Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.023763
Article

Tech Science Press

Federated Learning for Privacy-Preserved Medical Internet of Things

Navod Neranjan Thilakarathne[1], G. Muneeswari[2], V. Parthasarathy[3], Fawaz Alassery[4], Habib Hamam[5], Rakesh Kumar Mahendran[6] and Muhammad Shafiq[7,*]

[1]Faculty of Technology, University of Colombo, Colombo, Srilanka
[2]School of Computer Science and Engineering, VIT-AP University, Amaravati, India
[3]Department of Computer Science Engineering, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, India
[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
[5]Faculty of Engineering, Moncton University, NB, E1A3E9, Canada
[6]Department of Electronics and Communication Engineering, Vel Tech Multitech Dr. Rangarajan Dr.Sakunthala Engineering College, Chennai, India
[7]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, 38541, Korea
*Corresponding Author: Muhammad Shafiq. Email: shafiq@ynu.ac.kr

Received: 20 September 2021; Accepted: 21 October 2021

Abstract: Healthcare is one of the notable areas where the integration of the Internet of Things (IoT) is highly adopted, also known as the Medical IoT (MIoT). So far, MIoT is revolutionizing healthcare because it provides many advantages for the benefit of patients and healthcare personnel. The use of MIoT is becoming a booming trend, generating a large amount of IoT data, which requires proper analysis to infer meaningful information. This has led to the rise of deploying artificial intelligence (AI) technologies, such as machine learning (ML) and deep learning (DL) algorithms, to learn the meaning of this underlying medical data, where the learning process usually occurs in the cloud or telemedicine servers. Due to the exponential growth of MIoT devices and widely distributed private MIoT data sets, it is becoming a challenge to use centralized learning AI algorithms for such tasks. In this connection, federated learning (FL) is gaining traction as a possible method of learning on devices that do not need to migrate private and sensitive data to a central cloud. The terminal equipment and the central server in FL only share learning model updates to ensure that sensitive data is always kept secret. Even though this has recently become a promising research area, no other research has been conducted on this topic recently. In this paper, we synthesize recent literature and FL improvements to support FL-driven MIoT applications and services in healthcare. The findings of this research help stakeholders in academia and industry to realize the competitive advantage of the most advanced privacy preserved MIoT systems based on federal learning.

Keywords: IoT; deep learning; machine learning; federated learning

1 Introduction

The revolution in the healthcare sector has spawned a large number of MIoT applications, each of which can access large amounts of data and requires extensive analysis [1]. Over the years, MIoT or well known as use of IoT driven technologies in healthcare, has shown great potential in many medical applications, such as disease diagnosis, patient condition monitoring, remote health monitoring, wearable devices, fitness programs, emergency care, elderly care, epidemic management, etc. [2,3]. Day after day, due to various factors such as the recent COVID-19 pandemic [3], the rise of chronic diseases, and the elderly population [2,3], the usage of these MIoT applications has skyrocketed, which has led to the generation and collection of large amounts of medical data. Traditionally, in a typical MIoT setup, all of these patient pathology data, and environmental data are first collected by these MIoT devices, and then sent to the cloud through base stations to train statistical learning models to infer the meaning of data for prediction, which is also known as AI [2,4–8]. However, in the past, simple data transaction models were used. When using these AI methods, one party collects data and transmits the data to the other party, and the other party cleans and fuses the data. Finally, third party will use aggregated data to develop models that can be used by others. Therefore, the problem we face is that our data is isolated like island, and we are prohibited from collecting, fusing and using data in different locations for AI processing. Hence, AI practitioners have huge difficulties in figuring out how to legally solve data fragmentation and isolation problems [8–10].

The exponential growth of MIoT applications has led to the exponential growth of the technology [1,3–5] leading to the creation and accumulation of large amounts of data. The feasibility of clinical research is often hindered by problems in data communication and access especially in terms of privacy issues, owing to the fact that such medical data usually involve personal identifiable information (PII) and sensitive pathological information unique to patients [1,4–7], where it would also violate laws and regulations. For example, the Health Insurance Circulation and Accountability Act (HIPAA) [8]; and the General Data Protection Regulation (GDPR) [1,9] suggest data privacy and protection of PII. According to the latest statistics [3–6,9,10], it is clear that the growing IoT devices will contribute to economic growth worth 5 to 12 trillion US dollars whereas the IoT in healthcare market is expected to reach about 534 billion by 2025, which clearly provides us with a forecast of the amount of data that the entire healthcare ecosystem will generate as the market expands [10–15]. In order to overcome this problem, including the aforementioned data fragmentation and isolation issues, FL allows the use of decentralized optimization methods for privacy protection data analysis, while maintaining data security and decentralization [1,2,10–16]. On the other hand, with the more effective expansion of IoT networks and the increasing privacy issues in typical IoT environments over a long period of time, typical AI technologies that rely on collecting and accumulating all data in one place for further analysis may become endanger the privacy of aggregated data [16–22]. In this case, this kind of FL manifests itself as a collaborative and distributed AI method [22–28] that allows training of decentralized IoT devices without data sharing [28–30], thereby protecting data privacy [8,30–35].

1.1 Contributions and the Significance of Study

FL is used in various activities within the focus of this research (i.e., MIoT) to realize intelligent and universal medical services by enabling DL and ML models without the need to disclose sensitive patient data in between multiple medical institutions. Therefore, medical institutions with medical data do not need to share medical records with each other, so as to better protect the privacy of medical data. The data model is trained locally and uploaded to the aggregation (or central) server for global computations. By doing so, FL has achieved a collaborative medical environment between different hospitals to achieve faster patient diagnosis and treatment while maintaining user privacy [36–42], which has become very popular during the recent COVID-19 pandemic for collaborative learning between multiple medical institutions for drug discovery and disease diagnosis [1,2,8,9,42–44]. We note that FL and its progress have been extensively discussed in the literature. However, there is currently no research that conducts a comprehensive review of FL and the IoT in healthcare. Some research has been done on FL and IoT, but as far as we know, no major efforts have been made on MIoT. The lack of research in this area motivated us to conduct a comprehensive evaluation of FL in MIoT, highlighting the most important aspect of FL which is data privacy, which signifies our work among all other research in this area. In terms of other reviews done on this subject, we were not able to find any related reviews, which proves that, our study is the first of this kind. Hence owing to this significance of our review we believe this would help other researchers towards carrying our further study and research, where it would contribute to the new knowledge in this area and for the betterment of MIoT based healthcare.

