Collaborative Segmentation of COVID-19 From non-IID Topographies in the Internet of Medical Things (IoMT)

Ahmed Sleem[1], Ibrahim Elhenawy[2]

[1]Ministry of communication and information technology, Egypt
Thebes Higher Institute for Computer and Administrative Sciences, Egypt
[2] Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt
Email: Ahmedsleem8000@gmail.com; ielhenawy@zu.edu.eg

Abstract

The Internet of Medical Things (IoMT) offers numerous advantages in the diagnosis, monitoring, and treatment of a wide variety of illnesses for both patients. COVID-19 has caused a global pandemic and turned out to be the utmost crucial danger threatening the whole world. Thus, scholars' attention moved toward Deep learning (DL) and IoMT for developing automated systems for COVID-19 diagnosis and/or prognosis based on chest computed tomography (CT) scans, and it has shown great success in several tasks, including classification and segmentation. Nevertheless, developing and training a superior DL approach necessitates accumulating a substantial amount of patients' CT scans together with their labels. This is an expensive and time-consuming task that restricts attaining large enough data from a single site/institution, However, owing to the necessity for protecting data privacy, it is difficult to accumulate the data from several sites and store them at a centralized server. Federated learning (FL) alleviates the need for centralized data by spreading the public segmentation model to different institutional models, training the segmentation model at the institution, and followingly calculating the mean of the parameters in the public model. Nevertheless, researchers advocated that private information could be restored using the parameters of the model. This study presents a privacy-protection technique for the challenge of multi-site COVID-19 segmentation. To tackle the challenge, we introduce the FL technique, in which a distributed optimization procedure is developed, and randomization techniques are proposed to change the joint parameters of private institutional segmentation models. Bearing in mind the complete heterogeneity of COVID-19 distributions from diverse institutions, we develop two domain adaptation (DA) techniques in the proposed FL design. We explore several applied characteristics of optimizing the FL approach and analyze the FL approach in comparison with alternate training approaches. Finally, the results validate that it is auspicious to employ multi-site non-shared CT scans to improve the COVID-19 infection segmentation.

Keywords: Deep Learning; COVID-19 Diagnosis; Segmentation; Multi-site Data; Federated Learning; Domain.

1. INTRODUCTION

The term "Internet of Things" (IoT) is used to describe a network in which everyday objects can exchange data and perform complex computations with one another. These technologies are now an integral part of everyday life [1, 2]. Multiple industries have implemented on-demand services centered on the Internet of Things, including those dealing with environmental monitoring, defense, healthcare information technology, transportation, and building automation. Internet of Medical Things (IoMT) services stands out because they are used directly for human health issues [3]. In the context of IoMT, "Things" can refer to numerous devices, such as those used for cardiac monitoring or infusion pumps used to administer a set volume of fluid to a patient. Various kinds of sensing devices are used in IoMT, each of which is tailored to a certain set of characteristics. Sensor data on health can be collected and processed for use in enhancing daily life, but there is a risk that patients' privacy will be compromised due to communications among smart devices

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

[4]. Access to the collected data is made available to patients, users, or HealthCare (HC) professionals via the Cloud Server (CS) [5]. Elderly care services are becoming increasingly reliant on IoMT [6]. IoMT is also susceptible to cyberattacks [7] due to the nature of its instantaneous access and monitoring. Stolen and postponed data causes malfunctions and downtime in the network, therefore obviously these attacks have a negative impact on network performance [9]. When sensors communicate via an unsecured channel, protecting patients' personal information is a top concern for researchers [10, 12]. Despite the presence of various security techniques, the IoT lacks higher-order security. Complex data encryption techniques are challenging to implement in IoT devices because of the limited power available in these gadgets [13], [14]. As a result, there is a need for lightweight security mechanisms that may increase the security measures of IoT data with minimal impact on the devices' ability to communicate and process information [15]. Authentication is the most important factor in IoT since it enables the verification of each entity. IoT features, however, will need to work together with them to implement authentication [16]–[18]. Efficacious security solutions for issues of confidentiality, privacy, authentication, and integrity have been the focus of extensive study in the discipline of cryptography [19], [20]. Some scholars have recently examined the difficulties of privacy in the healthcare IoT, as well as the provenance and trustworthiness of the data in great detail [28], [29]. As controlling security on the IoMT is currently difficult, this article provides methods for doing so. More security and privacy issues have surfaced in IoMT goods as there has been an explosion in product variety. Since a breach in IoMT data can put patients' lives in jeopardy, its sensitivity level is substantially higher than that of data from other IoT applications. Therefore, it is imperative that IoMT stakeholders opt for stringent safety precautions. While much of the literature provide point solutions to security problems, we present a comprehensive security architecture in this paper. In this piece, we propose a new security paradigm for IoMT and conduct an analysis of existing approaches. The proposed system employs the exponential K-anonymity (EKA) algorithm to preserve user privacy following authentication. In order to determine which pieces of information should be kept secret and which should be made public, we propose a deep learning improved Elman neural network (IENN) model. After that, the information is sent to the cloud server in a safe manner by means of rooted elliptic curve cryptography with Vigenère cipher (RECC-VC). When all is said and done, data are saved utilizing blockchain technology to guarantee their authenticity.

