Chapter 3
Federated Learning for Internet of Things

Ying Li, Qiyang Zhang, Xingwei Wang, Rongfei Zeng, Haodong Li, Ilir Murturi, Schahram Dustdar, and Min Huang

3.1 Introduction

The Internet of Things (IoT) possesses the immense potential to revolutionize numerous industries and aspects of daily life by facilitating the seamless integration of the physical world with digital systems (Tataria et al. 2021). It allows for the creation of smart homes, smart cities, industrial automation, precision agriculture, healthcare monitoring, and an array of other innovative applications. To effectively

Y. Li
College of Computer Science and Engineering, Northeastern University, Shenyang, China

Distributed Systems Group, TU Wien, Vienna, Austria
e-mail: liying1771@163.com

Q. Zhang
State Key Laboratory of Network and Switching, Beijing University of Posts and Telecommunications, Beijing, China

Distributed Systems Group, TU Wien, Vienna, Austria
e-mail: qyzhang@bupt.edu.cn

X. Wang (✉) · H. Li
College of Computer Science and Engineering, Northeastern University, Shenyang, China
e-mail: wangxw@mail.neu.edu.cn; 1ihaodong0811@163.com

R. Zeng
College of Software, Northeastern University, Shenyang, China
e-mail: zengrf@swc.neu.edu.cn

I. Murturi · S. Dustdar
Distributed Systems Group, TU Wien, Vienna, Austria
e-mail: imurturi@dsg.tuwien.ac.at; dustdar@dsg.tuwien.ac.at

M. Huang
College of Information Science and Engineering, Northeastern University, Shenyang, China
e-mail: mhuang@mail.neu.edu.cn

P. K. Donta et al. (eds.), *Learning Techniques for the Internet of Things*,
https://doi.org/10.1007/978-3-031-50514-0_3

implement these intelligent applications, a substantial quantity of IoT devices is indispensable (Saad et al. 2019; Al-Fuqaha et al. 2015). According to recent statistics, the rapid growth of the IoT is expected to result in an astonishing number of 125 billion IoT devices by 2030 (SEMICONDUCTORDIGEST n.d.). Alongside this massive proliferation of devices, the amount of data generated by these IoT devices is predicted to be monumental. It is estimated that by 2025, the total data volume generated by connected IoT devices worldwide will reach an astounding 79.4 zettabytes (ZBs) (Statista n.d.). The exponential expansion of network size and data volume within the IoT systems presents an exceptional opportunity to harness the power of artificial intelligence (AI) algorithms. These algorithms have the capability to efficiently process and analyze immense data quantities, thereby extracting valuable insights and facilitating decision-making processes with remarkable efficacy.

In the traditional approach, data gathered by IoT devices is transmitted to cloud servers or data centers, where it is uploaded and processed in a centralized manner. However, this approach is no longer sustainable due to several reasons (Ying et al. 2023): Firstly, data owners are becoming increasingly concerned about privacy issues associated with transmitting their data to centralized servers. Secondly, the traditional approach introduces significant propagation delays, which are unacceptable for applications requiring real-time decision-making. Lastly, transferring large volumes of data to the centralized server for processing puts a strain on the backbone network, impacting its performance and capacity. To address the privacy and latency issues associated with traditional IoT, mobile edge computing (MEC) (Abbas et al. 2017; Cao et al. 2019; Donta et al. 2023) emerged as a paradigm where data processing and analysis occur closer to the data source, reducing data transmission, latency, and reliance on centralized infrastructure. However, it may still involve transmitting raw data to centralized locations for model training, raising privacy concerns.

Against the backdrop of increasingly stringent data privacy regulations, federated learning (FL) (McMahan et al. 2017a; Kairouz et al. 2021) has emerged as a promising solution to tackle privacy concerns in IoT environments. FL, as a privacy-preserving distributed machine learning paradigm, facilitates collaborative and decentralized ML while ensuring that raw data remains within the client's domain, thereby not being transmitted to a central server (Zeng et al. 2021). In FL, the learning process takes place locally on each client within the network, where each client trains its own local models utilizing its own data, while the central server exclusively aggregates and shares the new global model updates. This approach guarantees the preservation of data privacy since sensitive information remains on the clients and is not exposed to the central server or other clients in the FL network. Moreover, FL maintains data utility by aggregating model updates from each client, enabling the central server to create an updated global model that captures knowledge from diverse distributed data, resulting in improved accuracy and generalization capabilities. Specifically, the several benefits that FL offers for IoT as outlined below:

- **Enhanced Data Privacy:** FL ensures data privacy and reduces the risk of data breaches or unauthorized access by keeping raw data on the clients and eliminating the need to transmit sensitive information to a central server, thereby preserving data privacy and enhancing security measures.
- **Reduced Latency and Bandwidth Requirements:** FL minimizes the need for frequent data transmission between clients and the central server by performing local model training on each client, resulting in reduced latency and bandwidth requirements. This makes FL highly suitable for real-time or latency-sensitive IoT applications, ensuring efficient and responsive data processing.
- **Efficient Resource Utilization:** FL optimizes resource utilization by leveraging the computational power of edge devices within the IoT network, distributing the learning process. This reduces the burden on the central server and makes FL well-suited for resource-constrained IoT devices, ensuring efficient utilization of limited resources.
- **Robustness to Device Heterogeneity:** FL is designed to handle the heterogeneity present in IoT networks, accommodating devices with diverse characteristics such as varying hardware configurations or data distributions. FL achieves this by allowing local model training on individual devices, enabling each device to contribute to the global model irrespective of its specific capabilities or data characteristics. This ensures effective utilization of the collective knowledge within the IoT network while accommodating device heterogeneity.
- **Improved Scalability:** FL facilitates large-scale collaboration across numerous IoT devices, enabling each device to actively participate in the training process and contribute its local model update to enhance the global model. The scalable approach efficiently utilizes the vast amount of distributed data available in IoT environments, resulting in improved model performance and leveraging the collective intelligence of the entire IoT network.

Overall, FL provides significant benefits for IoT, including preserving data privacy, reducing latency, optimizing resource efficiency, handling device heterogeneity, and enabling scalability. These advantages make FL a valuable approach for effectively leveraging distributed IoT data while ensuring privacy and maximizing learning performance. In this work, we present state-of-the-art advancements in FL for IoT. The rest of this work is organized as follows. Section 3.2 provides an introduction to preliminary work on FL for IoT. Section 3.3 explores various applications of FL for IoT. Section 3.4 provides the current research challenges and future directions in the field of FL for IoT. Finally, Sect. 3.5 concludes the paper.

3.2 Federated Learning and Internet of Things: Preliminaries

In this section, we first present the fundamental knowledge of FL and IoT. Next, we briefly introduce the overview of FL for IoT.

3.2.1 Federated Learning

Recent advancements in AI and the proliferation of IoT devices have led to exponential growth in data. In addition, concerns over data privacy and security have also risen. In response to these concerns, FL provides a viable solution to address these challenges by facilitating collaborative ML without compromising individual privacy. FL leverages the distributed nature of data and allows local learning on IoT devices, promoting data privacy while facilitating collaborative intelligence. Here, we introduce the fundamental concept of FL and subsequently present several significant categories of FL specifically for IoT networks. Specifically, the architectural overview of FL for IoT is provided as shown in Fig. 3.1.

