IEEE Open Journal of the
Computer Society

Received 16 August 2022; accepted 8 September 2022. Date of publication 14 September 2022;
date of current version 30 September 2022. The review of this paper was arranged by Associate Editor Peng Li.

Digital Object Identifier 10.1109/OJCS.2022.3206407

Collaborative Federated Learning for Healthcare: Multi-Modal COVID-19 Diagnosis at the Edge

ADNAN QAYYUM [1], KASHIF AHMAD [2] (Senior Member, IEEE), MUHAMMAD AHTAZAZ AHSAN [1],
ALA AL-FUQAHA [3], AND JUNAID QADIR [4] (Senior Member, IEEE)

[1] Information Technology University, Lahore 54000, Pakistan
[2] Department of Computer Science, Munster Technological University, T12 P928 Cork, Ireland
[3] Information and Computing Technology Division, College of Science and Engineering (CSE), Hamad Bin Khalifa University, Doha 2713, Qatar
[4] Department of Computer Science and Engineering, College of Engineering, Qatar University, Doha 2713, Qatar

CORRESPONDING AUTHOR: JUNAID QADIR (e-mail: jqadir@qu.edu.qa)

This work was supported by NPRP under Grant 13S-0206-200273, through the Qatar National Research Fund (a Member of Qatar Foundation).

ABSTRACT Despite significant improvements over the last few years, cloud-based healthcare applications continue to suffer from poor adoption due to their limitations in meeting stringent security, privacy, and quality of service requirements (such as low latency). The edge computing trend, along with techniques for distributed machine learning such as federated learning, has gained popularity as a viable solution in such settings. In this paper, we leverage the capabilities of edge computing in medicine by evaluating the potential of intelligent processing of clinical data at the edge. We utilized the emerging concept of clustered federated learning (CFL) for an automatic COVID-19 diagnosis. We evaluate the performance of the proposed framework under different experimental setups on two benchmark datasets. Promising results are obtained on both datasets resulting in comparable results against the central baseline where the specialized models (i.e., each on a specific image modality) are trained with central data, and improvements of 16% and 11% in overall F1-Scores have been achieved over the trained model trained (using multi-modal COVID-19 data) in the CFL setup on X-ray and Ultrasound datasets, respectively. We also discussed the associated challenges, technologies, and techniques available for deploying ML at the edge in such privacy and delay-sensitive applications.

INDEX TERMS Distributed computing, machine learning, smart healthcare.

I. INTRODUCTION

Over the past few years, there has been an increasing interest in deploying machine learning (ML) algorithms on edge devices to reduce data exchange between edge devices and centralized servers [1]. This enables consumers and corporations to enjoy and explore new opportunities in different application domains, such as automotive, security, surveillance, and healthcare [2]. The potential of edge-enabled ML is particularly useful for healthcare settings where protecting patients' privacy and ensuring other constraints like ethical data use are profoundly important [3]. Moreover, edge computing can enable unprecedented health services, e.g., remote healthcare delivery. In general, healthcare centers in remote areas lack advanced medical equipment and other healthcare facilities, resulting in poorer access to health services for the people living there. Therefore, edge-based intelligent data processing capabilities can significantly augment the capacity and efficacy of healthcare while ensuring the privacy of the data.

A typical IoT environment for smart healthcare is illustrated in Fig. 1 in which data collected by different sensors is processed at the edge for different applications using ML techniques. Once the ML predicts an event, the edge devices trigger an action or request service in the cloud. ML algorithms can also be executed concurrently in the cloud as well as at the edge as shown in the figure. However, with local data

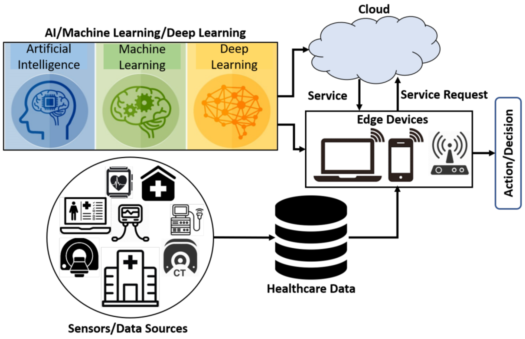


FIG. 1. An illustration of AI/ML at edge in an IoT empowered healthcare environment.

storage and processing resources (through cloud computing), such applications enjoy a significant improvement in terms of processing time by avoiding networking congestion. More importantly, real-time processing at the edge improves the performance of delay-sensitive applications, such as healthcare by avoiding any potential latency or delay occurred during data transmission between end devices and the cloud. In addition, ML at the edge results in increased security and privacy as sending data back and forth from the cloud may lead to security threats.

In this paper, we leverage the capabilities of edge computing in medicine by analyzing and evaluating the potential of intelligent processing of clinical visual data related to COVID-19 at the edge allowing the remote healthcare centers to benefit from the multi-modal collaborative learning paradigm without sharing any information about the modality of the local data and the data itself. A number of recent research efforts have focused on diagnosing COVID-19 using AI and data science methods [4]; relatively little work has however focused on using edge AI for COVID-19 diagnosis.

To this aim, we utilize an emerging concept of clustered federated learning (CFL) and propose a CFL-based collaborative learning framework for an automatic multi-modal COVID-19 diagnosis. Our approach is well suited to the task of COVID-19 diagnosis as visual data (i.e., CT scans, X-rays, and ultrasound) is collected at different centers and could be used to build a joint/shared ML model in a cloud-edge infrastructure being able to diagnose COVID-19 in both X-ray and Ultrasound images (without the requirement of sharing data with a cloud or a central entity). The proposed framework is evaluated on two benchmark datasets under different experimental setups and we have achieved encouraging results using CFL that are comparable with the baseline results (when the model is trained with central data). We also discuss in detail the potential applications, associated challenges, technologies, tools, and techniques available for deploying ML at the edge in such privacy and delay-sensitive applications. *We note that we use the term multi-modal model to represent a single model capable of diagnosing COVID-19 in both X-ray and Ultrasound imagery when provided separately.*

The main contributions of the paper are as follows:

1) To highlight the potential of intelligent processing of clinical data at the edge, we propose a collaborative learning framework for COVID-19 diagnosis by leveraging a CFL approach enabling remote healthcare centers to benefit from each other's data without sharing the data itself and associated information.
2) We also demonstrate how the performance of conventional FL is affected by the divergence of the distribution of data from different sources (i.e., X-ray and Ultrasound imagery), and how CFL can help to mitigate the adverse impact.
3) We also highlight the potential challenges and enabling factors that enable the deployment of ML/DL models to the edge.
4) Finally, we elaborate on the open research issues related to deploying ML at the edge for healthcare applications that require further investigation.

Organization of the paper: The rest of the paper is organized as follows. Section II provides a broad discussion of the related work on automated COVID-19 diagnosis as well as the different challenges encountered in deploying ML on the edge along with a discussion on enabling technologies. The case study on collaborative learning for multi-modal diagnosis of COVID-19 is presented in Section III and results are presented in Section IV. A discussion on the advantages and limitations of our proposed CFL framework for multi-modal COVID-19 diagnosis is provided in Section V. Various open research issues that require further investigation are presented in Section VI. Finally, we conclude in Section VII.

II. BACKGROUND

A. EXISTING AUTOMATED COVID-19 DIAGNOSIS WORK

COVID-19 has been a strong focus of the research community in 2020, especially after it was declared in March by the World Health Organization (WHO) to be a pandemic, with diverse efforts focusing on diagnosis [5], treatment [6], and the development of the potential vaccine [7]. Data science methods—particularly, ML and data visualization techniques—are playing a major role in the international response against the COVID-19 pandemic with some key applications being risk assessment, contact tracking, fake news detection, sentiment analysis, and screening and diagnosis [4]. The focus of this paper is on automated screening and diagnosis; we shall discuss next some of the prominent related techniques relying on different types of information (e.g., audio and visual data) that have been proposed.

