future internet

MDPI

Review

Federated Learning and Its Role in the Privacy Preservation of IoT Devices

Tanweer Alam [1,*] and Ruchi Gupta [2]

[1] Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia
[2] Department of Computer Science, Ajay Kumar Garg Engineering College, Ghaziabad 201015, India
* Correspondence: tanweer03@iu.edu.sa

Abstract: Federated learning (FL) is a cutting-edge artificial intelligence approach. It is a decentralized problem-solving technique that allows users to train using massive data. Unprocessed information is stored in advanced technology by a secret confidentiality service, which incorporates machine learning (ML) training while removing data connections. As researchers in the field promote ML configurations containing a large amount of private data, systems and infrastructure must be developed to improve the effectiveness of advanced learning systems. This study examines FL in-depth, focusing on application and system platforms, mechanisms, real-world applications, and process contexts. FL creates robust classifiers without requiring information disclosure, resulting in highly secure privacy policies and access control privileges. The article begins with an overview of FL. Then, we examine technical data in FL, enabling innovation, contracts, and software. Compared with other review articles, our goal is to provide a more comprehensive explanation of the best procedure systems and authentic FL software to enable scientists to create the best privacy preservation solutions for IoT devices. We also provide an overview of similar scientific papers and a detailed analysis of the significant difficulties encountered in recent publications. Furthermore, we investigate the benefits and drawbacks of FL and highlight comprehensive distribution scenarios to demonstrate how specific FL models could be implemented to achieve the desired results.

Keywords: federated learning; artificial intelligence; privacy; security; machine learning

Citation: Alam, T.; Gupta, R. Federated Learning and Its Role in the Privacy Preservation of IoT Devices. *Future Internet* **2022**, *14*, 246. https://doi.org/10.3390/fi14090246

Academic Editors: Georgios Kambourakis

Received: 27 July 2022
Accepted: 14 August 2022
Published: 23 August 2022

1. Introduction

Federated learning was introduced in 2016 by Brendan McMahan [1]. Local data are used to download and integrate the current model into the system. A single federated and enhanced global model is then supplied to the devices because these locally trained models are combined (i.e., weighted on average) [2].

1.1. FL Basics

FL generally enables ML to extract data from various datasets stored at different locations. This method allows several organizations to work in partnership on model advancement, not including distributing confidential information. Shared models have been exposed to a much broader range of data than a single internal entity during multiple training processes [3]. In other words, FL focuses on ML by not requiring data to be integrated into a single location. Instead, the model is trained in multiple domains with multiple iterations [4]. FL is a computational approach that involves training the algorithms on shared smart devices or platforms that hold local training datasets that are not shared. The server is responsible for managing the training procedure, which consists of the following essential steps:

1. Implementing the training algorithm.
2. Assembling all learning results for devices.

3. Changing the global model.
4. Notifying devices after the global model-based improvement and preparing for the next training session.

In the meantime, devices represent digital assets on a secure server and can apply the training model to their data [5]. When the server accesses a model, each device initiates the training process. Then, a set of communication rules is used to send the learning results to the server. Compared to single classification algorithms, this approach is radically different. High-performance processes usually begin with small data samples transmitted to a data center [6].

It is possible for several actors to develop robust learning models that do not incorporate the distribution of information, which allows them to address many significant concerns, such as the security of data, the privacy of data, and access to data [7]. The local and global models in FL are shown in Figure 1.

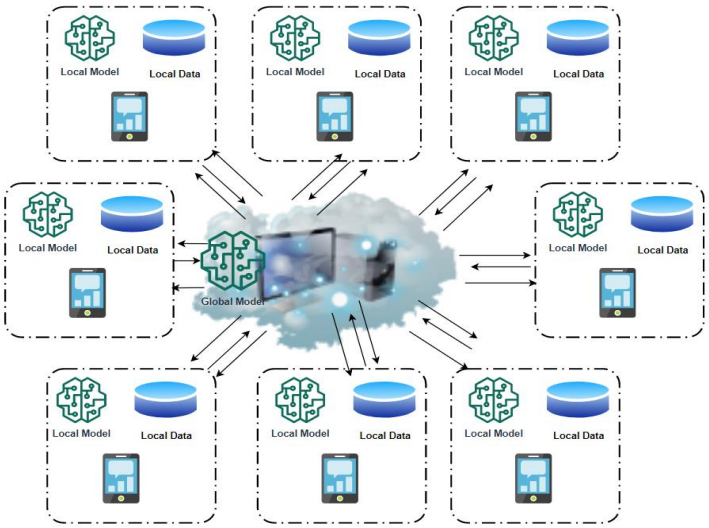

Figure 1. Local vs. global models in FL.

1.2. Roles of FL Applications

The applications of FL have expanded to various fields, including security, telecommunications, the Internet of Things, and medicine. FL seeks to prepare an ML algorithm without directly sharing data samples, such as artificial neural networks, using various local data available in current situations. Figure 2 shows the development of FL between 2016 and 2022 (Google Trends) [8]. A common goal is to train local models in local data samples and perform a periodic exchange of bounds (such as deep neural network strengths and perceptions) among these local nodes to produce a universal model distributed by the whole device. The most significant difference between FL and distributed delivery is the supposition of local databases, as the distributed learning initiative aims to simulate IoT device performance. In contrast, FL aims to train on different databases. Although federated learning introduces a single model on multiple servers, it is common to assume that the local databases are evenly distributed and approximately equal in size.

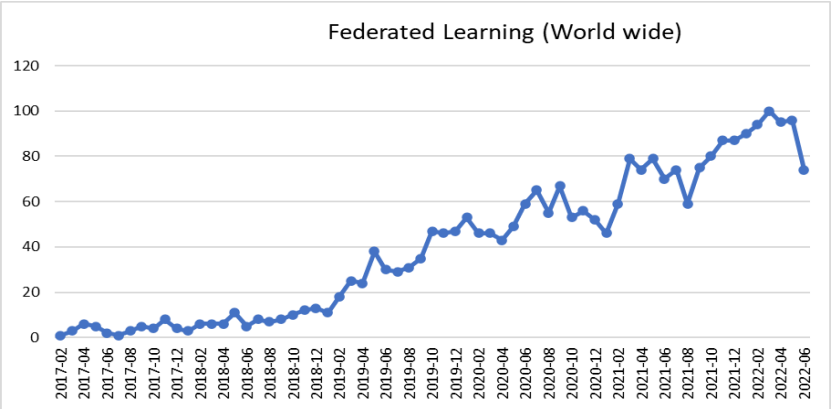

Figure 2. FL between 2016 and 2022 (Google Trends).

Instead, the datasets are usually different, and the sizes could be extensive instructions of implication [9]. The clients participating in federated learning may be inefficient because they deeply trust less-efficient communications and battery-powered IoT devices than clients participating in distributed data, where shared nodes interact with high computing power [10]. FL works like this: The client machine installs the current model, updates it with data from its device, and then encapsulates the improvements as a small, targeted change. This adjustment is only when the model is transferred to the server through secured connections. It may easily be coupled with other device improvements to strengthen the sharing models [11]. The user's device maintains all training data, and no updates are saved on the cloud. The cloud service is utilized during the learning process to schedule FL, set different algorithms, and link all the participating nodes [12]. The service is responsible for selecting the connections starting the preparation stage and compiling the accepted model updates. The server can be a bottleneck as all selected nodes must submit updates to an association [13]. IoT devices can join a distributed learning environment to find a global model. Since model updates are exchanged between related devices without establishing a central server, this avoids single-point failure. However, the network topology can affect the learning process's efficiency.

Various applications are used on smart and IoT devices [14]. Most current FL strategies assume local models share the same structure as the global model context. Heterogeneous FL (HeteroFL), a modern digital learning system, has recently been developed to meet the needs of a wide range of computer-enabled and highly connected customers. The HeteroFL method can produce a single tendency model while training multiple local models with a wide range of dynamic variables. Our study begins with exploring and discussing the various ML structures before reviewing the FL. Throughout this study, the authors offer a novel classification of FL themes and research fields based on a massive review of the innovative enabling issues and existing previous works [15], which differs from prior surveys in the area. A complete control system, in this sense, includes a wide variety of demanding features, contributions, and documentation trends, such as basic program models and projects, application domains, privacy and security, and resource management.

The authors also go through some of the most pressing issues and current research indications [16]. The authors discuss key challenges and present research indicators for effective FL programs. People nowadays create massive volumes of information on networked machines such as mobile devices or IoT gadgets, portable health products, etc. Artificial intelligence (AI) is already ubiquitous and essential in all relevant domains, enhancing our lives and recognizing the abundance of data and the scarcity of ML models. In short, deep learning (DL) is driving today's AI explosion. It has produced an embarrassment of agendas that are used by people all over the world daily. On the other hand, despite the rapid development of DL, existing methods continue to support cloud-centric applications. The list of abbreviations used in this study is shown in Table 1.

Table 1. List of abbreviations.