3.2.1.1 Fundamental FL Concept

The FL system for the IoT network consists of five distinct entities that collectively contribute to its operation and effectiveness:

1. **Admin**: The administrator serves as the overseer of the FL system's overall operation, including managing the coordination among the various entities involved, ensuring system stability and security, and addressing any technical issues or updates that may arise.
2. **Model Engineer**: The model engineer is responsible for developing the ML model, defining the training protocol for the FL system, and executing model evaluation.
3. **Aggregation Server/Blockchain**: The aggregation server or blockchain coordinates the FL training process by collecting and aggregating the model updates from the participating clients.
4. **Clients**: Clients represent the devices or organizations that contribute their local data and computational resources to the FL training process (Zeng et al. 2020).
5. **End users**: End users refer to individuals or organizations that utilize the trained ML model to make predictions or decisions.

3.2.1.2 The Typical Process of FL Training for IoT

Let $\mathcal{K} = \{1, 2, \ldots, K\}$ represent the set of clients actively participating in the collaborative training of FL models, leveraging their IoT devices to perform IoT tasks. Each client $k \in \mathcal{K}$ possesses a local dataset $\mathcal{D}^k$ that may undergo changes over time. The size of the local dataset is denoted by $|\mathcal{D}^k|$. For local model training, each client can selectively choose a subset $\varkappa^k \subseteq \mathcal{D}^k$ from its local dataset, and the size of the chosen subset is indicated by $|\varkappa^k|$. Next, we present the typical process of FL training for IoT.

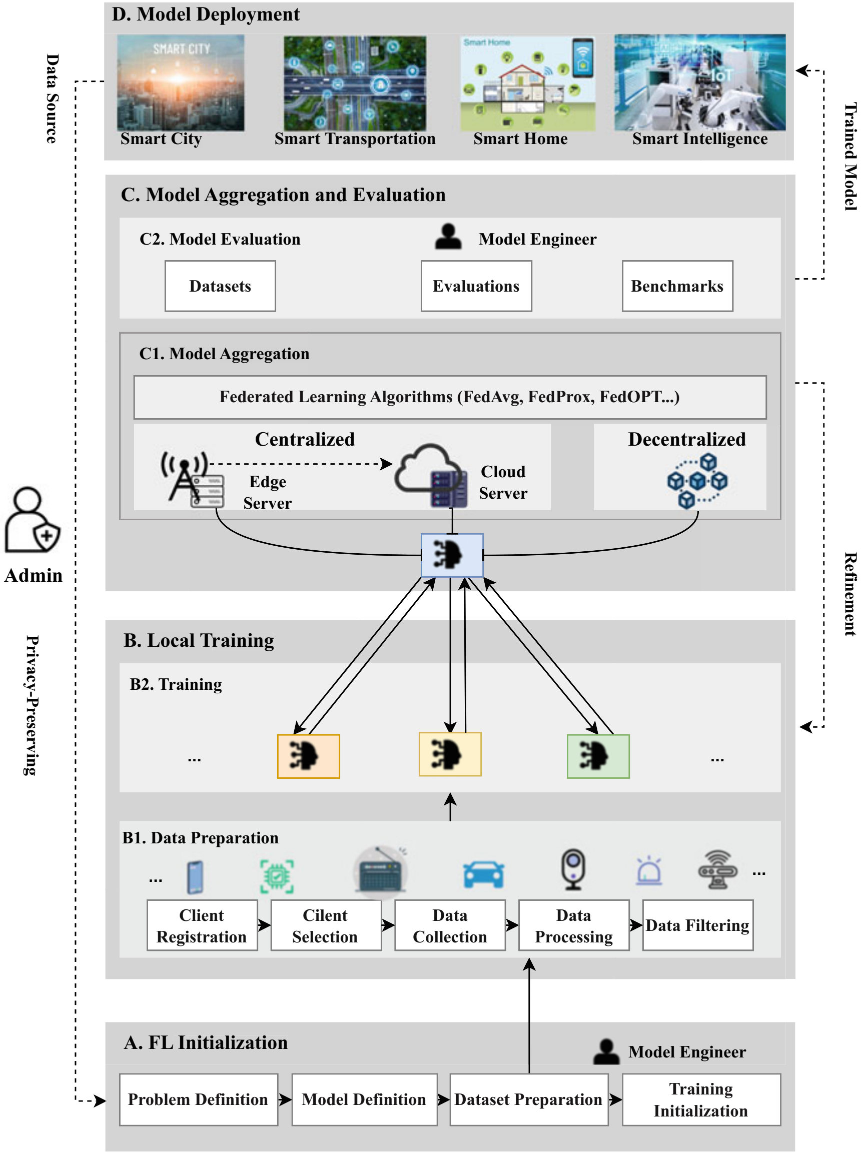


Fig. 3.1 The architecture of federated learning for IoT

Step 1: Client Selection. Client selection plays a crucial role in determining the participating clients in the training process, which influences the performance of the trained model. Let $\mathcal{K}^s$ denote the set of selected clients, and $|\mathcal{K}^s|$ represents the number of clients chosen for participation.

Step 2: Download Global Model. During this step, the clients initiate the process by downloading the global model that was aggregated by the central server in the previous round t. (In the first round, the global model is randomly initialized.)

$$w_t^k = w_t \tag{3.1}$$

where w_t represents the downloaded global model in round t.

Step 3: Local Training. After downloading the global model, the clients undertake local training based on their local datasets, utilizing the downloaded model as a new starting point:

$$w_{t+1}^k = w_t^k - \eta \triangledown L^k \left(w_t^k ; \varkappa^k \right). \tag{3.2}$$

where η is the step size, $L^k(w_t^k; \varkappa^k)$ is the local loss function of client k in the round t, and w_{t+1}^k denotes the trained local model of client k in the round t.

Step 4: Upload Local Model Updates. The trained local models are then sent back to the aggregation server or blockchain for aggregation.

Step 5: Global Aggregation. The aggregation server or blockchain combines the model updates from participating clients using an appropriate algorithm, thereby creating a unified global model that represents the collective knowledge of all clients:

$$w_{t+1} = \frac{\sum_{k \in \mathcal{K}^s} |\varkappa^k| w_{t+1}^k}{\sum_{k \in \mathcal{K}^s} |\varkappa^k|} \tag{3.3}$$

where w_{t+1} denotes the aggregated global model in the round $t+1$.

The training process in FL typically consists of multiple rounds, each consisting of T iterations, to achieve convergence, and the termination of the training process depends on the specific objectives and requirements related to accuracy and training time. The objective of FL is to obtain the optimal weights for the global model w^* by minimizing the global loss function $L(w)$ (McMahan et al. 2017b):

$$L(w) = \frac{\sum_{k \in \mathcal{N}^s} |\varkappa^k| L^k(w; \varkappa_k)}{\sum_{k \in \mathcal{N}^s} |\varkappa^k|}. \tag{3.4}$$

where $L^k(w; \varkappa_k)$ represents the loss function for a subset $\varkappa_k$ of client k when the global model's weight is given to w.

$$w^* = \arg\min_w L(w). \tag{3.5}$$

3.2.1.3 The Architecture of Federated Learning for IoT Networks

Figure 3.1 portrays a comprehensive and well-structured depiction of the architecture of FL for IoT networks. This architecture facilitates the integration of FL techniques into IoT systems, enabling collaborative and privacy-preserving ML across distributed IoT devices. The architecture comprises several key components, each playing a vital role in the FL process.