Because of its superior efficiency and usefulness, the Internet-of-Medical-Things (IoMT) framework has gained widespread acceptance and implementation to date. Using deep learning, the IoMT can automate the diagnosis and prognosis of a wide range of diseases, which will greatly aid in the delivery of high-quality, cost-effective healthcare [1, 2]. Relatively few works, though, look into the diagnostic IoMT by means of telehealth and deep-learning-based threats on the services provided on IoMT devices, in particular the IoMT-based AI services. Virtual reality technologies and metaverse [4]-[6] all relate to the real/virtual environments formed by graphic design and gadgets, and their use has spread extensively in the medical area, particularly in the context of telemedicine.

With the significant success that AI techniques have had in many illness detection tasks [1], the newly released COVID-19 has become the most critical research issue for the AI research community at the start of 2020. From a medical standpoint, reverse transcription-polymerase chain reaction (RT-PCR) is the gold standard for detecting COVID-19 infection. However, the efficiency and the speed of making conclusions concerning those under suspicion are hampered by the severe requirements for assessing surroundings and the lack of technology. Furthermore, it has been shown that the RT-PCR test has a high rate of false negative results [2]. To supplement the RT-PCR [4], radiological images (RIs) such as computed tomography (CT), X-rays [3, 4], and ultrasound frames have been used. Among these, CT scans have been proven to work for diagnosis, severity forecasts, and tracking the progression of infection [5-12].
More recently, a variety of deep learning (DL) approaches have been developed to aid COVID-19 diagnosis from radiographic images [6]. These approaches could be categorized into classification-based approaches and segmentation-based approaches. The key purpose of classification-based approaches often uses convolutional neural networks (CNNs) to learn to discriminate COVID-19 patients from common pneumonia patients and from normal cases [4]. On the other hand, the segmentation-based approaches seek to automatically localize/detect and segment the infected areas in the lung CT scans, which enables saving much time and effort wasted in manual segmentation of COVID-19 lesions and helps to mitigate the problems of inter- and intra-observer variabilities, while affording vital information for accelerating diagnosis and the patients monitoring process [9].

Despite the recent AI studies for detecting COVID-19 lesions from 2D/3D CT scans. It remains a challenging task due to several shortcomings and issues ignored and uncovered by the current literature. These issues could be summarized as follow.
First, developing efficient DL for efficient segmentation usually necessitates a vast training set. However, collecting such huge COVID-19 data from the same site is not obtainable in healthcare, leading to a deficiency of accuracy and generalizability of the models. Hence, sharing huge quantities of CT data is necessary to save the effort and time needed to acquire and annotate huge COVID-19 CT datasets from a single source/site [13],[14]. Nevertheless, multiple issues

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

facing data sharing including the concerns of patients about the privacy of their data, the worries of the hospital about losing the patients' trust when their data get shared, and the health systems worried that contestants will be able to use their data when they compete for customers. **Second,** the domain shift is incurred due to utilizing CT scans from diverse parties. Various domains of data are shared as the institutions often have a variety of techniques for acquiring and collecting data including different scanners, manufacturers, and scanning protocols. Recent work in domain adaptation (DA) methods have shown great success in learning from heterogeneous data in the era of medical image analysis [18-21].