Abbreviation	Means
FL	Federated Learning
IoT	Internet of Things
ML	Machine Learning
AI	Artificial Intelligence
DL	Deep Learning
CAGR	Compound annual growth rate
BFSI	Banking, finance, and insurance
SBN	Static Batch Normalization
FC	Federated cloud
HeteroFL	Heterogeneous Federated Learning
SGD	Stochastic gradient descent
FDBS	Federated database systems
PRLC	Pulling Reduction with Local Compensation
FedAvg	Federated Averaging
BlockFL	Blockchain-based federated learning
MEC	Mobile edge computing
TCP CUBIC	Transmission control protocol and Cubic Curve Binary Increase Congestion

1.3. Importance of FL

The global knowledge market is expected to grow at a compound annual growth rate (CAGR) of 44.1%, from $1.03 billion in 2016 to USD 8.81 billion in 2022 [17]. Growing technological breakthroughs and data processing are the primary drivers of growth in the e-learning industry. The banking, finance, and insurance (BFSI) sector contribute significantly to the current ML market, with life science and healthcare showing rapid growth. Other verticals contributing to the data include government and defense, energy resources, telecommunications, and manufacturing. To enable more innovative applications, ML must extract delicate parameters from data generated separately from the verticals [18]. North America will be the largest ML market by the end of 2022, with the rest accounting for the remaining top five markets.

The IoT market is expected to grow by 24.7 percent from its current value of USD 190 billion by 2026. The IoT market and other industries are being driven by telecom, transportation, manufacturing, healthcare, government, retail, and BFSI. The BFSI sector accounts for the majority of the total. The Asia Pacific region generated the most revenue in 2018, USD 74.5 billion, and was expected to maintain its lead in the IoT market in 2019. China has the highest share in the Asia Pacific region. Aside from the market stake for ML and IoT, the amount of research literature published this year was higher than the previous year. Based on the information presented above, it is predicted that opportunities for research narratives will emerge soon as a result of ML and IoT [19].

1.4. Challenge

Recent surveys and scholars have studied FL. First, we provided an overview of FL. Second, there are numerous solutions to major implementation issues [20]. During the learning process, FL necessitates regular communication among devices. As a result, switching the constraints of the ML standard requires sufficient local processing capacity, recollection, and a high bandwidth connection. However, the equipment also prevents data transmission, which is necessary before beginning ML in the transitional stage. However, devices commonly used in FL, such as IoT devices or smartphones connected to Wi-Fi networks, are restricted from communicating. Even though models cost more to

transmit data, FL methods may not be appropriate [21]. Figure 3 depicts the FL [22] model updating. FL includes several mathematical tasks:

i. Differences between different local portions of data: Each node may have some bias towards multiple individuals, and the size of databases may vary significantly.
ii. Temporary heterogeneity: the database distribution for each area may vary over time.
iii. Database interaction of each node is a requirement.
iv. The database for each node may need to be overwritten by default.
v. Disappearing training data may allow attackers to go after the domain standard.
vi. Due to the lack of global training data, it is necessary to identify the undesirable options that feed into the training, such as age and gender.
vii. Limited or complete model loss is renewed due to node failure affecting the global standard.

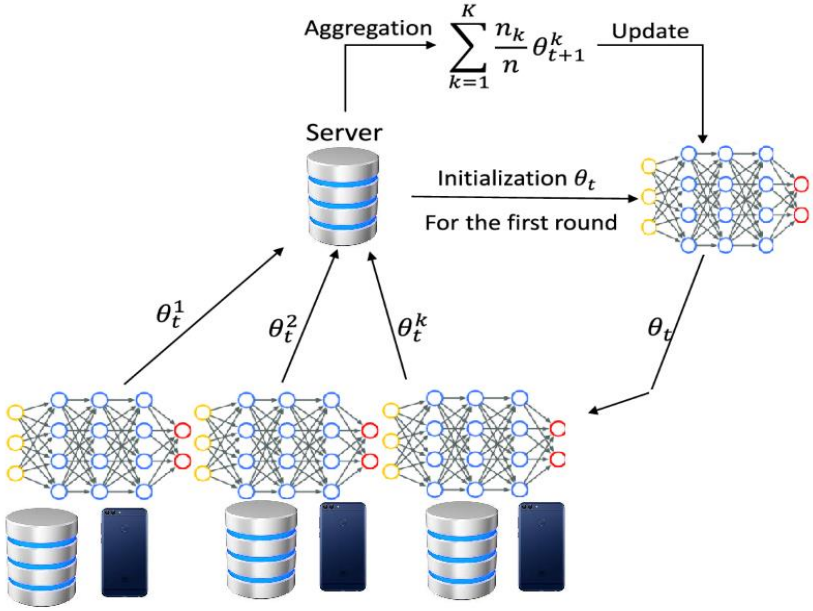

Figure 3. Models are updating in FL.

FL would be the unique form of intelligence that uses limited knowledge and training to provide learning to the device's edge or immediately to the user. It uses a highly recent training facility called "emergence in AI" because it was concerned with information security. Security and privacy challenges with FL must be recognized, analyzed, and documented before FL can become ubiquitous and widely adopted in the research field [22]. It is recommended in circumstances wherein privacy and security are essential. A clear picture and awareness of risk considerations will allow the FL initiator/recipient to build a secure environment while delivering research successfully. Our research aims to investigate FL data privacy characteristics, which may aid in explaining the relationship between collective AI models and the privacy-preserving vision [23]. The authors describe how to begin assessing current issues in Florida and a comprehensive assessment of the privacy protection issues that must be addressed in a comprehensive study [24]. To our knowledge, FL is associated with fewer privacy concerns than security risks. Communication issues and background hacking are the most specific security risks, while targeted attacks are critical for FL's privacy. We conclude our research with a prediction for future

research. While research is ongoing, understanding FL's security and privacy risks are not advanced [25]. Such a study thoroughly examines FL security in terms of official definitions, achievements, and challenges, distinguishing it from previous implementations. As a result of this work, data scientists and cybersecurity researchers may be able to create FL solutions that will alleviate future challenges.

1.5. Contributions

A summary of recent field publications is formed, such as (a) providing a breakdown and introduction to FL implementation methods and strategies. (b) Identifying and assessing security threats in FL and FL-based domains. In ML-related attacks, FL strategies are used. (c) Identifying and evaluating privacy threats, remediation methods, and tradeoffs in FL privacy protection strategies. (d) Disseminating information about security measures and future indicators that will improve security and privacy when FL is implemented.

1.6. Organization of Paper

This is how the entire paper is organized. The background information on FL and the basic working process are presented in Section 2. The Section 3 contains information from the federated database on FL. Section 4 discusses the research methods. Similarly, Section 5 presents the roles of FL in preserving privacy. The discussion is presented in Section 6. Section 7 summarizes the conclusion.

2. Related Works

Four years ago, a massive change occurred in the operation of Learning Machines because of personal concerns and ideas. Table 2 shows the previous studies.

Table 2. Previous related papers.

Ref. No.	Authors	Year	Title/Topic
[7]	Lim, Wei Yang Bryan, et.al.	2020	FL in mobile edge networks
[8]	Chamikara, M. A. P., et.al.	2021	Privacy preservation in FL
[11]	Zhang, H., et.al.	2020	Engineering FL systems
[13]	Mothukuri, V., et.al.	2021	Security and privacy in FL
[20]	Zhang, C., et.al.	2021	FL
[21]	Li, Q., et.al.	2019	FL systems
[22]	Aledhari, M., et.al.	2020	FL
[23]	Kulkarni, V., et.al.	2020	FL
[26]	Li, L., et.al.	2020	A Survey on FL
[27]	Zhan, Y., et.al.	2021	Mechanism Design for FL
[28]	Li, L., et.al.	2020	Applications in FL
[29]	Zhu, H., et.al.	2021	From FL to federated neural architecture
[30]	Kolias, C., et.al.	2022	Wireless intrusion detection
[31]	Pham, Q. V., et.al.	2022	Aerial access networks for federated learning
[32]	Ghimire, B., and Rawat, D. B.	2022	Federated learning for cybersecurity
[33]	Zhang, T., et.al.	2022	Federated learning for the Internet of Things

2.1. Introduce the Term FL

With the first publication of federated measurements in telecommunication environments in 2016 [1], FL emerged as a relevant research topic. Reducing communication pressure during the FL process is another crucial feature of a successful study. In 2017 and 2018, the publications highlighted the advancement of resource allocation policies, focusing on reducing the need for communication between gossiping areas and a strong manifestation of various privacy attacks. Other research focuses on lowering training bandwidth through augmentation and quantization approaches, where ML models are augmented and quantized.

Other research focuses on minimizing training bandwidth through augmentation and quantization approaches, wherever ML models are augmented and compacted before being assigned to other nodes [26]. So far, only the best-performing networks have been considered. Another research guideline jointly analyzes the training of different local models with various computational problems to produce a single effective global model. Federated learning is a modern learning system that aims to improve the learning capabilities of each agent without revealing confidential information, patterns, or learning objectives.

2.2. Improve the Learning Capabilities

The FL is a new learning system aiming to improve each agent's learning capabilities without disclosing confidential information, patterns, or learning objectives. A new model known as FL is being developed in addition to integrated systems and on-site analysis to create a new ML application design [27]. It is a secret method that saves previously used processes and stores original sensitive information in gadgets. It installs localized artificial intelligence learning to minimize information transmission to the greatest extent possible. A combination of learned and shared models is formed on a remote database to integrate and exchange information generated by users. This paper investigates and compares various ML deployment structures before conducting an in-depth and comprehensive analysis. Unlike FL, which frequently necessitates using an intermediary controller to schedule learning and practice, FL aims to provide agents with agreements to use and learn from one another without needing a global model. Using FL approaches ensures data security or encryption, which is a significant advantage. There was no way to import, view, or share position data. Accessing the database is extremely difficult because it is divided into position sections [34]. In FL, only the ML parameters are shared.

