Thrun et al. *Learning to learn*. Springer Science & Business Media, 2012.

[171] Rich Caruana. Multitask learning. *Machine learning*, 28(1):41–75, 1997.

[172] Theodoros Evgeniou et al. Regularized multi–task learning. In *ACM SIGKDD*, 2004.

[173] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, and Vikas Chandra. Federated learning with non-iid data. *arXiv preprint arXiv:1806.00582*, 2018.

[174] Luca Corinzia et al. Variational federated multi-task learning. *arXiv:1906.06268*, 2019.

[175] Hubert Eichner et al. Semi-cyclic stochastic gradient descent. *arXiv:1904.10120*, 2019.

[176] Mikhail Khodak, Maria Florina-Balcan, and Ameet Talwalkar. Adaptive gradient-based meta-learning methods. *arXiv preprint arXiv:1906.02717*, 2019.

[177] Iddo I Eliazar and Igor M Sokolov. Measuring statistical heterogeneity: The pietra index. *Physica A: Stat. Mech. App.*, 389(1):117–125, 2010.

[178] Daliang Li and Junpu Wang. Fedmd: Heterogenous federated learning via model distillation. *arXiv preprint arXiv:1910.03581*, 2019.

[179] Clement Fung, Chris JM Yoon, and Ivan Beschastnikh. Mitigating sybils in federated learning poisoning. *arXiv preprint arXiv:1808.04866*, 2018.

[180] Ashish Kumar, Saurabh Goyal, et al. Resource-efficient machine learning in 2 kb ram for the internet of things. In *ICML*, 2017.

[181] Urmish Thakker, Jesse Beu, et al. Compressing rnns for iot devices by 15-38x using kronecker products. *arXiv preprint arXiv:1906.02876*, 2019.

[182] Urmish Thakker, Jesse Beu, Dibakar Gope, Ganesh Dasika, and Matthew Mattina. Run-time efficient rnn compression for inference on edge devices, 2019.

[183] Chirag Gupta, Arun Sai Suggala, et al. Protonn: Compressed and accurate knn for resource-scarce devices. In *ICML*, 2017.

[184] Weizhe Hua, Yuan Zhou, Christopher De Sa, Zhiru Zhang, and G. Edward Suh. Channel gating neural networks, 2018.

[185] Xueqin Huang, Urmish Thakker, Dibakar Gope, and Jesse Beu. Pushing the envelope of dynamic spatial gating technologies. In *Proceedings of the 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, AIChallengeIoT '20, page 21–26, New York, NY, USA, 2020. Association for Computing Machinery.

[186] Ravi Raju, Dibakar Gope, Urmish Thakker, and Jesse Beu. Understanding the impact of dynamic channel pruning on conditionally parameterized convolutions. In *Proceedings of the 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, AIChallengeIoT '20, page 27–33, New York, NY, USA, 2020. Association for Computing Machinery.

[187] Xitong Gao, Yiren Zhao, Łukasz Dudziak, Robert Mullins, and Cheng zhong Xu. Dynamic channel pruning: Feature boosting and suppression, 2018.

[188] Xin Wang, Fisher Yu, Zi-Yi Dou, Trevor Darrell, and Joseph E. Gonzalez. Skipnet: Learning dynamic routing in convolutional networks. In *Proceedings of the European Conference on Computer Vision (ECCV)*, September 2018.

[189] Jin Tao, Urmish Thakker, Ganesh Dasika, and Jesse Beu. Skipping rnn state updates without retraining the original model. SenSys-ML 2019, page 31–36, New York, NY, USA, 2019. Association for Computing Machinery.

[190] Noam Shazeer, Azalia Mirhoseini, Krzysztof Maziarz, Andy Davis, Quoc Le, Geoffrey Hinton, and Jeff Dean. Outrageously large neural networks: The sparsely-gated mixture-of-experts layer, 2017.

[191] S. Liu, Z. Du, J. Tao, D. Han, T. Luo, Y. Xie, Y. Chen, and T. Chen. Cambricon: An instruction set architecture for neural networks. In *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*, pages 393–405, 2016.