Next, we have summarized the key contributions of this paper as follows.

- We have reviewed some of the major opportunities created by FL in the context of MIoT, and analyzed some major issues, difficulties and future prospects.
- We have categorized recent literature, highlighting key features and contributions, so that readers and future researchers can better understand the current status of academic achievements on this topic.
- We have evaluated the possible applications of FL in MIoT in detail, juxtaposed the scope of these applications, and these terms range from basic to recent and future developments.

1.2 Outline of Study

In order to provide a comprehensive review the rest of this study is structured as follows. Section 2 briefly discussed the ubiquitous MIoT environment and FL, and emphasized their key characteristics, laying the foundation for our research. Section 3 investigates in detail the application areas of FL in MIoT and the work related to taxonomy. Section 4 assesses challenges and future directions. Finally this research ends with a conclusion section.

2 MIoT and Federated Learning

2.1 MIoT

The expansion of the IoT has led to more and more connected objects communicating with each other via the Internet, which is supported by machine-to-machine (M2M) communications, including IoT in healthcare. These MIoT devices in the healthcare environment (e.g., smart thermometers, blood pressure monitors, blood glucose monitors, infusion pumps, wearable medical devices, medical imaging devices, fitness trackers, injectable medical sensing devices, hospital monitoring devices, etc.), collect various medical data, and then aggregate these data for further processing to obtain meaningful insights about the patient's condition [1,2,10–15]. In this regard, many AI technologies including DL and ML have been applied to the training of statistical data models to perform intelligent decision-making in order to gain insights from ubiquitous MIoT devices. In most cases, this computation takes place in a remote data center (or cloud) for the purpose of learning and modeling. Even if these AI computation place in the cloud (or remote server), it is often affected by the amount of data, storage, and processing power, which often hinders the proper explosion of data. According to recent research, by 2021, nearly 850 ZB of data will be generated at the edge of the network through various digital things around us [10]. On the other hand, it is estimated that by 2021, the global data center traffic will also reach 20.6 ZB [3–9,10,15]. However, the data to be learned contains highly sensitive pathological information, and the use of a third-party untrusted cloud (or remote server) may lead to privacy risks, such as data leakage and typical information security attacks or network attacks, while being transmitted through the communication medium. Therefore, this lays the foundation for the introduction of a novel and innovative AI learning method to protect the privacy of network edge data, which we will discuss in the next section.

2.2 Federated Learning

Google recommends FL as a solution to the problem of using a central server to train a shared global model from distributed data sets scattered on a large number of clients/devices, while avoiding data leakage [1,2,4,5,8]. Initially, they used FL to train an ML model based on globally distributed mobile phones by protecting user data. In simple terms, FL can be referred to as training statistical data models on contaminated data centers or remote devices while maintaining data localization [5–8]. Due to the continuous increase in the number of IoT devices in recent years, a large amount of data is generated, and due to its ever-increasing extensive computing and processing capabilities, as well as the privacy issues we mentioned earlier, it is recommended to store the data locally and push the computations to the edge of the network with edge computing [6–8]. However, as the storage and processing capabilities of devices in decentralized networks increase over time, it becomes possible to utilize more local resources on each device. This leads to an increase in the demand for FL, which makes it possible to directly investigate statistical models of remote devices. This learning method is completely different from learning in a traditional distributed environment and requires progress in large-scale AI technology, distributed optimization and data privacy [15–20]. According to recent research, almost all major service providers have adopted FL technology [1,6,8,9,11,39]. Examples include using wearable medical devices to predict emergency medical events, such as the risk of a heart attack. Wearable medical devices and other non-medical IoT devices, such as self-driving cars, may have multiple sensors that allow them to acquire, aggregate, react, and adapt to incoming data in real time [33–36]. For example, when predicting the risk of cardiovascular disease, medical equipment may require the latest models of various pathological information to safely operate and predict risks in real time, and building aggregate models in these scenarios may fail due to the privacy of highly sensitive patient medical data concerns and limited connectivity of devices. Therefore, FL technology can be used to train models in these types of situations so that they can quickly respond to changes while respecting user privacy [10–15].

On the other hand, when it comes to medical organizations or hospitals, they can be seen as devices in the FL context, which contain large amounts of data used to predict healthcare. However, due to strict medical regulations and laws (e.g., HIPAA and GDPR [1,4,5,9,10]), various privacy practices, laws and ethical barriers require data to always be on the local site [6,7]. In this case, FL provides significant benefits for such medical institutions because it can reduce the pressure on the medical network while also allowing private and collaborative learning between these institutions. The classic FL problem involves studying a single statistical model from basic data stored on two to millions of online devices distributed globally. The data owner can choose to learn this model. However, due to legal and ethical restrictions, the device is stored and processed locally [15,17,19]. Therefore, the ultimate goal is to minimize the objective functions in [6,8–11] as follows,

$$\min_{w} \quad F(w), \quad \text{where } F(w) := \sum_{k=1}^{m} p_k F_k(w) \tag{1}$$

where m denotes total number of devices or data owners who need to train models. $p_k \geq 0$ and $\sum_k p_k = 1$, and F_k the local objective function for the *k-th* device. $F(w)$ is also defined as the experimental risk over indigenous medical data. $F_k(w) = \frac{1}{n_k}\sum_{jk=1}^{nk} f_{jk}(w; x_{jk},\ y_{jk})$, where n_k is the number of data samples available locally. p_k is a user defied term, which states relative impact on each of the participating device.

Fig. 1 shows the FL-MIoT architecture and the communication process in a typical FL model training process, which includes many client devices. In our case, the MIoT device and the aggregation server are located at the service access point. The general communication process of FL-MIoT includes several steps [9,10,12–15]. In the system initialization and device selection stage, the aggregator selects accurate MIoT tasks (e.g., activity recognition, predicting event probability) and sets learning parameters. These learning parameters include detailed information about the number of communication rounds and learning rates required to achieve an optimized global model. Then in the local model training and update phase, once the server completes the initial configuration, it creates a new model and distributes it to the MIoT clients to start distributed training. Then each client uses its own data set to train the local model, and then minimizes the loss function to calculate the update. Finally, in the model aggregation and download stage, a new global model is generated by collecting all model changes from the local client and solving the optimization problem on the server.