Key cryptographic methods can also be used to increase security. These considerations can be encoded before being shared between learning sequences, and exact computations can be performed on encrypted data without releasing it. In addition to such safeguards, these parameters may continue revealing information about simple data samples [35] by running specific queries against databases. As a result, the assumption about spatial performance is a significant concern that can be addressed by decoupling privacy from robust integration [36,37]. Successful measurement, which has emerged as a privacy concern in federated learning [38–40], limits the use of DL models. Static Batch Normalization (SBN) can keep deep neural networks private. SBN normalizes batch data during the training phase rather than monitoring active measurement. Only statistics for hidden inputs from local data are provided after the model estimate [41,42]. Local models are appropriate for the FL system because they do not necessitate the loading of active measures by expertise [43]. Because local models only store user data, data leaks are drastically reduced. The most recent findings provide specific recommendations for creating successful IoT applications.

2.3. Privacy-Preserving

The protection of user privacy is an essential feature of FL. However, it differs significantly from standard big data privacy preservation techniques such as privacy separation

and K-Order confidentiality [44–46]. Federated learning primarily protects user privacy by exchanging protected restrictions, even though unknowns cannot obtain source data [47–49]. Both FL assurances would not jeopardize data security during the device phase, and no GDPR or other concerns would arise. FL is divided into three types for data delivery: horizontal FL, simple FL, and FL techniques [50–52]. Horizontal federated transfer learning is sufficient when two user databases are more advanced but slightly higher. Straight FL is available when the user characteristics of the two databases are marginally higher, but the users are more experienced. When the dual databases' user and device feature match, the authors can use the switch to learn how to fix the lack of data or identifiers. FL investigates distribution across multiple devices and distributed computing [53–55].

Distributed ML includes the impact of distributed publishing models, distributed data, and allocated ML. Examples of supplied ML include the effects of distributed broadcasting models that deliver distribution data and distributed device distribution functions [56]. The factor server in ML provided is one of the fast training methods for ML models. It manages data across multiple distributed nodes and allocates resources via a dependable key server to achieve the best training results. In contrast to distributed ML, each task node in FL owns its own data and participates in model training.

In addition, key cryptographic methods can be used to increase security. These considerations can be encoded before being shared between learning sequences, and exact computations can be performed on encrypted data without releasing it. In addition to such safeguards, these parameters may continue revealing information about simple data samples [35] by running specific queries against databases. As a result, the assumption about spatial performance is a significant concern that can be addressed by decoupling privacy from robust integration [36,37]. Successful measurement, which has emerged as a source of privacy concern in federated learning [38–40], limits the use of DL models. Static Batch Normalization can be used to keep deep neural networks private (SBN). SBN normalizes batch data during the training phase rather than monitoring active measurement. Only statistics for hidden inputs from local data are provided after the model estimate [41,42]. Local models are appropriate for the FL system because they do not necessitate the loading of active measures by expertise [43]. Because local models only store user data, data leaks are drastically reduced. The most recent findings provide specific recommendations for creating successful IoT applications.

2.4. FL Developments

The advancement of FL is not well-known in culture as a modern privacy-preserving paradigm. The following examples show how federated learning works. We suppose that many different companies collaborate to learn standards. Additionally, it is almost impossible to collect the data of all parties without the consent of the users [28,57]. Alternatively, a company should use its data to train an ML model framework. It assumes that all groups create a working model, but due to their companies' minimal and incomplete data, it is hard to train a suitable ML [58,59]. The goal of FL is to find solutions to these problems. The FL ensures that no details about their business location are revealed. Boundaries are shared between clients and server encryption to create a global model based on the nonviolation of privacy [60].

Since its inception in 2016, FL has constantly been evolving [61–64]. This section also considers the following open policies (asynchrony, security, and privacy) in addition to the fundamentals (as described above). In the event of a dangerous attack on dispersed devices, FL can lead to data leakage while it helps protect sensitive data [29,65,66]. For example, such a leak could be caused by stochastic gradient descent (SGD) in the application process. This makes it challenging to protect privacy and safety in Florida. For algorithm performance, IoT infrastructure's rapid growth in network traffic has become a major technical concern. FL's ability to link a variety of devices needs the use of efficient algorithms to identify running applications [67,68]. For example, the Federated Averaging

(FedAvg) algorithm is used for local computation and update computation and privacy separation algorithms to minimize time overhead. The FL-related algorithms still need to be optimized when dealing with big data due to limited computing power. For the application of technology [69–72], FL greatly influences smart city applications. It covers almost every aspect, especially finance, medical care, transportation, etc. With FL, models can be trained on data corresponding to different levels [73,74]. FL will train models that cannot be federated directly by hospitals, such as smart healthcare.

On the other hand, FL uses input-sensitive data without compromising privacy or conquering the data key. The correctness of a model could be significantly enhanced by combining big data [75,76]. IoT devices will become more intelligent through the successful use of FL. Table 3 shows the year-wise contribution to the research of FL.

Table 3. Year-wise contribution to the research of federated learning.

Year	Ref	Contribution
2016	[1]	Introduce the term FL
2016	[77]	To enhance the functioning of the global model and decrease communications load.
2017	[48,78]	Studies of attacks on privacy.
2018	[67,72,76,79,80]	Development of resource allocation strategies
2019	[5,71,81]	Proof of FL in Blockchain
2019	[14,37]	Improving privacy using FL
2019	[25,44]	Resource allocation strategies
2019	[39,43,50,57]	Applied Federated Learning in wireless communications on mobile edge
2019	[47,49,51],	Applied Federated Learning on-device personalization
2019	[59,62,82]	Applied Federated Learning for data privacy in big data
2020	[3]	VerifyNet for secure and verifiable FL
2020	[4,18,56,83]	Privacy-preserving Blockchain-based FL
2020	[19,84]	FL in 5G mobile network
2020	[24]	FL in Resource Optimizations
2020	[36,61]	FL implementation in healthcare
2020	[54]	Human mobility Prediction using FL
2020	[63]	FedCoin payment system
2020	[85–87]	Applied FL on IoT devices
2020	[88]	FL in smart city sensing
2021	[2]	FL in traffic flow prediction
2021	[8]	FL-based distributed machine learning
2021	[38]	FL for 6G
2021	[58]	MHAT: FL-based model aggregation training scheme

The gradual expansion of FL has opened new opportunities for people from all aspects of life. This paper addresses the use of FL in smart cities, including communications, healthcare, and the Internet of Things [85,89,90]. Smart cities are expected to grow presently due to the use of FL. A more naturalistic environment that enriches everyone will be created by FL participating in all aspects of life.

2.5. FL Development Issues

Several FL deployment issues negatively impact IoT growth, including computational performance, heterogeneity, security, and resource integration [82]. For this reason, the authors have created a list of possible solutions to these problems. Below is the list:

Distribution of FL

Wireless resource restrictions and acoustic data can impact FL integration and local model training. By combining the available communication resources, the authors can create a gradient-based sparsity scheme [91]. The authors tend to the dataset and select devices with sufficient power for model training.

Surprising FL Collection

Statistical variability is already present in many machine datasets. It has a significant impact on FL convergence performance [81]. The authors can select the preceding machines in a dataset that satisfies a certain level of reliability.

FL security

During training, inappropriate memory devices may be present. The incorrect learning model parameters affect the device's accuracy. The authors could use blockchain [92] to verify the upkeep of storage devices. FL mobile users are disrupted when uplinks become congested and consume uplink communication resources. The authors may devise a plan to distribute resources using the game principle. We can integrate those resources more efficiently if authors link all storage devices that assist one block.

2.6. FL Applications

While specific performers require training models on more significant datasets, although they could not allow the data, they may use federated learning [86]. The technology still requires good communication among local servers and low computing energy for every point.

Self-driving vehicles

Autonomous vehicles use ML skills such as computer vision to detect obstructions and ML to alter the environment's pace to avoid dangerous situations (e.g., road explosion). The typical cloud technique may be a safety issue due to the enormous number of self-driving vehicles and the need for them to respond quickly to real-world events [84,93]. Security concerns may arise due to the considerable number of self-driving cars and the need to react swiftly to real-world situations. As a result of its ability to reduce data transfer, FL can aid in accelerating learning progress.

Medicine: a digital existence

FL aims to explain information management and confidentiality challenges by training distributed algorithms without sharing data. The modern method of combining data comes at the cost of sensitive concerns such as patient privacy and data security throughout many organizations. The capability to prepare ML models at scale in many health settings, not transmitting sensitive technical information, is a solution. The Future of Digital Health by FL was published in *Nature Digital Medicine* in 2020, and the writers discuss how organized learning can result from the potential of digital healthiness.

Protecting the sensitive data

ML methods are widely utilized in Industry 4.0 to increase the productivity of manufacturing processes while maintaining high security. On the other hand, protecting the sensitive data of industrial and manufacturing companies is essential. Since the learning algorithms do not reveal sensitive data, they can solve these challenges.

3. From Federated Database to FL

Federated computing has become an attractive research area in computer science under various distributed situations. Until the mid-1990s, numerous federated database system (FDBS) studies were conducted. FDBS is a non-profit data collection organization that provides similar services. The three key elements of FDBS, as shown in the previous research, are independence, diversity, and distribution.

3.1. Independence

The data collection system (DBS) that participates in FDBS is autonomous and is controlled separately and independently. Without FDBS, groups can still manage the data [77].

3.2. Differentiation

The FDBSs' data management systems may differ from one another. Differences can be observed in data formats, languages, program requirements, and communication capacities. FDBS data distribution may vary from one DBS to the next due to several DBSs before the FDBS's construction. Horizontally classified data can be placed on various DBSs or duplicated across several DBSs.