FL Initialization: FL initialization refers to the process of setting up the initial conditions and parameters before commencing the FL process. This stage is crucial as it establishes the foundation for subsequent iterations of model training and aggregation in a FL system. The initialization process in FL typically involves the following key steps: Define the problem by identifying data sources, and target tasks, and specifying performance metrics for model evaluation (step 1). After problem definition, the model engineer designs a model architecture for FL, which includes selecting optimization algorithms, defining model parameters, and determining data partitioning among participating clients (step 2). Then, the dataset is prepared by the data owners, who are responsible for the collection or generation of the data specifically intended for training the model (step 3). Afterwards, the training process is initiated by the central server, which provides the participating clients with the initial model parameters, either through random initialization or by leveraging pre-training on a large dataset (step 4).

Local Training: Local learning in FL refers to the process by which clients perform model training using their locally available data. Prior to local training, a crucial step is to perform data preparation, which encompasses client registration, client selection, data collection, data processing, and data filtering, ensuring the availability of diverse and relevant data that is appropriately formatted for subsequent local training in the FL process. Client registration refers to the initial step in FL where eligible clients or IoT devices voluntarily enroll themselves in the FL system, typically by registering with the central server or a designated entity (step 1). After that, client selection in FL is executed as a strategic process that involves carefully choosing a subset of clients from the registered pool for each iteration, considering criteria such as device capabilities, data quality, and diversity, to ensure their representative and effective participation (step 2). Next, the process of data collection gathers data from the selected clients, where each client contributes its locally stored or generated data (step 3). Subsequently, data processing involves the necessary preprocessing and transformation of collected data to prepare it for model training, aiming to enhance data quality and facilitate efficient learning (step 4). Last but not least, data filtering plays a critical role in data preparation by selectively removing or filtering out data samples or features based on predefined criteria, effectively eliminating outliers, noise, or irrelevant information that could potentially disrupt the training process or compromise privacy (step 5). After the completion of data preparation, each selected client independently trains its local model based on the data available locally.

Model Aggregation and Evaluation: Following the completion of local training, the subsequent step in FL entails aggregating the local model updates to create a new global model. This aggregation process can be carried out using various approaches, including the use of a cloud server, an edge server, a combination of cloud server and edge server, and even leveraging blockchain technology (the details as introduced in Sect. 3.2.2). As a subsequent step, the aggregated global model is evaluated to assess its performance and generalization ability (Ying et al. 2023a). Evaluation metrics, such as accuracy, precision, and F1 score, are commonly used to measure the model's effectiveness in achieving the desired task objectives. Additionally, the evaluation phase also involves comparing the performance of the FL model with other benchmark models or existing approaches to validate its efficacy and identify areas for improvement. If the specific objectives and requirements concerning the performance (such as accuracy) are achieved, the training process could be terminated.

Model Deployment: Upon completion of the training phase, the trained model can be deployed for making predictions on some IoT applications that perform FL model training or previously unseen IoT applications. However, in certain scenarios, it may be necessary to fine-tune the model using new data in order to adapt to evolving conditions or enhance its performance.

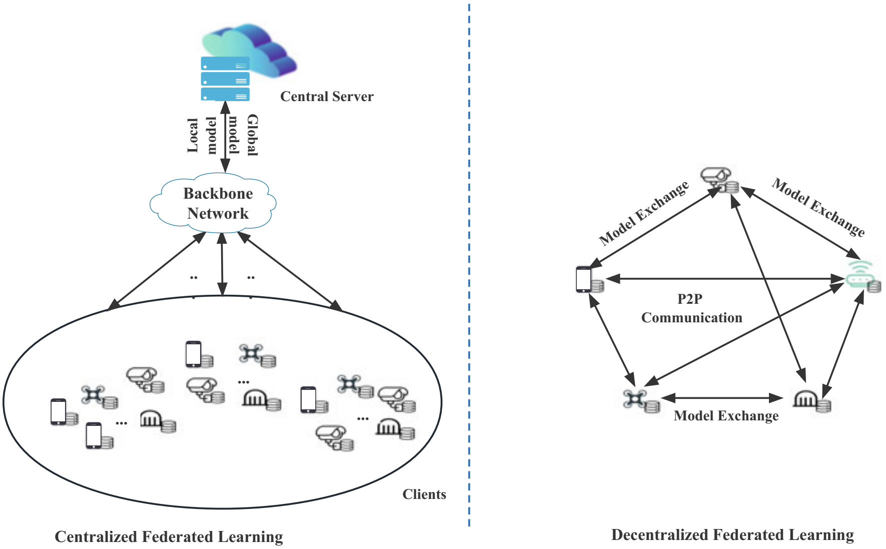
3.2.2 Types of Federated Learning for IoT

In this subsection, we present the classification of FL approaches based on their networking structure, centralization levels, and participating clients. By comprehending these categories, informed decisions can be made when implementing FL in IoT applications.

3.2.2.1 Types of FL for IoT Based on Networking Structure

From a networking structure perspective, FL can be categorized into two main classes, including centralized FL and decentralized FL, as illustrated in Fig. 3.2.

Centralized FL refers to the FL setting where a central server acts as the main coordinator during the learning process. In this approach, the training data remains distributed across multiple clients, but the coordination and aggregation of model updates are performed by the central server. The FL framework entails the central server distributing the global model to the clients, who subsequently perform local training using their own local datasets. After training, the clients transmit their locally updated model to the central server. The central server then aggregates these model updates, resulting in an improved global model. This iterative process of model distribution, local training, and aggregation is repeated across multiple rounds to enhance the performance of the global model.



Centralized Federated Learning

Decentralized Federated Learning

Fig. 3.2 Types of federated learning models for IoT networks

Decentralized FL, on the other hand, involves a more distributed and peer-to-peer approach. In this class of FL, there is no central server that coordinates the learning process. Instead, the participating clients form a network and collaborate directly with each other to train a shared global model. The clients exchange model updates with their neighboring devices and use those updates to refine their own local models. The collaboration and communication between the clients can occur in various ways, such as through P2P communication (blockchain) and direct device-to-device communication (Bluetooth, Wi-Fi Direct) in the network. The decentralized nature of this approach provides benefits such as improved privacy, reduced reliance on a single point of failure, and potential scalability advantages.

Both centralized FL and decentralized FL offer distinct advantages and considerations. The selection between these two classes hinges upon several factors, including the nature of the data, privacy requirements, communication capabilities, computational resources, and specific use case requirements. These factors play a pivotal role in determining the most suitable approach for a given scenario.

3.2.2.2 Types of Centralized Federated Learning

Centralized federated learning is a widely adopted architecture in IoT systems, encompassing various implementations such as cloud-based FL, edge-based FL, and cloud-edge-based FL. These architectures leverage the centralized coordination and management provided by a central server while incorporating different computing and communication trade-offs to suit specific IoT scenarios.