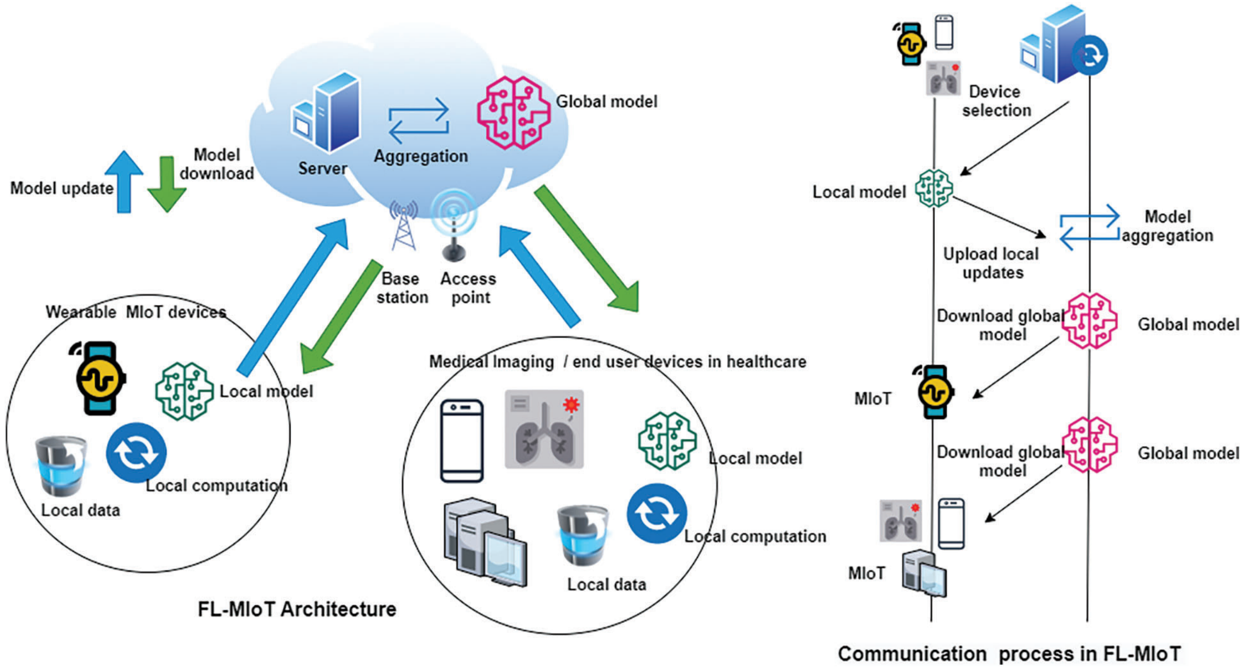

Figure 1: FL–MIoT architecture and communication process

2.3 Classification of FL

We can divide FL into two main categories called data partition and network structure [14,15]. According to the distribution of training data in the sample and feature space, the data partition can be further divided into three different categories: vertical FL (VFL), horizontal FL (HFL), and federated transfer learning (FTL). On the other hand, the network structure can be divided into two categories: decentralized and centralized FL (DFL and CFL). In VFL, it solves the problem of training AI models across client networks on the same sample set with different feature sets. In addition, local data samples are combined to train a shared AI model, which uses a variety of encryption mechanisms to enhance privacy [9,10,15]. In the HFL system, using the local data set from the local client device, which has the same feature space but different sample space, all local client devices train the global FL model. However, due to the shared feature space, client devices can use the same AI model for local model training. Each client then trains on the local data to compute local updates, which can be hidden through encryption or differential privacy (DP). The aggregation server collects all local updates from participating clients, calculates the next global update without accessing local data, and then sends the global update back to the local client for the next round of local training until the target accuracy is reached [15,16]. FTL is an extension of VFL to participate in the learning process with different sample spaces and feature spaces. In this setting, encryption technology can also be used to preserve privacy and ensure security during learning [14–16].

Fig. 2 shows the configuration of HFL, VFL and FTL [1,9–15,17,19,26–30,44–47]. With CFL, the client uses their data set to train the FL model in parallel in a single training cycle, using a central server for coordination [9–15]. After the client transmits the learned parameters to the central server, the server aggregates them using a weighted average method. Therefore, at the end of the training, each customer will have a global model and a personalized model. However, the central server is considered a key element of the CFL network, which is used to propagate model changes to client participants, and to protect the privacy and security of training data. On the other hand, the DFL method contains a network topology that does not require any central server [9–15]. The arrangement of CFL and DFL is shown in Fig. 3. In each communication cycle, customers use their own data sets for local training, just like in a peer-to-peer (P2P) network where all customer participants are linked. In this method, each client uses model aggregation to establish a global update consensus by aggregating model updates obtained from neighboring clients through P2P communication. Due to this arrangement, the decentralized technology is more scalable than the centralized approach and does not require a central server for calculations. In addition, it is obvious that the DFL can be further expanded through P2P-based blockchain technology to further expand the capabilities of the DFL system. By doing so, model changes may be offloaded to the blockchain ledger for secure model aggregation and dissemination [16–20].

