big data and cognitive computing

MDPI

Review

Applications and Challenges of Federated Learning Paradigm in the Big Data Era with Special Emphasis on COVID-19

Abdul Majeed [1,*], Xiaohan Zhang [2] and Seong Oun Hwang [1,*]

[1] Department of Computer Engineering, Gachon University, Seongnam 13120, Korea
[2] School of Law, Zhejiang University City College, Hangzhou 310015, China
* Correspondence: ab09@gachon.ac.kr (A.M.); sohwang@gachon.ac.kr (S.O.H.); Tel.: +82-31-750-5327 (S.O.H.)

Abstract: Federated learning (FL) is one of the leading paradigms of modern times with higher privacy guarantees than any other digital solution. Since its inception in 2016, FL has been rigorously investigated from multiple perspectives. Some of these perspectives are extensions of FL's applications in different sectors, communication overheads, statistical heterogeneity problems, client dropout issues, the legitimacy of FL system results, privacy preservation, etc. Recently, FL is being increasingly used in the medical domain for multiple purposes, and many successful applications exist that are serving mankind in various ways. In this work, we describe the novel applications and challenges of the FL paradigm with special emphasis on the COVID-19 pandemic. We describe the synergies of FL with other emerging technologies to accomplish multiple services to fight the COVID-19 pandemic. We analyze the recent open-source development of FL which can help in designing scalable and reliable FL models. Lastly, we suggest valuable recommendations to enhance the technical persuasiveness of the FL paradigm. To the best of the authors' knowledge, this is the first work that highlights the efficacy of FL in the era of COVID-19. The analysis enclosed in this article can pave the way for understanding the technical efficacy of FL in medical field, specifically COVID-19.

Keywords: federated learning; COVID-19; medical; privacy preservation; statistical heterogeneity

Citation: Majeed, A.; Zhang, X.; Hwang, S.O. Applications and Challenges of Federated Learning Paradigm in the Big Data Era with Special Emphasis on COVID-19. *Big Data Cogn. Comput.* **2022**, *6*, 127. https://doi.org/10.3390/bdcc6040127

Academic Editor: Fabrizio Baiardi

Received: 1 September 2022
Accepted: 20 October 2022
Published: 26 October 2022

1. Introduction

In recent years, artificial intelligence (AI) techniques have been highly successful in assisting mankind in various ways, such as improved healthcare, ambient assisted living, smart services, awareness/forecasting of future events, etc. Three major elements have significantly contributed to the success of AI developments in real-life scenario(s): (i) the availability of big data stemming from diverse sources, (ii) advancements in newer learning models as well as computational power, and (iii) the evolution of deep learning (DL) models and high-performance computing infrastructures [1]. FL has various market use cases and commercial applications focusing on data science, healthcare, industry, and education [2]. Despite their many benefits, AI techniques face multiple challenges due to poor quality and unstructured data, the non-availability of data for certain tasks, and/or the inability to handle and process data originating from the real-time domain. Though AI has shown a very huge success rate and many remarkable developments exist worldwide, most domains (e.g., real-time, personal data-driven applications, etc.) are still not in a position to leverage AI techniques commercially due to the following major concerns:

- Users are highly concerned about their data privacy, and therefore, acquiring and using personal data is very challenging.
- The confidentiality of personal data (also known as users' data) can be compromised because the data are mostly collected in some central place (e.g., server) for central learning (CL).
- Most processing in CL-based environments is performed in a black-box manner. Hence, privacy violations cannot be restricted.

- The data concerning an individual can be of multiple types such as spatial-temporal activities, demographics, medical data, and physiological readings, to name a few. Depending on the diversity and size of data, the chances of privacy breaches can be very much higher in CL environments.

As cited above, privacy has been a major concern in the adoption of AI techniques in commercial environments. Recently, most digital applications such as contact tracing apps developed for containing the spread of the novel coronavirus disease 2019 (COVID-19) were not welcomed by many people across the globe due to privacy concerns [3]. Thanks to the emergence of the federated learning (FL) paradigm, many privacy issues can be addressed proactively [4]. FL is considered a privacy-aware ML model in which privacy is ensured by not centralizing personal data at some central place (e.g., servers). Specifically, FL is a special case of distributed machine or deep learning (ML or DL), which enables N clients to jointly build an ML/DL model across decentralized data sources without explicitly aggregating the data at some central place [5]. The key difference between FL and centralized learning (CL) is given in Equation (1):

$$\text{Case(CL } | | \text{ FL)} = \begin{cases} \text{data} \rightarrow \text{algorithms}, & \text{CL} \\ \text{algorithms} \rightarrow \text{data}, & \text{FL} \end{cases} \tag{1}$$

By bringing algorithms close to data, FL is regarded as one of the mainstream solutions for privacy preservation. Due to its core abilities such as breaking data island and data silo problems, FL has received considerable attention from the research community, and FL applications are expanding to many fields, including healthcare, finance, supply chains, smart cities, robotics, and education. Furthermore, FL can work with many advanced techniques such as blockchain, the Internet of Things (IoT), the industrial IoT (IIoT), and edge/fog computing infrastructures. In the coming years, FL will likely replace central ML/DL-based systems and be widely used in many commercial sectors. Recently, FL has emerged as a viable solution for securing critical infrastructures such as the IoT from a privacy preservation point of view [6]. FL has helped preserve the privacy of healthcare data [7], cloud computing environments [8], vehicular environments [9], edge computing [10], big industrial data [11], and medical systems [12] and has helped in intrusion detection and privacy preservation in IoT systems [13]. Furthermore, FL has been extensively used to preserve privacy in AI applications, collectively called privacy-preserving AI [14]. Unfortunately, the FL paradigm has various issues due to its decentralized architecture. For example, the invisibility of training data, centralized aggregation, and the training process on the client's side can result in some security and privacy issues [15]. Furthermore, due to decentralized processes, convergence and client retention/selection is also very challenging. Recently, many studies have been designed to advocate the uses of FL in many sectors, and to lower the security and privacy attacks. However, the extended taxonomy of FL's applications with special emphasis on COVID-19 remained unexplored. In this paper, we investigate the recent advancements in the FL paradigm to highlight the significance of FL in the modern era and the challenges impacting FL's broad adoption in commercial settings.

Although FL has been widely used in many sectors, the future of healthcare is deeply connected with the success of FL because the privacy preservation of medical data is imperative [16]. The recent COVID-19 pandemic has also tested the technical strength of FL, and it was widely used to handle many parts of this pandemic [17]. Some of the noticeable applications of FL in the COVID-19 era are: COVID-19 detection from x-ray images [18,19], clinical outcome prediction [20], mortality prediction [21], pre-processing of COVID-19 data [22], COVID-19 vulnerability map construction [23], privacy-preserving data collection [24,25], Ct-image-based COVID-19 detection [26,27], infected regions segmentation [28], and face mask detection in dense crowds [29]. Considering these innovative applications, the concrete and complete overview of FL in the context of COVID-19 is meaningful and important, which is the main motivation behind this research. We affirm, with the contributions of previous generic surveys [30–34], that our focus is on COVID-19-

related FL developments, which remained unexplored in the current literature. In addition, none of the previous surveys have highlighted the synergies of FL with other emerging technologies to fulfill its promises in the context of COVID-19. The major contributions of this paper are given as follows:

- *A review of the applications of FL to COVID-19:* This article discusses the technical applications of FL along with model and data details focusing on COVID-19, which can help understand recent state-of-the-art (SOTA) developments of the FL paradigm.
- *Synergies of FL with other technologies:* This work highlights the synergies of FL with other technologies that are imperative for privacy preservation, broadening application horizons, and/or enhancing service scenarios. This extended knowledge assists in understanding the technology stack of the FL paradigm.
- *Review of open-source FL frameworks:* This work analyzes the recent open-source development of FL paradigms which can help in designing scalable and reliable FL models in the medical field by addressing their limitations.
- *Potential challenges and future research directions:* This work suggests valuable technical recommendations to address the key challenges of this SOTA decentralized paradigm.
- To the best of the authors' knowledge, this is the first work centering FL with regard to COVID-19, and we believe this could pave the way to understanding FL's role in the COVID-19 era.

The rest of this paper is structured as follows: Section 2 discusses the background of the FL paradigm including working methodology (e.g., clients and server responsibilities), main types, and emerging research areas concerning the FL paradigm. Section 3 presents technical applications of the Fl in the context of COVID-19. Section 4 presents the latest synergies of FL with the other emerging technologies to enhance the privacy level as well as the application horizon of FL technology. Section 5 discusses the open-source implementations of FL with a special focus on medical-related developments. Section 6 highlights the challenges of FL in modern times and suggests valuable recommendations to address those challenges. Section 7 compares this work with the existing works. We conclude this paper in Section 8.

2. Background of Federated Learning

In this section, we describe the background of the FL for the clarity of the readers. Specifically, we demonstrate the working mechanism of FL, its types, and hot research areas centering on the FL paradigm.

2.1. Federated Learning: A State-of-the-Art (SOTA) Development for Privacy-Preservation

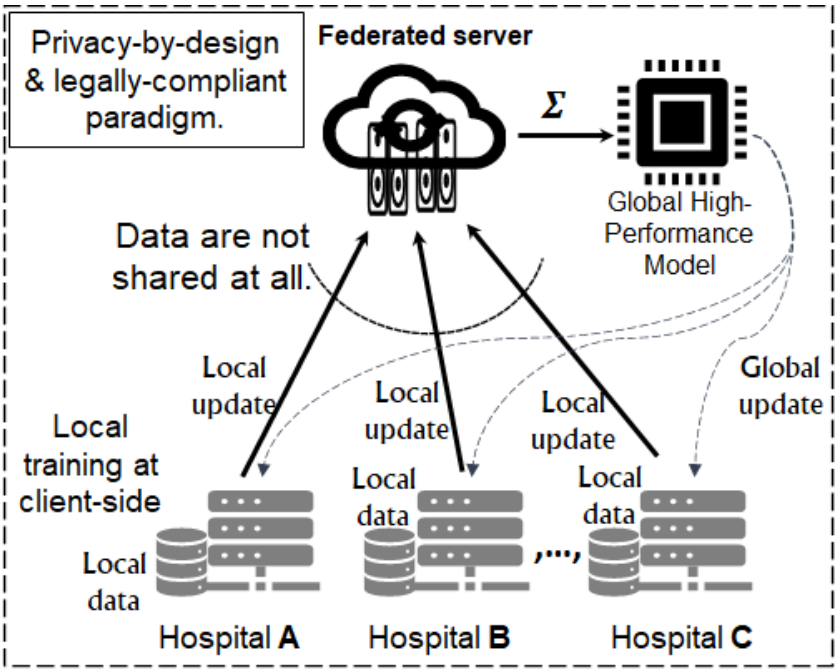
A typical FL paradigm includes one central server denoted with S, N clients/participants, and a training protocol/algorithm that works in multiple rounds. The FL paradigm does not centralize data, and therefore, it is a privacy-preserved solution. The rigorous application of privacy regulations is not needed because the FL paradigm is legally compliant. The FL paradigm is the solution for data islands/silos and the data winter problem (https://redasci.org/, accessed on 10 August 2022). Figure 1a presents a high-level overview of the Fl paradigm. There are M rounds in the FL paradigm. The conceptual overview of one round is given in Figure 1b. As shown in Figure 1a, in each round's global model, ΔW, performance is checked, updated, and shared among participating entities (e.g., clients and S) involved in the paradigm. The FL process is repeated several times until some defined criterion/condition is met. Figure 1b illustrates a detailed procedure of one round in the FL paradigm.