A number of efforts have focused on automated image analysis in a bid to speed up the COVID-19 diagnosis process [8]. To this aim, three different medical imaging modalities, namely computerized tomography (CT), Ultrasound scans, and X-radiation (X-ray), have been mostly exploited. To facilitate research on image-based solutions for COVID-19 diagnosis, several datasets have been collected and made publicly available [8], [9]. For instance, Maghdid et al. [9] collected a comprehensive dataset containing a total of 170

X-rays and 361 CT scan images from different sources. Cohen et al. [10] also provide a collection of X-rays and CT scans of confirmed COVID-19 patients. A collection of COVID-19 patients' CT scans has also been made publicly available for research purposes in [11], [12]. Born et al. [13], [14], on the other hand, provide a lung ultrasound (POCUS) dataset that contains samples for three classes, i.e., COVID-19, pneumonia, and healthy/normal.

A vast majority of the image-based solutions for COVID-19 diagnosis relies on CT scan images. For instance, Wan et al. [15] proposed a deep learning model for extracting COVID-19's specific features/textures in CT scans of confirmed cases to extract useful clinical insight before the pathogenic tests. An evaluation of a reasonable amount of confirmed cases showed encouraging results with an average test accuracy of 73.1%. Butt et al. [16] proposed a two-phase solution for COVID-19 diagnosis in CT scans. Initially, a pre-trained 3D Convolutional Neural Network (CNN) is employed to extract potential infectious regions in CT scans followed by a CNN-based classification framework to classify the candidate regions into COVID-19, influenza, and non-infectious regions. Li et al. [17] also proposed a 3D CNN-based framework to extract both local and global deep features for diagnosis COVID-19 in CT scans. One of the key challenges to CNN-based solution is the unavailability of a large-scale CT scans datasets. In order to deal with the challenge, Afshar et al. [18] proposed a Capsule Networks based deep learning framework, namely COVID-CAPS, for COVID-19 diagnosis in X-ray images. Moreover, to further enhance the capabilities of the proposed model, the authors used an external dataset composed of 94, 323 frontal view chest X-ray images for pre-training and transfer learning purposes.

There are also methods relying on X-ray images for COVID-19 diagnosis. For instance, in [19] a pre-trained deep model is fine-tuned on X-ray images for COVID-19 diagnosis. Similarly, Sethy et al. [20] trained a Support Vector Machine (SVM) classifier on features extracted via ResNet-50 [21] from X-ray images for classification of COVID-19 and non-COVID-19 cases. Ali et al. [22] evaluated the performance of several existing deep models in diagnosing COVID-19 in X-ray images. Islam et al. [23] on the other hand proposed a deep framework combining CNNs and Recurrent Neural Networks (RNNs) for diagnosis of COVID-19 in X-ray images. Initially, features are extracted with a CNN, which are then feed into a Long short-term memory (LSTM) for diagnosis/detection purposes. Kassani et al. [24] provide a detailed evaluation of several existing deep models and classification algorithms to find a best combination for COVID-19 diagnosis in both X-ray and CT scans. However, both modalities are treated individually. The deep models are used for feature extraction, which is then fed into different classification algorithms.

Some image-based COVID-19 diagnosis methods also rely on a recently introduced concept of Federated Learning (FL) to ensure data privacy in a collaborative learning environment, where several hospitals can participate in training a global ML model. For instance, in [25] a deep model is collaboratively trained in a federated learning environment on CT scans collected from different sources. Kumar et al. [26] on the other hand proposed a blockchain-FL-based framework for collecting data (CT scans) from different hospitals, and collaboratively training a global deep model. Moreover, several exiting deep models have also been evaluated in the proposed federated learning framework. In [27], a federated learning technique is employed for training a global model on electronic health records from various hospitals to predict mortality within seven days in hospitalized COVID-19 patients.

Recent works in diagnosing COVID-19 either use a single modality, i.e., only X-ray images or only CT images. To the best of our knowledge, there is no work done that use multiple data modalities to learn the COVID-19 features. As described above, most of the work uses traditional ML techniques like using CNNs to extract the features from CNNs. Moreover, some image-based FL techniques have been developed but they also use a single data modality. Also, there are several challenges in deploying ML at the edge that include privacy and security of the data, data heterogeneity, presence of adversaries, non-availability of large training data at different edge devices, and communication overheads that make it difficult to learn a joint model with good performance. A few major such challenges are described next.

B. CHALLENGES IN DEPLOYING ML AT THE EDGE

1) RESOURCE SCARCITY AND HETEROGENEITY

Heterogeneous edge devices with varying computational, storage and communication resources are a major bottleneck for the deployment of ML on the edge. ML algorithms in general and deep learning (DL) in particular require a large amount of computational and processing resources making the deployment of ML impractical in several edge computing applications. DL models are usually large and are computationally expensive, as both the training of a deep model and its inferences are typically performed on power-hungry GPUs and servers while, the edge devices are designed to be operated at low power and usually have frugal memory, therefore, deploying DL models on the edge devices is very challenging. One another important challenge is the availability of a power source at edge device, i.e., a battery with long power backup is always desirable in a typical edge computing network. In addition, the size of the network and systems constraints is also a major challenge that can result in only a few devices being active at a time [28].

2) NETWORK COMMUNICATION

The heterogeneity of the computational and communication resources also led to slow and unstable communication. In addition to resource heterogeneity, there are other considerations as well, e.g., the Internet upload speed is typically much slower than the download speed [2]. Therefore, in an edge computing environment in which ML/DL models are being trained on the client site stable and powerful Internet connection is always desirable, otherwise, the unstable clients will be disconnected from the network that will result in a drop in performance. On the other hand, deploying ML at the edge saves expensive communication, i.e., we do not require the local (raw) data to be transmitted to the cloud/server.

3) DATA HETEROGENEITY

Medical data is generally heterogeneous in nature due to several reasons, such as sources and modality of the health records, dimensionality, and variation in the data acquisition devices and protocols. The literature indicates that such heterogeneous data poses challenges for several FL algorithms [29]. One of the potential directions of future research in the domain is to propose FL algorithms capable of coping with the challenges associated with heterogeneous data. The literature already reports some efforts in this direction [30], [31].

4) STATISTICAL HETEROGENEITY

The statistical heterogeneity, due to data generated by different types of devices in an edge computing environment, can lead to many efficiency challenges. For instance, the optimization/training of a ML/DL hyperparameters becomes difficult, which directly affect its performance. To address the statistical heterogeneity techniques such meta-learning can be used that can enable device-specific modeling [32].

5) PRIVACY AND SECURITY CHALLENGES

Despite being able to train joint models with sharing data in a collaborative learning environment using FL, privacy and security challenges arise with the presence of malicious devices. For instance, an adversary can learn sensitive information using the model parameters and the shared model. As shown in [33], privacy-related information can be inferred from the shared weights even without getting access to the data itself. To restrain leakage of privacy-related information from the shared model, different privacy-preserving techniques can be leveraged, such as cryptographic approaches and differential privacy [34].

6) ADVERSARIAL ML

Despite the state of the art performance of ML/DL techniques in solving complex tasks, these techniques have been found vulnerable to carefully crafted adversarial examples [35]. In a federated learning setup, a client or multiple clients can be compromised to realize the attacks on the whole network. For instance, local poisoning attacks using compromised attacker devices are presented in [36]. The authors demonstrated that their proposed attacks can increase the error rates of the distributively trained model on four real-world datasets. Moreover, a systematic review focused on different adversarial ML attacks and defenses for cloud-hosted ML models can be found in [37].

C. ENABLING TECHNOLOGIES: BUILDING BLOCKS FOR ML AT EDGE

1) SCHEMES FOR DEPLOYING ML AT THE EDGE

In recent years, enormous growth has been observed in the computational power of edge devices, allowing them to play a more important role than just collecting data in IoTs. ML can contribute significantly in fully utilizing the potential of edge devices in numerous exciting applications (e.g., smart healthcare using wearables technologies and AI-empowered sensors, etc.) and turn them into more useful components of an IoT environment [38]. ML could be employed at the edge in several ways, such as inference, sensor fusion, transfer learning, generative models, and self-improving devices. In this section, we briefly describe some of the most commonly used schemes.