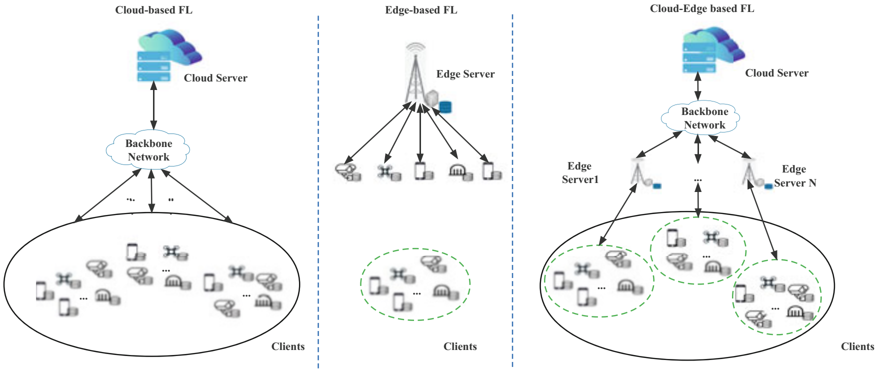


Fig. 3.3 The overview of federated learning for centralized IoT networks

In cloud-based FL, a large number of clients, potentially reaching millions (Bonawitz et al. 2019), contribute large datasets required for DL, as depicted on the left side in Fig. 3.3. However, communication with cloud servers is slow and unpredictable, resulting in inefficient training processes due to network congestion. The communication efficiency and convergence rate in Federated Averaging (FedAVG) involve a trade-off where more local computation is performed at the cost of reduced communication. Despite this, cloud-based FL benefits from the ability to access vast training samples on cloud servers.

On the other hand, edge-based FL has emerged as a response to the increasing demand for decentralized and real-time ML capabilities in IoT and edge computing environments, as depicted in the middle of Fig. 3.3. In edge-based FL, the server is placed closer to the edge, such as base stations. This architecture reduces computation latency as it aligns with the communication latency to the edge parameter server. While edge-based FL offers the advantage of faster local model updates, it has limitations in terms of the number of clients' access to each server, resulting in performance losses.

To address these challenges, a hierarchical FL system, called cloud-edge-based hierarchical FL (Liu et al. 2020; Wu et al. 2020), has been proposed, as depicted on the right side in Fig. 3.3. The architecture integrates the strengths of both cloud-based and edge-based FL approaches. It effectively harnesses the extensive training data available on cloud servers while enabling rapid model updates through local clients deployed on edge servers. Compared to cloud-based FL, the cloud-edge-based hierarchical FL significantly reduces expensive communication with the cloud servers. This reduction is accomplished through the integration of efficient client updates by edge servers, resulting in noteworthy decreases in both runtime and the number of local iterations required. Conversely, the cloud-edge-based hierarchical FL framework surpasses edge-based FL in terms of model training efficacy due to the cloud servers' access to more extensive data.

Centralized FL architectures, including cloud-based FL, edge-based FL, and cloud-edge-based FL, offer distinct advantages and trade-offs in IoT systems.

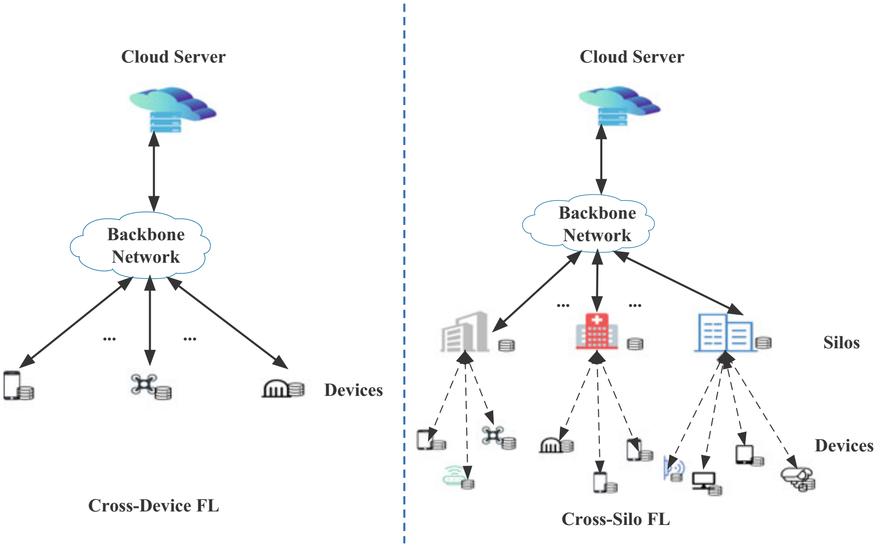


Fig. 3.4 Types of federated learning for IoT networks based on participating clients

Cloud-based FL excels in scalability and model performance but raises concerns regarding privacy, latency, and communication. In contrast, edge-based FL prioritizes privacy preservation, low latency, and efficient bandwidth utilization, but faces challenges related to resource constraints and hardware heterogeneity. Cloud-edge-based FL strikes a balance between privacy, latency, communication, and resource utilization, yet necessitates careful orchestration and deployment considerations. By comprehending the unique characteristics of each architecture and considering specific requirements, it helps to make well-informed decisions to select the most suitable FL approach for their IoT systems.

3.2.2.3 Types of Federated Learning for IoT Based on Participating Clients

According to the setting based on participating clients, FL for IoT can be classified into two types, cross-device FL and cross-silo FL, as illustrated in Fig. 3.4.

Cross-device FL refers to the scenario where the distributed devices participating in the FL process belong to different individuals or organizations, where the number of clients is big and the data size provided by each client is small (Rehman et al. 2021; Yang et al. 2022). These devices can be personal smartphones, tablets, or other IoT devices owned by different users. Each device holds its own local data and contributes to the FL process by performing local model training using its own data. The model updates are then transferred and aggregated across the devices to obtain a global model. Cross-device FL enables collaborative learning while preserving data privacy since the data remains on the devices and is not centralized.

Unlike cross-device FL, cross-silo FL involves the collaboration of multiple organizations that possess separate data silos, typically with a smaller number of organizations but with larger data volumes and many IoT devices within each organization. Each data silo represents a distinct dataset owned by a different organization (Li et al. 2023), such as different hospitals, cities, or industries. In this scenario, the organizations collaborate to train a shared global model by exchanging model updates while keeping their data locally. The data from each silo is not shared with other organizations, maintaining data privacy and security. Cross-silo FL enables the collaborative training of a more comprehensive model by leveraging diverse datasets from multiple organizations without directly sharing the raw data.

The classification of FL into cross-device and cross-silo types provides a clear distinction between scenarios involving individual devices owned by different users and scenarios involving separate organizations with their own data silos. The selection between these types depends on specific contextual factors such as data ownership, collaboration requirements, privacy considerations, and the nature of the FL for IoT applications.

3.2.3 FL Framework for IoT

This subsection provides a comprehensive overview of different frameworks that have been developed specifically for the implementation of FL for IoT networks:

(1) **FedML:** FedML is an open-source research framework that helps in developing and implementing FL algorithms (He et al. 2020). It consists of two main components: FedML-core and FedML-API. FedML-core is the low-level API component responsible for distributed communication and model training. FedML-API, built upon FedML-core, is the high-level API component that simplifies the implementation of distributed algorithms in FL. FedML is distinguished by its ability to facilitate FL on real-world hardware platforms. Notably, FedML incorporates two on-device FL testbeds, namely, FedML-Mobile and FedML-IoT, both of which are constructed using actual hardware platforms. This feature strengthens FedML's practicality and enables researchers to conduct FL experiments in authentic mobile and IoT environments.