3.3. Federated Cloud Computing

With the advent of cloud computing, many studies on federated cloud computing have been conducted recently, provisioning and managing many external and internal computing services through a Federated Cloud (FC). The concept of a cloud partnership provides additional cost savings through partial outsourcing to low-cost regions. The two primary components of integrated clouds are resource migration and resource offloading. Moving resources from one cloud provider to another is the initial step. Migration permits the movement of resources. Second, deconstructionism enables the domain-specific application of identical service capabilities. For instance, data can be categorized and processed across many providers.

3.4. Multi-Resource Scheduling

Information can be classified and processed across multiple providers using the same computational concept [79,94]. Overall, multi-resource scheduling is critical to developing an integrated cloud system. FL and standard assembly systems have some similarities and differences. First and foremost, the concept of an association is still sustainable. The standard and fundamental concept is the collaboration of numerous independent groups [95]. Therefore, group heterogeneity and independence can be utilized in FL. Secondly, several critical elements in the strategy of allocated techniques remain. For example, the way data are shared between groups can have an impact on system performance. Integrated systems, on the other hand, focus on various collaborations and constraints. FLs are more concerned with the secure settlement between multiple parties, while FDBSs is concerned with distributed data management and FCs with resource management. FLs present new challenges, such as developing a distributed training algorithm and protecting data while considering privacy constraints.

4. Methods

In FL, automated variations can alter the ineffectiveness of the entire training process. Four types of variations can be used to resolve the heterogeneousness problem of the approach: concurrent, transmission devices detection, the attack detection mechanism, and model diversity, which have all been discussed.

4.1. Asynchronous Communication

Around specific information, the base is two universal policies for parallelization based on the algorithm: similar and parallel connections [87,96]. However, since the synchronizing mechanism is easily broken in the face of many devices, good communication is essential when learning federated tasks. It uses a limited amount of information to discover parallel and asynchronous processes that could assist resolve the training device flexibility challenge.

4.2. Device Sensing

Not all machines are needed to undergo the entire training phase in FL. The machine is such chosen that the user can participate in one part of the event on one device and another part of the event on another device. Device sensing takes the opportunity to participate in training [83]. Machines play a role in interdisciplinary training to address the problem of resources. The selection increases the number of clients in the training process while improving model outcomes. Kang and colleagues created a marketing strategy focused on contract instruction to entice powerful local devices to enhance learning accuracy through a more effective learning process. The paper [97] introduced the FL model, which randomly selects user gradients to upload to the server for global training of a model. In another paper [98], the authors proposed the privacy-preserving FL in fog computing to achieve continuous contact. Pulling reduction with local compensation (PRLC) focuses on FL. The basic concept behind PRLC is that only one iteration can be performed at a time. The key idea behind PRLC is that only a subset of devices participates in the model updates in each iteration, with non-participating devices being modified locally using the PRLC approach to close the difference through the global standard. Ultimately, the PRLC method has better scaling and has the same interconnection rate as the non-compressed method in the presence of high congestion and inconsistencies.

4.3. Fault Tolerance Process

A fault-tolerant approach, especially in a file-distributed environment, can prevent the system from failing in an unstable network environment [78]. While various devices work collectively, the system breakdown can involve other machines. FL is currently a hot research topic. The authors also need to consider system acceptance in an interactive learning environment. To comply with machine resource constraints, [88] focused on an applied learning approach and created a monitor system to evaluate the most exemplary exchange among local renewal and global integration of factors. By reducing the interaction, [99] improved the corresponding speed features of the random gradient distribution algorithm. Other studies that do not include direct computer involvement do not affect the efficacy of federated learning in multi-task achievement [80]. Figure 4 shows the device-to-device (D2D) communication without data exchanges in FL [100].

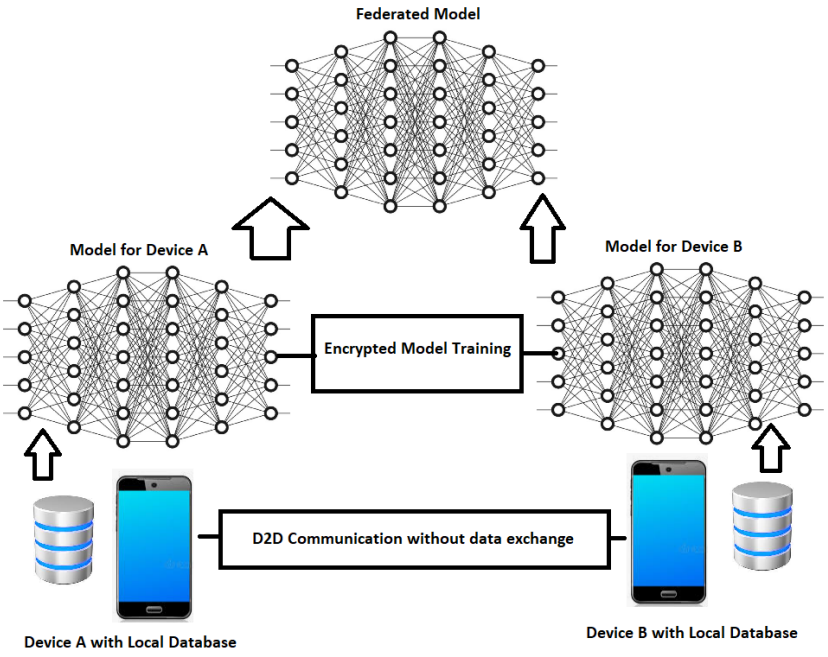

Figure 4. D2D communication without data exchange in FL.

Another way to deal with computer failures is to use computational code to implement a redundancy algorithm. Incorrect mobile device data can lead to cheating in organizational learning. Article [101] proposes an FL program that focuses on natural employee selection and can efficiently avoid mischievous assaults and disruptions.

4.4. Model Heterogeneity

An incomparable system solves the device heterogeneity problem very well in a memory-sharing system. Although distributed systems have benefited from asynchronous improvements, the issue of device communication delays increases device heterogeneity [102]. The need for real-time communication in a co-learning process is the first option for resolving system discrepancies in a non-compliant communication system.

5. Roles of FL in Privacy-Preserving

As information is stored on multiple platforms and communities become more aware of privacy issues, the standard circular training method for artificial intelligence (AI) models faces significant challenges. FL has emerged as a promising effect in this new reality [103]. FL's current protocol design emphasizes the vulnerability that attackers can exploit inside and outside the organization to ensure confidentiality. As a result, educating FL users about the privacy implications of the FL process layout is critical. There is currently little research on this topic. The current section fills an essential void in the FL process.

5.1. Threat Model and Attacks

A comprehensive overview of this exciting topic is provided through a brief overview of the concept of FL and the unique taxonomy encompassing the threat models and the two primary attacks on FL, including (1) dangerous attacks and (2) false attacks. The authors describe the potential for future research in powerful privacy protection and highlight the various attacks' assumptions, significant challenges, and fundamental ideas. FL provides a conditional training model that does not require information communication and encourages members to enter and exit the organization's restrictions. Current research, however, indicates that FL may not provide adequate privacy guarantees, as communication of standard informs during the training process may reveal confidential information and even receive deep leaks, either from a third party or a critical service [104,105].

Nonetheless, a small percentage of slopes can display data about local devices. In just a few repetitions, the nefarious assailant could completely steal training information from gradients. The FL protocol can be (1) a potentially malicious service that detects separate updates over time, disrupting the training procedure and controller participants' views across global boundaries, or (2) any participant who can identify the land parameter and control its loading [106,107]. Malicious participants can modify their inputs or overload the backend of a global standard. These attacks pose a severe threat to FL because, in an intermediate understanding, only the server can infringe on the participants' privacy. In contrast, in FL, any participant, even if not coerced, can invade the other participants' privacy in the approach. As a result, understanding the terms used in this attack is critical. FL testing focuses on the larger aspect of the process that allows FL to function. [108]. This paper addresses the recent increase in warnings to settlement FL to address the research community's critical gap in public understanding. The authors of FL programs primarily focus on two types of insider threats: (1) a toxic hazard: this addresses the recent rise in threats compromising FL in the research community to close this critical gap in public understanding [109]. (2) Unfounded attacks on the contributor's secret progress to FL attacks threat models [110,111].

Insider and outsider attacks are both possible. Internal attacks are possible during the transmission of data from the server FL to the system's participants. Spying attacks on the interaction network between contributors, the FL service, and the consumers of the

last FL model are external attacks when used as a capability. Internal attacks are frequently more powerful than external attacks because they amplify the opponent's strength. These can be one of three varieties.

5.2. Single Attack

The unintended contributor attempts to defeat the paradigm by confidently splitting a set of selected inputs.

Dangerous Byzantine Invasion

Byzantine participants act arbitrarily, causing their results to have the same dissemination as the relevant model notifies, making them complicated to obtain.

Sybil Attack

To launch an effective attack on FL, adversaries can imitate multiple participant accounts or select previously delayed members. They attempt to investigate the unique circumstances of other participants while remaining trusting in the FL protocol. Only federated observers or intermediate gradients are considered active adversaries, not training data or angles from other authorized participants. The active or malicious opponent learns the independent instances of trusted contributors in dangerous situations and differs from the FL procedure by unnecessarily adapting, replaying, or editing communications.