- *Inference:* The inference capabilities of ML, which aims predicting unseen objects/classes based on the previous knowledge/trained data, help the IoTs to perform different activities, such as cancer prognosis, brain tumor classification, and other clinical data analysis at the edge devices resulting in reduced latency and bandwidth in telemedicine [39].
- *Sensor Fusion:* ML in conjunction with signal processing algorithms can be used for the fusion of information from different sensors enabling efficient utilization of the available information. With fusion capabilities, individual sensors in an IoT environment can be converted into sophisticated synthetic sensors to solve complex problems more accurately. For instance, in healthcare data from several sensors/sources can be combined efficiently to predict a clinical event, such as heart failure [40].
- *Transfer Learning:* Transfer learning, which aims to reutilize the knowledge of one domain in another domain by fine-tuning a pre-trained model trained on a larger dataset, can help them to learn on a smaller dataset with less computational resources. In an IoT environment and in particular, in healthcare applications where the data is scarcely available, the transfer learning technique can be used to balance workload and latency where the pre-trained models are put at the cloud and are shared among edge devices to be fine-tuned for specific tasks [41].
- *Generative Models:* Generative learning can also be useful in edge computing where generative models can be used for the approximation of the original data at the clouds to be used for training models at edge devices for applications with less training samples or to solve complex tasks with minimal computation from the clouds. Generative deep models have already been explored for the generation of synthetic medical images [42].

- *Self-improving devices:* In a typical IoT environment, ML techniques can also be used to enable end devices to optimize their performance and improve continuously based on the collected data and behaviors of other devices. Such strategies help to configure the devices faster which ultimately leads to faster and efficient implementation and deployment.

2) HARDWARE OPTIMIZATION TECHNIQUES

For successful deployment of ML at the edge, the two critical requirements of edge computing—namely (i) low power consumption, and (ii) high performance—need to be fulfilled. Thus, off-the-shelf solutions are not practical to intelligent processing of data at the edge devices, and custom hardware architectures need to be developed. In this section, we discuss some hardware optimization techniques to optimize hardware resources for deploying ML at the edge.

a) Decentrailized Distributed Computing: In edge computing, computations are completely or largely performed on end devices in a distributed computing fashion. Also, edge computing brings data, applications, and services closer to end devices while eliminating the need for centralized clouds that requires infrastructure decentralization, such kind of decentralization can be efficiently achieved using blockchain technologies [43]. Therefore, computational resources can be shared among end/edge devices by employing blockchain and smart contracts technologies thus allowing computational resources demanding ML applications to be deployed at the edge. For instance, different design requirements and challenges in designing a decentralized edge computing and IoT ecosystem are presented in [44]. This study is specifically focused on the need of using decentralized trust schemes for the elimination of trust in centralized entities and highlights the potential of using distributed ledger technology, i.e., blockchain for achieving the feature of decentralization. The backbone of blockchain technologies is the distributed consensus mechanism enabling secure communication among trust-less participants without the intervention of a central controlling unit. There are many facets of blockchain with different distributed consensus methods that can be used for edge-centric IoT systems [45].

b) AI Co-Processors: Portable intelligent and dedicated co-processors are considered to be the driving force for deploying AI/ML models at the edge. Different types of specialized processors can be integrated into a single system or chip thus forming a heterogeneous computing paradigm optimized for a specific type of task. In general, AI co-processors have two common features: (1) enables parallel computing using multiple mini-cores; (2) enables accelerated data fetching using distributed memory that is placed right to mini-cores.

D. ALGORITHMIC OPTIMIZATION TECHNIQUES

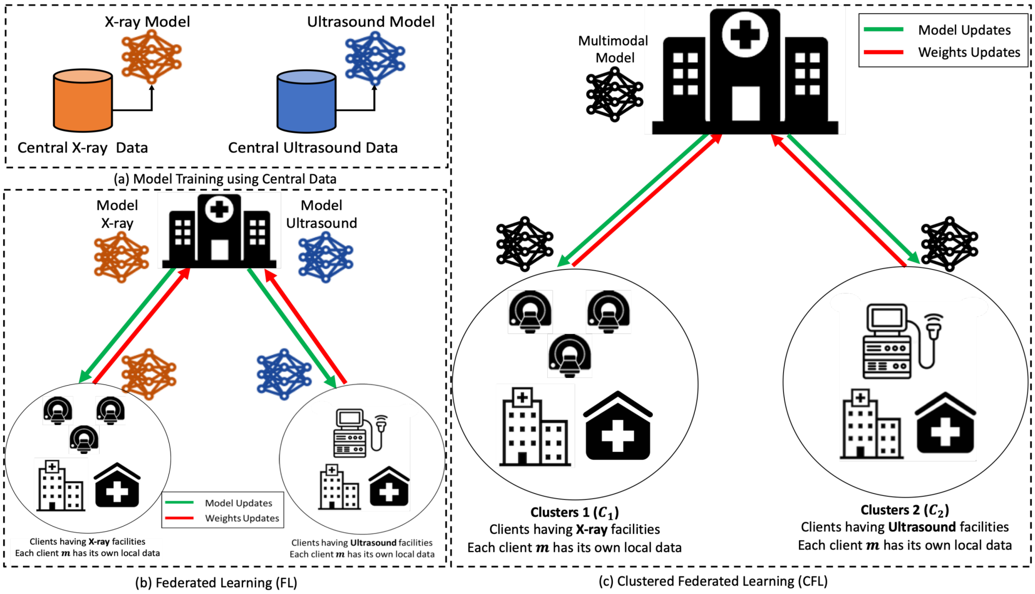
The development and advancement of ML algorithms are promising aspects that facilitate the successful application of ML at the edge. In this regard, various algorithms and techniques can be leveraged to enhance and reduce the computation of the parameters in ML models by exploiting different properties such as sparsity. The widely used methods are described below.

- *Parameter Efficient Networks:* To efficiently deploy ML models at the edge, computation and memory-efficient architectures of ML/DL models are highly desirable. To facilitate embedded ML computing, various architectures of ML models have been proposed in the literature that can be leveraged to deploy ML models on the edge, e.g., Mobile Net [46] and SqueezeNet [47]. These architectures are designed with a key focus on reducing computation costs associated with the training and inferences of ML models while maintaining accuracy. An overview of communication efficient ML approaches can be found in [48].
- *Network Pruning:* The literature suggests that a penalty of neurons in the trained model does not contribute towards the final accuracy, therefore, such neurons can be prune to save some memory. Google's Learn2Compress[1] has found that neurons can be reduced by a factor of 2 while retaining an overall accuracy of 97%. To this aim, several algorithms have been proposed in the literature, such as learning important connections and weights among neurons [49] and learning structural sparsity in deep models [50]. Moreover, many ML models perform parameter computation using 32-bit float values. On the other hand, edge devices typically operate on 8-bit values or less. Therefore, the model size can be significantly reduced by reducing precision.
- *Network Distillation:* Network distillation is a method for transferring knowledge learned by a larger model to a smaller model. Together with transfer learning, which deals with the transfer of knowledge learned from one domain to another domain, network distillation holds the substantial potential to significantly reduce model size without comprising much on performances in terms of accuracy. In addition, network distillation can be benefited from other hyperparameters tuning algorithms as well. For instance, the distillation method has been successfully used for application-specific and resource-constrained IoT platforms [51].

III. COVID-19 DIAGNOSIS USING COLLABORATIVE FEDERATED LEARNING

In this section, we consider the problem of developing a single ML model for classification of chest images from multiple sources (such as X-rays and Ultrasound). Consider a clustered federated learning (CFL) setup as shown in Fig. 2 resembles the actual federated learning settings [52]. Clients in each cluster represent the healthcare entities (remote medical imaging facilities) and major hospitals or other government entities (e.g., ministry of health) play the role of the cloud server facilitating the weights aggregation and updates. The

[1] https://ai.googleblog.com/2018/05/custom-on-device-ml-models.html


X-ray Model
Ultrasound Model
Central X-ray Data
Central Ultrasound Data
Model X-ray
Model Ultrasound
Clients having X-ray facilities
Each client m has its own local data
Model Updates
Weights Updates
Clients having Ultrasound facilities
Each client m has its own local data
Multimodal Model
Model Updates
Weights Updates
Clusters 1 (C_1)
Clients having X-ray facilities
Each client m has its own local data
Clusters 2 (C_2)
Clients having Ultrasound facilities
Each client m has its own local data

(a) Model Training using Central Data

(b) Federated Learning (FL)

(c) Clustered Federated Learning (CFL)

FIG. 2. The proposed clustered federated learning based collaborative learning paradigm (Fig. 2(c)) versus the method of model training using central data (Fig. 2(a)) and the conventional federated learning model training method for multiple modalities (Fig. 2(b)). The term “clients” refers to hospitals, clinics, and medical imaging facilities.

key motivation for using clustered federated learning (CFL) is its potential to learn a single model from data of multiple modalities, e.g., two modalities in our case (X-ray and Ultrasound). Also, we note that a single multi-modal can not be learned via conventional FL (as shown in Fig. 2, where conventional FL requires two separate models to be learned for each modality, i.e., X-ray and Ultrasound). The problem formulation for collaborative learning is described below.