In Figure 1b (a), clients obtain a global model update (e.g., ΔW) from the central server. Afterward, each client computes a local model weight independently based on the local data in Figure 1b (b). Subsequently, in Figure 1b (c), all local updates of each client are sent

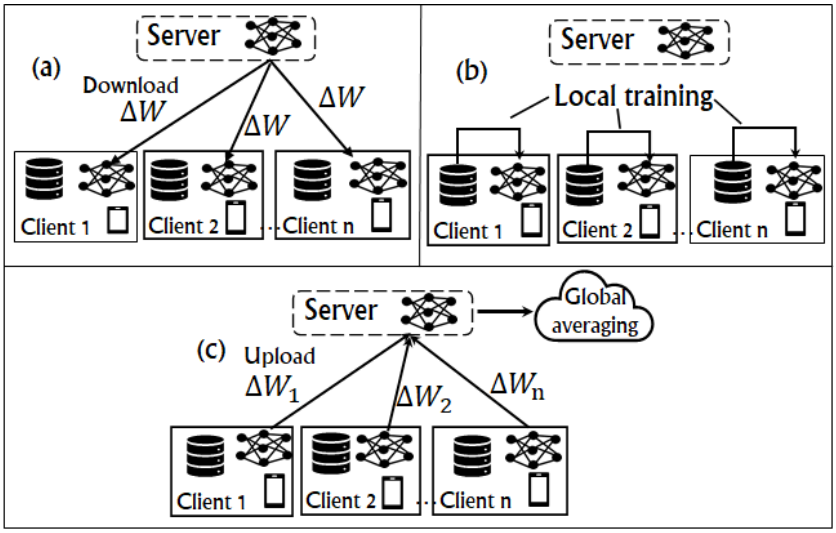
back to the central server for joint analysis (i.e., aggregation). The aggregator function, F, employed at the server side for federated averaging at epoch/time t is given in Equation (2):

$$g(t) = \frac{1}{N}\sum_{i=1}^{N} \Delta W_i^t \tag{2}$$

where N denotes the total number of clients, $F(t)$ is a global weight at time/epoch t, and ΔW_i^t represents the gradient update for the client i at epoch t.



(**a**)



(**b**)

Figure 1. Technical overview of the FL paradigm. (**a**) Overview of FL paradigm; (**b**) Practical illustration of one round of FL (reformulated from [35]).

In the FL paradigm, clients and servers carry out a variety of functions to accomplish collaborative learning tasks. The generic overview of tasks performed by each participating

entity is given in Table 1. In some cases, the number of tasks can vary depending upon the target domain/scenario.

Table 1. Functions/activities performed by clients and server in the FL paradigm.

Entity	Key Functions
Clients	Obtaining parameters from the central server. Training the AI model with parameters obtained from a central server and local data. Uploading local gradients to the server for aggregation.
Server	Sharing parameters with all participants/clients. Acquiring local gradients from all participants. Computing aggregated global model (F) utilizing local gradients. Updating model parameters with new in each t. Filtering malicious gradients/updates using anomaly detection or any other method.

The data on which AI models are trained on the client side can be independent and identically distributed (i.i.d.) or non-i.i.d., depending upon the scenario. The latter case is more challenging as it can slow the convergence model and result in poor accuracy.

2.2. Classification/Types of the Federated Learning Paradigm

As shown in Figure 2, FL approaches can be classified into three main categories, namely, horizontal FL, vertical FL, and federated transfer learning (FTL) [36]. Horizontal FL is the ML/DL in cases where multiple datasets from different clients are not identical in the sample space but identical in the feature space. For instance, the datasets originating from different hospitals can denote the same feature space, i.e., the patients' information, but not identical in the sample space, i.e., the data from diverse/different patients. In vertical FL, the clients can have the data with identical sample space but with non-identical feature space. An example of vertical FL can be the bank statement and information on the online shopping history of the same group of users. FTL applies to multiple datasets that are non-identical with regard to both the sample space and the feature space.

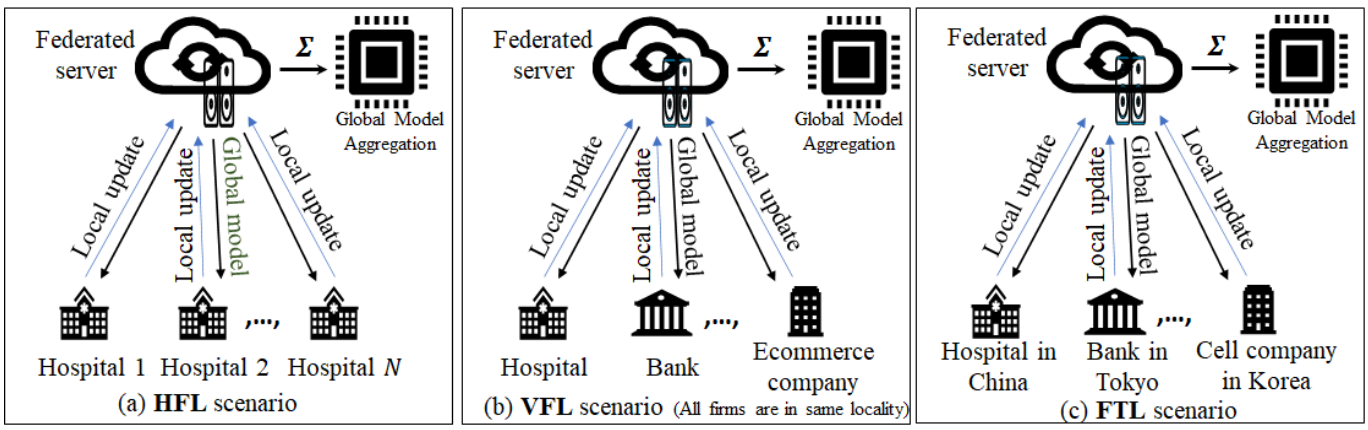


Figure 2. Overview of the classification in the FL paradigm.

2.3. Focus of Recent Studies on FL Paradigm

Research on the FL paradigm is underway from multiple perspectives. Figure 3 describes the hot research areas that are under investigation to enhance the efficacy of the FL paradigm.

In addition to the key research areas mentioned in Figure 3, FL has been extensively investigated from multiple perspectives (e.g., hyper-parameters optimization, personalized FL, attacks on FL systems) [37]. The compact overview of key areas can enable researchers to choose a niche area for further research. The rest of this paper highlights FL's significance/use in the COVID-19 context.

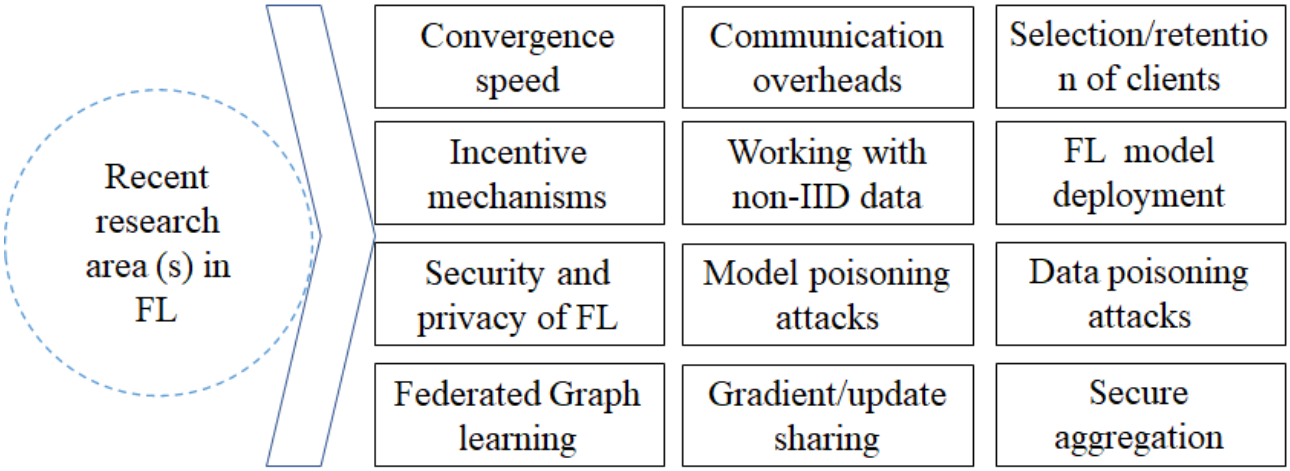


Figure 3. Overview of the recent research area(s) of federated learning.

3. Technical Applications of Federated Learning in the Context of COVID-19

FL has demonstrated its effectiveness in many sectors, including supply chains, robotics, finance, smart cities, smart healthcare, natural language processing and modeling, the insurance sector, social networks, and the IoT, to name a few. In this paper, our focus is on healthcare and especially COVID-19, and therefore, we summarize the achievements of FL in the healthcare sector only. Before presenting the detailed applications of FL in the COVID-19 era, we present the overall applications of FL in the healthcare domain in Figure 4.

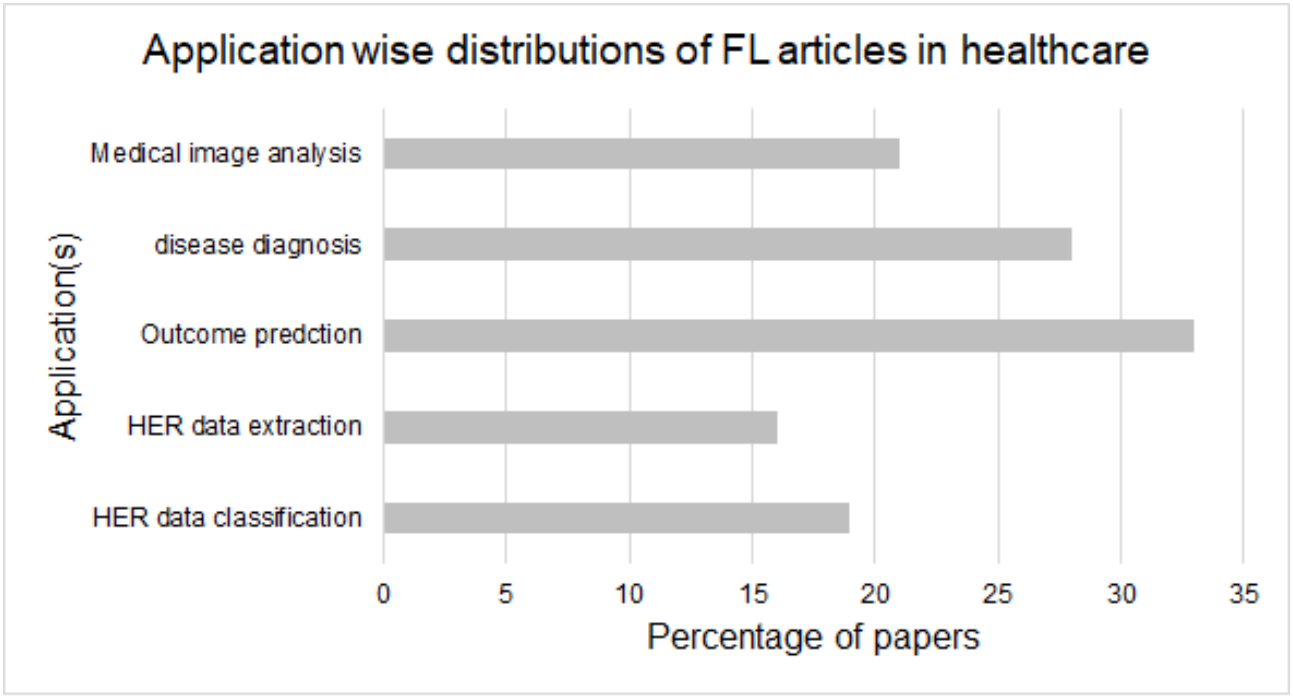


Figure 4. Overview of the FL applications in healthcare (Adopted from [38]).