5.3. Attacks during Training Phase

Attacks during the training stage aim to understand, control, or distort the model of FL. Through the training stage, an attacker may use information-infecting attacks to negotiate the reliability of the training data gathering or toxic pattern attacks to negotiate the honesty of the training method. The attacker could also initiate attacks or a combination of threats to all participants. An escape/exploration attack is a type of attack that targets the monitoring phase. It generally causes no disruption to the target model but may produce negative results or gather information about the model's properties. The usefulness of such an attack is defined by the adversary's knowledge of the model [112]. White-box attacks (e.g., with full access to the model FL) and black-box attacks (e.g., without access to the model FL) are two types of attacks in the inference phase (e.g., only being able to query the model FL). The move-to-model in FL is damaged from similar attacks as in a typical ML environment where the targeted model is used as maintenance. It also makes the model available to any malicious client. As a result, FL must make extra efforts to protect itself from white-box attacks.

5.4. FL Structure for Effective Interaction and Privacy Safety

Some authors [113] have presented a revolutionary FL architecture for efficient communication and privacy protection that increases IoT performance. Transmission control protocol and cubic curve binary increase congestion have improved the Wi-Fi network's data delivery variations. Finally, a good training model was found. Building a federated cloud video computing framework for IoT based on DL meets the needs of app users. At the same time, metrics are used to reduce uplink communication and network bandwidth costs. FL also enables shared reading of speculative models by computational devices.

5.5. Blockchain FL

The advancement of blockchain technology has brought forth a recent trend for IoT development. The formation of blockchain-based FL (BlockFL) effectively erases the revival of the local learning model. That manages a compatible strategy and presents data analysis to determine the optimal performance. Some researchers have created blockchain-approved features for secure data sharing in industrial IoT [114]. By using a shared data model, this process effectively protects the privacy of the data. It has excellent accuracy, effectiveness, and security compared to an accurate database. The current approach of FL relies on the reliable assumptions of the client to identify more secure computers of

organizations that are vulnerable to malicious client attacks. Consistency and devolution blockchains are the foundations of the framework. They use specific local model updates and trusted data sources.

5.6. Learning at the Edge with Federated Computing

A high-performance application has resulted from the association of FL with edge computing. Edge and cloud computing can meet the demand for cloud capacity and facilities at the network's edge. In this context, FL has observed the introduction of a 4G/5G edge computing platform for vehicles [115]. This model results from a federated investigation of real-world datasets from significant electric vehicle (EV) manufacturers. Customization for the driver, asynchronous performance, and safety protection are all benefits of this strategy.

Moreover, using Smart IoT in custom-made FL will minimize the adverse effects of heterogeneity in many ways. At the same time, the FL-based frameworks should efficiently utilize the limited bandwidth. At the same time, the authors need to integrate DL methods with FL frames and mobile device programs. This will make mobile edge computing more efficient. In distributed training, the existing FL startup mode accepts processing points to coordinate a local training prototype. This result is in the formation of FL, which depends on the most focused types and the maximum bandwidth of the server.

However, participants transmit user information immediately to the cloud, posing a risk of privacy violations. Consequently, like decentralized training, federated training requires participants and servers to work together to train a single machine learning algorithm. Every participant has exchanged local measurements with the central service that gathers all distributions and provides the outcomes to every other participant to accelerate the model's optimization. In the end, the service where every user would have the best service specifications is used. Compared to centrally controlled training, federated training eliminates the chance of privacy issues becoming violated.

FL focuses on the problem of supervised machine learning, mapping input data U_i to output labels V_i. The input-output (U_i, V_i) pair size is (n, n + 1). For the loss function $f_i(L)$, which assesses how well a model predicts an ith sample using model L, FL tries to optimize using the following objective function.

Min $f(L)$, where

$$f(L) = \frac{1}{n}\sum_{i=1}^{n} \mathrm{f}(U_i, V_i, \mathrm{L})$$

$$f(L) = \frac{1}{n} f_i(L)$$

It is necessary to alter the objective function because the training data are scattered over several remote clients, much like in FL. It is known as $|Pk|$ when a client k receives a partition from the whole dataset P. $nk = |Pk|$ data samples are held by each of the K clients participating in the FL.

$$f(L) = \sum_{i=1}^{k} \frac{nk}{n} Pk(\mathrm{L})$$

where

$$Pk(L) = \frac{1}{nk}\sum_{i=1}^{k} f_i(\mathrm{L})$$

In Fl, there are two distinct phases of existence. There are epochs at the local and global levels. As opposed to how often the training algorithm is executed in a client's dataset, the number of times a whole federated round is completed is known as a global epoch. The server sends all clients a baseline model (abbreviated as w) to begin training. Each client's model is updated using their local data and it is trained for local epochs. As a result, L, a client model, will receive and communicate modifications to the server. Based on the sample size, the server computes the weighted average of client updates for the next training cycle. Globally federated Fed Averaging will have completed one round. Because it would be costly to communicate each client's gradient update for each round of training, local epoch training is used to reduce communication costs on the client's side. As a decentralized machine learning solution, FL is often referred to as a decentralized training system.

On the other hand, network power distribution between nodes is very similar to that of the data center. The author of [116] proposes that the bandwidth between sites can increase the communication speed. It starts by sharing gossip and network bandwidth information. Second, it makes the most of the available bandwidth between the nodes and the workers by utilizing it to its maximum potential. It increases by mixing speed and decreasing the number of communication cycles. Currently, the standard implementation of system FL uses a centralized parameter server to organize a broad network of participating devices. Devices will train local models using the datasets that they have collected. The sync server's locations can update at determined intervals [117]. Any changes made to the model are replicated across all other nodes inside the system. However, this approach has high additional costs because of its substantial bandwidth. As a result, a technique for synchronizing levels on all levels was utilized [118]. They began by partitioning the model into groups where each group had the same number of model parameters that did not interact. Second, they organize the departments, some of which are structured according to the classifications of the IoT devices. Third, they split into big groups, increasing their bandwidth capacity. Sharing communication costs reduces the cost and increases the assembly speed.

In the manuscript of [119], the authors proposed a comprehensive consolidation learning strategy and FL frameworks for mobile edge systems. This can potentially promote mobile edge computing (MEC). The In-Edge AI framework has been signed in this process. It will utilize the exchange of learning boundaries between a resource and an edge node. Finally, it achieves the optimal optimization performance and raises the input level. The fact that offloading requires wireless data transmission is the key to solving this problem [120,121]. The edges are assigned communication aids and computer equipment based on the full use of the communication and federated computer-integration program. This also allows it to hover and cache MEC program archives simultaneously. In addition, training organizations that operate throughout a geographically extensive range have used FL as a foundation for their operations. The results of this process are summarized in the following steps. (1) The amount of data that can be utilized is restricted. (2) It conforms to the network's mobile and cellular communication conditions. (3) It facilitates the connection of a wide range of user devices to a natural mobile network. (4) It guarantees the safety of private data.

6. Discussion

Traditional ML employs an intermediate approach to training design, necessitating the integration of training samples with a single machine or data center. Large AI companies such as Google, Facebook, and Amazon have amassed massive amounts of data and

stored them in a database where machine learning models are trained. This single training method, however, is private, especially for phone users. This is because cell phones can contain sensitive data for their owners. Users of mobile phones must sell their privacy to be trained or to obtain the best model with a training method. Compared to a single training method, integrated learning is a low-level training method that allows mobile phones worldwide to learn an ML model while retaining all private data, including potentially confidential data, within the machine. A well-trained intelligence algorithm may be able to assist mobile devices while also revealing critical privacy information on the cloud. However, because deep learning is rapidly expanding, existing techniques enable a cloud-centric formulation in which information is recorded and interpreted. It provides an accurate assessment of FL discussions and research fields, as well as the FL paradigm's efforts and contributions to current research and industry trends [122].

Furthermore, researchers provide in-depth reviews and thorough fundamental analysis, including the model's technical characteristics and the entire FL system. In addition, the authors discuss the challenges and open jobs of interest. Furthermore, they investigate the challenges and potentially fruitful directions that future development could take, resulting in new generations of FL technology. The authors' recommendations for the study are organized to consider both the projected FL domain and the overarching themes of system model and design, installation domains, privacy and security, and resource management. This analysis will be useful for academics who are starting or continuing research on machine learning solutions in medical IoT, advanced analytics, networking, automation, power systems, modelling, information retrieval, or information security [30–33].

Existing methods for protecting privacy face new challenges in a federated environment. Aside from providing complete privacy assurances, they are also critical in developing computationally affordable, communication-efficient, and drop-tolerant systems without significantly sacrificing accuracy. The central server can see the accurate aggregated results for each round even though it cannot see any local updates. This assurance is provided by the lossless SMC approach, which preserves original accuracy while ensuring the highest level of privacy. However, the resulting system increases communication costs significantly. As an added benefit, differential privacy can be combined with model compression techniques to reduce communication while increasing privacy. In this section, for example, the authors highlight additional challenges related to federation-related issues such as production and benchmarking and a few intriguing research paths (expensive communication, systems heterogeneity, statistical heterogeneity, and privacy concerns).

1. Non-traditional communication methods: The authors are unsure how much communication federated learning will necessitate. It is well known that machine learning optimization approaches lack precision; this error can promote generalization. In massive or statistically diverse networks, the behavior of one-shot or divide-and-conquer communication methods is identified, just as in traditional data center environments. Unlike in the federated setting, however, no theoretical analysis or scaled evaluation of one-shot/few-shot heuristics has yet been completed.