A. PROBLEM FORMULATION

In this task, we are interested in learning a shared model M_s in a collaborative fashion using clustered federated learning (CFL). As shown in Fig. 2, there are two clusters each having different kind of imaging modality, i.e., cluster 1 (C_1) has clients having X-ray imagining facility and clients in cluster 2 (C_2) posses ultrasound imagining facilities, therefore, each cluster C_k is disjoint and has different data distribution $\mathcal{D}_k$. Each client m in cluster C_k has drawn its samples $z^{k,1}, \ldots, z^{k,m}$ from the distribution $\mathcal{D}_k$ such that there are no overlapping samples among the clients. We have formulated the problem of collaborative learning as supervised learning problem such that each sample $z^{k,m}$ contains a pair of data sample $x^{k,m}$ and its corresponding class label $y^{k,m}$, denoted by $z^{k,m} = (x^{k,m}, y^{k,m})$. Furthermore, we assume that each client does not have any knowledge either about the identity and data of every other client within the same cluster as well as in the other cluster. The major hospital (aka server) shares a shared model M_s and initial weights W_0 with each client of every cluster. After receiving the M_s and W_0, each client trains the shared model (i.e., M_s) using its own local data $D_{k,m}$, where $k = \{1, 2\}$ and m denotes the number of clients in each cluster C_k. After that, every client in each cluster shares the learned weights $W_{m,r}$ to the server, where m represents the client and r denotes the communication round/iteration number. After receiving the weight updates from each client, the server performs federated averaging using (1).

$$W_r = \frac{1}{n} \sum_{i}^{n} w_i \times W_i \tag{1}$$

Where, n denotes the total number of clients participating in the CFL setup (i.e., $n = |C_1| + |C_2|$) and w is a weighting factor that specifies the weight-age given to the weights of each client. Then the server updates the new weights (i.e., update its copy of M_s with W_r) and performs the inference using its multi-modal test data (the two modalities, i.e., X-ray and Ultrasound are merged to make the testing data multi-modal). After testing the performance of M_s at the communication round r, the server shares the updated weights W_r with all clients in each cluster and repeats the process until the specified criteria or desired performance is achieved. The algorithm for collaborative multi-modal learning using CFL is presented in Algorithm 1.

B. EXPERIMENTAL SETUP

1) DATA DESCRIPTION

For this study, two datasets from different sources one containing chest X-ray [10] and chest ultrasound images [13], are used. We formulated the problem as binary classification, i.e., differentiating between COVID-19 chest images and normal chest images. Each dataset is divided into two parts, i.e., a training set and a testing set using a split of 80% and 20%, respectively. The training portion (i.e., 80%) of each dataset is

Algorithm 1: Collaborative Learning From Data of Different Sources and Modality Using CFL.

```
Input: Shared Model $M_s$, Clusters $k$, Initial Model Weights $W_0$, Set of Clients $m$, Communication Rounds $R$, Epochs $E$, Batch Size $B$, and Learning Rate $\eta$
Output: Updated Weights $W_r$
Initialize: $W_0$, $R$, $E$, $B$, and $\eta$ for $r = 1, \ldots, R$ do
    for $i = 1, \ldots, k$ in parallel do
        for $j = 1, \ldots, m$ in parallel do
            if $r == 1$ then
                $W_{i,m} \leftarrow W_0$  $M_s \leftarrow W_0$  for $e \in E$ do
                    Using $B$ & $\eta$ Train $M_s$ using $z^{i,j} = (x^{i,j}, y^{i,j})$ Get $W_j$ from $M_s$
                end
            else
                $M_s \leftarrow W_r$  for $e \in E$ do
                    Using $B$ & $\eta$ Train $M_s$ using $z^{i,j} = (x^{i,j}, y^{i,j})$ Get $W_j$ from $M_s$
                end
            end
        end
        $W_{i,r} = \frac{1}{m} \sum_{j=1}^{m} w_j \times W_j$
    end
    Return: $W_r = \frac{1}{k} \sum_{i=1}^{k} W_{i,r}$
end
```

TABLE 1. The Distribution of Training and Testing Data of X-Ray and Ultrasound Datasets Over Different Classes

Data	Class	Training Data (80%)	Test Data (20%)
X-ray	COVID-19	179	44
	Healthy	1072	269
Ultrasound	COVID-19	319	80
	Healthy	116	30

further divided into different parts, depending upon the number of clients in that cluster. The distribution of training and testing data of X-ray and Ultrasound datasets over different classes is shown in Table 1. Moreover, the testing sets from both datasets are merged to develop a joint testing set that will be used by the server for the evaluation of the performance of a shared model that is being trained in a collaborative fashion using CFL.

We further note that the datasets used in this study have inter and intra class variability in terms of image size and quality, contrast and brightness level, and positioning of subjects, an example is shown in Fig. 3. This is not surprising as these publicly available databases are not standard datasets for COVID-19 detection, and have been curated from different sources and evolving with time [53]. Moreover, it is evident from Table 1 that these datasets are highly imbalanced. These limitations make the training of a generalized model more difficult.

2) MODEL ARCHITECTURE AND IMPLEMENTATION DETAILS

In our experiments, we have used the VGG16 model with one extra convolutional layer and three fully connected layers stacked before its original output layer having units of 128, 64, and 32, respectively. The overall architecture of modified VGG16 has fourteen convolutional layers, six pooling layers, and six dense layers. The output layer is modified according to the number of classes in the problem at hand (i.e., for binary classification) and binary cross entropy loss was used for model optimization. Each image is first converted into a gray-scale image, which is then resized to a dimension of 256 × 256. Moreover, the resized images are normalized before feeding into the model. The model is trained using *Adam* optimizer with a learning rate of 0.0001 at each client. We use different types of standard data augmentation techniques for training the models. Furthermore, to address the problem of imbalanced classes, we propose to use focal loss [54], which is suited for such issues in binary classification tasks. The class imbalance also refers to the scarcity of data, i.e., when we have a limited labeled data for a particular class. So the class which has more data points can be easily classified with respect to those which have few data points. Focal loss deals with such a problem in a way that it takes the limited class samples as hard samples and tries to improve the model's performance for every class so that model does not overfit on only one class having more samples. Specifically, the focal loss adds a modulating factor $(1 - p_t)^\gamma$ to the standard cross-entropy loss, where $\gamma \geq 0$ is a tunable focusing parameter whose values can vary in the range [0,5]. The α-balanced variant of focal loss is defined in (2), where α balances the importance of positive/negative examples [54]. The optimal values for α and γ can be selected experimentally. For a binary classification problem, alpha controls the easy and hard examples (miss classified) and gamma controls the weights of positive and negative classes.

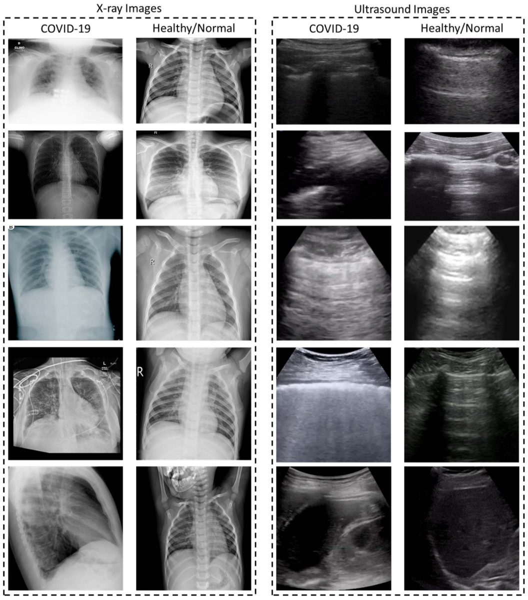


FIG. 3. The depiction of inter and intra class variations observed in COVID-19 datasets (X-ray [10] and Ultrasound [13]).

$$FL(p_t) = -\alpha_t (1 - p_t)^\gamma \log(p_t) \tag{2}$$

We note that for the implementation of the proposed work we used *TensorFlow* ML library, and all experiments are performed in a simulated environment. The results of the different experiments are described in the next section.