As shown in Figure 4, FL has been contributing significantly to the healthcare sector with diverse applications. The input to these applications are data of patients in the form of electronic health records (EHR), data from wearables, sensor readings, demographics, vital signs, images, X-rays, medical histories, and visuals, audio, and videos of various body organs. FL trains high-quality models for neurological (and other) disease diagnoses. Recently, FL and other AI-based developments have been used to assist doctors in performing various activities in hospitals. In the coming years, FL will be one of the mainstream

technologies in performing various operations/services. Some studies explored the use of FL in tumor identification using ultrasound images and compared FL architecture and traditional AI architectures [39]. In this analysis, FL was proven more effective than the traditional ML/DL-based training architectures. Some studies have explored the usage of FL in hearing aids, survival prediction in patients with lung cancer, and confidentiality-aware data processing [40–42]. Ngo et al. [43] developed a SOTA approach by combining DL and FL for diagnosing cerebellar ataxia (CA) using image data. The proposed approach yields higher diagnosis accuracy without feature engineering and ensures data privacy in real-life deployable scenarios. Islam et al. [44] proposed an FL-based secure data-collection method from IoT devices using drones and blockchain. The proposed approach yields better results in proof of concept experiments, highlighting multiple benefits such as data collection, storage, privacy preservation, security, and execution time. Similarly, FL has also contributed to lowering the effects of this pandemic on the general public when vaccines were unavailable. At present, there are various commercial deployments of FL to control COVID-19 using a variety of data sources. FL can work with many digital technologies, and therefore, the application/use of FL is more dominant than traditional AI techniques. Through a detailed analysis of the SOTA published in the past three years, we summarize practical examples of FL in Table 2.

Table 2. Recently developed/proposed practical applications of FL in the context of COVID-19.

Practical FL Application	AI Methods Used	Data Used	Representative Ref.
Detection of COVID-19 infection	Capsule Network	CT images	Kumar et al. [45]
Outcome prediction	Pre-trained ResNet-34	X-ray (CXR), vital signs, demographic, and lab values	Flores et al. [46]
Lung abnormalities detection	CNN-based model	Medical images	Dou et al. [47]
COVID-19 region segmentation	Semi-supervised learning	Chest Computed Tomography	Yang et al. [48]
Detection of COVID-19	Generative adversarial networks	COVID-19 images	Nguyen et al. [49]
Segmentation of lungs contaminated area	3D UNet	CT Image of Lung	Aswathy et al. [50]
Epidemic model using mobility	Multi-task learning	Real-time mobility data sets	Kumaresan et al. [51]
Automated infection detection	Chest X-ray images	Convolutional neural networks	Ohata et al. [52]
Classification of COVID-19 & pneumonia	DenseNet-201	X-ray images	Alhudhaif et al. [53]
Identification of contaminated places	ResNet50	Thermal images	Das et al. [54]
Prediction of COVID-19 at early stage	Multiple ML algorithms	Patient community features	Singh et al. [55]
Detecting COVID-19's presence	ResNet-18	X-ray and CT scan	Kochgaven et al. [56]
Discovery of COVID-19	Alex net	CT images	Chen et al. [57]
Classification of +ve and -ve cases	Deep CNN	CXR images	Laouarem et al. [58]
Prediction of COVID-19 disease	CNN model	Chest X-rays	Malhotra et al. [59]
Medical resources' demand prediction	CETL method	Heterogeneous data	Song et al. [60]
Severity assessment of COVID-19	Variants of neural networks	chest X-ray	Le et al. [61]
Prediction of COVID-19 disease	CNN models	Electronic Medical Records	Senthilkumar et al. [62]
Risk assessment system	MK-DNN model	Location maps	Wang et al. [63]
Community-level vulnerability estimations map	SIR models	Location data	Chen et al. [64]

Table 2. *Cont.*

Practical FL Application	AI Methods Used	Data Used	Representative Ref.
Privacy of patient data	2D CNN model	X-ray images and symptoms	Ho et al. [65]
Accurate prediction of COVID-19 cases	Hybrid capsule network	Lung CT images	Durga et al. [66]
COVID-related symptoms detection	CNN model	Sensors data	Rahman et al. [67]
COVID-19 detection	KNN classifier	Demographics data	Mukherjee et al. [68]
Monitoring of COVID-19	KNN + CNN + LSTM	Symptom data	Aljumah et al. [69]
COVID-19 suspects prediction	ML [1] techniques	sensors and IoT data	Mir et al. [70]
Epidemic trend analysis	T-SIRGAN model	Surveillance data	Wang et al. [71]
Controlling outbreak	J48 decision tree	wearable sensors	Bhatia et al. [72]
Breathing pattern analysis	Clustering methods	Sensors data	Hidayat et al. [73]
Infected patients monitoring	ANN model	Symptomatic results	Rathee et al. [74]
Tracking health status of infected patients	FPGA prototype	Sensory data	AlOmani et al. [75]
Medical information sharing	CNN model	EHR data	Salim et al. [76]
Analysis of vaccine-related tweets in social networks	RNN model	Tweets data	Singh et al. [77]
Diagnosis of COVID-19	Vision transformer	CXR images	Park et al. [78]
Privacy protection of healthcare data	NB + RF	Genomic data	Islam et al. [79]
Tackling data diversity	Vision transformers	Masked images	Yan et al. [80]

[1] SVM, decision tree, naïve Bayes, logistic regression, and neural network.

As shown in Table 2, FL has many practical applications in the context of COVID-19. These applications have helped many entities in lowering the severe effects of COVID-19. Further information about the applications of FL in medical fields can be learned from previous survey [81–84]. Based on the extensive analysis, we found that most FL applications in the COVID-19 context are detection, prediction, diagnosis, and forecasting. In addition, the most commonly used data types are X-rays, images, and data from wearables. From the AI model's point of view, CNN and common ML models were frequently used in experiments. This knowledge can assist researchers in customizing existing developments as well as proposing new models for enhancing accuracy, precision, recall, F_1 score, etc. Apart from the data sources mentioned in Table 2, some FL applications have used signals data as well in improving medical services focusing on COVID-19 [85–87]. The implementation of FL with these heterogenous data sources helped in constraining the spread of the virus in a privacy-preserving way. In addition to FL, many other digital technologies have also contributed to lowering the effects of the pandemic on the general public. In Figure 5, we summarize the key technologies that have helped mankind mostly in the pre-vaccine era.

As shown in Figure 5, many technical developments have been made across the globe to combat the virus. In addition, the developments of contactless services have also boosted AI-related developments across the globe. In the post-COVID-19 era, more disruptive technologies will further reshape the industry.

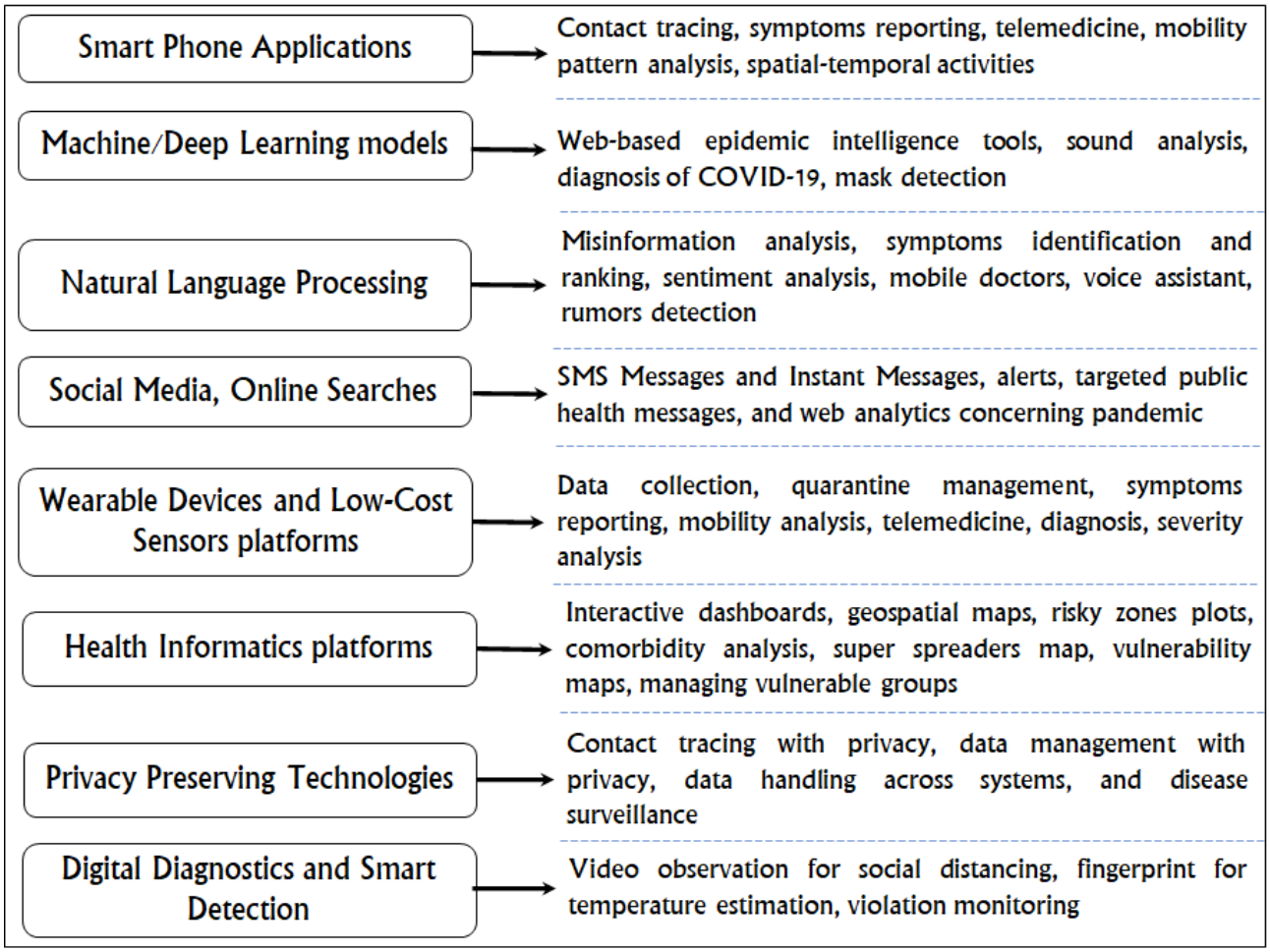


Figure 5. Overview of key technologies other than FL that have contributed to handling the pandemic (Adopted and enhanced from [88]).

4. Recent Synergies of Federated Learning with Other Emerging Technologies in the Context of COVID-19

Due to the distributed nature, the invisibility of training data, and untrustworthy clients' behavior, FL could not unleash much of its potential [89]. For example, FL failed to fully protect training data from adversaries because sometimes gradients/parameter sharing can weaken the privacy of participants. Similarly, due to the open nature of training, any party (including malicious entities) can join the system, and corrupt the training process with either wrong data or wrong models. Furthermore, FL cannot guarantee that the number of participants in the initial rounds will remain until the end of the training process. To overcome these challenges, FL has been extensively integrated with other emerging technologies. For example, to protect the privacy of training data, FL has been integrated with the differential privacy [90]. To further protect personal data in industrial settings, FL has established synergy with the blockchain [91,92]. In Table 3, we highlight the main synergies of FL with other emerging technologies in the context of COVID-19.

Table 3. Synergy of FL with other emerging technologies.