[192] Nigel Stephens, Stuart Biles, Matthias Boettcher, Jacob Eapen, Mbou Eyole, Giacomo Gabrielli, Matt Horsnell, Grigorios Magklis, Alejandro Martinez, Nathanael Premillieu, and et al. The arm scalable vector extension. *IEEE Micro*, 37(2):26–39, Mar 2017.

[193] Y. Chen, T. Krishna, J. S. Emer, and V. Sze. Eyeriss: An energy-efficient reconfigurable accelerator for deep convolutional neural networks. *IEEE Journal of Solid-State Circuits*, 52(1):127–138, 2017.

[194] Tianshi Chen, Zidong Du, Ninghui Sun, Jia Wang, Chengyong Wu, Yunji Chen, and Olivier Temam. Diannao: A small-footprint high-throughput accelerator for ubiquitous machine-learning. *ACM SIGARCH Computer Architecture News*, 42(1):269–284, 2014.

[195] Ananda Samajdar, Parth Mannan, Kartikay Garg, and Tushar Krishna. Genesys: Enabling continuous learning through neural network evolution in hardware, 2018.

[196] Urmish Thakker, Ganesh Dasika, Jesse Beu, and Matthew Mattina. Measuring scheduling efficiency of rnns for nlp applications, 2019.

[197] Liangzhen Lai, Naveen Suda, and Vikas Chandra. Cmsis-nn: Efficient neural network kernels for arm cortex-m cpus, 2018.

[198] Skanda Koppula, Lois Orosa, A Giray Yağlıkçı, Roknoddin Azizi, Taha Shahroodi, Konstantinos Kanellopoulos, and Onur Mutlu. Eden: Enabling energy-efficient, high-performance deep neural network inference using approximate dram. In *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, pages 166–181, 2019.

[199] Mohsen Imani, Mohammad Samragh, Yeseong Kim, Saransh Gupta, Farinaz Koushanfar, and Tajana Rosing. Rapidnn: In-memory deep neural network acceleration framework, 2018.

[200] Catherine D. Schuman, Thomas E. Potok, Robert M. Patton, J. Douglas Birdwell, Mark E. Dean, Garrett S. Rose, and James S. Plank. A survey of neuromorphic computing and neural networks in hardware, 2017.

[201] D. Kim, J. Kung, S. Chai, S. Yalamanchili, and S. Mukhopadhyay. Neurocube: A programmable digital neuromorphic architecture with high-density 3d memory. In *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*, pages 380–392, 2016.

[202] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *Proceedings of Machine Learning and Systems*, 2:429–450, 2020.

[203] Yang Zhao, Jun Zhao, Mengmeng Yang, Teng Wang, Ning Wang, Lingjuan Lyu, Dusit Niyato, and Kwok-Yan Lam. Local differential privacy based federated learning for internet of things. *IEEE Internet of Things Journal*, 2020.

[204] Om Thakkar, Galen Andrew, and H Brendan McMahan. Differentially private learning with adaptive clipping. *arXiv preprint arXiv:1905.03871*, 2019.

[205] Youyang Qu, Longxiang Gao, Tom H Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, 7(6):5171–5183, 2020.

[206] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Blockchain and federated learning for privacy-preserved data sharing in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(6):4177–4186, 2019.

[207] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. Privacy-preserving blockchain-based federated learning for iot devices. *IEEE Internet of Things Journal*, 2020.

[208] Yong Li, Yipeng Zhou, Alireza Jolfaei, Dongjin Yu, Gaochao Xu, and Xi Zheng. Privacy-preserving federated learning framework based on chained secure multi-party computing. *IEEE Internet of Things Journal*, 2020.

[209] Yu Zhang, Tao Gu, and Xi Zhang. Mdldroid: a chainsgd-reduce approach to mobile deep learning for personal mobile sensing, 2020.