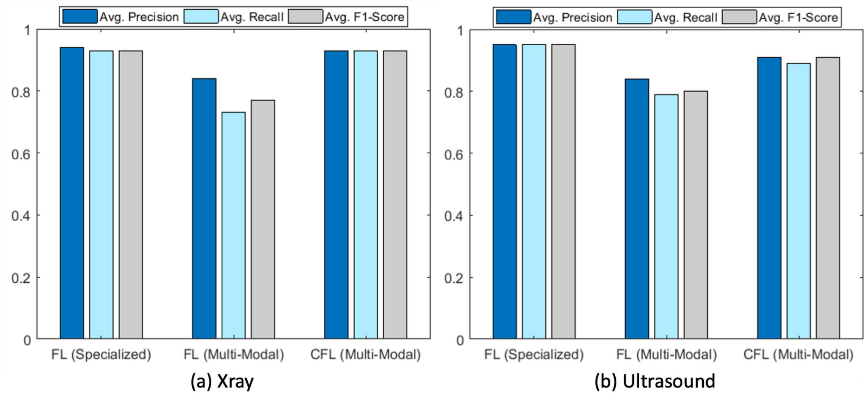


FIG. 4. Comparison of clustered federated learning (CFL) with two baselines (i.e., the specialized models (trained with conventional FL independently for each modality) and conventional federated learning (when the model is trained using multi-modal data)) in terms of average values of precision, recall, and F1-score on X-ray and Ultrasound imagery.

TABLE 2. Parameters of Clustered Federated Learning (CFL) Experiments

Parameter (s)	Value (s)
Communication Rounds	30, 50, & 100
Epochs	5 & 10
Batch Size	16 & 32
Learning Rate	$1e^{-3}$

IV. EXPERIMENTS AND RESULTS

In order to show the effectiveness of the proposed multi-modal collaborative learning framework for COVID-19 diagnosis, we performed several experiments. On one side, we aim to evaluate and compare the performances of CFL against two baselines, namely (i) *specialized FL baseline*, and the (ii) *multi-modal*[2] *conventional FL*. Since CFL aims to tackle the convergence issues of conventional FL schemes due to the diverse distribution of the data, the two baselines, we believe, are appropriate options as a comparison benchmark instead of the state of the art methods for COVID-19 diagnosis. We note that due to the limitations of the dataset, we only consider the divergence in distribution of the data in terms of the nature of the data (i.e., the distribution of ultrasound and X-ray images is different). The first baseline shows the best-case scenario, where separated models for each type of imagery, which we termed as specialized models, are trained in a FL environment. The individual models are trained on X-ray and Ultrasound images with a learning rate of 0.0001 and a batch size of 32 resulting into two separate models one for each modality (i.e., X-ray and Ultrasound). The second baseline represents the experimental setup of a conventional FL environment, where the data is distributed among different clients, and a shared ML model is built in a federated environment. The parameters used in different experiments can be found in Table 2.

Table 3 and Fig. 4 provides the experimental results per class and overall (per dataset) results, respectively, in terms of precision, recall, and F1-Score. Since the data set is not balanced, so we believe, alone accuracy is not enough to evaluate the proposed method. For performance evaluation of the three experimental setups (i.e., the two baselines and CFL), we kept the similar experimental setup where we first train the baseline models with a batch size of 16 (for each modality) and then we train the same model in CFL fashion (i.e., using multi-modal settings) with 5 epochs of local training with a batch size of 16. Then we evaluated the collaboratively trained model with the test data from each cluster (modality), i.e., X-ray and Ultrasound. As can be seen in the Fig. 4, overall comparable results are observed for multi-modal model trained using CFL compared with the specialized two models trained in a conventional FL environment using X-ray and Ultrasound imagery separately. On the other hand, we can see that CFL performance is considerably better than the performance of multi-modal model trained in a conventional federated learning environment. Moreover, it is evident from the figure that a collaboratively trained model is capable of recognizing the test of images from different modalities without having explicit knowledge about these modalities. Moreover, overall better results are obtained on ultrasound images (Fig. 4(a)) compared to X-ray imagery (Fig. 4(b)) for all models.

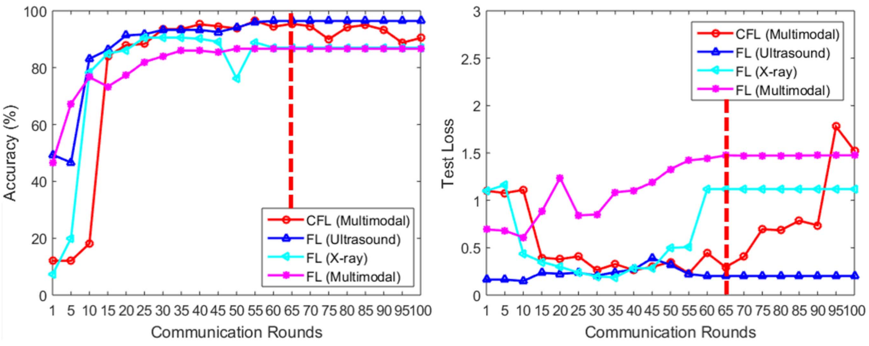
In Fig. 5, we provide the comparison of the three experimental setups (i.e., specialized models trained in conventional FL settings, multi-modal models trained in a conventional FL and CFL environments) in terms of accuracy and loss at different communication rounds. The figure depicts that the proposed CFL model (which is trained using multi-modal data) provides comparable performance with that of specialized FL models (that are separately trained for each modality). Moreover, it is also evident from the figure that the model trained using multi-modal data in conventional FL settings gets over-fitted after 50 communication rounds. On the counter side, the model keeps on learning in CFL setting, though it also tends to show over-fitting behavior at later stage communication round as evident in the Fig. 5. The vertical red line shown on Fig. 5(a) and (b) shows the inflection point beyond which the parameters of the specialized machine learning models of the two clusters (i.e., X-ray and

[2] By the term multi-modal we mean images acquired using different imagining techniques, i.e., modalities (e.g., X-ray and Ultrasound).

TABLE 3. COMPARISON AGAINST THE TWO BASELINES IN TERMS OF PRECISION, RECALL, AND F1-SCORE

Dataset	Class	Federated Learning (Specialized*)			Federated Learning (multi-modal)			Clustered FL (multi-modal)		
		Precision	Recall	F1-Score	Precision	Recall	F1-Score	Precision	Recall	F1-Score
X-ray	COVID-19	0.73	0.82	0.77	0.30	0.68	0.41	0.71	0.82	0.76
	Healthy	0.97	0.95	0.96	0.93	0.74	0.82	0.97	0.94	0.96
Ultrasound	COVID-19	0.97	0.95	0.97	0.94	0.76	0.84	0.93	0.95	0.94
	Healthy	0.88	0.93	0.90	0.58	0.87	0.69	0.86	0.80	0.83

Promising results are obtained by CFL, outperforming the conventionfal FL while slightly lower performance is obtained compared to central baseline with the added advantage of improved privacy and data security.
*A separate model is trained in federated learning settings for each modality.



(a) Xray

(b) Ultrasound

FIG. 5. Comparison of clustered federated learning (CFL) with the specialized models (trained with conventional FL independently for each modality, i.e., X-ray and Ultrasound) and conventional federated learning (when the model is trained using multi-modal data) over increasing number of communication rounds.

ultrasound) start to diverge from each other. This diversion limits the extent to which the multimodal model can be generalized to fit the underlying multimodal data (i.e., X-ray and ultrasound). Therefore, Fig. 5(b) provides the insight that the federated learning rounds should be stopped as soon as the inflection point in the value of the loss function is reached. This inflection point identified the number of rounds beyond which the multimodal machine learning model cannot be enhanced. Such an overfitting behavior can be mitigated by developing application-specific model architectures and by using appropriate regularization techniques such as using a learning rate scheduler.