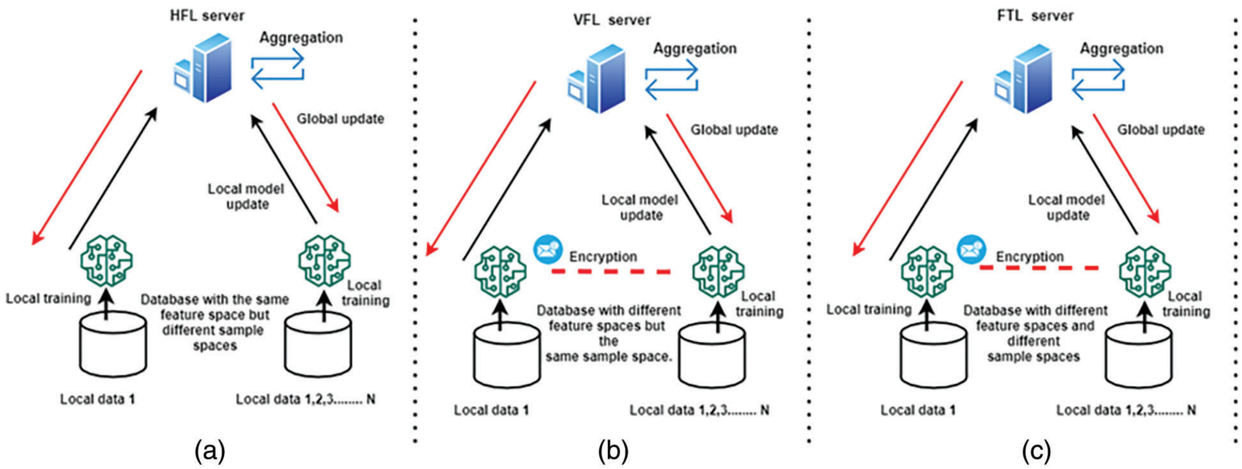

Figure 2: Types of FL models with data partitioning. (a) Horizontal Federated Learning (HFL), (b) Vertical Federated Learning (VFL), (c) Federated Transfer Learning (FTL)

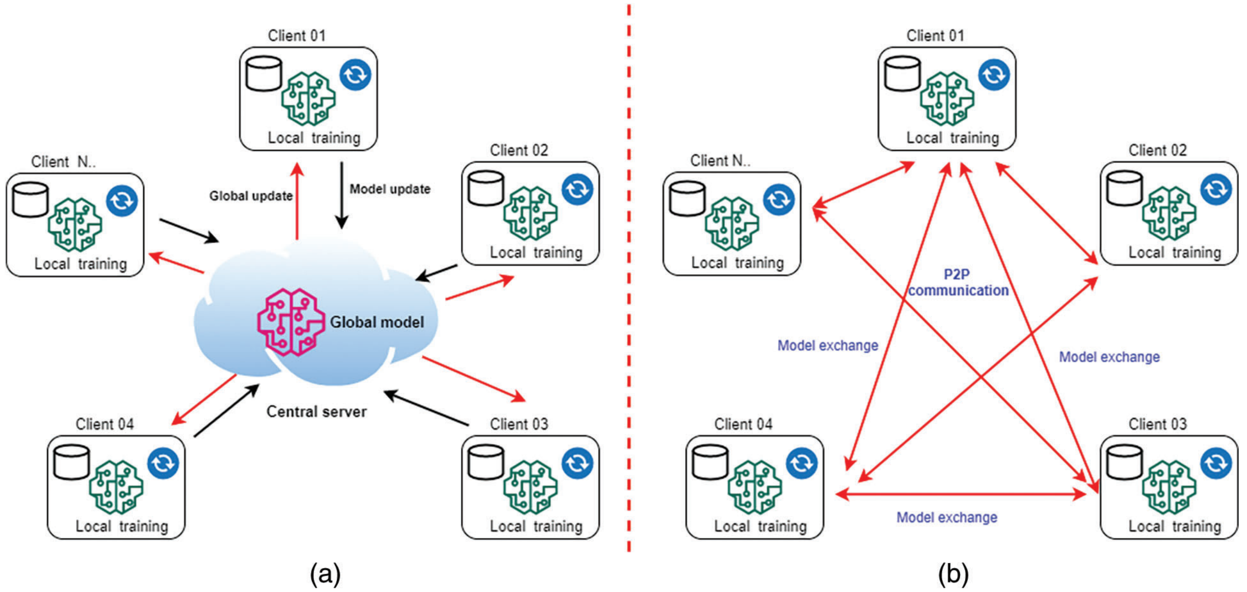

Figure 3: Types of FL models based on the networking structure. (a) Centralized Federated Learning (CFL), (b) Decentralized Federated Learning (DFL)

3 Applications of FL for MIoT and Related Work

In a typical MIoT environment, AI-based applications (such as ML and DL) have been used to learn insights from the underlying medical data for various purposes such as disease diagnosis, medical image analysis, clinical trials, drug discovery, and electronic health records (EHR), etc. A basic problem in this environment is the privacy issues caused by sharing patient data with the cloud or remote data centers to train medical data [10,12,17,19,26,28]. On the other hand, compared with other fields such as smart agriculture or surveillance, the amount of data related to the MIoT system is highly sensitive, as shown in the HIPPA medical regulations [10,15,21]. This means that deleting or omitting metadata such as patient information does not provide sufficient privacy protection, especially in complex healthcare environments. Since traditional AI methods rely on a central server to perform analysis, this is obviously ineffective in this case because data must be exchanged. Therefore, in this case, FL can combine more knowledge and enhanced privacy awareness to provide alternative options. In the next section, we will study FL and its main applications in MIoT, as described in the literature.

3.1 Enables Collaborative Learning

FL is an ML setting in which many partners (hospitals, pharmaceutical companies, or independent researchers) can collaborate to solve challenging research problems (e.g., COVID-19 drug discovery [26,27,30,47–50]) without sharing or centralizing data [9,10,15,20]. This approach allows medical teams to train their models on larger, previously inaccessible data sets, improving the predictive and AI capabilities of ML algorithms, thereby obtaining improved results in a shorter time and overcoming data privacy issues. Some examples include FL-based drug discovery involving multiple pharmaceutical companies through collaborative FL networks [20,23,26,27,30] and clustering of patients, disease diagnosis, and clinical trials to predict mortality and length of hospital stay.

3.2 Analyzing the EHR Data

The collected patient pathology information is usually stored in digital form and in the form of EHR, which is very important for medical investigations, disease diagnosis and identifying the suitable treatment plans [20,21,23,32]. EHRs contain systematic and random biases, which limit the generality of the results, even though they provide a large amount of patient data for the study. FL is a reasonable way for medical institutions to connect to EHR data, allowing them to share their experience instead of their data while maintaining privacy. In these cases, the iterative benefits of learning from large and diverse medical data sets will significantly improve the performance of the underlying FL model.