Synergy	Objective Achieved	Relevant Literature
FL + Homomorphic encryption	Privacy preservation of data/parameters	Fang et al. [93]
FL + Edge computing	Robust data analytics	Hakak et al. [94]
FL + Internet of Things (IoT)	Quick detection of COVID-19	Laxmi et al. [95]
FL + Industrial IoT	IIoT data caching and offloading for medical services	Nguyen et al. [96], Hazra et al. [97]
FL + Cloud computing	Analyzing infection trends and response plans	Pang et al. [98]
FL + 5G architecture	Sharing of general diagnosis models between hospitals	Wang et al. [99]
FL + Reinforcement learning	Prediction of side-effects of COVID-19	Jaladanki et al. [100]
FL + Local differential privacy	Privacy preservation of sensitive data	Yang et al. [101]
FL + Global differential privacy	Privacy preservation of imaging data	Ulhaq et al. [102]
FL + Functional encryption	Privacy preservation of gradients and communication	Rahman et al. [103]
FL + AI+ IoT	Prevention and control of COVID-19 pandemic	Chen et al. [104]
FL + Robotics	Seamless data collection and processing	Wu et al. [105]
FL + IoMT	Federated healthcare system with privacy controls	Aouedi et al. [106]
FL + FLOP	Privacy protection via a partial model sharing strategy	Yang et al. [107]
FL + GAN	Identification of missing information and generation	Peng et al. [108]
FL + DNN	Prioritization of data in the training process of DL models	Li et al. [109]
FL + B5G + UAVs	Data collection in a privacy-preserving manner	Nasser et al. [110]
FL + Computational intelligence (CI)	Enhancement of data quality and equality in CI	Peyvandi et al. [111]
FL + Case-based reasoning	Solving concept drift issues in healthcare	Jaiswal et al. [112]
FL + CFmMIMO	Improve convergence speed	Vu et al. [113]
FL + SMC (secure multi-party computation)	Prevent leakage of sensitive information in local models	Li et al. [114]

Apart from the analysis presented in Table 3, some recent surveys have highlighted the synergies in one or more aspects of the FL paradigm [115,116]. Furthermore, the synergies of FL are increasing data day by day to improve various technical aspects of this technology [117,118]. These synergies have also extended the applicability of this technology to many commercial and industrial sectors. Furthermore, some of these integrations are made to lower the communication and computation overheads of this technology [119]. In addition, some integrations are improving the privacy aspects of this technology [120]. In

the coming years, the synergies of this paradigm with emerging technologies are likely to expand to advance its capabilities.

5. Open Source Implementation Frameworks of Federated Learning

In this section, we discuss the open-source implementations of the FL paradigm that have been experimentally tested on some real-world datasets. Although many open-source frameworks have been developed in the recent past, we present only the main frameworks that are accessible for rapid validation and experimentation in Figure 6. Most frameworks listed in Figure 6 can work with any dataset, but only a few provide robust support against attacks (i.e., Privacy FL). The tutorials and documentation about most frameworks are incomplete/partial except for OpenFL and PySft. Only a few frameworks provide support for other libraries and data partitioning. Most frameworks run on traditional CPUs, and only a few can run on large-scale hardware such as graphical processing units (GPUs). In addition to these open source developments, some propriety frameworks such as IBM FL [121], Substra [122], and NVIDIA CLARA [123], etc., have also been developed, which are not yet publicly available for rapid testing and validation. Moreover, there exists an open-source implementation of FL for some other emerging technologies (e.g., the IoT) [124]. Interestingly, only two frameworks (e.g., OpenFL and Fed-BioMed) provide support for medical applications. By using the FL frameworks listed in Figure 6, possible risks of exposing patients' sensitive health-related information can be resolved. In addition, the FL strategy enhances the training performance on medical data by exploiting big and large-scale datasets and offloading most processing to the local devices in a network, which would not be possible with the centralized AI technique.

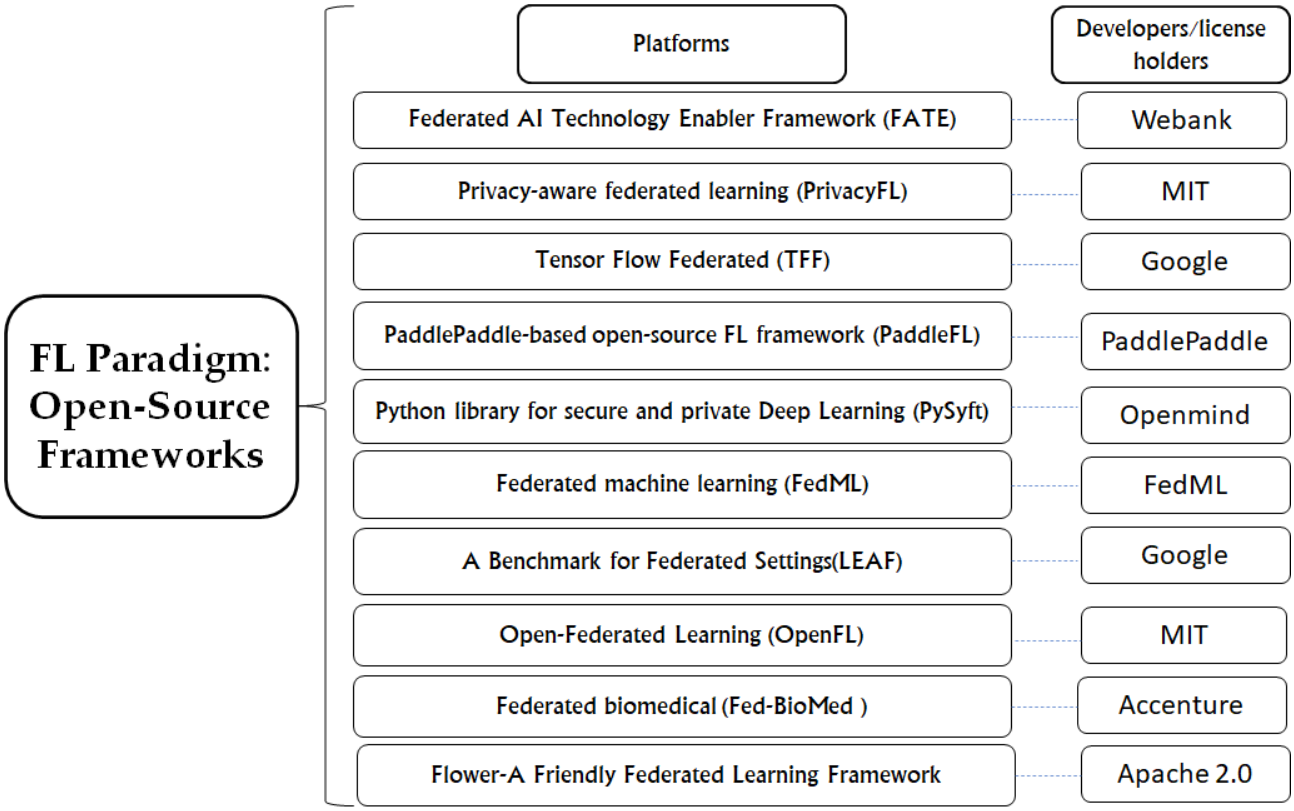


Figure 6. Open-source implementations of the FL paradigm (i.e., open source FL frameworks).

To provide technical information concerning two medical-related frameworks, we compare both frameworks on technical grounds in Table 4. The analysis presented in Table 4 can help to understand and further improve the implantation of these frameworks.

Lastly, these implementations have been used as the baseline in most studies and have been rigorously enhanced.

Table 4. Detailed comparison of medical implementation of Fl frameworks.

Features	OpenFL	Fed-BioMed
Implementation language	Python	Python
Working mechanism	Distributed	Distributed
Development tools/libraries	PyTorch and TensorFlow	Scikit-Learn and PyTorch
Development status	Fully Developed	Under development
Ability to work with diverse datasets	Yes	Yes
Additional support for privacy-preservation	No	No
Executing malicious activities	Easy	Easy
Customization (working with many libraries)	Full support	Partial support
Work packages information	Available	Partially available
Communication and computation overheads	Very high	High
Favorable hardware architecture	CPU, GPU	CPU, GPU
Data sources	Heterogeneous	Image and text
Scalability	High	Yet to be tested
Data partitioning services	Full support	Partial support
Vulnerability to model and data poisoning attacks	Medium	High
Potentials of commercialization	High	Average
Practical applications	Exist	Yet to be tested for
Documentation and use cases	Available	Partial availability

6. Challenges and Recommendations

When it comes to the actual deployment of FL in real-life healthcare settings, there exist multiple challenges. Although some challenges have been described in the previous research, a clear picture from all perspectives is still missing. In this work, we highlight most challenges of the FL paradigm and suggest valuable recommendations to address those challenges. As shown in Figure 7, we have categorized these FL challenges into nine main categories, which remained unexplored in the current literature.

Apart from the challenges cited in Figure 7, explainability, transparency, and fairness are also the main challenges of FL in the context of healthcare [125,126]. We will present each of these challenges in detail in the following paragraphs.

Client-related challenges: In the FL paradigm, clients are regarded as independent, which means they can perform most activities autonomously. Hence, they can leave the system at any time, which can lead to longer convergence and disturbs the training process [127]. The prevention of the client's dropout is a longstanding challenge in FL. In addition, the selection of clients who can contribute good models/data is also a non-trivial task. In some cases, clients make bots with each other to carry out any sort of malicious activities, which makes FL results unreliable or corrupts the training process. In addition, some clients hold up the data/model and delay the convergence speed. All these client-related challenges can degrade the performance of the FL paradigm.

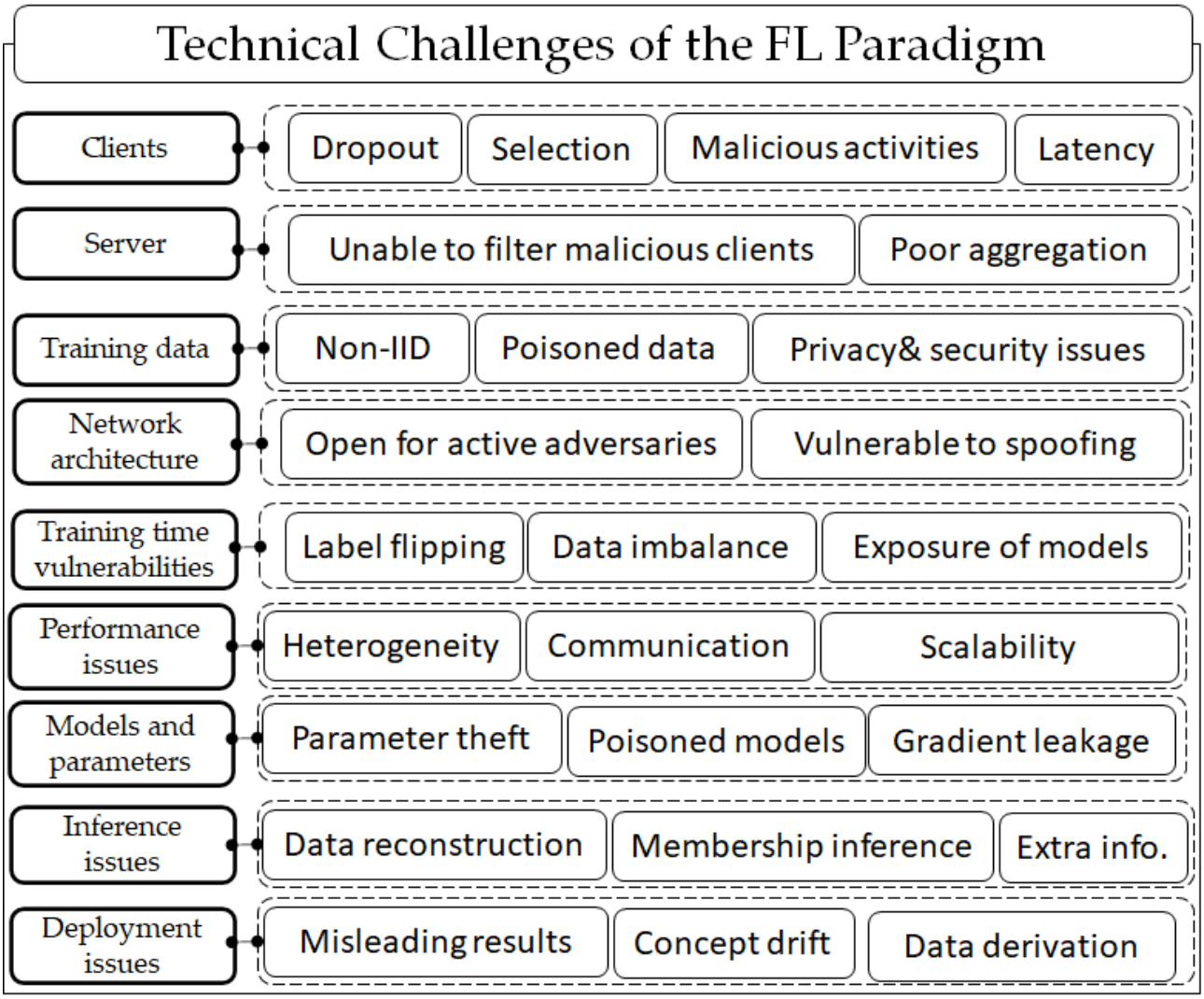


Figure 7. Technical challenges of the FL paradigm from the perspective of COVID-19.