[210] Suyu Ge, Fangzhao Wu, Chuhan Wu, Tao Qi, Yongfeng Huang, and Xing Xie. Fedner: Privacy-preserving medical named entity recognition with federated learning, 2020.

[211] Tao Qi, Fangzhao Wu, Chuhan Wu, Yongfeng Huang, and Xing Xie. Fedrec: Privacy-preserving news recommendation with federated learning, 2020.

[212] Muhammad Ammad-ud din, Elena Ivannikova, Suleiman A Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. Federated collaborative filtering for privacy-preserving personalized recommendation system. *arXiv preprint arXiv:1901.09888*, 2019.

[213] Di Chai, Leye Wang, Kai Chen, and Qiang Yang. Secure federated matrix factorization. *arXiv preprint arXiv:1906.05108*, 2019.

[214] Mingqing Chen, Rajiv Mathews, Tom Ouyang, and Françoise Beaufays. Federated learning of out-of-vocabulary words, 2019.

[215] Florian Hartmann, Sunah Suh, Arkadiusz Komarzewski, Tim D. Smith, and Ilana Segall. Federated learning for ranking browser history suggestions, 2019.

[216] Peihua Yu and Yunfeng Liu. Federated object detection: Optimizing object detection model with federated learning. In *Proceedings of the 3rd International Conference on Vision, Image and Signal Processing*, pages 1–6, 2019.

[217] Binhang Yuan, Song Ge, and Wenhui Xing. A federated learning framework for healthcare iot devices. *arXiv preprint arXiv:2005.05083*, 2020.

[218] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N Asokan, and Ahmad-Reza Sadeghi. Dïot: A federated self-learning anomaly detection system for iot. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 756–767. IEEE, 2019.

[219] Shunpu Tang, Wenqi Zhou, Lunyuan Chen, Lijia Lai, Junjuan Xia, and Liseng Fan. Battery-constrained federated edge learning in uav-enabled iot for b5g/6g networks. *arXiv preprint arXiv:2101.12472*, 2021.

[220] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, pages 45–59, 2016.

[221] Yufeng Zhan, Peng Li, Zhihao Qu, Deze Zeng, and Song Guo. A learning-based incentive mechanism for federated learning. *IEEE Internet of Things Journal*, 7(7):6360–6368, 2020.

[222] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.

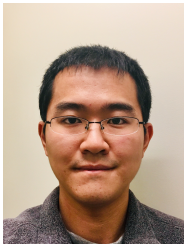
[223] Yunus Sarikaya and Ozgur Ercetin. Motivating workers in federated learning: A stackelberg game perspective. *IEEE Networking Letters*, 2019.

[224] Radu Jurca and Boi Faltings. An incentive compatible reputation mechanism. In *EEE International Conference on E-Commerce, 2003. CEC 2003.*, pages 285–292. IEEE, 2003.

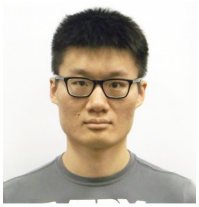
[225] Ronghua Xu, Yu Chen, and Jian Li. MicroFL: A lightweight, secure-by-design edge network fabric for decentralized IoT systems. In *NDSS*, 2020.

Ahmed Imteaj is currently a PhD candidate and graduate assistant at the Knight Foundation School of Computing and Information Sciences at Florida International University. He is also a research lab member of Sustainability, Optimization, and Learning for InterDependent networks laboratory (solid lab) at Florida International University. His research interests span federated learning, Internet of Things (IoT), machine learning, blockchain, sensor networks, cyber-physical-social resilience, and optimization. He holds a B.Sc. degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh in 2015. From 2015 to 2018, he worked as a Lecturer at International Islamic University Chittagong (IIUC), Chittagong, Bangladesh. Ahmed's work on federated learning for IoT environments is the recipient of the best paper award from "2019 IEEE Conference on Computational Science & Computational Intelligence" and won the second place at 2021 Florida International University GSAW Scholarly Forum. Ahmed has published more than 30 referred journals and conference papers.