3.3 Medical Imaging

Another example of the application of FL in the MIoT environment is medical imaging, which is used for tasks such as brain tumor segmentation, diagnosis using computed tomography (CT) and magnetic resonance imaging (MRI) medical scans, in cooperation with multiple medical institutions. The FL for medical imaging can be found in [10,18,19,24–27,30,31,50].

3.4 Related Work

We have outlined the research overview and the recent developments of the FL in IoT field in Tab. 1. In this part, we also present taxonomy of related work, highlighting the main features and contributions. For a better understanding, the underlying use cases and ML/DL types are highlighted. Then we also highlighted the FL client and aggregator in the FL-MIoT network, as shown in Tab. 2.

Table 1: Existing surveys on FL in IoT in general or MIoT

Reference, Year	IoT in general	MIoT specific	Key contributions
[8], 2019	✓		The author introduces a secure FL framework, which includes HFL, VFL, and FTL, and includes an investigation of FL.
[9], 2021	✓		In this research, the author introduces FL's latest developments in FL-driven IoT applications; provides a classification of related work, highlighting open research challenges and solutions.
[11], 2020	✓		The author examined the unique qualities and limitations of FL, conducted a comprehensive review of existing technologies, and identified various future research areas.
[13], 2020		✓	This study explores how FL is used in healthcare to stimulate its services, and the challenges and issues that must be addressed.
[14], 2019	✓		The author described how they used TensorFlow to create the FL system, and the resulting high-level design. Some unresolved issues and their possible solutions are also discussed.
[15], 2021	✓		This article discusses the application of FL in IoT, and explains the integration of FL and IoT with different technologies.
[16], 2020	✓		This article provides an overview of FL and a technical review of FL supporting technologies, protocols, and applications.
[17], 2020		✓	The author studies AI methods for FL-based security, and privacy protection, including potential attack vectors and future prospects, with a focus on medical imaging applications.
[28], 2020		✓	In this article, an overview of patient privacy and distributed FL is discussed as viable options for maintaining medical records and their limitations and potential are discussed.

(Continued)

Table 1 (continued)

Reference, Year	IoT in general	MIoT specific	Key contributions
[36], 2021		✓	This article investigates the key concepts and architectural patterns in FL, and discusses the role of FL in the healthcare sector.
[37], 2020	✓		This article discusses data preservation technology in the IoT from the perspective of FL-based security and privacy.
[38], 2020	✓		This article reviews the use of FL in wireless communications and its responsibilities in 5G applications and edge computing.
[39], 2020	✓		This article discusses the integration of FL in edge networks and draws attention to the challenges associated with implementation.
[40], 2020			This study investigated the impact of FL on privacy. However, it does not consider FL in the IoT systems. Emphasizes data privacy challenges, attacks, and possible solutions.
[41], 2021			This research examines in detail the key ideas, software engineering problems and solutions in FL.
[42], 2019			This study introduced an overview of FL system architecture, ML, privacy aspects and communication architecture.

Table 2: Taxonomy of FL–MIoT applications in healthcare

Reference, Year	Use case	Type	FL Client	FL Aggregator	Key Contributions
[1], 2020	Disease diagnosis	DNN	MIoT devices	Central server	Introduced a new MIoT FL framework to reduce communication overhead.
[10], 2020	Medical imaging	CNN	Hospitals	Central server	The author proposes an FL framework for analyzing multi-center brain image data.
[18], 2019	Medical imaging	DNN	MIoT devices	Central server	In this article, the author investigated the feasibility of using the DP method to protect patient data in FL settings for brain tumor segmentation.
[19], 2020	Medical imaging	–	Hospitals	Central server	An FL method for medical image analysis using decentralized iterative optimization randomization is introduced.
[21], 2019	EHR	–	Hospitals	Central server	The authors proposed a decentralized FL framework to manage EHR data.
[23], 2021	EHR	LR	Hospitals	Central aggregation server	FL is used to aggregate local clinical data from multiple institutions and predict the survival rate of COVID-19 patients.
[24], 2019	Medical imaging	–	Hospitals	Central server	The author proposes an FL framework that allows secure access and meta-analysis of biological data.

(Continued)

Table 2 (continued)

Reference, Year	Use case	Type	FL Client	FL Aggregator	Key Contributions
[25], 2020	Medical imaging	–	Hospitals	Federated Server	The authors introduce FL-based medical image classification.
[26] /2021	Medical imaging	CNN	Hospitals	Central server	FL technology is used to identify CT scan abnormalities related to COVID-19.
[27], 2020	Medical imaging	DNN	Hospitals	Central server	FL is used for COVID-19 data training and testing to evaluate efficacy.
[30], 2021	Medical imaging	–	MIoT devices	Central server	The author uses Keras and TensorFlow to jointly develop a ML model to evaluate X-ray images of COVID-19 patients.
[31], 2021	Medical imaging	CNN	Medical institutions	Central server	The concept of cluster FL (CFL) is used for automatic diagnosis of COVID-19.
[32], 2019	EHR	SVM and LR	Hospitals	Central server	The author proposed an FL framework for learning a global model using distributed health data stored locally.
[43] / 2021	Medical imaging	CNN	Medical institutions	Medical institutions	An FL structure for COVID-19 medical image classification is proposed.
[44], 2019	Medical institutions	CNN	Data centers	Medical data centers	A P2P network composed of medical institutions is proposed in FL technology.
[45], 2019	Medical institutions		Data workers	Data workers	The authors proposed a DFL integrated with blockchain for healthcare.
[46], 2020	Medical institutions	CNN	Medical institutions	Central cloud server	Using FL, a system for joint activity recognition is proposed.
[47], 2020	Medical institutions	CNN	MIoT devices	Cloud server	FL technology in healthcare paradigm based on the cloud edge is proposed.
[48], 2020	HER	–	EHR data owners	Data center	The authors introduced the secure FL framework for EHR management.
[49], 2019	EHR	SVM	Medical institutions	Data center	The author proposes an FL for distributed EHR drug response prediction.
[50], 2018	EHR	SVM	Medical users	Data center	A distributed binary classification based on FL and ML for healthcare is proposed.