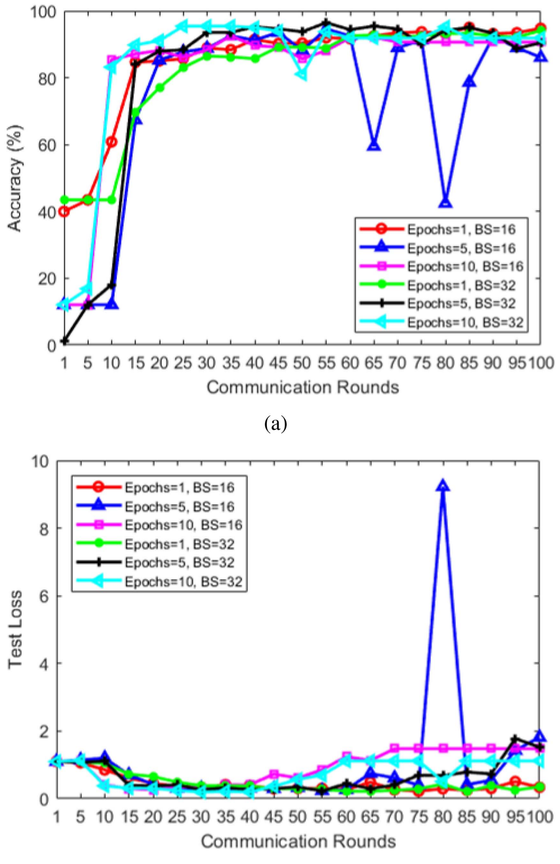
Here we evaluate the performance of the proposed CFL-based framework while considering different computational capabilities of edge devices. Specifically, to evaluate data heterogeneity, we used different batch sizes, and to evaluate computational heterogeneity, we used a different number of epochs for local model training. The effect of increasing the number of epochs for local model training (at client-side) with different batch sizes (i.e., 16 and 32) is shown in Fig. 6. The following conclusions can be drawn from the figure that reflects the resource heterogeneity of the edge devices. From Fig. 6, we can see that when we start increasing the number of epochs for local model training (i.e., depicting edge devices enough computations resources to process more epochs), it does not perform well for a batch size of 16 (this indicates that the edge device needs to acquire more data for training). This trend is opposite to the learning trend when the model was trained using 1 epoch (this suggests that the edge devices with limited computational resources should train the local model with small batches of data). Moreover, Fig. 6 highlights that increasing the number of epochs for training local models provides time efficiency and saves communication cost, i.e., the shared models achieve good accuracy at fewer communication rounds (as shown in Fig. 6). Similarly, model performance on test data while using 10 epochs of local training is also depicted in Fig. 6. A similar trend about the batch size can be observed from the figure as we encountered for 5 epochs of training thus suggesting that it's not a good idea to increase the number of epochs for local training of the models at the client-side when the edge devices have a small amount of data. Moreover, it can be observed from Fig. 6 that with increasing the number of epochs for local model training the batch size of 32 performs better as compared to a batch size of 16. This suggests that when the client has enough amount of data for local model training and computational resources to train the model for a higher number of epochs, we will get the increased performance of the overall CFL framework in return.

V. DISCUSSIONS

In this section, we discuss the advantages and limitations of our proposed CFL framework for multi-modal COVID-19 diagnosis.

A. ADVANTAGES

Some key lessons learned from the experiments conducted in this work highlighting the potential of the proposed CFL framework are: (1) CFL ensures the privacy of the user's local data, as it does not need to be shared with the server for central training; (2) The communication payload of model weights is far less than the payload of sharing actual data,



(a)

(b)

FIG. 6. The depiction of model performance, Fig. 6(a), and loss, Fig. 6(b), on multi-modal test data over increasing number of communication rounds using 1, 5, and 10 epochs of training with different batch sizes (i.e., 16 and 32).

therefore, it saves bandwidth and as well as time; (3) It enables the collaborative learning of multi-modal features by shared model M_s without sharing any explicit information about the modality of the local data and the data itself; (4) More importantly, compared to the conventional FL, CFL ensures better performance in presence of divergence in the data distribution. The divergence in the distribution could be in terms of the distribution of negative and positive samples per class as well as in terms of the nature of data samples as detailed earlier; and (5) This particular use-case demonstrates the potential of the method in medical applications where remote smaller healthcare units can benefit from this collaborative learning method.

B. CHALLENGES AND LIMITATIONS

Despite above-mentioned benefits, there are some challenges and limitations as well, e.g., efficiency, security issues, and the optimization of CFL parameters is difficult. Moreover, there is a trade-off in the model performance when we compare model trained using central data and model trained with distributed data using federate learning. While the literature argues that in critical human-centric applications, such as healthcare, both privacy and performance of AI models are crucial [3]. FL ensures the privacy of ML models at the cost of a reduction in the performance [28], [29], [55]. One of the key challenges for FL algorithms in healthcare applications is maintaining the balance between privacy and performance of the FL model.

In addition, for multi-modal distributively dispersed data, the development of personalized models that are tailored to these modalities is required for local training, which will enhance the efficiency of the shared model and as well as of the models on the client side. For instance, from our experiments, we have learned that the performance of the model being trained in CFL settings starts degrading after a particular point (i.e., communication round). Thus highlighting the need for early stopping and the development of optimal stopping criteria except the maximum allowed communication rounds.

VI. OPEN RESEARCH ISSUES

A. DEVELOPING PERSONALIZED APPROACHES

The edge computing network is potentially more heterogeneous as compared to any other central network and clients in an edge computing network vary due to data acquisition resources [56], such as communication, computational, and storage resources, etc. Moreover, as discussed above in the paper, clients can significantly vary due to statistical heterogeneity, which is usually a great challenge in realistic settings. For example, as we discussed in the above section, developing a multi-modal collaborative learning framework for COVID-19 diagnosis has efficiency challenges due to the aforementioned heterogeneity issues. Therefore, to handle such heterogeneities, the development of personalized and client-specific ML/DL approaches is required. On the other hand, if such challenges are not addressed, they will ultimately result in the development of a biased and inefficient global model that will favor a particular FL client over another (i.e., the model will provide higher performance on some clients and lower performance on others), thus limiting the application of FL in critical applications like healthcare.

B. ADVERSARIALY ROBUST ML

The edge computing network is more prone to security threats, as the edge computing network is an ideal environment for adversaries that aim to get desired outcomes or incentives for breaching the network security and privacy of participating agents. This phenomenon becomes, even more, worse with the integration of ML/DL models that are vulnerable to adversarial attacks, which have been already shown effective for different healthcare applications [57]. For instance, an adversarial attack on CT scanners in an actual hospital environment by manipulating the hospital's network has already been realized in the literature [58] and threats of adversarial ML for ML and IoT empowered COVID-19 detection systems are highlighted in [59]. To restrain the adversarial attacks, different defensive techniques have been proposed in the literature. However, the adversarially robust methods developed so far are attack specific, i.e., they only work for particular attacks for which they were developed and fail to withstand unforeseen attacks. Therefore, the development of adversarially robust ML/DL models is still an open research problem that demands a proportionate amount of interest from the community with the advancement of ML/DL techniques. The literature highlights that the neural network parameters shared between the client and server in FL can be used to reconstruct the input data [60]. Moreover, different attacks can be realized on models being trained in FL settings, e.g., property inference attack [61], data poisoning attack [62], and model poisoning attack [63], etc. A taxonomy of different attacks that can be realized on FL can be found in [64]. Therefore, for the successful deployment of ML/DL models on the edge, in particular, for developing robust healthcare applications, the development of adversarially robust models is of utmost importance.

C. ASYNCHRONOUS DISTRIBUTED ML

In distributed computing, two approaches are widely used for communication, i.e., synchronous and asynchronous. These approaches are ideal for scenarios where data is instantly available for instance in the central picture archiving and communication system (PACS) of a hospital. However, in realistic settings, the data collection or acquisition might get delayed due to any reason, such as due to some network issue or unavailability of I/O device, etc. Moreover, it is possible that the client (i.e., a small healthcare entity) in an ML-based collaborative computing network is not active at the current iteration/communication round due to some inherent issue, this will result in a delay in the federated parameters update process and will eventually affect the system's overall performance. Therefore, it is worth studying and developing asynchronous approaches for facilitating shared model training for healthcare applications using distributed data. Moreover, it has been envisioned that ML methods will play a very crucial role in 6 G architectures [65]. In critical human-centric applications, such as healthcare, both privacy and performance of AI models are crucial [3]. FL ensures the privacy of ML models at the cost of a reduction in the performance [28], [29], [55]. One of the key challenges for FL algorithms in healthcare applications is maintaining the balance between privacy and performance of the FL model.