(2) **Flower:** Flower is an open-source Python library developed by IBM Research that simplifies the implementation of FL systems by providing a high-level interface and abstraction layer (Beutel et al. 2020). It supports popular ML frameworks like PyTorch and TensorFlow, handling model update aggregation, client sampling, communication protocols, and FL system evaluation. Flower's architecture allows for experiments at global and local levels, separating client selection, parameter aggregation, and evaluation through strategy abstraction. It accommodates heterogeneous client platforms and implementations, manages

complexities like connection handling, and offers a simplified environment for researchers.

(3) **TensorFlow-Federated (TFF):** TFF is an open-source framework developed by Google that extends TensorFlow for FL (Blog n.d.). It offers tools and libraries for building and deploying ML models in federated settings, incorporating federated computations and aggregations. TFF consists of two layers: FL, providing high-level interfaces for seamless integration of existing ML models, and FC, offering lower-level interfaces for custom-federated algorithms using TensorFlow and distributed communication operators. This modular approach promotes flexibility and adaptability, empowering users to leverage FL according to their specific needs and research goals.

(4) **PySyft:** PySyft is an open-source Python library that aims to provide privacy-preserving ML and secure multiparty computation techniques (Ryffel et al. 2018). It integrates with popular DL frameworks such as PyTorch and TensorFlow, allowing users to perform privacy-enhancing tasks such as FL, encrypted computation, and differential privacy. PySyft leverages secure multiparty computation protocols, homomorphic encryption, and other cryptographic techniques to ensure the confidentiality and privacy of data in distributed learning scenarios. It offers an essential toolkit for building privacy-enhancing applications and fostering trust in collaborative ML environments.

(5) **LEAF:** LEAF, which stands for Low-resource Environments for Aggregation and FL, is a research framework and benchmark suite designed for FL under resource-constrained environments (Caldas et al. 2018). LEAF offers a curated collection of datasets, benchmarks, and evaluation metrics explicitly designed to evaluate the efficacy of FL algorithms in scenarios characterized by limited computational resources, constrained bandwidth, or energy constraints. By providing a standardized platform, LEAF facilitates benchmarking and comparative analysis of diverse algorithms and methodologies, thereby fostering advancements in FL techniques for resource-constrained settings. This framework plays a pivotal role in promoting research and innovation in privacy-preserving machine learning within challenging resource limitations.

(6) **FATE:** FATE, short for Federated AI Technology Enabler, is an open-source FL platform developed by WeBank's AI department (FedAI n.d.). FATE is a framework that aims to address the challenges of privacy, security, and trust in FL, providing a secure and reliable environment for FL system development. By offering a comprehensive suite of tools and components, including FL algorithms, distributed computing protocols, secure computation mechanisms, and privacy protection techniques, FATE enables the development and deployment of large-scale FL systems across diverse domains such as finance, healthcare, and smart cities. FATE plays a significant role in advancing FL research and innovation, contributing to the establishment of robust and privacy-preserving FL practices in various academic and industrial contexts.

(7) **Paddle FL:** Paddle FL is a federated learning framework developed by PaddlePaddle, an open-source deep learning platform (Ma et al. 2019). It is a comprehensive framework that facilitates FL using PaddlePaddle. It supports

various FL scenarios and integrates with PaddlePaddle's distributed computing capabilities to provide efficient strategies for model update aggregation, communication, and synchronization. With flexible options for model architectures, optimization algorithms, and customization, Paddle FL enables developers to create tailored FL systems. It focuses on scalability, efficiency, and privacy preservation, allowing for the training of large-scale models on distributed data sources while ensuring data security.

3.3 Federated Learning for IoT Applications

This section offers a comprehensive discussion on the integration of FL into various essential IoT applications. These applications encompass smart healthcare, vehicular IoT, smart cities, smart industries, and cybersecurity.

3.3.1 FL for Smart Healthcare

The IoT revolution has demonstrated significant potential for numerous healthcare applications, leveraging the vast amount of medical data collected through IoT devices. However, the increasing demands for privacy and security of healthcare data have resulted in each IoT device becoming an isolated data island. To tackle this challenge, the emergence of FL has introduced new possibilities for healthcare applications (Yuan et al. 2020; Chen et al. 2020; He et al. 2023b). FL enables collaborative and privacy-preserving machine learning, with immense potential to transform the landscape of smart healthcare. It empowers healthcare service providers to collectively leverage their data and knowledge, thereby enhancing the performance of diagnoses (Elayan et al. 2021) while adhering to stringent data privacy regulations and ethical considerations (Singh et al. 2022).

3.3.2 FL for Vehicular IoT

Vehicular IoT systems, encompassing cooperative autonomous driving and intelligent transport systems (ITS), are particularly susceptible to privacy breaches due to the abundance of devices and privacy-sensitive data. FL holds significant promise as an effective approach to address privacy concerns and optimize resource utilization in future vehicular IoT systems (Du et al. 2020). By preserving data privacy, fostering collaboration, and leveraging localized computing capabilities, FL can enable the realization of efficient and privacy-preserving cooperative autonomous driving (Li et al. 2021; Nguyen et al. 2022) and intelligent transport networks (Manias & Shami 2021; Zhao et al. 2022). However, further research and development efforts are necessary to tailor FL algorithms to the specific requirements of vehicular IoT systems and overcome challenges related to scalability, heterogeneity, and trustworthiness. By addressing these challenges, FL can pave the way for the widespread deployment of secure and privacy-preserving vehicular IoT systems, contributing to safer and more efficient transportation networks.

3.3.3 FL for Smart City

Smart cities are rapidly evolving ecosystems that leverage various IoT technologies to enhance urban services and infrastructure. However, the massive amount of data collected by IoT devices raises significant concerns regarding privacy and resource efficiency. FL has emerged as a promising approach to address privacy concerns and optimize resource utilization in smart city environments, offering significant potential for enhancing the efficiency and privacy of smart city applications (Jiang et al. 2020). By enabling distributed model training and preserving data privacy, FL can facilitate the development of more efficient and privacy-preserving smart city systems. The adoption of FL in smart city deployments requires further research and development to address challenges related to heterogeneity, model consistency, network dynamics, and trustworthiness. By overcoming these challenges, FL can contribute to the realization of intelligent and privacy-conscious smart city ecosystems, promoting sustainable urban development and improving the quality of life for citizens (Imteaj & Amini 2019; Qolomany et al. 2020; He et al. 2023a).

3.3.4 FL for Smart Industry

Smart industry, powered by industrial Internet of Things (IIoT) technologies, poses unique challenges concerning privacy and resource efficiency. FL presents a promising approach to address these challenges by offering privacy preservation and resource optimization in smart industry applications (Pham et al. 2021), enhancing privacy preservation while improving resource efficiency in industrial IoT deployments. However, additional research and development efforts are necessary to overcome challenges related to network heterogeneity, model synchronization, and security. Addressing these challenges would enable FL to unlock the full potential of smart industry, fostering efficient and privacy-conscious industrial processes, and facilitating data-driven decision-making for enhanced productivity and competitiveness (Li et al. 2022; Yang et al. 2021; Qolomany et al. 2020; Ma et al. 2021).