We noticed that the main use cases of FL technology in MIoT are EHR data analysis, medical imaging, drug discovery, disease diagnosis, and collaborative learning between medical institutions where most of the research was published after 2019, signifying the novelty of the subject. In order to obtain better performance and enhanced privacy in FL technology, various FL applications and encryption schemes have been used. These encryption mechanisms are also integrated with the blockchain to increase privacy protection to improve FL model delivery and communication privacy. In addition, up to now, in the collaborative learning between medical institutions, FL has many applications for drug discovery and various applications in learning COVID-19 [1–3] (see Tab. 2). As owing to the novelty of the subject, a few research works have been done (see Tab. 1), which also signify the importance of our review.

4 Challenges and Future Directions

4.1 Challenges

FL technology faces multiple issues including data security and privacy to prevent data leakage and comply with privacy protection laws and regulations such as GDPR and HIPPA. This technology also needs to improve the communication efficiency between client participants and the central server [10,11,14–20]. Therefore, when deploying an optimized FL model, all these constraints must be resolved. In addition, a suitable FL solution in the real world will be hindered by many challenges, such as learning privacy, communication overhead, system heterogeneity, statistical heterogeneity, and regulatory compliance, as described below.

4.1.1 Privacy

Privacy is considered to be a major issue for FL because it is believed that online data sharing will endanger the privacy of sensitive medical data [1,2]. In a typical FL scenario, privacy can be classified into two aspects: global and local privacy. The model changes made at each round must be secret to all untrusted third parties other than the central server in order to maintain global privacy whereas local privacy necessitates that the changes be kept hidden from the server as well. FL protects the data created on each device by only exchanging model updates instead of original data (such as gradient information) [9,11]. This is because sending model updates during the training process may leak highly sensitive medical information to a central server or a third party. In this regard, there are existing methods that use technologies such as Secure Multi-Party Computing (SMC) or DP to improve FL privacy. However, these methods usually sacrifice model performance in the process. Therefore, this trade-off is interesting and considered to be the main difficulty in implementing privacy preserving FL systems in healthcare. In this case, SMC is very suitable for the FL situation, that is, each client uses a combination of encryption and unintentional transmission to jointly calculate its private data. For example, a public key encryption method using homomorphic encryption, in which any party can use a known public key to encrypt its data, and then perform calculations on the data encrypted by others using the same public key. SMC cannot prevent an opponent from knowing certain personal information, even if it ensures that neither party will exchange any information with each other or with any third party. On the other hand, DP is a unique theoretical method to protect personal data privacy, which has been widely used in various industries such as SVM, boosting and DL research. It ensures that the addition or deletion of variables has no substantial impact on the results of any research, and is therefore widely used in FL research to avoid indirect leakage. However, DP can only protect the client from data leakage to a limited extent, and it may damage the accuracy of prediction to a certain extent, which will be a disadvantage [10–15]. Furthermore, new approaches for introducing a reduced form of local privacy by reducing the strength of possible adversaries are being developed for circumstances where robust privacy assurance is required. This method provides higher model performance than tight local privacy and provides greater privacy assurances than global privacy. Nonetheless, differential privacy may be used in conjunction with model compression techniques to minimize communication costs while preserving privacy.

4.1.2 Communication Overhead

In the FL network, communication is a major issue, which is also related to the privacy issues of transmitting raw data and bulk data. Since there are millions of devices in a typical FL network, network communication is usually slower than local computations performed on local devices, which will become a bottleneck. Therefore, efficient communication technology must be developed as part of the training process to iteratively transmit smaller messages or model updates instead of sending the entire data set over the network. When reducing the amount of communication in each setting, two factors can be considered; reducing the number of communication rounds, and reducing the number of messages communicated in each communication round [10,11].

4.1.3 Systems Heterogeneity

Each device in the federated network may have different processing capacity, storage and communication capabilities due to the heterogeneity of hardware (e.g., different storage capacity, memory capacity), network connection (e.g., 3G, 4G, or 5G), and power (battery power). This heterogeneity usually prevents maximum efficiency when implementing FL. On the other hand, it is important that most IoT devices, including MIoT, are heterogeneous by default, because the ecosystem does not have universal standards. However, device-related restrictions can often prevent the device from being active at all times such as energy restrictions, network connection issues. Therefore, in the FL network, when communicating with the central server, the client device may suddenly exit the network. In turn, this could affect the performance of the model. Therefore, the heterogeneous nature of equipment greatly exacerbates the problems of laggard mitigation and fault tolerance. FL technology expects low-level clients to be able to accept heterogeneous hardware and be resilient to network device failures [5–10].

4.1.4 Statistical Heterogeneity

Devices often create and collect data in different distributed ways over the network. In addition, the number of data points on different devices may vary greatly. In addition, there may be an underlying structure that represents the interaction between the device and its related distribution. This data production paradigm violates the assumption of independent and identical distribution widely held in distributed optimization, increases the risk of laggards, and may increase the complexity of modeling, analysis, and evaluation [10,11]. Although a typical FL attempts to train a single global model, there are other possibilities, such as using a multi-task learning framework to learn multiple local models at the same time. In this sense, there is also a strong connection between leading FL and meta-learning.

4.2 Future Directions

FL is currently an active and ongoing research field. In recent times this has gained higher attention for its potential to offer privacy-preserving distributed learning solutions between medical organizations incorporating various technologies like blockchain and encryption mechanisms to improve the privacy of data and enable complex learning from heterogeneous data. In this regard, our main focus is to outline here the key research directions that we can see in the FL of MIoT in the future.

4.2.1 Advancement of Privacy Preserving Solutions

The privacy of the FL network includes the local and global privacy levels of all devices in the network (including the aggregation server). However, when it comes to the overall privacy of the entire federal network, we may also need to consider privacy in a more granular way at the device level. Obviously, recent research focuses on developing methods to deal with hybrid privacy (device or sample specific) based on current methods, focusing on each device level to improve security [12,17,44,47,49]. The blockchain can be integrated with FL to provide better protection for the sensitive data of distributed learning, because all transaction details can be stored in the blockchain in the network ledger.

4.2.2 Complex Learning

In a typical MIoT environment, data may come from various sources and may not be tagged due to its complexity. Therefore, future research will focus more on performing exploratory data analysis or performing more complex and supplicated learning tasks, such as reinforcement learning. This will also provide solutions for the scalability, privacy, and heterogeneity of performing complex learning [50].