Servers-related challenges: In the FL paradigm, the server is responsible for the orchestration of the local models, aggregating models, and sharing the global model. However, in some cases, multiple attacks can be executed on the server by adversaries, which makes the FL system untrustworthy. Since the server is only concerned with the model weights without deep inspection, it cannot filter malicious clients, which degrades the performance of the FL paradigm. In some cases, gradients/parameters are exposed to adversaries during aggregation. All these server-related challenges can degrade the performance of the FL paradigm.

Training-data-related challenges: In the FL paradigm, training data are the most important element because the quality of FL models depends on the training data. There exist multiple challenges with regard to the quality of data. In addition, the privacy of the training data is one of the hot challenges in the FL paradigm [128]. Recently, the non-i.i.d. nature of the training data poses various technical challenges in the FL paradigm, and their solution has become more urgent than ever. In addition, guaranteeing the quality of data and preventing it from poisoning the paradigm is also one of the main challenges [129]. To truly benefit from the potential of FL, training-data-related challenges need robust solutions.

Poisoning-attacks-related challenges: In the FL paradigm, two main challenges that make the FL system unreliable in terms of results are: data poisoning and model poisoning. In the former attack, wrong data are used in training the local mode. In the latter attack, wrong local models are being sent to the central server [130,131]. Both these attacks have been investigated to enhance the trustworthiness of FL results. Furthermore, many strategies,

even such as compromising privacy, have been suggested to eliminate these attacks [132]. To truly benefit from the potential of FL, both these challenges need a robust solution from the research community.

COVID-19-related challenges: In the COVID-19 era, due to the rapid rise in the amount of data, processing large and high-dimensional datasets has become challenging [133]. Furthermore, due to privacy concerns, good-quality data cannot be obtained easily. In these circumstances, FL can contribute toward resolving the data winter problem. However, the lack of a well-defined method for deploying FL methods in real life hinders the progress of AI-related methods. In addition, privacy issues such as data reconstruction make the deployment of FL very hard. Furthermore, identifying clients that can contribute good data in the FL paradigm remains challenging. Lastly, processing heterogeneous sources of data and deriving knowledge if it is very challenging. Furthermore, studying all dynamics of COVID-19 is still challenging because good-quality data for some aspects of this pandemic are not available for research purposes.

Apart from the challenges discussed above, handling inference and training time vulnerabilities in the FL paradigm is also very challenging. Luo et al. [134] discussed the possibility of inference attacks on FL systems through which potential privacy leakages can occur in real-life scenarios. Through this approach, the authors highlighted the need to preserve the privacy of prediction outputs in the vertical FL. Qiu et al. [135] highlighted the possibility of relation leakage and node leakage, leading to severe privacy breaches from graph data in vertical FL. Ha et al. [136] highlighted the possibility of inference attacks on the client side in FL systems using the generative adversarial networks (GANs) model. The authors have shown that some DL models can learn "unintended" features that can expose personal information to adversarial participants/clients. Rassouli et al. [137] have shown that in FL systems, an adversary can perfectly reconstruct a substantial number of features when the number of predictions is large enough. These kinds of data reconstruction attacks enable full training data disclosure in most cases. Zhang et al. [138] proposed a GAN-enhanced method for launching a membership inference attack in FL systems. The authors achieved a 98% attack accuracy and identified two main reasons (i.e., diversity in training data and overfitted FL models) for the success of such attacks. To address these inference attacks, many defense strategies have also been developed [139–141]. Further information about inference attacks and their corresponding defense can be learned from a recent study [142]. Recently, security and privacy issues have been rigorously investigated by many researchers [143]. In the future, more defense mechanisms will be needed to provide a solid defense against many emerging inference attacks (e.g., feature detection, extraction, feature disclosure, label disclosure, data reconstruction, membership inference, unintended features, feature information, etc.). Recently, addressing statistical heterogeneity in training data across clients/devices has also become one of the hot challenges in the FL paradigm [144]. Concept drift makes the FL learning process more complicated because of the higher inconsistency between existing and upcoming data. Traditional concept drifts handling techniques (e.g., chunk-based and ensemble-learning-based) are unsuitable in the FL frameworks due to the heterogeneity of local devices [145]. Similarly, handling some data types such as genome data in the FL environments poses various challenges [146]. Considering these challenges, robust solutions are needed to address all of the above-mentioned challenges. In Table 5, we propose technical recommendations to address these challenges by analyzing the existing open-source developments, as well as the detailed synthesis of published literature. The detailed guidelines presented in Table 5 can contribute to enhancing the technical effectiveness of this recent paradigm.

Table 5. Valuable recommendations to address technical challenges in the FL paradigm.

FL Aspect(s)	Recommendation(s)
Clients	Development of multi-criteria (i.e., activeness, data quality, computing resources, etc.) incentive mechanisms to retain potential clients.
Server	Implementation of anomaly detection algorithms for filtering malicious clients/local-models/updates.
Training data	(i) Analyzing the distributions of data concerning balance and adding synthetic samples for minority classes. (ii) Implementation of privacy solutions such as differential privacy or encryption for securing it. (iii) Implementation of secure data sharing strategies to remove poisoned samples.
Network Architecture	(i) Implementation of subspace clustering concepts to lower communication overheads. (ii) Implementation of light-weight encryption techniques for securing parameters/gradients in transit. (iii) Implementation of verifiable computing protocol at the server side for verification of local models.
Training time vulnerabilities	(i) Implementation of diversity-aware training methods to prevent biased decisions. (ii) Implementation of lightweight algorithms to handle evasion attacks. (iii) Implementation of secure algorithms for the security of local models.
Performance issues	(i) Implementation of parallel computing algorithms for enhancing scalability. (ii) Implementation of algorithms that do not share local models frequently (i.e., partial information sharing methods). (iii) Implementation of edge/fog computing models to donate some computing to nearby devices. (iv) Implementation of computing offloading methods to prevent cold start problems. (v) Implementation of low-cost convergence criteria.
Models and parameters	(i) Implementation of secure methods for communication between clients and server. (ii) Implementation of clustering methods to share information in the clustered form. (iii) Implementation of methods for filtering wrong models.
Inference issues	(i) Implementation of secure methods for preventing data reconstruction attacks. (ii) Implementation of methods for hiding details of training data. (iii) Restricting access to data/results by analyzing the sensitivity-based analysis of the queries.
Deployment issues	(i) Forming multidisciplinary teams to analyze the risks of deployment. (ii) Implementation of explainability, fairness, and trustworthy functionalities for results understanding. (iii) Proposing GPU-based implementations to address scalability, communication, and computing issues.

7. Comparisons and Discussion

In this section, we compare our work with the existing state-of-the-art (SOTA) studies in multiple aspects. Although many studies have highlighted the potential of the FL paradigm in the medical field, only a few studies have focused on the applications of the FL paradigm in the COVID-19 era. To compare our work, we selected seven SOTA and recently published studies centering on the FL paradigm in the medical field. We have chosen various parameters for fair comparisons to prove the significance of our work in the body of knowledge. Table 6 presents the in-depth analysis and comparison of our work with the existing SOTA studies.

Table 6. Multi-criteria-based detailed comparison of the proposed work with existing SOTA studies.

Criteria	[17]	[30]	[38]	[81]	[84]	[106]	[126]	Ours
Study Focus	**COVID-19 Detection**	**FL System Design**	**Generic Healthcare Apps**	**General Healthcare Apps**	**General Healthcare**	**Data Handling**	**Smart Healthcare**	**FL Apps in COVID-19 Era**
Number of app with regard to the virus	1	0	4	9	7	12	4	36
FL challenges	×	×	○	○	○	○	○	✓
Data types	×	×	○	○	○	○	○	✓
OS frameworks	×	×	×	×	×	×	×	✓
Medical libraries	×	×	×	×	×	×	×	✓
TR	×	×	×	×	×	×	×	✓
FL synergies	×	×	×	×	×	×	×	✓
Deployment issues	×	×	×	×	×	×	○	✓
Other technologies' roles	×	×	×	×	×	×	○	✓
FL research area(s)	×	×	×	×	×	×	×	✓

Abbreviations: apps (applications), OS (Open source), TR (technical recommendations. Key: ✓⇒ available/reported and ×⇒ not available/not reported, ○ → partially covered (or discussed).

As shown in Table 6, our work has covered many more aspects of FL with regard to COVID-19 than the previous SOTA studies. In addition, this is the first work that has comprehensively covered FL's role in the recent pandemic. The contents enclosed in this article can pave the way for understanding this leading technological role in the medical field, especially related to COVID-19. In addition, our work is the first that highlights the open-source developments of FL, which can assist in understanding the development status of this paradigm. In recent years, FL has been fused with multiple technologies (i.e., the industrial internet of things (IIoT), blockchain, edge computing, etc.) to address the privacy and security issues in real-life domains [147]. Although FL can solve many cybersecurity-related issues, the FL paradigm is prone to multiple attacks due to its decentralized architecture. Therefore, more approaches are needed to address cybersecurity-related issues in FL-based systems.

The major contributions of this work compared to previous studies are: (i) higher coverage of FL applications in terms of numbers (i.e., 36) in the era of COVID-19; (ii) through discussion of challenges faced by FL paradigm which are either ignored or barely discussed by previous studies; (iii) systematic discussion of data types which were used to lower the spread of COVID-19; (iv) highlighted the open-source frameworks that have recently been developed along with their in-depth details; (v) a discussion and analysis of open source frameworks that were being developed specifically for the medical domain; (vi) it is the first study to provide recommendations to address the technical deficiencies of the FL paradigm; (vii) it is the first study that pinpoints and discusses the synergies of FL with other emerging technologies; (viii) the systematic coverage of issues that can emerge in FL deployment; (ix) a discussion about other COVID-19-fighting digital technologies; and (x) a detailed discussion of hot research area(s) targeting the FL paradigm. Furthermore, our study has covered many FL applications in the COVID-19 era that remained unexplored in previous works. Furthermore, this is the first study that discussed FL applications along with AI models and data details. This work can pave the way to providing the recent status of FL developments in the COVID-19 era.

8. Conclusions and Future Work

In the big data era, there is a growing demand for the responsible use of data to draw fair, unbiased, and impartial decisions with the help of data science tools to improve the quality of many real-world services (e.g., healthcare, recommendation, navigation, smart cities, mobile doctors, etc.). Since data have a huge impact on the advancements of real-life services/decisions, data must therefore be shared on a large scale with analysts/researchers. Unfortunately, data distribution at a wider scale is not possible due to privacy concerns, and many companies are reluctant to share aggregated personal data. Thanks to the rapid development in the FL paradigm, personal data orchestration at a central place is no longer required while the AI model can still be trained on them locally. In this paper, we present a technical overview including applications and challenges of the FL paradigm with a special emphasis on COVID-19 in the big data era. Although there are some review papers on FL applications in the medical domain, they paid less attention to FL applications in the context of the COVID-19 pandemic. To fill this gap, we presented an in-depth review of the FL applications and challenges in the context of COVID-19. In the future, we intend to cover the taxonomy of FL applications involving both independent and identically distributed (IID) and non-IID data in the medical field [148–150]. Finally, we intend to discuss the hardware and software challenges in the deployment of FL models in real-life scenarios.