3.3.5 FL for Cybersecurity

Cybersecurity has become a critical issue in the digital age, requiring effective solutions to detect threats and protect privacy. With the continuous expansion of IoT services and applications, the decentralization paradigm has attracted a lot of attention from government, academia, and industry in cybersecurity and ML for IoT. FL has gained prominence as a promising approach for addressing cybersecurity challenges, offering innovative solutions to enhance the security and efficiency of IoT systems. The concept of federated cybersecurity (FC) (Ghimire & Rawat 2022) is considered revolutionary, as it paves the way for a more secure and efficient future in IoT environments by effectively detecting security threats, improving accuracy, and enabling real-time response in network systems (Belenguer et al. 2022; Attota et al. 2021; Issa et al. 2023; Liu et al. 2020). Future advancements in FL algorithms and privacy-enhancing techniques will further strengthen the effectiveness and scalability of FL for cybersecurity applications, contributing to a more secure digital landscape.

3.4 Research Challenges and Directions

Despite the aforementioned benefits, the implementation of FL for IoT still faces numerous challenges, as outlined below.

3.4.1 Heterogeneity of IoT Devices

The heterogeneity observed among IoT devices poses significant challenges to the implementation of FL in IoT applications. This heterogeneity encompasses both data heterogeneity and device heterogeneity. To address these challenges, it is essential to develop adaptive FL algorithms capable of accommodating the diverse capabilities of IoT devices. Additionally, FL algorithms need to consider the limitations of resource-constrained environments and limited power sources. To mitigate these constraints, it is crucial to incorporate energy-efficient strategies and optimization techniques that minimize computational and communication overhead. Moreover, the dynamic nature of IoT networks introduces further challenges related to device mobility and connectivity fluctuations. FL algorithms should account for device mobility, enabling seamless model synchronization and training continuity even during device joins or departures, as well as intermittent connectivity. To overcome the heterogeneity of IoT devices, future research should prioritize the development of adaptive and robust FL algorithms (Sun et al. 2020) capable of effectively handling varying capabilities (Li et al. 2022; Wang et al. 2021; Pang et al. 2020; Chen et al. 2021), resource constraints (Imteaj et al. 2022; Savazzi et al. 2020), and dynamic network conditions (Wang et al. 2021).

3.4.2 Limited Computational Resources

The implementation of FL for IoT applications encounters challenges arising from the limited computational resources available on IoT devices. These devices possess constraints in processing power, memory, and energy, which impede the execution of complex ML algorithms necessary for FL. To address this issue, it is crucial to develop resource-efficient FL algorithms that employ techniques such as model compression, lightweight architectures, and efficient communication protocols. These techniques aim to minimize the computational overhead associated with FL operations. The heterogeneity of computational resources among devices further complicates the design of FL algorithms, necessitating the adoption of adaptive approaches capable of adjusting computational requirements based on device capabilities and availability. Moreover, ensuring energy efficiency is of paramount importance, and FL algorithms should incorporate strategies such as reducing device participation frequency and duration, employing compressed model updates, and leveraging local computation to minimize energy consumption. Therefore, future research should focus on the development of resource-constrained algorithms (Imteaj et al. 2021) that achieve a balance between computational efficiency, model accuracy, and energy consumption, while also exploring techniques for adaptive resource allocation (Nguyen et al. 2020), and energy optimization (Yu et al. 2021) to facilitate the effective deployment of FL in resource-constrained IoT environments.

3.4.3 Communication and Bandwidth Limitations

The successful implementation of FL for IoT applications faces significant challenges attributed to limitations in communication and bandwidth (Brown et al. 2020). IoT devices operate within resource-constrained environments characterized by restricted network bandwidth, intermittent connectivity, and diverse communication protocols. To address these challenges, communication-efficient FL algorithms can minimize data transmission and reduce reliance on continuous connectivity through techniques such as model compression (Itahara et al. 2020; Bernstein et al. 2018), client selection (McMahan et al. 2017c; Li et al. 2021), and sparse updates (Thonglek et al. 2022). Additionally, adaptive strategies for communication scheduling can optimize bandwidth utilization (Hönig et al. 2022; Diao et al. 2020). These approaches enable communication-efficient FL algorithms that minimize data transmission, reduce reliance on continuous connectivity, and optimize bandwidth utilization. By leveraging these techniques, FL can be effectively applied to

IoT environments, unlocking the potential for distributed machine learning while accommodating the unique constraints of resource-constrained IoT devices.

3.4.4 Privacy and Security Concerns

Privacy and security concerns pose significant challenges to the implementation of FL for IoT applications (Briggs et al. 2021). FL involves the sharing and aggregation of sensitive data from multiple devices, raising concerns about data privacy and potential security breaches. To address these concerns, robust privacy-preserving techniques should be developed, such as differential privacy (Zhao et al. 2020; Zhou et al. 2020) and blinding technique (Fu et al. 2020; Zhou et al. 2020). These techniques ensure that individual device data remains private and secure during the FL process. In addition, securing FL against potential attacks and malicious participants is crucial. FL algorithms should incorporate mechanisms for detecting and mitigating adversarial behavior, such as anomaly detection (Liu et al. 2020; Cui et al. 2021). Furthermore, implementing robust authentication and access control mechanisms prevents unauthorized devices from participating in the FL process (Li et al. 2022). Compliance with data privacy regulations and ethical considerations is essential in FL for IoT. Adhering to regulatory frameworks like the General Data Protection Regulation (GDPR) and integrating privacy-by-design principles ensures transparent and privacy-preserving FL processes.

3.4.5 Scalability and Management

The successful implementation of FL for IoT applications is impeded by scalability and management concerns. Scalability encompasses the FL system's ability to effectively handle a large number of participating clients and increasing data volumes. As the IoT system expands with a growing number of clients and data sources, FL algorithms need to efficiently manage the aggregation of model updates and ensure timely convergence. Thus, the development of scalable FL architectures and distributed optimization techniques become crucial to accommodate the growing scale of IoT deployments. Furthermore, effective management of FL systems is paramount for their seamless operation. This entails various tasks such as device registration, model synchronization, performance monitoring, and fault tolerance. The development of comprehensive management frameworks and protocols is necessary to ensure the reliability, availability, and performance of FL systems within dynamic IoT environments. To address the challenges associated with scalability and management in FL for IoT, future research should prioritize the development of scalable and efficient algorithms capable of handling large-scale deployments and increasing data volumes (Imteaj et al. 2022; Savazzi et al.

2020; Rahman et al. 2020). Additionally, robust management frameworks need to be designed to facilitate seamless client management, model synchronization, and system monitoring, thus contributing to the successful deployment and operation of FL in IoT environments (Li et al. 2022; Rey et al. 2022; Khan et al. 2020; Cui et al. 2021).