4.2.3 Heterogeneity Diagnostics

Recent studies have used indicators such as local differences and bulldozers to quantify statistical heterogeneity. However, due to the heterogeneous nature of federated networks, these metrics cannot be easily estimated before training. This is currently an unresolved topic; we expect this to be resolved through future research [10,15].

4.2.4 Data Quality

FL has the ability to connect all isolated medical institutions so that they can exchange experiences while maintaining anonymity and maintaining the best level of privacy. On the other hand, most healthcare systems suffer from inefficiency and data overload. There is no universal data standard, so the quality of data obtained from multiple sources varies. In addition, if unclean data is used as a sample, the evaluation results seem to be worthless. Therefore, understanding how to clean, correct and improve medical data is essential for the quality development of FL models [9,10,15,20].

4.2.5 Incentive Mechanisms

Due to the IoT and various third-party websites, more and more smartphone healthcare applications are compatible with wearable devices. In addition, the data collected in hospitals or medical institutions, these wearable devices provide another kind of data that is very important to researchers and their users. On the other hand, in the process of joint model training, the client will experience a lot of communication and computational overhead. If there are no well-designed incentive measures, this will hinder participation in FL tasks [50]. Therefore, another key issue may arise, that is, to develop an effective incentive system to encourage devices with good data to participate in FL [9,10,15,20].

4.2.6 Personalization

Based on the recent studies [9,10,15,20]; it is evident that as of now there isn't much focus on how to customize FL models to better meet industry demands. As a result, being able to customize FL models will result in improved design and overall applicability, which would gain more attention in future.

5 Conclusion

In this study, we analyzed FL in MIoT, which is a novel learning paradigm that can provide additional privacy for learning data compared with traditional AI methods. In addition, the data privacy and protection law does not allow stakeholders to directly access personally identifiable data in order to serve the mutual research and development of common issues between the medical academia and industry (such as COVID-19). However, FL allows multiple stakeholders to learn from sensitive medical data and create a collaborative learning environment to ensure the privacy of the underlying data. This is completely different from typical AI learning where data is organized in a central location. Therefore, this FL paradigm will soon be applied to all aspects of IoT-based healthcare, for disease diagnosis, clinical trials, drug discovery, etc., to learn from data and elevate IoT-based healthcare to a new level. We have discussed the unique characteristics of FL and the accompanying issues in MIoT, because the use of FL in healthcare is growing rapidly due to recent demand. We have conducted a comprehensive review of the taxonomy that provides highlights of the related works, their key contributions and unique features. We have found some outstanding issues worthy of further investigation and future research. It would be beneficial for academia and industry to work together to solve these challenges. Therefore, as this is the first review in this area up to the best of our knowledge, we believe that, this research will provide a useful reference for FL in the MIoT discipline and carrying out future research in this area.

Acknowledgement: We deeply acknowledge Taif University for supporting this study through Taif University Researchers Supporting Project Number (TURSP-2020/150), Taif University, Taif, Saudi Arabia.

Funding Statement: This work was supported by Taif University (in Taif, Saudi Arabia) through the Researchers Supporting Project Number (TURSP-2020/150).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Yuan, S. Ge and W. Xing, "A federated learning framework for healthcare IoT devices," *arXiv preprint arXiv: 2005.05083*, 2020.

[2] N. N. Thilakarathne, M. K. Kagita and T. R. Gadekallu, "The role of the Internet of Things in health care: A systematic and comprehensive study," *International Journal of Engineering and Management Research (IJEMR)*, vol. 10, no. 4, pp. 145–159, 2020.

[3] N. N. Thilakarathne, "Review on the use of ICT driven solutions towards managing global pandemics," *Journal of ICT Research & Applications*, vol. 14, no. 3, pp. 207–224, 2021.

[4] The purpose of big data in digital health and IoT, *Biotaware,* 2021. [Online]. Available: https://www.biotaware.com/blog/purpose-big-data-digital-health-and-iot/.

[5] IoT in Healthcare: Benefits, challenges, and use cases, 2021. [Online]. Available: http://www.aimprosoft.com/blog/iot-in-healthcare-benefits-challenges-cases/.

[6] How to improve healthcare systems with IoT and big data, *Technology Consulting,* 2016. [Online]. Available: https://www.kelltontech.com/kellton-tech-blog/how-improve-healthcare-systems-iot-and-big-data.

[7] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," *Healthcare Informatics Research*, vol. 22, no. 3, pp. 156–163, 2016.

[8] Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[9] L. U. Khan, W. Saad, Z. Han, E. Hossain and C. H. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[10] S. Silva, A. Altmann, B. Gutman and M. Lorenzi, "A general open-source frontend framework for federated learning in healthcare," in *Proc. Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning*, Lima, Peru, pp. 201–210, 2020.

[11] T. Li, A. K. Sahu, A. Talwalkar and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[12] M. Ammad-Ud-Din, E. Ivannikova, S. A. Khan, W. Oyomno, Q. Fu *et al.,* "Federated collaborative filtering for privacy-preserving personalized recommendation system," *arXiv preprint arXiv: 1901.09888*, 2020.

[13] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth *et al.,* "The future of digital health with federated learning," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–7, 2020.

[14] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman *et al.,* "Towards federated learning at scale: System design," *arXiv preprint arXiv: 1902.01046*, 2019.

[15] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li *et al.,* "Federated learning for Internet of Things: A comprehensive survey," *arXiv preprint arXiv: 2104.07914*, 2021.

[16] M. Aledhari, R. Razzak, R. M. Parizi and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020.

[17] G. A. Kaissis, M. R. Makowski, D. Rockers and R. F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence*, vol. 2, no. 6, pp. 305–311, 2020.

[18] W. Li, F. Milletarì, D. Xu, N. Rieke, J. Hancox *et al.,* "Privacy-preserving federated brain tumor segmentation," in *Proc. Int. Workshop on Machine Learning in Medical Imaging*, Shenzhen, China, pp. 133–141, 2019.

[19] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola *et al.,* "Ventola multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," *Medical Image Analysis*, vol. 65, pp. 101765, 2020.

[20] Q. Li, B. He and D. Song, "Model-contrastive federated learning," in *Proc. of the IEEE/CVF Conf. on Computer Vision and Pattern Recognition*, Nashville, USA, pp. 10713–10722, 2021.