Author Contributions: Conceptualization, A.M., X.Z. and S.O.H.; methodology, A.M. and X.Z.; software, A.M. and S.O.H.; validation, A.M., X.Z. and S.O.H.; investigation, A.M., X.Z. and S.O.H.; resources, A.M. and S.O.H.; data curation, A.M., X.Z. and S.O.H.; writing—original draft preparation, A.M. and X.Z.; writing—review and editing, A.M., X.Z. and S.O.H.; visualization, A.M.; supervision, S.O.H.; project administration, S.O.H.; funding acquisition, A.M. and S.O.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data and studies that were used to support the findings of this study are included within this article.

Acknowledgments: The authors would like to thank the editor and reviewers for their insightful comments and valuable suggestions, which helped improve the quality of the paper significantly.

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

References

1. Alazab, M.; RM, S.P.; Parimala, M.; Maddikunta, P.K.; Gadekallu, T.R.; Pham, Q.V. Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3501–3509. [CrossRef]
2. Banabilah, S.; Aloqaily, M.; Alsayed, E.; Malik, N.; Jararweh, Y. Federated learning review: Fundamentals, enabling technologies, and future applications. *Inf. Process. Manag.* **2022**, *59*, 103061. [CrossRef]
3. Chan, E.Y.; Saqib, N.U. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Comput. Hum. Behav.* **2021**, *119*, 106718. [CrossRef] [PubMed]
4. Wainakh, A.; Guinea, A.S.; Grube, T.; Mühlhäuser, M. Enhancing privacy via hierarchical federated learning. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020.
5. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2019**, *13*, 1–207.
6. 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. [CrossRef]
7. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
8. Fang, C.; Guo, Y.; Wang, N.; Ju, A. Highly efficient federated learning with strong privacy preservation in cloud computing. *Comput. Secur.* **2020**, *96*, 101889. [CrossRef]
9. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Federated learning for data privacy preservation in vehicular cyber-physical systems. *IEEE Netw.* **2020**, *34*, 50–56. [CrossRef]
10. Liu, G.; Wang, C.; Ma, X.; Yang, Y. Keep your data locally: Federated-learning-based data privacy preservation in edge computing. *IEEE Netw.* **2021**, *35*, 60–66. [CrossRef]
11. Zhao, B.; Fan, K.; Yang, K.; Wang, Z.; Li, H.; Yang, Y. Anonymous and privacy-preserving federated learning with industrial big data. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6314–6323. [CrossRef]
12. Połap, D. Fuzzy Consensus with Federated Learning Method in Medical Systems. *IEEE Access* **2021**, *9*, 150383–150392. [CrossRef]
13. Ruzafa-Alcazar, P.; Fernandez-Saura, P.; Marmol-Campos, E.; Gonzalez-Vidal, A.; Ramos, J.L.; Bernal, J.; Skarmeta, A.F. Intrusion Detection based on Privacy-preserving Federated Learning for the Industrial IoT. *IEEE Trans. Ind. Inform.* **2021**. [CrossRef]
14. Cheng, Y.; Liu, Y.; Chen, T.; Yang, Q. Federated learning for privacy-preserving AI. *Commun. Acm* **2020**, *63*, 33–36. [CrossRef]
15. Ding, J.; Tramel, E.; Sahu, A.K.; Wu, S.; Avestimehr, S.; Zhang, T. Federated learning challenges and opportunities: An outlook. In Proceedings of the ICASSP 2022–2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, 23–27 May 2022.
16. Rieke, N.; Hancox, J.; Li, W.; Milletari, 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*, 119. [CrossRef]
17. Naz, S.; Phan, K.T.; Chen, Y.P. A comprehensive review of federated learning for COVID-19 detection. *Int. J. Intell. Syst.* **2022**, *37*, 2371–2392. [CrossRef]
18. Zhang, W.; Zhou, T.; Lu, Q.; Wang, X.; Zhu, C.; Sun, H.; Wang, Z.; Lo, S.K.; Wang, F.Y. Dynamic-fusion-based federated learning for COVID-19 detection. *IEEE Internet Things J.* **2021**, *8*, 15884–15891. [CrossRef]
19. Abdul Salam, M.; Taha, S.; Ramadan, M. COVID-19 detection using federated machine learning. *PLoS ONE* **2021**, *16*, e0252573. [CrossRef]
20. Dayan, I.; Roth, H.R.; Zhong, A.; Harouni, A.; Gentili, A.; Abidin, A.Z.; Liu, A.; Costa, A.B.; Wood, B.J.; Tsai, C.S.; et al. Federated learning for predicting clinical outcomes in patients with COVID-19. *Nat. Med.* **2021**, 27, 1735–1743. [CrossRef]
21. Vaid, A.; Jaladanki, S.K.; Xu, J.; Teng, S.; Kumar, A.; Lee, S.; Somani, S.; Paranjpe, I.; De Freitas, J.K.; Wanyan, T.; et al. Federated learning of electronic health records to improve mortality prediction in hospitalized patients with COVID-19: Machine learning approach. *JMIR Med. Inform.* **2021**, *9*, e24207. [CrossRef]
22. Fourati, L.C.; Samiha, A.Y. Federated learning toward data preprocessing: COVID-19 context. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021.
23. Chen, J.J.; Chen, R.; Zhang, X.; Pan, M. A privacy preserving federated learning framework for COVID-19 vulnerability map construction. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021.

24. Ahmed, J.; Nguyen, T.N.; Ali, B.; Javed, A.; Mirza, J. On the Physical Layer Security of Federated Learning based IoMT Networks. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef]
25. Samuel, O.; Omojo, A.B.; Onuja, A.M.; Sunday, Y.; Tiwari, P.; Gupta, D.; Hafeez, G.; Yahaya, A.S.; Fatoba, O.J.; Shamshirb, S. IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef] [PubMed]
26. Florescu, L.M.; Streba, C.T.; Şerbănescu, M.S.; Mămuleanu, M.; Florescu, D.N.; Teică, R.V.; Nica, R.E.; Gheonea, I.A. Federated Learning Approach with Pre-Trained Deep Learning Models for COVID-19 Detection from Unsegmented CT images. *Life* **2022**, *12*, 958. [CrossRef] [PubMed]
27. Bhattacharya, A.; Gawali, M.; Seth, J.; Kulkarni, V. Application of Federated Learning in building a robust COVID-19 Chest X-ray classification Model. *arXiv* **2022**, arXiv:2204.10505.
28. Zhang, Q.; Ren, X.; Wei, B. Segmentation of infected region in CT images of COVID-19 patients based on QC-HC U-net. *Sci. Rep.* **2021**, *11*, 22854 .
29. Zhu, R.; Yin, K.; Xiong, H.; Tang, H.; Yin, G. Masked face detection algorithm in the dense crowd based on federated learning. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 8586016. [CrossRef]
30. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; Li, Y.; Liu, X.; He, B. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Trans. Knowl. Data Eng.* **2021**. [CrossRef]
31. Liu, J.; Huang, J.; Zhou, Y.; Li, X.; Ji, S.; Xiong, H.; Dou, D. From distributed machine learning to federated learning: A survey. *Knowl. Inf. Syst.* **2022**, *64*, 885–917. [CrossRef]
32. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
33. 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. [CrossRef]
34. Kumar, Y.; Singla, R. Federated learning systems for healthcare: Perspective and recent progress. In *Federated Learning Systems. Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 141–156.
35. Asad, M.; Moustafa, A.; Ito, T. FedOpt: Towards communication efficiency and privacy preservation in federated learning. *Appl. Sci.* **2020**, *10*, 2864. [CrossRef]
36. Du, Z.; Wu, C.; Yoshinaga, T.; Yau, K.L.; 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. [CrossRef]
37. Li, Y.; Ding, B.; Zhou, J. A Practical Introduction to Federated Learning. In Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD'22), Washington, DC, USA, 14–18 August 2022; pp. 4802–4803. [CrossRef]
38. Antunes, R.S.; André da Costa, C.; Küderle, A.; Yari, I.A.; Eskofier, B. Federated Learning for Healthcare: Systematic Review and Architecture Proposal. *ACM Trans. Intell. Syst. Technol. TIST* **2022**, *13*, 1–23. [CrossRef]
39. Lee, H.; Chai, Y.J.; Joo, H.; Lee, K.; Hwang, J.Y.; Kim, S.M.; Kim, K.; Nam, I.C.; Choi, J.Y.; Yu, H.W.; et al. Federated learning for thyroid ultrasound image analysis to protect personal information: Validation study in a real health care environment. *JMIR Med. Inform.* **2021**, *9*, e25869. [CrossRef]
40. Szatmari, T.I.; Petersen, M.K.; Korzepa, M.J.; Giannetsos, T. Modelling audiological preferences using federated learning. In Proceedings of the Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization, Genoa, Italy, 12–18 July 2020; pp. 187–190.
41. Zerka, F.; Urovi, V.; Vaidyanathan, A.; Jaiman, V.; Leijenaar, R.T.; Walsh, S.; Gabrani-Juma, H.; Woodruff, H.C.; Dumontier, M.; Lambin, P. A blockchain based approach for Privacy Preserving distributed learning-Grade Group Prediction for Prostate Cancer Patients. *Distrib. Learn. Optim. Radiomics Knowl.* **2022**, *135*. [CrossRef]
42. Ribero, M.; Henderson, J.; Williamson, S.; Vikalo, H. Federating recommendations using differentially private prototypes. *Pattern Recognit.* **2022**, *129*, 108746. [CrossRef]
43. Ngo, T.; Nguyen, D.C.; Pathirana, P.N.; Corben, L.A.; Delatycki, M.B.; Horne, M.; Szmulewicz, D.J.; Roberts, M. Federated Deep Learning for the Diagnosis of Cerebellar Ataxia: Privacy Preservation and Auto-Crafted Feature Extractor. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2022**, *30*, 803–811. [CrossRef]
44. Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 972–976. [CrossRef]
45. Kumar, R.; Khan, A.A.; Kumar, J.; Golilarz, N.A.; Zhang, S.; Ting, Y.; Zheng, C.; Wang, W. Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Sens. J.* **2021**, *21*, 16301–16314. [CrossRef]
46. Flores, M.; Dayan, I.; Roth, H.; Zhong, A.; Harouni, A.; Gentili, A.; Abidin, A.; Liu, A.; Costa, A.; Wood, B.; et al. Federated Learning used for predicting outcomes in SARS-COV-2 patients. *Res. Sq.* **2021**. [CrossRef]
47. Dou, Q.; So, T.Y.; Jiang, M.; Liu, Q.; Vardhanabhuti, V.; Kaissis, G.; Li, Z.; Si, W.; Lee, H.H.; Yu, K.; et al. Federated deep learning for detecting COVID-19 lung abnormalities in CT: A privacy-preserving multinational validation study. *NPJ Digit. Med.* **2021**, *4*, 60. [CrossRef]
48. Yang, D.; Xu, Z.; Li, W.; Myronenko, A.; Roth, H.R.; Harmon, S.; Xu, S.; Turkbey, B.; Turkbey, E.; Wang, X.; et al. Federated semi-supervised learning for COVID region segmentation in chest CT using multi-national data from China, Italy, Japan. *Med. Image Anal.* **2021**, *70*, 101992. [CrossRef] [PubMed]

49. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Zomaya, A.Y. Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet Things J.* **2021**, *9*, 10257–10271. [CrossRef]
50. Aswathy, A.L.; Vinod Chandra, S.S. Cascaded 3D UNet architecture for segmenting the COVID-19 infection from lung CT volume. *Sci. Rep.* **2022**, *12*, 3090.
51. Kumaresan, M.; Kumar, M.S.; Muthukumar, N. Analysis of mobility based COVID-19 epidemic model using Federated Multitask Learning. *Math. Biosci. Eng.* **2022**, *19*, 9983–10005. [CrossRef] [PubMed]
52. Ohata, E.F.; Bezerra, G.M.; das Chagas, J.V.; Neto, A.V.; Albuquerque, A.B.; de Albuquerque, V.H.; Reboucas Filho, P.P. Automatic detection of COVID-19 infection using chest X-ray images through transfer learning. *IEEE/CAA J. Autom. Sin.* **2020**, *8*, 239–248. [CrossRef]
53. Alhudhaif, A.; Polat, K.; Karaman, O. Determination of COVID-19 pneumonia based on generalized convolutional neural network model from chest X-ray images. *Expert Syst. Appl.* **2021**, *180*, 115141. [CrossRef]
54. Das, A.K.; Dey, D.; Chatterjee, B.; Dalai, S. A transfer learning approach to sense the degree of surface pollution for metal oxide surge arrester employing infrared thermal imaging. *IEEE Sens. J.* **2021**, *21*, 16961–16968. [CrossRef]
55. Singh, P.; Kaur, R. Implementation of the QoS framework using fog computing to predict COVID-19 disease at early stage. *World J. Eng.* **2021**, *19*, 80–89. [CrossRef]
56. Kochgaven, C.; Mishra, P.; Shitole, S. Detecting Presence of COVID-19 with ResNet-18 using PyTorch. In Proceedings of the 2021 International Conference on Communication Information and Computing Technology (ICCICT), Mumbai, India, 25–27 June 2021.
57. Chen, X.; Shao, Y.; Xue, Z.; Yu, Z. Multi-Modal COVID-19 Discovery with Collaborative Federated Learning. In Proceedings of the 2021 IEEE 7th International Conference on Cloud Computing and Intelligent Systems (CCIS), Xi'an, China, 7–8 November 2021.
58. Laouarem, A.; Kara-Mohamed, C.; Bourenane, E.B.; Hamdi-Cherif, A. A deep learning model for CXR-based COVID-19 detection. In Proceedings of the 2021 International Conference on Engineering and Emerging Technologies (ICEET), Istanbul, Turkey, 27–28 October 2021.
59. Malhotra, R.; Patel, H.; Fataniya, B.D. Prediction of COVID-19 Disease with Chest X-rays Using Convolutional Neural Network. In Proceedings of the 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2–4 September 2021; pp. 545–550.
60. Song, Q.; Zheng, Y.J.; Yang, J.; Huang, Y.J.; Sheng, W.G.; Chen, S.Y. Predicting Demands of COVID-19 Prevention and Control Materials via Co-Evolutionary Transfer Learning. *IEEE Trans. Cybern.* **2022**. [CrossRef]
61. Le Dinh, T.; Lee, S.H.; Kwon, S.G.; Kwon, K.R. COVID-19 Chest X-ray Classification and Severity Assessment Using Convolutional and Transformer Neural Networks. *Appl. Sci.* **2022**, *12*, 4861. [CrossRef]
62. Senthilkumar, G.; Sasidhar, V.J.; Saravana Kumar, S.; Vignesh, E. Disease Prediction Systems for COVID with Electronic Medical Records. *Int. J. Innov. Sci. Res. Technol.* **2021**, *6*, 8–10.
63. Wang, Q.; Guo, Y.; Ji, T.; Wang, X.; Hu, B.; Li, P. Toward Combatting COVID-19: A Risk Assessment System. *IEEE Internet Things J.* **2021**, *8*, 15953–15964. [CrossRef]
64. Chen, R.; Li, L.; Ma, Y.; Gong, Y.; Guo, Y.; Ohtsuki, T.; Pan, M. Constructing Mobile Crowdsourced COVID-19 Vulnerability Map with Geo-Indistinguishability. *IEEE Internet Things J.* **2022**, 9, 17403–17416. [CrossRef]
65. Ho, T.T.; Tran, K.D.; Huang, Y. FedSGDCOVID: Federated SGD COVID-19 Detection under Local Differential Privacy Using Chest X-ray Images and Symptom Information. *Sensors* **2022**, *22*, 3728. [CrossRef]
66. Durga, R.; Poovammal, E. FLED-Block: Federated Learning Ensembled Deep Learning Blockchain Model for COVID-19 Prediction. *Front. Public Health* **2022**, *10*, 892499. [CrossRef]
67. Rahman, M.A.; Hossain, M.S. An internet-of-medical-things-enabled edge computing framework for tackling COVID-19. *IEEE Internet Things J.* **2021**, *8*, 15847–15854. [CrossRef]
68. Mukherjee, R.; Kundu, A.; Mukherjee, I.; Gupta, D.; Tiwari, P.; Khanna, A.; Shorfuzzaman, M. IoT-cloud based healthcare model for COVID-19 detection: An enhanced k-Nearest Neighbour classifier based approach. *Computing* **2021**. [CrossRef]
69. Aljumah, A. Assessment of machine learning techniques in IoT-based architecture for the monitoring and prediction of COVID-19. *Electronics* **2021**, *10*, 1834. [CrossRef]
70. Mir, M.H.; Jamwal, S.; Mehbodniya, A.; Garg, T.; Iqbal, U.; Samori, I.A. IoT-Enabled Framework for Early Detection and Prediction of COVID-19 Suspects by Leveraging Machine Learning in Cloud. *J. Healthc. Eng.* **2022**, *2022*, 7713939. [CrossRef]
71. Wang, H.; Tao, G.; Ma, J.; Jia, S.; Chi, L.; Yang, H.; Zhao, Z.; Tao, J. Predicting the Epidemics Trend of COVID-19 Using Epidemiological-Based Generative Adversarial Networks. *IEEE J. Sel. Top. Signal Process.* **2022**, *16*, 276–288. [CrossRef]
72. Bhatia, M.; Manocha, A.; Ahanger, T.A.; Alqahtani, A. Artificial intelligence-inspired comprehensive framework for COVID-19 outbreak control. *Artif. Intell. Med.* **2022**, *127*, 102288. [CrossRef] [PubMed]
73. Hidayat, S.N.; Julian, T.; Dharmawan, A.B.; Puspita, M.; Chandra, L.; Rohman, A.; Julia, M.; Rianjanu, A.; Nurputra, D.K.; Triyana, K.; et al. Hybrid learning method based on feature clustering and scoring for enhanced COVID-19 breath analysis by an electronic nose. *Artif. Intell. Med.* **2022**, *129*, 102323. [CrossRef] [PubMed]
74. Rathee, G.; Garg, S.; Kaddoum, G.; Wu, Y.; Jayakody, D.N.; Alamri, A. ANN assisted-IoT enabled COVID-19 patient monitoring. *IEEE Access* **2021**, *9*, 42483–42492. [CrossRef] [PubMed]
75. AlOmani, G.Y.; Darwesh, A.D.; AlSennei, S.A.; Buabbas, H.A.; AlGhareeb, A.F.; Ahmed, H.O. COVID-19 Symptoms Monitoring Sensor Network for Isolation Rooms at Hospitals. In Proceedings of the 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON), Palermo, Italy, 14–16 June 2022; pp. 741–745.

76. Salim, M.M.; Park, J.H. Federated Learning-based secure Electronic Health Record sharing scheme in Medical Informatics. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef] [PubMed]
77. Singh, M.; Bansal, S. A Proposed Federated Learning Model for Vaccination Tweets. In Proceedings of the International Conference on Computational Intelligence in Pattern Recognition, Howrah, India, 23–24 April 2022; pp. 383–392.
78. Park, S.; Kim, G.; Kim, J.; Kim, B.; Ye, J.C. Federated split task-agnostic vision transformer for COVID-19 CXR diagnosis. *Adv. Neural Inf. Process. Syst.* **2021**, *34*, 24617–24630.
79. Islam, T.U.; Ghasemi, R.; Mohammed, N. Privacy-Preserving Federated Learning Model for Healthcare Data. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0281–0287.
80. Yan, R.; Qu, L.; Wei, Q.; Huang, S.C.; Shen, L.; Rubin, D.; Xing, L.; Zhou, Y. Label-Efficient Self-Supervised Federated Learning for Tackling Data Heterogeneity in Medical Imaging. *arXiv* **2022**, arXiv:2205.08576.
81. Shyu, C.R.; Putra, K.T.; Chen, H.C.; Tsai, Y.Y.; Hossain, K.T.; Jiang, W.; Shae, Z.Y. A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. *Appl. Sci.* **2021**, *11*, 11191.
82. Nguyen, D.C.; Pham, Q.-V.; Pathirana, P.N.; Ding, M.; Seneviratne, A.; Lin, Z.; Dobre, O.; Hwang, W.-J. Federated learning for smart healthcare: A survey. *ACM Comput. Surv. CSUR* **2022**, *55*, 1–37. [CrossRef]
83. Xia, Q.; Ye, W.; Tao, Z.; Wu, J.; Li, Q. A survey of federated learning for edge computing: Research problems and solutions. *High-Confid. Comput.* **2021**, *1*, 100008. [CrossRef]
84. Joshi, M.; Pal, A.; Sankarasubbu, M. Federated Learning for Healthcare Domain-Pipeline, Applications and Challenges. *ACM Trans. Comput. Healthc.* **2022**. [CrossRef]
85. Agbley, B.L.; Li, J.; Haq, A.U.; Bankas, E.K.; Ahmad, S.; Agyemang, I.O.; Kulevome, D.; Ndiaye, W.D.; Cobbinah, B.; Latipova, S. Multimodal melanoma detection with federated learning. In Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 17–19 December 2021; pp. 238–244.
86. Fan, J.; Wang, X.; Guo, Y.; Hu, X.; Hu, B. Federated Learning Driven Secure Internet of Medical Things. *IEEE Wirel. Commun.* **2022**, *29*, 68–75. [CrossRef]
87. Sun, L.; Wu, J. A Scalable and Transferable Federated Learning System for Classifying Healthcare Sensor Data. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef]
88. Budd, J.; Miller, B.S.; Manning, E.M.; Lampos, V.; Zhuang, M.; Edelstein, M.; Rees, G.; Emery, V.C.; Stevens, M.M.; Keegan, N.; et al. Digital technologies in the public-health response to COVID-19. *Nat. Med.* **2020**, *26*, 1183–1192. [CrossRef]
89. Bouacida, N.; Mohapatra, P. Vulnerabilities in federated learning. *IEEE Access* **2021**, *9*, 63229–63249. [CrossRef]
90. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.; Poor, H.V. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3454–3469. [CrossRef]
91. 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. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
92. Li, Z.; Liu, J.; Hao, J.; Wang, H.; Xian, M. CrowdSFL: A secure crowd computing framework based on blockchain and federated learning. *Electronics* **2020**, *9*, 773. [CrossRef]
93. Fang, H.; Qian, Q. Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet* **2021**, *13*, 94. [CrossRef]
94. Hakak, S.; Ray, S.; Khan, W.Z.; Scheme, E. A framework for edge-assisted healthcare data analytics using federated learning. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 3423–3427.
95. Laxmi Lydia, E.; Anupama, C.S.; Beno, A.; Elhoseny, M.; Alshehri, M.D.; Selim, M.M. Cognitive computing-based COVID-19 detection on Internet of things-enabled edge computing environment. *Soft Comput.* **2021**. [CrossRef]
96. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Poor, H.V. Federated learning for industrial internet of things in future industries. *IEEE Wirel. Commun.* **2021**, *28*, 192–199. [CrossRef]
97. Hazra, A.; Adhikari, M.; Nandy, S.; Doulani, K.; Menon, V.G. Federated-Learning-Aided Next-Generation Edge Networks for Intelligent Services. *IEEE Netw.* **2022**, *36*, 56–64. [CrossRef]
98. Pang, J.; Huang, Y.; Xie, Z.; Li, J.; Cai, Z. Collaborative city digital twin for the COVID-19 pandemic: A federated learning solution. *Tsinghua Sci. Technol.* **2021**, *26*, 759–771. [CrossRef]
99. Wang, R.; Xu, J.; Ma, Y.; Talha, M.; Al-Rakhami, M.S.; Ghoneim, A. Auxiliary diagnosis of COVID-19 based on 5G-enabled federated learning. *IEEE Netw.* **2021**, *35*, 14–20. [CrossRef]
100. Jaladanki, S.K.; Vaid, A.; Sawant, A.S.; Xu, J.; Shah, K.; Dellepiane, S.; Paranjpe, I.; Chan, L.; Kovatch, P.; Charney, A.W.; et al. Development of a federated learning approach to predict acute kidney injury in adult hospitalized patients with COVID-19 in New York City. *medRxiv* **2021**. [CrossRef]
101. Yang, G.; Wang, S.; Wang, H. Federated learning with personalized local differential privacy. In Proceedings of the 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021; pp. 484–489.
102. Ulhaq, A.; Burmeister, O. COVID-19 imaging data privacy by federated learning design: A theoretical framework. *arXiv* **2020**, arXiv:2010.06177.

103. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *IEEE Access* **2020**, 8, 205071–205087. [CrossRef]
104. Chen, S.W.; Gu, X.W.; Wang, J.J.; Zhu, H.S. AIoT used for COVID-19 pandemic prevention and control. *Contrast Media Mol. Imaging* **2021**, *2021*, 3257035. [CrossRef]
105. Wu, C.; Peng, C.; Du, Z.; Gao, L.; Yoshinaga, T.; Ji, Y. Toward Agile Information and Communication Framework for the Post-COVID-19 Era. *IEEE Open J. Comput. Soc.* **2021**, *2*, 290–299. [CrossRef]
106. Aouedi, O.; Sacco, A.; Piamrat, K.; Marchetto, G. Handling Privacy-Sensitive Medical Data with Federated Learning: Challenges and Future Directions. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef]
107. Yang, Q.; Zhang, J.; Hao, W.; Spell, G.P.; Carin, L. Flop: Federated learning on medical datasets using partial networks. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, Singapore, 14–18 August 2021; pp. 3845–3853.
108. Peng, L.; Wang, N.; Dvornek, N.; Zhu, X.; Li, X. Fedni: Federated graph learning with network inpainting for population-based disease prediction. *IEEE Trans. Med. Imaging* **2022**. [CrossRef]
109. Li, X.C.; Gan, L.; Zhan, D.C.; Shao, Y.; Li, B.; Song, S. Aggregate or Not? Exploring Where to Privatize in DNN Based Federated Learning under Different Non-IID Scenes. *arXiv* **2021**, arXiv:2107.11954.
110. Nasser, N.; Fadlullah, Z.M.; Fouda, M.M.; Ali, A.; Imran, M. A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept. *Comput. Netw.* **2022**, *205*, 108672. [CrossRef]
111. Peyvandi, A.; Majidi, B.; Peyvandi, S.; Patra, J.C. Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0. *Multimed. Tools Appl.* **2022**, *81*, 25029–25050. [CrossRef]
112. Jaiswal, A.; Yigzaw, K.Y.; Öztürk, P. F-CBR: An Architecture for Federated Case-Based Reasoning. *IEEE Access*. **2022**. [CrossRef]
113. Vu, T.T.; Ngo, D.T.; Ngo, H.Q.; Dao, M.N.; Tran, N.H.; Middleton, R.H. Joint Resource Allocation to Minimize Execution Time of Federated Learning in Cell-Free Massive MIMO. *IEEE Internet Things J.* **2022**. [CrossRef]
114. Li, Y.; Zhou, Y.; Jolfaei, A.; Yu, D.; Xu, G.; Zheng, X. Privacy-preserving federated learning framework based on chained secure multiparty computing. *IEEE Internet Things J.* **2020**, *8*, 6178–6186. [CrossRef]
115. Duan, M.; Liu, D.; Ji, X.; Wu, Y.; Liang, L.; Chen, X.; Tan, Y.; Ren, A. Flexible clustered federated learning for client-level data distribution shift. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 2661–2674. [CrossRef]
116. Xu, J.; Glicksberg, B.S.; Su, C.; Walker, P.; Bian, J.; Wang, F. Federated learning for healthcare informatics. *J. Healthc. Inform. Res.* **2021**, *5*, 1–9. [CrossRef]
117. Wibawa, F.; Catak, F.O.; Kuzlu, M.; Sarp, S.; Cali, U. Homomorphic Encryption and Federated Learning based Privacy-Preserving CNN Training: COVID-19 Detection Use-Case. In Proceedings of the EICC 2022: European Interdisciplinary Cybersecurity Conference, Barcelona, Spain, 15–16 June 2022; pp. 85–90.
118. Aich, S.; Sinai, N.K.; Kumar, S.; Ali, M.; Choi, Y.R.; Joo, M.-I.; Kim, H.-C. Protecting personal healthcare record using blockchain & federated learning technologies. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 13–16 February 2022.
119. Cui, L.; Su, X.; Zhou, Y. A Fast Blockchain-based Federated Learning Framework with Compressed Communications. *arXiv* **2022**, arXiv:2208.06095.
120. Liu, Z.; Chen, S.; Ye, J.; Fan, J.; Li, H.; Li, X. DHSA: Efficient Doubly Homomorphic Secure Aggregation for Cross-silo Federated Learning. *arXiv* **2022**, arXiv:2208.07189.
121. Ludwig, H.; Baracaldo, N.; Thomas, G.; Zhou, Y.; Anwar, A.; Rajamoni, S.; Ong, Y.; Radhakrishnan, J.; Verma, A.; Sinn, M.; et al. Ibm federated learning: An enterprise framework white paper v0.1. *arXiv* **2020**, arXiv:2007.10987.
122. Galtier, M.N.; Marini, C. Substra: A framework for privacy-preserving, traceable and collaborative machine learning. *arXiv* **2019**, arXiv:1910.11567.
123. Nvidia, C. An Application Framework Optimized for Healthcare and Life Sciences Developers. Virtual Workshop under DSxConference. 2020. Available online: https://www.perdanauniversity.edu.my/dsx/product/nvidia-clara-an-application-framework-optimized-for-healthcare-and-life-sciences-developers/ (accessed on 10 August 2022).
124. Kholod, I.; Yanaki, E.; Fomichev, D.; Shalugin, E.; Novikova, E.; Filippov, E.; Nordlund, M. Open-source federated learning frameworks for IoT: A comparative review and analysis. *Sensors* **2020**, *21*, 167. [CrossRef] [PubMed]
125. Strobel, M.; Shokri, R. Data Privacy and Trustworthy Machine Learning. *IEEE Secur. Priv.* **2022**, *20*, 44–49. [CrossRef]
126. Rahman, A.; Hossain, M.; Muhammad, G.; Kundu, D.; Debnath, T.; Rahman, M.; Khan, M.; Islam, S.; Tiwari, P.; Band, S. Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. *Clust. Comput.* **2022**, 1–41. [CrossRef]
127. Wu, W.; He, L.; Lin, W.; Mao, R. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 1539–1551. [CrossRef]
128. 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. [CrossRef]
129. Tolpegin, V.; Truex, S.; Gursoy, M.E.; Liu, L. Data poisoning attacks against federated learning systems. In Proceedings of the European Symposium on Research in Computer Security, Guildford, UK, 14–18 September 2020; pp. 480–501.
130. Zhou, X.; Xu, M.; Wu, Y.; Zheng, N. Deep model poisoning attack on federated learning. *Future Internet* **2021**, *13*, 73. [CrossRef]

131. Fang, M.; Cao, X.; Jia, J.; Gong, N. Local model poisoning attacks to Byzantine-Robust federated learning. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Boston, MA, USA, 12–14 August 2020; pp. 1605–1622.
132. Shejwalkar, V.; Houmansadr, A.; Kairouz, P.; Ramage, D. Back to the drawing board: A critical evaluation of poisoning attacks on production federated learning. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; pp. 1354–1371.
133. Majeed, A.; Hwang, S.O. A Privacy-Assured Data Lifecycle for Epidemic-Handling Systems. *Computer* **2022**, *55*, 57–69. [CrossRef]
134. Luo, X.; Wu, Y.; Xiao, X.; Ooi, B.C. Feature inference attack on model predictions in vertical federated learning. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021.
135. Qiu, P.; Zhang, X.; Ji, S.; Du, T.; Pu, Y.; Zhou, J.; Wang, T. Your Labels Are Selling You Out: Relation Leaks in Vertical Federated Learning. *IEEE Trans. Dependable Secur. Comput.* **2022**. [CrossRef]
136. Ha, T.; Dang, T.K. Inference attacks based on GAN in federated learning. *Int. J. Web Inf. Syst.* **2022**. [CrossRef]
137. Rassouli, B.; Varasteh, M.; Gunduz, D. Privacy Against Inference Attacks in Vertical Federated Learning. *arXiv* **2022**, arXiv:2207.11788.
138. Zhang, J.; Zhang, J.; Chen, J.; Yu, S. Gan enhanced membership inference: A passive local attack in federated learning. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020.
139. Xie, Y.; Chen, B.; Zhang, J.; Wu, D. Defending against Membership Inference Attacks in Federated learning via Adversarial Example. In Proceedings of the 2021 17th International Conference on Mobility, Sensing and Networking (MSN), Exeter, UK, 13–15 December 2021.
140. Zhang, Y.; Zhou, H.; Wang, P.; Yang, G. Black-box based limited query membership inference attack. *IEEE Access* **2022**. [CrossRef]
141. Lee, H.; Kim, J.; Ahn, S.; Hussain, R.; Cho, S.; Son, J. Digestive neural networks: A novel defense strategy against inference attacks in federated learning. *Comput. Secur.* **2021**, *109*, 102378. [CrossRef]
142. Rodríguez-Barroso, N.; Jiménez-López, D.; Luzón, M.V.; Herrera, F.; Martínez-Cámara, E. Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges. *Inf. Fusion* **2022**, *90*, 148–173. [CrossRef]
143. Gosselin, R.; Vieu, L.; Loukil, F.; Benoit, A. Privacy and Security in Federated Learning: A Survey. *Appl. Sci.* **2022**, *12*, 9901. [CrossRef]
144. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl. Based Syst.* **2021**, *216*, 106775. [CrossRef]
145. Chen, Y.; Chai, Z.; Cheng, Y.; Rangwala, H. Asynchronous federated learning for sensor data with concept drift. In Proceedings of the 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 15–18 December 2021; pp. 4822–4831.
146. Nawaz, M.S.; Fournier-Viger, P.; Shojaee, A.; Fujita, H. Using artificial intelligence techniques for COVID-19 genome analysis. *Appl. Intell.* **2021**, *51*, 3086–3103. [CrossRef]
147. Boopalan, P.; Ramu, S.P.; Pham, Q.V.; Dev, K.; Maddikunta, P.K.; Gadekallu, T.R.; Huynh-The, T. Fusion of Federated Learning and Industrial Internet of Things: A survey. *Comput. Netw.* **2022**, *212*, 109048. [CrossRef]
148. Ma, X.; Zhu, J.; Lin, Z.; Chen, S.; Qin, Y. A state-of-the-art survey on solving non-IID data in Federated Learning. *Future Gener. Comput. Syst.* **2022**, *135*, 244–258. [CrossRef]
149. Duan, S.; Liu, C.; Cao, Z.; Jin, X.; Han, P. Fed-DR-Filter: Using global data representation to reduce the impact of noisy labels on the performance of federated learning. *Future Gener. Comput. Syst.* **2022**, *137*, 336–348. [CrossRef]
150. Yoo, J.H.; Son, H.M.; Jeong, H.; Jang, E.H.; Kim, A.Y.; Yu, H.Y.; Jeon, H.J.; Chung, T.M. Personalized federated learning with clustering: Non-IID heart rate variability data application. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 20–22 October 2021.