3.4.6 Federated Domain Generalization

Federated domain generalization (FDG) is a critical consideration in implementing FL for IoT applications as it pertains to the ability of FL models to effectively generalize across diverse data domains collected from various clients or locations within IoT environments (Ying et al. 2023b). Domain shift can lead to performance degradation when models are deployed in new or unseen domains. Addressing FDG necessitates the development of robust techniques like domain adaptation (Wu & Gong 2021; Zhang et al. 2023), transfer learning (Shenaj et al. 2023; Zhang & Li 2021), and meta-learning (Chen et al. 2021; Lin et al. 2020), which aim to enhance the generalization capabilities of FL models across diverse domains by leveraging knowledge from multiple domains and incorporating domain-awareness mechanisms. Addressing data distribution heterogeneity in FL is essential to prevent biased models that excel on certain devices but underperform on others, stemming from variations in data distributions. Techniques like data augmentation (Duan et al. 2019; Yang & Soatto 2020) and adaptive aggregation (Yang et al. 2022; Shenaj et al. 2023) can be employed to mitigate distributional differences and improve the generalization performance of FL models across devices. Future research should prioritize the development of techniques and algorithms that effectively address domain shifts and data distribution heterogeneity in order to enhance the generalization capabilities of FL models, ensuring robust performance across diverse domains and IoT devices.

3.5 Conclusion

FL is a significant research area within the IoT environment. This work provides a comprehensive introduction to the field of FL for IoT, serving as a valuable resource for researchers seeking in-depth insights into FL in the IoT environment. By covering the theoretical foundations of FL, the architecture of FL for IoT, the different types of FL for IoT, FL frameworks tailored for IoT, diverse FL for IoT applications, and future research challenges and directions pertaining to FL for IoT, it provides a comprehensive view of the field. This work offered herein aims to offer valuable insights to researchers and inspire further research for novel advancements in privacy-preserving FL techniques for IoT.

References

Abbas, Nasir, et al. 2017. Mobile edge computing: A survey. *IEEE Internet of Things Journal* 5 (1): 450–465.

Al-Fuqaha, Ala et al. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17 (4): 2347–2376.

Attota, Dinesh Chowdary, et al. 2021. An ensemble multi-view federated learning intrusion detection for IoT. *IEEE Access* 9: 117734–117745.

Belenguer, Aitor, et al. 2022. A review of federated learning in intrusion detection systems for IoT. arXiv preprint. arXiv:2204.12443.

Bernstein, Jeremy, et al. 2018. signSGD: Compressed optimisation for non-convex problems. In *International Conference on Machine Learning*, 560–569. PMLR.

Beutel, Daniel J., et al. 2020. Flower: A friendly federated learning research framework. arXiv preprint. arXiv:2007.14390.

Blog, Tensorflow (n.d.). Introducing TensorFlow Federated. https://blog.tensorflow.org/2019/03/introducing-tensorflow-federated.html. Accessed Jun 15, 2023.

Bonawitz, Keith, et al. 2019. Towards federated learning at scale: System design. *Proceedings of Machine Learning and Systems* 1: 374–388.

Briggs, Christopher, et al. 2021. A review of privacy-preserving federated learning for the Internet-of-Things. In: *Federated Learning Systems: Towards Next-Generation AI*, 21–50.

Brown, Tom, et al. 2020. Language models are few-shot learners. *Advances in Neural Information Processing Systems* 33: 1877–1901.

Caldas, Sebastian, et al. 2018. Leaf: A benchmark for federated settings. arXiv preprint. arXiv:1812.01097.

Cao, Bin, et al. 2019. Intelligent offloading in multi-access edge computing: A state-of-the-art review and framework. *IEEE Communications Magazine* 57 (3): 56–62.

Chen, Yiqiang, et al. 2020. Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intelligent Systems* 35 (4): 83–93.

Chen, Zheyi, et al. 2021. Towards asynchronous federated learning for heterogeneous edge-powered internet of things. *Digital Communications and Networks* 7 (3): 317–326.

Cui, Lei, et al. 2021. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Transactions on Industrial Informatics* 18 (5): 3492–3500.

Diao, Enmao, et al. 2020. HeteroFL: Computation and communication efficient federated learning for heterogeneous clients. arXiv preprint. arXiv:2010.01264.

Donta, Praveen Kumar, et al. 2023. Learning-driven ubiquitous mobile edge computing: Network management challenges for future generation Internet of Things. *International Journal of Network Management* 33 (5): e2250.

Du, Zhaoyang, et al. 2020. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society* 1: 45–61.

Duan, Moming, et al. 2019. Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications. In *2019 IEEE 37th International Conference on Computer Design (ICCD)*, 246–254. Piscataway: IEEE.

Elayan, Haya, et al. 2021. Deep federated learning for IoT-based decentralized healthcare systems. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 105–109. Piscataway: IEEE.

FedAI. n.d. *An Industrial Grade Federated Learning Framework*. https://fate.fedai.org. Accessed Jun 15, 2023.

Fu, Anmin, et al. 2020. VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT. *IEEE Transactions on Industrial Informatics* 18 (5): 3316–3326.

Ghimire, Bimal, and Danda B. Rawat. 2022. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal* 9 (11): 8229–8249.

He, Chaoyang, et al. 2020. FedML: A research library and benchmark for federated machine learning. arXiv preprint. arXiv:2007.13518.

He, Qiang, Yu Wang, et al. 2023a. is in Early Access.

He, Qiang, Zheng Feng, et al. 2023b. is in Early Access.

Hönig, Robert et al. 2022. DAdaQuant: Doubly-adaptive quantization for communication-efficient Federated Learning. In *International Conference on Machine Learning*, 8852–8866. PMLR.

Imteaj, Ahmed, and M. Hadi Amini. 2019. 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)*, 1156–1161. Piscataway: IEEE.

Imteaj, Ahmed, et al. 2022. Federated learning for resource-constrained IoT devices: Panoramas and state of the art. In *Federated and transfer learning. Adaptation, learning, and optimization*, ed. Razavi-Far, R., Wang, B., Taylor, M.E., Yang, Q. vol. 27, 7–27. Cham: Springer.

Imteaj, Ahmed, Urmish Thakker, et al. 2021. A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal* 9 (1): 1–24.

Issa, Wael, et al. 2023. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys* 55 (9): 1–43.

Itahara, Sohei, et al. 2020. Lottery hypothesis based unsupervised pre-training for model compression in federated learning. In *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, 1–5. Piscataway: IEEE.

Jiang, Ji Chu, et al. 2020. Federated learning in smart city sensing: Challenges and opportunities. *Sensors* 20 (21): 6230.

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

Khan, Latif U., et al. 2020. Resource optimized federated learning-enabled cognitive internet of things for smart industries. *IEEE Access* 8: 168854–168864.

Li, Ang, et al. 2021. Hermes: an efficient federated learning framework for heterogeneous mobile clients. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 420–437.

Li, Huilin, et al. 2023. Privacy-preserving cross-silo federated learning atop blockchain for IoT. *IEEE Internet of Things Journal* 10 (24), 21176–21186. https://doi.org/10.1109/JIOT.2023.3279926.

Li, Yijing, et al. 2021. Privacy-preserved federated learning for autonomous driving. *IEEE Transactions on Intelligent Transportation Systems* 23 (7): 8423–8434.

Li, Ying, et al. 2023. VARF: An incentive mechanism of cross-silo federated learning in MEC. *IEEE Internet of Things Journal* 10 (17), 15115–15132. https://doi.org/10.1109/JIOT.2023.3264611.

Li, Ying, Xingwei Wang, Rongfei Zeng, Praveen Kumar Donta, et al. 2023a. Federated domain generalization: A survey. arXiv preprint. arXiv:2306.01334.

Li, Ying, Xingwei Wang, Rongfei Zeng, Praveen Kumar Donta, et al. 2023b. Federated domain generalization: A survey. arXiv preprint. arXiv:2306.01334.