D. TRACEABILITY AND ACCOUNTABILITY

Reproducibility of the systems and results is very critical in healthcare applications. However, compared to centralized training, several factors need to be considered and traced for the reproducibility of FL-based solutions for healthcare [29]. For instance, FL generally involves several clients having different environments, computational resources, software, and networks, which make it difficult to keep track of the FL system assets, such as training data and configurations, etc. Especially in non-trusted environments traceability and accountability require particular attention. One potential solution is to record all the hyper-parameters, the data, and parameters related to the experimental environment for all the clients. Moreover, the use of explainable AI (XAI) solutions in FL could also help researchers in identifying the components of the models (including both global and local) responsible for the performance degradation [66].

E. DATA AUDITING

Data auditing is one of the key phases of developing AI solutions for human-centric applications especially in healthcare [3]. In the FL environment, the data is distributed over several clients and the analysts generally don't have an access to all the data used for training the global model. In such a configuration, it is very challenging to analyze the risks associated with the data and their potential impact on the performance of the FL global model. One potential solution is the use of the standard auditing procedure/techniques across all the clients [67].

F. AI-INTEGRATED NEXT GENERATION COMPUTING FOR HEALTHCARE

Integration of AI with next-generation computing technologies like cloud computing, fog serverless technologies, or quantum computing has several challenges that need to be resolved [68]. The major issue is the availability of limited labeled data, and even if data is available, moving that data into the cloud is a major challenge for organizations that produce that data through their applications. Also, organizations need to shift their applications to the cloud so that the new data can be available on the cloud. Once data is available on the cloud, the challenges of data privacy and security arise. Moreover, the literature highlights that different attacks can be realized on cloud-hosted AI models [37]. Therefore, it requires specialized techniques like anonymization of data or the use of differential privacy to prevent security breaches of confidential information to adversaries attacking the system. Apart from these challenges, a lot of effort in terms of resources, investment, and training is required for organizations who wish to leverage AI to enhance their business processes.

Fog computing is used in a scenario where IoT devices require quick inference and fast response. Substantial work has been done that is focused on integrating AI with fog computing. However, there are a few challenges that remain unresolved and require special attention. Embedded AI in fog computing can speed up the user reaction time because when the demand for using a particular application increases, the quality of service (QoS) suffers. A combination of novel and efficient ML/DL algorithms can help optimize the performance of those time-intensive applications. Moreover, while deploying AI on the edge, the following research issues need to be considered. There is a need to develop the rules and regulations to use AI in edge computing as it has no ethical, social, or legal status yet. Small and inexpensive edge devices may be exploited by adversaries as they usually use third-party APIs.

New frameworks for software and toolkits must be prepared. There should be rules and regulations according to the local consequences of the geographical location when it comes to installing IoT devices that are manufactured by a different country.

Serverless is a cloud computing paradigm that uses native cloud services for its applications, and the integration of AI with serverless computing has some open challenges that need to be addressed. For example, switching to a cloud services provider is difficult because there is a lack of industry-wide standards. Also, the cloud service provider is responsible for events happening in the system. On the other hand, most of these systems lack transparency and it is difficult to understand the underlying infrastructure that the service provider is using. Therefore, considerable research attention is required to address the aforementioned challenges. Also, research attention is required to ensure that serverless computing is sustainable with a focus on smart workload consolidation and transmission of data like neural network learned weights with an acceptable trade-off in accuracy. Quantum computing, due to its unique computing technique, could replace AI in the future. Different applications of quantum computing can be applied in healthcare [69]. For example, in the pharmaceutical industry, personalized medicines can be suggested by quickly analyzing the genome structure. Another useful application of quantum computing is protein folding, which can help in the faster identification of drugs. Faster genome sequencing is still an issue to be resolved. Quantum computing machines can be used to make genome sequences quickly instead of using standard compute machines, which takes a lot of time and computation power.

VII. CONCLUSION

This article provides insights on how edge computing and machine learning advances can be used to provide a solution for COVID-19 diagnosis in an efficient privacy-aware manner thereby allowing remote healthcare units to benefit from collaborative learning paradigm without sharing local data. In particular, we propose using a clustered federated learning (CFL)-based collaborative learning framework to intelligently process visual data at the edge by training a multi-modal ML model capable of diagnosing COVID-19 in both X-ray and ultrasound imagery. Compared to the conventional FL, CFL is found to better cope with the divergence in distribution of data from different sources (i.e., X-ray and ultrasound imagery). In the current implementation, we consider the divergence in distribution due to the sources and nature of the data due to the limitations of the datasets. In the future, we will explore how CFL performs in the presence of variances in the distribution of the data in terms of the number of samples per client and incorporating resource heterogeneity at the client level such as computational and communication resources.

ACKNOWLEDGMENTS

The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] M. Satyanarayanan, “The emergence of edge computing,” *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[2] W. Y. B. Lim et al., “Federated learning in mobile edge networks: A comprehensive survey,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 2031–2063, Jul.–Sep. 2020.

[3] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, “Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges,” *Comput. Sci. Rev.*, vol. 43, 2022, Art. no. 100452.

[4] S. Latif et al., “Leveraging data science to combat COVID-19: A comprehensive review,” *IEEE Trans. Artif. Intell.*, vol. 1, no. 1, pp. 85–103, Aug. 2020.

[5] Y. W. Tang, J. E. Schmitz, D. H. Persing, and C. W. Stratton, “Laboratory diagnosis of COVID-19: Current issues and challenges,” *J. Clin. Microbiol.*, vol. 58, no. 6, 2020, Art. no. e00512-20.

[6] M. A. Hendaus, “Remdesivir in the treatment of coronavirus disease 2019 (Covid-19): A simplified summary,” *J. Biomol. Struct. Dyn.*, vol. 39, no. 10, pp. 3787–3792, 2021.

[7] P. J. Hotez, D. B. Corry, and M. E. Bottazzi, “COVID-19 vaccine design: The janus face of immune enhancement,” *Nature Rev. Immunol.*, vol. 20, no. 6, pp. 347–348, 2020.

[8] T. Ai et al., “Correlation of chest CT and RT-PCR testing in coronavirus disease 2019 (COVID-19) in China: A report of 1014 cases,” *Radiology*, 2020, Art. no. 200642.

[9] H. S. Maghdid, A. T. Asaad, K. Z. Ghafoor, A. S. Sadiq, S. Mirjalili, and M. K. Khan, “Diagnosing COVID-19 pneumonia from X-ray and CT images using deep learning and transfer learning algorithms,” *Multimodal Image Exploitation Learn.*, vol. 11734, pp. 99–110, 2021.

[10] J. P. Cohen, P. Morrison, L. Dao, K. Roth, T. Duong, and M. Ghassemi, “COVID-19 image data collection: Prospective predictions are the future,” *Mach. Learn. Biomed. Imag.*, vol. 1, Dec. 2020. [Online]. Available: https://melba-journal.org/papers/2020:002.html

[11] “COVID-19 CT segmentation dataset”. Accessed: Sep. 22, 2022. [Online]. Available:http://medicalsegmentation.com/covid19

[12] J. Zhao, Y. Zhang, X. He, and P. Xie, “COVID-CT-Dataset: A CT scan dataset about COVID-19,” 2020, *arXiv:2003.13865*.

[13] J. Born et al., “POCOVID-Net: Automatic detection of COVID-19 from a new lung ultrasound imaging dataset (POCUS),” *arXiv:2004.12084*.

[14] J. Born et al., “Accelerating detection of lung pathologies with explainable ultrasound image analysis,” *Appl. Sci.*, vol. 11, no. 2, 2021, Art. no. 672.

[15] S. Wang et al., “A deep learning algorithm using CT images to screen for corona virus disease (COVID-19),” *Eur. Radiol.*, vol. 31, no. 8, pp. 6096–6104, 2021.

[16] C. Butt, J. Gill, D. Chun, and B. A. Babu, “Deep learning system to screen coronavirus disease 2019 pneumonia,” *Appl. Intell.*, p. 1, 2020.

[17] L. Li et al., “Using artificial intelligence to detect COVID-19 and community-acquired pneumonia based on pulmonary CT: Evaluation of the diagnostic accuracy,” *Radiology*, vol. 296, no. 2, pp. E65–E71, 2020.