2. The authors used a variety of strategies, including local updates and model compression, to reduce the amount of communication in federated training. Creating a realistic federated learning system requires thoroughly examining the trade-offs between accuracy and communication in each tactic. While using the same communication resources as other strategies, the most effective methods will improve, achieving higher accuracy than any different strategy while employing the same range of communication/accuracy profiles. Similar in-depth experiments focusing on efficient neural network inference are required to adequately evaluate communication reduction options for federated learning.

3. Heterogeneity detection: Metrics such as local dissimilarity can be used to measure statistical heterogeneity. The following are open questions arising from the significance of these measures. Are there simple diagnostics for determining the degree of heterogeneity

in federated networks? Is it possible to develop diagnostics for measuring system heterogeneity? Can the convergence of federated optimization methods be improved by using current or new definitions of heterogeneity?

4. Expanding responsibilities: Remember that the techniques described thus far were designed with supervised learning, assuming that all federated network data have associated labels. Most of the data generated by realistic federated networks may not be labelled. Furthermore, as shown in (1), fitting a model to the data may not be the most difficult part of the job; instead, conducting some exploratory data analysis, calculating aggregate statistics, or implementing reinforcement learning may be. A wide range of issues, including scalability, heterogeneity, and privacy, are likely to be addressed in federated networks.

5. The use of FL in manufacturing raises several practical issues. When devices exhibit different behaviors at different times, the fundamental model for data creation changes over time.

6. While federated learning is still a relatively new field in the context of benchmarking, the authors must influence its development and ensure that it is based on real-world settings, assumptions, and datasets. Building on existing implementations and benchmarking tools to replicate empirical results and disseminate new approaches to FL is difficult.

7. Conclusions

As a result, FL is a new approach to cross-platform privacy security, which has been introduced. FL is used by many researchers and enterprises with privacy and security at the fore. FL can integrate the models of various user groups and update the federated model without revealing the original data when a lack of data hinders users from training suitable models. When users cannot read sufficient data labels, however, FL offers a secure mode of sharing and sends prototypes to distinct roles to address the problem of inadequate information classifications. This article begins with a general description of FL, continues with a discussion of the functional conditions of FL, and then concludes with a review of current issues and possible research challenges for FL. FL would be able to offer shared and federated security services for a wide range of applications, thereby assisting in the ongoing development of artificial intelligence.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are not used in this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. McMahan, B.H.; Moore, E.; Ramage, D.; Hampson, S.; Agüera y Arcas, B. Communication-efficient learning of deep networks from decentralized data. *arXiv* **2016**, arXiv:1602.05629.
2. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based Federated Learning for traffic flow prediction. *Futur. Gener. Comput. Syst.* **2021**, *117*, 328–337. https://doi.org/10.1016/j.future.2020.12.003.
3. Xu, G.; Li, H.; Liu, S.; Yang, K.; Lin, X. VerifyNet: Secure and Verifiable Federated Learning. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 911–926.
4. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2020**, *8*, 1817–1829. https://doi.org/10.1109/jiot.2020.3017377.
5. Qu, X.; Wang, S.; Hu, Q.; Cheng, X. Proof of Federated Learning: A novel energy-recycling consensus algorithm. *arXiv* **2019**, arXiv:1912.11745.
6. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2019**, *13*, 1–207.
7. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.-C.; Yang, Q.; Niyato, D.; Miao, C. Federated Learning in Mobile Edge Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. https://doi.org/10.1109/comst.2020.2986024.

8. Google Trends. Available online: https://trends.google.com/trends/explore?date=2016-07-01%202022-08-01&q=%2Fg%2F11hyd49kls (accessed on 1 August 2022).
9. Maheswaran, J.; Jackowitz, D.; Zhai, E.; Wolinsky, D.I.; Ford, B. Building privacy-preserving cryptographic credentials from federated online identities. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 9–11 March 2016; pp. 3–13.
10. Alam, T.; Benaida, M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. *Int. J. Interact. Mob. Technol. (iJIM)* **2018**, *12*, 74–84. https://doi.org/10.3991/ijim.v12i6.6776.
11. Zhang, H.; Bosch, J.; Olsson, H.H. Engineering Federated Learning Systems: A Literature Review. In *International Conference on Software Business*; Springer: Cham, Switzerland, 2020; pp. 210–218.
12. Lyu, L.; Yu, H.; Zhao, J.; Yang, Q. Threats to federated learning. In *Federated Learning*; Springer: Cham, Switzerland, 2020; pp. 3–16.
13. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Futur. Gener. Comput. Syst.* **2021**, *115*, 619–640. https://doi.org/10.1016/j.future.2020.10.007.
14. Hao, M.; Li, H.; Luo, X.; Xu, G.; Yang, H.; Liu, S. Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6532–6542. https://doi.org/10.1109/tii.2019.2945367.
15. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.S.; Poor, H.V. Federated Learning with Differential Privacy: Algorithms and Performance Analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3454–3469. https://doi.org/10.1109/tifs.2020.2988575.
16. Rodríguez-Barroso, N.; Stipcich, G.; Jiménez-López, D.; Ruiz-Millán, J.A.; Martínez-Cámara, E.; González-Seco, G.; Luzón, M.V.; Veganzones, M.A.; Herrera, F. Federated Learning and Differential Privacy: Software tools analysis, the Sherpa. ai Federated Learning framework and methodological guidelines for preserving data privacy. *Inf. Fusion* **2020**, *64*, 270–292.
17. Machine Learning Market by Vertical (BFSI, Healthcare and Life Sciences, Retail, Telecommunication, Government and Defense, Manufacturing, Energy and Utilities), Deployment Mode, Service, Organization Size, and Region—Global Forecast to 2022. Available online: https://www.researchandmarkets.com/research/c4gp8n/global_machine?w=4 (accessed on 13 August 2022).
18. Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2964–2973. https://doi.org/10.1109/tii.2020.3007817.
19. Isaksson, M.; Norrman, K. Secure Federated Learning in 5G mobile networks. *arXiv* **2020**, arXiv:2004.06700.
20. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl. Based Syst.* **2021**, *216*, 106775. https://doi.org/10.1016/j.knosys.2021.106775.
21. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; He, B. A survey on Federated Learning systems: Vision, hype and reality for data privacy and protection. *arXiv* **2019**, arXiv:1907.09693.
22. Aledhari, M.; Razzak, R.; Parizi, R.M.; Saeed, F. Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Access* **2020**, *8*, 140699–140725. https://doi.org/10.1109/access.2020.3013541.
23. Kulkarni, V.; Kulkarni, M.; Pant, A. Survey of personalization techniques for Federated Learning. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; IEEE: Pittsburgh, PA, USA, 2020; pp. 794–797.
24. Khan, L.U.; Pandey, S.R.; Tran, N.H.; Saad, W.; Han, Z.; Nguyen, M.N.; Hong, C.S. Federated Learning for edge networks: Resource optimization and incentive mechanism. *IEEE Commun. Mag.* **2020**, *58*, 88–93.
25. Wang, S.; Tuor, T.; Salonidis, T.; Leung, K.K.; Makaya, C.; He, T.; Chan, K. Adaptive Federated Learning in Resource Constrained Edge Computing Systems. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1205–1221. https://doi.org/10.1109/jsac.2019.2904348.
26. Li, L.; Fan, Y.; Lin, K.Y. A Survey on Federated Learning. In Proceedings of the 2020 IEEE 16th International Conference on Control & Automation (ICCA), Singapore, 9–11 October 2020; IEEE: Pittsburgh, PA, USA, 2020; pp. 791–796.
27. Zhan, Y.; Zhang, J.; Hong, Z.; Wu, L.; Li, P.; Guo, S. A Survey of Incentive Mechanism Design for Federated Learning. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1. https://doi.org/10.1109/tetc.2021.3063517.
28. Li, L.; Fan, Y.; Tse, M.; Lin, K.-Y. A review of applications in Federated Learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. https://doi.org/10.1016/j.cie.2020.106854.
29. Zhu, H.; Zhang, H.; Jin, Y. From Federated Learning to federated neural architecture search: A survey. *Complex Intell. Syst.* **2021**, *7*, 639–657. https://doi.org/10.1007/s40747-020-00247-z.
30. Kolias, C.; Kambourakis, G. TermID: A distributed swarm intelligence-based approach for wireless intrusion detection. *Int. J. Inf. Secur.* **2017**, *16*, 401–416. https://doi.org/10.1007/s10207-016-0335-z.
31. Pham, Q.-V.; Zeng, M.; Huynh-The, T.; Han, Z.; Hwang, W.-J. Aerial Access Networks for Federated Learning: Applications and Challenges. *IEEE Netw.* **2022**, *36*, 159–166. https://doi.org/10.1109/mnet.013.2100311.
32. Ghimire, B.; Rawat, D.B. Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 8229–8249. https://doi.org/10.1109/jiot.2022.3150363.
33. Zhang, T.; Gao, L.; He, C.; Zhang, M.; Krishnamachari, B.; Avestimehr, A.S. Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. *IEEE Internet Things Mag.* **2022**, *5*, 24–29. https://doi.org/10.1109/iotm.004.2100182.
34. Liu, Y.; Zhang, X.; Wang, L. Asymmetrically vertical Federated Learning. *arXiv* **2020**, arXiv:2004.07427.
35. Junxu, L.; Xiaofeng, M. Survey on privacy-preserving machine learning. *J. Comput. Res. Dev.* **2020**, *57*, 346.
36. Yuan, B.; Ge, S.; Xing, W. A Federated Learning framework for healthcare IoT devices. *arXiv* **2020**, arXiv:2005.05083.