Li, Ying, Yaxin Yu, and Xingwei, Wang. 2023. Three-tier storage framework based on TBchain and IPFS for protecting IoT security and privacy. *ACM Transactions on Internet Technology* 23 (3): 1–28.

Li, Yuanjiang, et al. 2022. An effective federated learning verification strategy and its applications for fault diagnosis in industrial IOT systems. *IEEE Internet of Things Journal* 9 (18): 16835–16849.

Li, Zonghang, et al. 2022. Data heterogeneity-robust federated learning via group client selection in industrial IoT. *IEEE Internet of Things Journal* 9 (18): 17844–17857.

Lin, Sen, et al. 2020. A collaborative learning framework via federated meta-learning. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 289–299. Piscataway: IEEE.

Liu, Lumin, et al. 2020. Client-edge-cloud hierarchical federated learning. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 1–6. Piscataway: IEEE.

Liu, Yi, et al. 2020. Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal* 8 (8): 6348–6358.

Ma, Lianbo, et al. 2021. TCDA: Truthful combinatorial double auctions for mobile edge computing in industrial Internet of Things. *IEEE Transactions on Mobile Computing* 21 (11): 4125–4138.

Ma, Yanjun, et al. 2019. PaddlePaddle: An open-source deep learning platform from industrial practice. *Frontiers of Data and Domputing* 1 (1): 105–115.

Manias, Dimitrios Michael, and Abdallah Shami. 2021. Making a case for federated learning in the internet of vehicles and intelligent transportation systems. *IEEE Network* 35 (3): 88–94.

McMahan, Brendan, et al. 2017a. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, 1273–1282. PMLR.

McMahan, Brendan, et al. 2017b. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, 1273–1282. PMLR.

McMahan, Brendan, et al. 2017c. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, 1273–1282. PMLR.

Nguyen, Anh, et al. 2022. Deep federated learning for autonomous driving. In *2022 IEEE Intelligent Vehicles Symposium (IV)*, 1824–1830. Piscataway: IEEE.

Nguyen, Van-Dinh, et al. 2020. Efficient federated learning algorithm for resource allocation in wireless IoT networks. *IEEE Internet of Things Journal* 8 (5): 3394–3409.

Pang, Junjie, et al. 2020. Realizing the heterogeneity: A self-organized federated learning framework for IoT. In *IEEE Internet of Things Journal* 8 (5): 3088–3098.

Pham, Quoc-Viet, et al. 2021. Fusion of federated learning and industrial internet of things: a survey. arXiv preprint. arXiv:2101.00798.

Qolomany, Basheer, et al. 2020. Particle swarm optimized federated learning for industrial IoT and smart city services. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, 1–6. Piscataway: IEEE.

Rahman, Sawsan Abdul, et al. 2020. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Network* 34 (6): 310–317.

Rehman, Muhammad Habib ur, et al. 2021. TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT. *IEEE Transactions on Industrial Informatics* 17 (12): 8485–8494.

Rey, Valerian, et al. 2022. Federated learning for malware detection in iot devices. *Computer Networks* 204: 108693.

Ryffel, Theo, et al. 2018. A generic framework for privacy preserving deep learning. arXiv preprint. arXiv:1811.04017.

Saad, Walid, et al. 2019. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network* 34 (3): 134–142.

Savazzi, Stefano, et al. 2020. Federated learning with cooperating devices: A consensus approach for massive IoT networks. *IEEE Internet of Things Journal* 7 (5): 4641–4654.

SEMICONDUCTORDIGEST. n.d. Number of connected IoT devices will surge to 125 billion by 2030. https://sst.semiconductor-digest.com/2017/10/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030. Accessed Jun 11, 2023

Shenaj, Donald, et al. 2023. Learning across domains and devices: Style-driven source-free domain adaptation in clustered federated learning. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 444–454.

Singh, Saurabh, et al. 2022. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems* 129: 380–388.

Statista. n.d. Data volume of internet of things (IoT) connections worldwide in 2019 and 2025. https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size. Accessed Jun 11, 2023

Sun, Wen, et al. 2020. Adaptive federated learning and digital twin for industrial internet of things. *IEEE Transactions on Industrial Informatics* 17 (8): 5605–5614.

Tataria, Harsh, et al. 2021. 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. *Proceedings of the IEEE* 109 (7): 1166–1199.

Thonglek, Kundjanasith, et al. 2022. Sparse communication for federated learning. In *2022 IEEE 6th International Conference on Fog and Edge Computing (ICFEC)*, 1–8. Piscataway: IEEE.

Wang, Han, et al. 2021. Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 153–163.

Wang, Zhiyuan, et al. 2021. Resource-efficient federated learning with hierarchical aggregation in edge computing. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, 1–10. Piscataway: IEEE.

Wu, Guile, and Shaogang Gong. 2021. Collaborative optimization and aggregation for decentralized domain generalization and adaptation. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 6484–6493.

Wu, Qiong, et al. 2020. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. *IEEE Open Journal of the Computer Society* 1: 35–44.

Yang, Hui, et al. 2021. BrainIoT: Brain-like productive services provisioning with federated learning in industrial IoT. *IEEE Internet of Things Journal* 9 (3): 2014–2024.

Yang, Seunghan, et al. 2022. *Client-agnostic Learning and Zero-shot Adaptation for Federated Domain Generalization*. Submitted to ICLR 2023.

Yang, Wenti, et al. 2022. A practical cross-device federated learning framework over 5g networks. *IEEE Wireless Communications* 29 (6): 128–134.

Yang, Yanchao, and Stefano Soatto. 2020. FDA: Fourier domain adaptation for semantic segmentation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 4085–4095.

Yu, Liangkun, et al. 2021. Jointly optimizing client selection and resource management in wireless federated learning for internet of things. *IEEE Internet of Things Journal* 9 (6): 4385–4395.

Yuan, Binhang, et al. 2020. A federated learning framework for healthcare IoT devices. arXiv preprint. arXiv:2005.05083.

Zeng, Rongfei, Chao Zeng, et al. 2021. A comprehensive survey of incentive mechanism for federated learning. arXiv preprint. arXiv:2106.15406.

Zeng, Rongfei, Shixun Zhang, et al. 2020. FMore: An incentive scheme of multi-dimensional auction for federated learning in MEC. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 278–288. Piscataway: IEEE.

Zhang, Liling, et al. 2023. Federated learning for IoT devices with domain generalization. *IEEE Internet of Things Journal* 10 (11) 9622–9633. https://doi.org/10.1109/JIOT.2023.3234977.

Zhang, Wei, and Xiang Li. 2021. Federated transfer learning for intelligent fault diagnostics using deep adversarial networks with data privacy. *IEEE/ASME Transactions on Mechatronics* 27 (1): 430–439.

Zhao, Jianxin, et al. 2022. Participant selection for federated learning with heterogeneous data in intelligent transport system. *IEEE transactions on intelligent transportation systems* 24 (1): 1106–1115.

Zhao, Yang, et al. 2020. Local differential privacy-based federated learning for internet of things. *IEEE Internet of Things Journal* 8 (11): 8836–8853.

Zhou, Chunyi, et al. 2020. Privacy-preserving federated learning in fog computing. *IEEE Internet of Things Journal* 7.11, pp. 10782–10793.