[18] P. Afshar, S. Heidarian, F. Naderkhani, A. Oikonomou, K. N. Plataniotis, and A. Mohammadi, “COVID-CAPS: A capsule network-based framework for identification of COVID-19 cases from X-ray images,” *Pattern Recognit. Lett.*, vol. 138, pp. 638–643, 2020.

[19] L. Wang, Z. Q. Lin, and A. Wong, “COVID-Net: A tailored deep convolutional neural network design for detection of COVID-19 cases from chest X-ray images,” *Sci. Rep.*, vol. 10, no. 1, pp. 1–12, 2020.

[20] P. K. Sethy and S. K. Behera, “Detection of coronavirus disease (COVID-19) based on deep features and support vector machine,” *Int. J. Math., Eng. Manage. Sci.*, vol. 5, no. 4, pp. 643–651, 2020.

[21] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *Proc. IEEE Conf. Comput. Vis. pattern Recognit.*, 2016, pp. 770–778.

[22] A. Narin, C. Kaya, and Z. Pamuk, “Automatic detection of coronavirus disease (COVID-19) using X-ray images and deep convolutional neural networks,” *Pattern Anal. Appl.*, vol. 24, no. 3, pp. 1207–1220, 2021.

[23] M. Z. Islam, M. M. Islam, and A. Asraf, “A combined deep CNN-LSTM network for the detection of novel coronavirus (COVID-19) using X-ray images,” *Informat. Med. Unlocked*, 2020, Art. no. 100412.

[24] S. H. Kassani, P. H. Kassasni, M. J. Wesolowski, K. A. Schneider, and R. Deters, "Automatic detection of coronavirus disease (COVID-19) in X-ray and CT images: A machine learning-based approach," *Biocybernetics Biomed. Eng.*, vol. 41, no. 3, pp. 867–879, 2021.

[25] Y. Xu et al., "A collaborative online AI engine for CT-based COVID-19 diagnosis," *medRxiv*, 2020.

[26] R. Kumar et al., "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16301–16314, Jul. 2021.

[27] A. Vaid et al., "Federated learning of electronic health records improves mortality prediction in patients hospitalized with COVID-19," *medRxiv*, 2020.

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

[29] N. Rieke et al., "The future of digital health with federated learning," *NPJ Digit. Med.*, vol. 3, no. 1, pp. 1–7, 2020.

[30] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," *Proc. Mach. Learn. Syst.*, vol. 2, pp. 429–450, 2020.

[31] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of FedAvg on non-IID data," 2019, *arXiv:1907.02189*.

[32] J. Li, M. Khodak, S. Caldas, and A. Talwalkar, "Differentially private meta-learning," in *Proc. Int. Conf. Learn. Representations*, 2020.

[33] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2019, pp. 691–706.

[34] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and robust machine learning for healthcare: A survey," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 156–180, 2021.

[35] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 998–1026, Apr.–Jun. 2020.

[36] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to Byzantine-robust federated learning," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1605–1622.

[37] A. Qayyum et al., "Securing machine learning in the cloud: A systematic review of cloud machine learning security," *Front. Big Data*, vol. 3, 2020, Art. no. 587139. [Online]. Available: https://www.frontiersin.org/article/10.3389/fdata.2020.587139

[38] G. Zhu, D. Liu, Y. Du, C. You, J. Zhang, and K. Huang, "Toward an intelligent edge: Wireless communication meets machine learning," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 19–25, Jan. 2020.

[39] G. Gobieski, B. Lucia, and N. Beckmann, "Intelligence beyond the edge: Inference on intermittent embedded systems," in *Proc. 24th Int. Conf. Architectural Support Program. Lang. Operating Syst.*, 2019, pp. 199–213.

[40] Y. Wang, W. Huang, F. Sun, T. Xu, Y. Rong, and J. Huang, "Deep multimodal fusion by channel exchanging," in *Advances in Neural Information Processing Systems*, vol. 33, H. Larochelle, M. Ranzato, R. Hadsell, M. F. Balcan, and H. Lin, Eds., New York, NY, USA: Curran Associates, Inc., 2020.

[41] Z. Zhou, H. Liao, B. Gu, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Jul./Aug. 2018.

[42] A. Qayyum, W. Sultani, F. Shamshad, J. Qadir, and R. Tufail, "Single-shot retinal image enhancement using deep image priors," in *Proc. Int. Conf. Med. Image Comput. Comput.- Assist. Interv.*, 2020, pp. 636–646.

[43] D. A. Booz, J. D. Dye, M. J. Dye, and E. F. Ford, "Decentralized autonomous edge compute coordinated by smart contract on a blockchain," U.S. Patent App. 15/082,559, Sep. 2017.

[44] I. Psaras, "Decentralised edge-computing and IoT through distributed trust," in *Proc. 16th Annu. Int. Conf. Mobile Syst. Appl. Serv.*, 2018, pp. 505–507.

[45] Y. Zhao et al., "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1817–1829, Feb. 2021.

[46] A. G. Howard et al., "Mobilenets: Efficient convolutional neural networks for mobile vision applications," 2017, *arXiv:1704.04861*.

[47] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5 MB model size," 2016, *arXiv:1602.07360*.

[48] Y. Shi, K. Yang, T. Jiang, J. Zhang, and K. B. Letaief, "Communication-efficient edge AI: Algorithms and systems," *IEEE Commun. Surv. Tut.*, vol. 22, no. 4, pp. 2167–2191, Oct.–Dec. 2020.

[49] S. Han, J. Pool, J. Tran, and W. Dally, "Learning both weights and connections for efficient neural network," in *Proc. Adv. neural Inf. Process. Syst.*, 2015, pp. 1135–1143.

[50] W. Wen, C. Wu, Y. Wang, Y. Chen, and H. Li, "Learning structured sparsity in deep neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 2074–2082.

[51] J. Yim, D. Joo, J. Bae, and J. Kim, "A gift from knowledge distillation: Fast optimization, network minimization and transfer learning," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2017, pp. 4133–4141.

[52] F. Sattler, K.-R. Müller, and W. Samek, "Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 8, pp. 3710–3722, Aug. 2020.

[53] M. J. Horry et al., "COVID-19 detection through transfer learning using multimodal imaging data," *IEEE Access*, vol. 8, pp. 149808–149824, 2020.

[54] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal loss for dense object detection," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2017, pp. 2980–2988.

[55] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3454–3469, 2020.

[56] K. Yang, T. Jiang, Y. Shi, and Z. Ding, "Federated learning via over-the-air computation," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2022–2035, Mar. 2020.

[57] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287–1289, 2019.

[58] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, "CT-GAN: Malicious tampering of 3 D medical imagery using deep learning," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 461–478.

[59] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, "Adversarial examples–security threats to COVID-19 deep learning systems in medical IoT devices," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9603–9610, Jun. 2021.

[60] F. Boenisch, A. Dziedzic, R. Schuster, A. S. Shamsabadi, I. Shumailov, and N. Papernot, "When the curious abandon honesty: Federated learning is not private," 2021, *arXiv:2112.02918*.

[61] Z. Wang, Y. Huang, M. Song, L. Wu, F. Xue, and K. Ren, "Poisoning-assisted property inference attack against federated learning," *IEEE Trans. Dependable Secure Comput.*, early access, Aug. 5, 2022, doi: 10.1109/TDSC.2022.3196646.

[62] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2020, pp. 480–501.

[63] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to {Byzantine-Robust} federated learning," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1605–1622.

[64] M. S. Jere, T. Farnan, and F. Koushanfar, "A taxonomy of attacks on federated learning," *IEEE Secur. Privacy*, vol. 19, no. 2, pp. 20–28, Mar./Apr. 2020.

[65] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[66] J. H. Yoo, H. Jeong, J. Lee, and T.-M. Chung, "Federated learning: Issues in medical application," in *Proc. Int. Conf. Future Data Secur. Eng.*, Springer, 2021, pp. 3–22.

[67] M. Kolhar, M. M. Abu-Alhaj, and S. M. Abd El-atty, "Cloud data auditing techniques with a focus on privacy and security," *IEEE Secur. Privacy*, vol. 15, no. 1, pp. 42–51, Jan./Feb. 2017.

[68] S. S. Gill et al., "Ai for next generation computing: Emerging trends and future directions," *Internet Things*, vol. 19, 2022, Art. no. 100514.

[69] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Quantum computing for healthcare: A review," Jun. 2022, doi: 10.36227/techrxiv.17198702.v3.