Urmish Thakker is a Deep Learning Researcher at SambaNova Systems. Before joining SambaNova, he worked with Arm Research, AMD, Texas Instruments and Broadcom. His research has primarily focused on efficient execution of neural networks on resource constrained devices. Specifically, he has worked on model quantization, pruning, structured matrices and low-rank decomposition. His work has led to patents, publications and contributions to various products across multiple companies. Urmish completed his Master's in Computer Science from UW Madison in US and Bachelor's from BITS Pilani in India.



Shiqiang Wang (S'13–M'15) received his Ph.D. from the Department of Electrical and Electronic Engineering, Imperial College London, United Kingdom, in 2015. Before that, he received his master's and bachelor's degrees at Northeastern University, China, in 2011 and 2009, respectively. He is a Research Staff Member at IBM T. J. Watson Research Center, NY, USA since 2016, where he was also a Graduate-level Co-op in the summers of 2014 and 2013. In the fall of 2012, he was at NEC Laboratories Europe, Heidelberg, Germany. His current research focuses on the interdisciplinary areas in distributed computing, machine learning, networking, optimization, and signal processing. Dr. Wang served as a technical program committee (TPC) member of several international conferences, including ICML, NeurIPS, ICDCS, AISTATS, IJCAI, IFIP Networking, IEEE GLOBECOM, IEEE ICC, and as an associate editor of the IEEE Transactions on Mobile Computing. He received the IEEE Communications Society Leonard G. Abraham Prize in 2021, IBM Outstanding Technical Achievement Award (OTAA) in 2019 and 2021, multiple Invention Achievement Awards from IBM since 2016, Best Paper Finalist of the IEEE International Conference on Image Processing (ICIP) 2019, and Best Student Paper Award of the Network and Information Sciences International Technology Alliance (NIS-ITA) in 2015.



Jian Li is an Assistant Professor of Computer Engineering with the Department of Electrical and Computer Engineering at Binghamton University, State University of New York (SUNY). He was a postdoc with the College of Information and Computer Sciences, University of Massachusetts Amherst from January 2017 to August 2019. He received the Ph.D. degree in Computer Engineering from Texas A&M University in December 2016, and B.E. degree from Shanghai Jiao Tong University in June 2012. His current research interests lie in the areas of reinforcement learning, online learning, network optimization, online algorithms and their applications in large scale networked systems.

M. Hadi Amini is an Assistant Professor at Knight Foundation School of Computing and Information Sciences at Florida International University. He is the director of Sustainability, Optimization, and Learning for InterDependent networks laboratory (www.solidlab.network). He received his Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University in 2019, where he received his M.Sc. degree in 2015. He also holds a doctoral degree in Computer Science and Technology. Prior to that, he received M.Sc. degree from Tarbiat Modares University in 2013, and the B.Sc. degree from Sharif University of Technology in 2011. His research interests include distributed optimization and learning algorithms, distributed computing and intelligence, sensor networks, interdependent networks, and cyber-physical-social resilience. Application domains include smart cities, energy systems, transportation networks, and healthcare.

Hadi is a life member of IEEE-Eta Kappa Nu (IEEE-HKN), the honor society of IEEE. He served as President of Carnegie Mellon University Energy Science and Innovation Club; as technical program committee of several IEEE and ACM conferences; and as the lead editor for a book series on "Sustainable Interdependent Networks" since 2017. He also serves as Associate Editor of SN Operations Research Forum and International Transactions on Electrical Energy Systems. He has published more than 100 refereed journal and conference papers, and book chapters. He edited/authored six books. He is the recipient of the best paper award from "2019 IEEE Conference on Computational Science & Computational Intelligence", FIU's Knight Foundation School of Computing and Information Sciences' "Excellence in Teaching Award", best reviewer award from four IEEE Transactions, the best journal paper award in "Journal of Modern Power Systems and Clean Energy", and the dean's honorary award from the President of Sharif University of Technology. (Homepage: www.hadiamini.com)