[21] S. Lu, Y. Zhang, Y. Wang and C. Mack, "Learn electronic health records by fully decentralized federated learning," *arXiv preprint arXiv: 1912.01792*, 2019.

[22] D. Li and J. Wang, "FedMD: Heterogenous federated learning via model distillation," *arXiv preprint arXiv: 1910.03581*, 2019.

[23] A. Vaid, S. K. Jaladanki, J. Xu, S. Teng, A. Kumar *et al.,* "Federated learning of electronic health records to improve mortality prediction in hospitalized patients with COVID-19: Machine learning approach," *JMIR Medical Informatics*, vol. 9, no. 1, pp. e24207, 2021.

[24] S. Silva, B. A. Gutman, E. Romero, P. M. Thompson, A. Altmann *et al.,* "Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data," in *Proc. IEEE Int. Sym. on Biomedical Imaging*, Venice, Italy, pp. 270–274, 2019.

[25] H. R. Roth, K. Chang, P. Singh, N. Neumark and W. Li, "Federated learning for breast density classification: A real-world implementation," in *Proc. Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning*, Lima, Peru, pp. 181–191, 2020.

[26] Q. Dou, T. Y. So, M. Jiang, Q. Liu, V. Vardhanabhuti *et al.,* "Federated deep learning for detecting COVID-19 lung abnormalities in CT: A privacy-preserving multinational validation study," *NPJ Digital Medicine*, vol. 4, no. 1, pp. 1–11, 2021.

[27] B. Liu, B. Yan, Y. Zhou, Y. Yang and Y. Zhang, "Experiments of federated learning for COVID-19 chest x-ray images," *arXiv preprint arXiv: 2007.05592*, 2020.

[28] F. Zerka, S. Barakat, S. Walsh, M. Bogowicz, R. T. H. Leijenaar *et al.,* "Systematic review of privacy-preserving distributed machine learning from federated databases in health care," *JCO Clinical Cancer Informatics*, vol. 4, no. 4, pp. 184–200, 2020.

[29] A. Ulhaq and O. Burmeister, "COVID-19 imaging data privacy by federated learning design: A theoretical framework," *arXiv preprint arXiv: 2010.06177*, 2020.

[30] M. Abdul Salam, S. Taha and M. Ramadan, "COVID-19 detection using federated machine learning," *PloS One*, vol. 16, no. 6, pp. e0252573, 2021.

[31] A. Qayyum, K. Ahmad, M. A. Ahsan, A. Al-Fuqaha and J. Qadir, "Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge," *arXiv preprint arXiv: 2101.07511*, 2021.

[32] O. Choudhury, A. Gkoulalas-Divanis, T. Salinities, I. Sylla, Y. Park *et al.,* "Differential privacy-enabled federated learning for sensitive health data," *arXiv preprint arXiv: 1910.02578*, 2019.

[33] R. K. Mahendran and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of medical things," *Computer Communications*, vol. 153, no. 1, pp. 545–552, 2020.

[34] R. K. Mahendran, P. Velusamy, R. Parthasarathy, J. Shanmugapriyan, P. Pandian *et al.,* "An efficient priority-based convolutional auto-encoder approach for electrocardiogram signal compression in Internet of Things based healthcare system," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. e4115, 2021.

[35] N. N. Thilakarathne and D. Wickramaaarachchi, "Improved hierarchical role based access control model for cloud computing," *arXiv preprint arXiv: 2011.07764*, 2020.

[36] J. Xu, B. S. Glicksberg, C. Su, P. Walker and J. Bian, "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021.

[37] C. Briggs, Z. Fan and P. Andras, "A review of privacy preserving federated learning for private IoT analytics," *arXiv preprint arXiv: 2004.11794*, 2004.

[38] S. Niknam, H. S. Dhillon and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

[39] W. Y. B. Lim, N. C. Luong, D. T. Hoang and Y. Jiao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[40] Z. Li, V. Sharma and S. P. Mohanty, "Preserving data privacy via federated learning: Challenges and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 3, pp. 8–16, 2020.

[41] S. K. Lo, Q. Lu, C. Wang, H. Y. Paik and L. Zhu, "A systematic literature review on federated machine learning: From a software engineering perspective," *ACM Computing Surveys*, vol. 54, no. 5, pp. 1–39, 2021.

[42] Q. Li, Z. Wen and B. He, "Federated learning systems: Vision, hype and reality for data privacy and protection," 2019. [Online]. Available: https://openreview.net/forum?id=KJyL1YRGhnw.

[43] R. Kumar, A. A. Khan, J. Kumar, A. Zakria, I. Ali *et al.,* "Blockchain-federated-learning and deep learning models for covid-19 detection using CT imaging," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 16301–16314, 2021.

[44] A. G. Roy, S. Siddiqui, S. Pölsterl, N. Navab and C. Wachinger, "Brain torrent: A peer-to-peer environment for decentralized federated learning," *arXiv preprint arXiv: 1905.06731*, 2019.

[45] J. Passerat-Palmbach, T. Farnan, R. Miller, S. Gross, H. L. Flannery *et al.,* "A blockchain-orchestrated federated learning architecture for healthcare consortia," *arXiv preprint arXiv: 1910.12603*, 2019.

[46] Y. Chen, X. Qin, J. Wang, C. Yu and W. Gao, "FedHealth: A federated transfer learning framework for wearable healthcare," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 83–93, 2020.

[47] Q. Wu, K. He and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 35–44, 2020.

[48] H. Chen, H. Li, G. Xu, Y. Zhang, X. Luo *et al.,* "Achieving privacy-preserving federated learning with irrelevant updates over e-health applications," in *Proc. IEEE Int. Conf. on Communications*, Ireland, pp. 1–6, 2020.

[49] O. Choudhury, Y. Park, T. Salinities, A. Gkoulalas-Divanis, I. Sylla *et al.,* "Predicting adverse drug reactions on distributed health data using federated learning," in *Proc. Annual Sym.*, vol. 2019, Washington, DC, USA, pp. 313, 2019.

[50] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, W. Shi *et al.,* "Federated learning of predictive models from federated electronic health records," *International Journal of Medical Informatics*, vol. 112, no. 3–4, pp. 59–67, 2018.