37. Truex, S.; Baracaldo, N.; Anwar, A.; Steinke, T.; Ludwig, H.; Zhang, R.; Zhou, Y. A hybrid approach to privacy-preserving Federated Learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, London, UK, 15 November 2019; pp. 1–11.
38. Yang, Z.; Chen, M.; Wong, K.K.; Poor, H.V.; Cui, S. Federated Learning for 6G: Applications, Challenges, and Opportunities. *arXiv* **2021**, arXiv:2101.01338.
39. Yang, H.H.; Liu, Z.; Quek, T.Q.; Poor, H.V. Scheduling policies for FL in wireless networks. *IEEE Trans. Commun.* **2019**, *68*, 317–333.
40. Mammen, P.M. Federated Learning: Opportunities and Challenges. *arXiv* **2021**, arXiv:2101.05428.
41. Cheng, Y.; Liu, Y.; Chen, T.; Yang, Q. Federated Learning for privacy-preserving AI. *Commun. ACM* **2020**, *63*, 33–36.
42. Lyu, L.; Xu, X.; Wang, Q.; Yu, H. Collaborative fairness in Federated Learning. In *Federated Learning*; Springer: Cham, Switzerland, 2020; pp. 189–204.
43. Ghosh, A.; Hong, J.; Yin, D.; Ramchandran, K. Robust Federated Learning in a heterogeneous environment. *arXiv* **2019**, arXiv:1906.06629.
44. Nishio, T.; Yonetani, R. Client selection for Federated Learning with heterogeneous resources in mobile edge. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 1–7.
45. Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; Das, A. Anonymizing data for privacy-preserving Federated Learning. *arXiv* **2020**, arXiv:2002.09096.
46. Huang, Y.; Chu, L.; Zhou, Z.; Wang, L.; Liu, J.; Pei, J.; Zhang, Y. Personalized Federated Learning: An attentive collaboration approach. *arXiv* **2020**, arXiv:2007.03797.
47. Wang, K.; Mathews, R.; Kiddon, C.; Eichner, H.; Beaufays, F.; Ramage, D. Federated evaluation of on-device personalization. *arXiv* **2019**, arXiv:1910.10252.
48. Geyer, R.C.; Klein, T.; Nabi, M. Differentially private Federated Learning: A client level perspective. *arXiv* **2017**, arXiv:1712.07557.
49. Bui, D.; Malik, K.; Goetz, J.; Liu, H.; Moon, S.; Kumar, A.; Shin, K.G. Federated user representation learning. *arXiv* **2019**, arXiv:1909.12535.
50. Tran, N.H.; Bao, W.; Zomaya, A.; Nguyen, M.N.; Hong, C.S. Federated Learning over wireless networks: Optimization model design and analysis. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April 2019–2 May 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 1387–1395.
51. Peterson, D.; Kanani, P.; Marathe, V.J. Private Federated Learning with domain adaptation. *arXiv* **2019**, arXiv:1912.06733.
52. Yu, F.; Rawat, A.S.; Menon, A.; Kumar, S. Federated Learning with only positive labels. In Proceedings of the International Conference on Machine Learning, Virtual Event, 13–18 July 2020; pp. 10946–10956.
53. Wang, L.; Xu, S.; Wang, X.; Zhu, Q. Towards Class Imbalance in Federated Learning. *arXiv* **2020**, arXiv:2008.06217.
54. Li, A.; Wang, S.; Li, W.; Liu, S.; Zhang, S. Predicting Human Mobility with Federated Learning. In Proceedings of the 28th International Conference on Advances in Geographic Information Systems, Seattle, WA, USA, 13 November 2020; pp. 441–444.
55. Guler, B.; Yener, A. Sustainable Federated Learning. *arXiv* **2021**, arXiv:2102.11274.
56. Pokhrel, S.R. WITHDRAWN: Towards efficient and reliable Federated Learning using Blockchain for autonomous vehicles. *Comput. Netw.* **2020**, 107431. https://doi.org/10.1016/j.comnet.2020.107431.
57. Qian, Y.; Hu, L.; Chen, J.; Guan, X.; Hassan, M.M.; Alelaiwi, A. Privacy-aware service placement for mobile edge computing via Federated Learning. *Inf. Sci.* **2019**, *505*, 562–570. https://doi.org/10.1016/j.ins.2019.07.069.
58. Hu, L.; Yan, H.; Li, L.; Pan, Z.; Liu, X.; Zhang, Z. MHAT: An efficient model-heterogenous aggregation training scheme for Federated Learning. *Inf. Sci.* **2021**, *560*, 493–503. https://doi.org/10.1016/j.ins.2021.01.046.
59. Doku, R.; Rawat, D.B.; Liu, C. Towards Federated Learning approach to determine data relevance in big data. In Proceedings of the 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), Los Angeles, CA, USA, 30 July 2019–1 August 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 184–192.
60. Sharghi, H.; Ma, W.; Sartipi, K. Federated service-based authentication provisioning for distributed diagnostic imaging systems. In Proceedings of the 2015 IEEE 28th International Symposium on Computer-Based Medical Systems, Sao Carlos, Brazil, 22–25 June 2015; IEEE: Pittsburgh, PA, USA, 2015; pp. 344–347.
61. Ge, S.; Wu, F.; Wu, C.; Qi, T.; Huang, Y.; Xie, X. FedNER: Privacy-preserving medical named entity recognition with Federated Learning. *arXiv e-prints* **2020**, arXiv:2003.09288.
62. Jiang, Y.; Konečný, J.; Rush, K.; Kannan, S. Improving Federated Learning personalization via model agnostic meta learning. *arXiv* **2019**, arXiv:1909.12488.
63. Liu, Y.; Ai, Z.; Sun, S.; Zhang, S.; Liu, Z.; Yu, H. Fedcoin: A peer-to-peer payment system for Federated Learning. In *Federated Learning*; Springer: Cham, Switzerland, 2020; pp. 125–138.
64. Zhan, Y.; Li, P.; Qu, Z.; Zeng, D.; Guo, S. A Learning-Based Incentive Mechanism for Federated Learning. *IEEE Internet Things J.* **2020**, *7*, 6360–6368. https://doi.org/10.1109/jiot.2020.2967772.
65. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Zhang, J. Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory. *IEEE Internet Things J.* **2019**, *6*, 10700–10714. https://doi.org/10.1109/jiot.2019.2940820.

66. Tuor, T.; Wang, S.; Ko, B.J.; Liu, C.; Leung, K.K. Data selection for Federated Learning with relevant and irrelevant data at clients. *arXiv* **2020**, arXiv:2001.08300.
67. Chen, F.; Luo, M.; Dong, Z.; Li, Z.; He, X. Federated meta-learning with fast convergence and efficient communication. *arXiv* **2018**, arXiv:1802.07876.
68. Zhuo, H.H.; Feng, W.; Xu, Q.; Yang, Q.; Lin, Y. Federated reinforcement learning. *arXiv* **2019**, arXiv:1901.08277.
69. Jiao, Y.; Wang, P.; Niyato, D.; Lin, B.; Kim, D.I. Toward an Automated Auction Framework for Wireless Federated Learning Services Market. *IEEE Trans. Mob. Comput.* **2020**, *20*, 3034–3048. https://doi.org/10.1109/tmc.2020.2994639.
70. Yao, X.; Huang, T.; Wu, C.; Zhang, R.; Sun, L. Towards faster and better Federated Learning: A feature fusion approach. In Proceedings of the 2019 IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 22–25 September 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 175–179.
71. Kim, Y.J.; Hong, C.S. Blockchain-based node-aware dynamic weighting methods for improving Federated Learning performance. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 1–4.
72. Nilsson, A.; Smith, S.; Ulm, G.; Gustavsson, E.; Jirstrand, M. A performance evaluation of Federated Learning algorithms. In Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning, Rennes, France, 10 December 2018; pp. 1–8.
73. Yurochkin, M.; Agarwal, M.; Ghosh, S.; Greenewald, K.; Hoang, N.; Khazaeni, Y. Bayesian nonparametric Federated Learning of neural networks. In Proceedings of the International Conference on Machine Learning, Long Beach, CA, USA, 9–15 June 2019; pp. 7252–7261.
74. van Berlo, B.; Saeed, A.; Ozcelebi, T. Towards federated unsupervised representation learning. In Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking, Heraklion, Greece, 27 April 2020; pp. 31–36.
75. Chandiramani, K.; Garg, D.; Maheswari, N. Performance Analysis of Distributed and Federated Learning Models on Private Data. *Procedia Comput. Sci.* **2019**, *165*, 349–355. https://doi.org/10.1016/j.procs.2020.01.039.
76. Sahu, A.K.; Li, T.; Sanjabi, M.; Zaheer, M.; Talwalkar, A.; Smith, V. On the convergence of federated optimization in heterogeneous networks. *arXiv* **2018**, arXiv:1812.06127, 3.
77. Sheth, A.P.; Larson, J.A. Federated database systems for managing distributed, heterogeneous, and autonomous databases. *ACM Comput. Surv.* **1990**, *22*, 183–236. https://doi.org/10.1145/96602.96604.
78. Anelli, V.W.; Deldjoo, Y.; Di Noia, T.; Ferrara, A. Towards effective device-aware Federated Learning. In *International Conference of the Italian Association for Artificial Intelligence*; Springer: Cham, Switzerland, 2019; pp. 477–491.
79. Konecný, J.; McMahan, H.B.; Yu, F.X.; Richtárik, P.; Suresh, A.T.; Bacon, D. Federated Learning: Strategies for improving communication efficiency. *arXiv* **2016**, arXiv:1610.05492.
80. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Zhao, S.; et al. Advances and open problems in Federated Learning. *arXiv* **2019**, arXiv:1912.04977.
81. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Ind. Informatics* **2019**, *16*, 4177–4186. https://doi.org/10.1109/tii.2019.2942190.
82. Lalitha, A.; Kilinc, O.C.; Javidi, T.; Koushanfar, F. Peer-to-peer Federated Learning on graphs. *arXiv* **2019**, arXiv:1901.11173.
83. Song, M.; Wang, Z.; Zhang, Z.; Song, Y.; Wang, Q.; Ren, J.; Qi, H. Analyzing User-Level Privacy Attack Against Federated Learning. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2430–2444. https://doi.org/10.1109/jsac.2020.3000372.
84. Liu, Y.; Peng, J.; Kang, J.; Iliyasu, A.M.; Niyato, D.; El-Latif, A.A.A. A Secure Federated Learning Framework for 5G Networks. *IEEE Wirel. Commun.* **2020**, *27*, 24–31. https://doi.org/10.1109/mwc.01.1900525.
85. Lim, H.-K.; Kim, J.-B.; Heo, J.-S.; Han, Y.-H. Federated Reinforcement Learning for Training Control Policies on Multiple IoT Devices. *Sensors* **2020**, *20*, 1359. https://doi.org/10.3390/s20051359.
86. Wu, Q.; He, K.; Chen, X. Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge Based Framework. *IEEE Open J. Comput. Soc.* **2020**, *1*, 35–44. https://doi.org/10.1109/ojcs.2020.2993259.
87. Chen, Y.; Ning, Y.; Rangwala, H. Asynchronous online Federated Learning for edge devices. *arXiv* **2019**, arXiv:1911.02134.
88. Hardy, S.; Henecka, W.; Ivey-Law, H.; Nock, R.; Patrini, G.; Smith, G.; Thorne, B. Private Federated Learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *arXiv* **2017**, arXiv:1711.10677.
89. Cheng, K.; Fan, T.; Jin, Y.; Liu, Y.; Chen, T.; Yang, Q. Secureboost: A lossless Federated Learning framework. *arXiv* **2019**, arXiv:1901.08755.
90. Amiri, M.M.; Gündüz, D. Federated Learning over wireless fading channels. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3546–3557.
91. Pandey, S.R.; Tran, N.H.; Bennis, M.; Tun, Y.K.; Manzoor, A.; Hong, C.S. A Crowdsourcing Framework for On-Device Federated Learning. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3241–3256. https://doi.org/10.1109/twc.2020.2971981.
92. Qin, Z.; Li, G.Y.; Ye, H. Federated Learning and wireless communications. *arXiv* **2020**, arXiv:2005.05265.
93. Savazzi, S.; Nicoli, M.; Rampa, V. Federated Learning with Cooperating Devices: A Consensus Approach for Massive IoT Networks. *IEEE Internet Things J.* **2020**, *7*, 4641–4654. https://doi.org/10.1109/jiot.2020.2964162.
94. Lalitha, A.; Shekhar, S.; Javidi, T.; Koushanfar, F. Fully decentralized Federated Learning. In Proceedings of the Third Workshop on Bayesian Deep Learning (NeurIPS), Montréal, QC, Canada, 7 December 2018.
95. Mills, J.; Hu, J.; Min, G. Communication-Efficient Federated Learning for Wireless Edge Intelligence in IoT. *IEEE Internet Things J.* **2019**, *7*, 5986–5994. https://doi.org/10.1109/jiot.2019.2956615.

96. Du, Z.; Wu, C.; Yoshinaga, T.; Yau, K.-L.A.; Ji, Y.; Li, J. Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues. *IEEE Open J. Comput. Soc.* **2020**, *1*, 45–61. https://doi.org/10.1109/ojcs.2020.2992630.
97. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. https://doi.org/10.1109/tvt.2020.2973651.
98. Zhou, C.; Fu, A.; Yu, S.; Yang, W.; Wang, H.; Zhang, Y. Privacy-Preserving Federated Learning in Fog Computing. *IEEE Internet Things J.* **2020**, *7*, 10782–10793. https://doi.org/10.1109/jiot.2020.2987958.
99. Jiang, J.C.; Kantarci, B.; Oktug, S.; Soyata, T. Federated Learning in Smart City Sensing: Challenges and Opportunities. *Sensors* **2020**, *20*, 6230. https://doi.org/10.3390/s20216230.
100. Alam, T. Federated Learning approach for privacy-preserving on the D2D communication in IoT. In *International Conference on Emerging Technologies and Intelligent Systems*; Springer: Cham, Switzerland, 2021; pp. 369–380.
101. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated Learning: Challenges, methods, and future directions. *IEEE Signal Processing Mag.* **2020**, *37*, 50–60.
102. Li, Z.; Sharma, V.; Mohanty, S.P. Preserving Data Privacy via Federated Learning: Challenges and Solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 8–16. https://doi.org/10.1109/mce.2019.2959108.
103. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.R. DÏoT: A federated self-learning anomaly detection system for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; IEEE: Pittsburgh, PA, USA, 2019; pp. 756–767.
104. Wang, S.; Chen, M.; Yin, C.; Saad, W.; Hong, C.S.; Cui, S.; Poor, H.V. Federated Learning for task and resource allocation in wireless high altitude balloon networks. *arXiv* **2020**, arXiv:2003.09375.
105. Chen, D.; Xie, L.J.; Kim, B.; Wang, L.; Hong, C.S.; Wang, L.C.; Han, Z. Federated Learning based mobile edge computing for augmented reality applications. In Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 17–20 February 2020; IEEE: Pittsburgh, PA, USA, 2020; pp. 767–773.
106. Feng, J.; Rong, C.; Sun, F.; Guo, D.; Li, Y. PMF: A privacy-preserving human mobility prediction framework via Federated Learning. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2020**, *4*, 1–21.
107. Bakopoulou, E.; Tillman, B.; Markopoulou, A. A Federated Learning approach for mobile packet classification. *arXiv* **2019**, arXiv:1907.13113.
108. Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; Das, A. Differential privacy-enabled Federated Learning for sensitive health data. *arXiv* **2019**, arXiv:1910.02578.
109. Ye, D.; Yu, R.; Pan, M.; Han, Z. Federated Learning in vehicular edge computing: A selective model aggregation approach. *IEEE Access* **2020**, *8*, 23920–23935.
110. Saputra, Y.M.; Nguyen, D.N.; Hoang, D.T.; Vu, T.X.; Dutkiewicz, E.; Chatzinotas, S. Federated Learning Meets Contract Theory: Energy-Efficient Framework for Electric Vehicle Networks. *arXiv* **2020**, arXiv:2004.01828.
111. Liu, Y.; Yu, J.J.Q.; Kang, J.; Niyato, D.; Zhang, S. Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach. *IEEE Internet Things J.* **2020**, *7*, 7751–7763. https://doi.org/10.1109/jiot.2020.2991401.
112. Gursoy, M.E.; Inan, A.; Nergiz, M.E.; Saygin, Y. Privacy-Preserving Learning Analytics: Challenges and Techniques. *IEEE Trans. Learn. Technol.* **2016**, *10*, 68–81. https://doi.org/10.1109/tlt.2016.2607747.
113. Rieke, N.; Hancox, J.; Li, W.; Milletarì, F.; Roth, H.R.; Albarqouni, S.; Bakas, S.; Galtier, M.N.; Landman, B.A.; Maier-Hein, K.; et al. The future of digital health with Federated Learning. *NPJ Digit. Med.* **2020**, *3*, 1–7. https://doi.org/10.1038/s41746-020-00323-1.
114. Rahman, S.A.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A Survey on Federated Learning: The Journey from Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet Things J.* **2020**, *8*, 5476–5497. https://doi.org/10.1109/jiot.2020.3030072.
115. Zheng, Z.; Zhou, Y.; Sun, Y.; Wang, Z.; Liu, B.; Li, K. Federated Learning in Smart Cities: A Comprehensive Survey. *arXiv* **2021**, arXiv:2102.01375.
116. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated Learning for internet of things: Recent advances, taxonomy, and open challenges. *arXiv* **2020**, arXiv:2009.13012.
117. Briggs, C.; Fan, Z.; Andras, P. A Review of Privacy-preserving Federated Learning for the Internet-of-Things. *arXiv* **2020**, arXiv-2004.
118. Fantacci, R.; Picano, B. Federated Learning framework for mobile edge computing networks. *CAAI Trans. Intell. Technol.* **2020**, *5*, 15–21. https://doi.org/10.1049/trit.2019.0049.
119. Abdel-Basset, M.; Moustafa, N.; Hawash, H.; Ding, W. Federated Learning for Privacy-Preserving Internet of Things. In *Deep Learning Techniques for IoT Security and Privacy*; Springer: Cham, Switzerland, 2022; pp. 215–228.
120. Alam, T.; Ullah, A.; Benaida, M. Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. *J. Ambient Intell. Humaniz. Comput.* **2022**, 1–14. https://doi.org/10.1007/s12652-021-03663-2.
121. Alam, T. Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things. *Wirel. Pers. Commun.* **2022**, 1–17. https://doi.org/10.1007/s11277-022-09780-1.
122. Gupta, R.; Alam, T. Survey on Federated-Learning Approaches in Distributed Environment. *Wirel. Pers. Commun.* **2022**, *125*, 1631–1652. https://doi.org/10.1007/s11277-022-09624-y.