To address the beforementioned and unstudied challenges, this paper introduces a federated learning framework for privacy-protected multi-institution COVID-19 segmentation and investigates numerous hands-on characteristics of the federated model's interaction regularity compared to other PP techniques. We investigate two randomization techniques to prevent data reconstruction from the parameters. Besides, to the extreme of our realization, this study first investigates DA techniques in federated segmentation of medical images to tackle the problem of the domain shift caused by heterogeneity in data distributions. For this, we introduce the Assortment of Specialists (AoS) technique and the Federated Domain Generalization (FDG) technique. Furthermore, we propose to assess segmentation performance using different privacy-protection techniques.

The following outline has been devised for the subsequent parts of the paper: The pertinent research work is presented in Section II, Section III addresses the strategy that has been recommended for this study, and Section IV presents the empirical settings, observations, correlations analyses, and drawbacks. In the final section, section V, the conclusions as well as the future directions of the work are discussed.

2. RELATED WORK

A. Artificial intelligence for COVID-19

For classifying COVID-19 from CAP using CT images, Ouyang et al [4] proposed dual-sampling 3D CNN to mitigate the impact of the imbalanced distribution of the sizes of the infection regions and exploit these regions for deciding pneumonia type. Kang et al [5] proposed to learn latent multi-view representations, that straightly project features into the class space. wherein the complementarity between diverse categories of features is well investigated to enable realizing better classification performance. A weakly-supervised 3D DL model for classification and lesion localization was created by Wang et al. [6]. The COVID-19 lesions were localised after the lung zone was segmented using a pre-trained UNet, and the segmented 3D lung zone was applied to forecast the influenza kind and the activated zones formed by the base classifier were utilised to pinpoint the lesions. Two unique 3D-ResNets based on prior-attention residual learning were proposed by Wang et al. [7]. (PARL). In this setup, a single 3D-ResNet is used as a binary classifier to identify whether or not influenza is present. At the same time, the PARL modules create an attention map to aid the second 3d-ResNet in its learning to classify influenza. Han et al [8] introduced an interpretable 3D deep multi-instance learning framework, in which patient-level annotation is given to a CT volume that is regarded as a bag of instances. Besides, the work [31] developed an extended reality (XR) system based on a combination of DL and IoMT that provided a remedy for COVID-19 telemedicine diagnostic. More, the work [32] put many DL-based COVID-19 diagnostic approaches using real-world adversarial scenarios to the test (AEs). Then, it performed many experiments to confirm that DL models that fail to incorporate safeguards against malicious interference remain susceptible to such attacks. Finally, it demonstrated the attack modeling results, AE design method, and AE perturbations of the current DL-based COVID-19 clinical purposes in detail.

In view of COVID-19 lesion segmentation, in order to improve its representations, Fan et al. [9] created a semi-supervised method called Inf-Net, which uses a parallel partial decoder to fuse the complicated features and generate a global map. Using a new non-local DL module, Xie et al. [10] introduced a relational model (i.e., RTSU-Net) that takes the use of architectural linkages by learning pictorial and geometric links between convolutional features in order to create self-attention weights. The authors of [11] introduced a novel semi-supervised method for effective segmentation of 2019-nCov infection from relatively small numbers of annotated lung CT scans. The difficulty of this study was the fact that there were so few annotated cases of COVID-19 infection from which to draw meaningful conclusions. To achieve this, they propose a new Encoder-decoder (E-D) model with two independent paths for few-shot segmentation. Addressing the large-scene-small-object problem, Zhou et al. [12] provide a new DL that, in order to improve segmentation accuracy, breaks down the 3D segmentation work into three separate 2D segmentation operations. The work [33] proposed an interactive attention refinement network to enhance the precision with which COVID-19-affected regions are separated from the surrounding landscape (Attention RefNet). The end-to-end training process for the segmentation network can be facilitated by connecting the interactive attention refinement network. As a means of enhancing crucial characteristics in both segmentation and refinement networks, we suggest a skip-connection attention

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

component and a grain module for improving crucial seeds (positions) in active refinements, respectively. More, the work [34] proposed to efficiently annotate CT scans of the lungs for COVID-19 infections, it developed a relation-driven collaborative learning model that draws on prior knowledge about lesions other than COVID. Two types of encoders make up the model: a generic one that takes in information about lung lesions in general and uses data from multiple lesions that aren't caused by COVID, and a task-specific one that uses data about COVID-19 infections. The work [35] extracted COVID lesions from CT images, we offer a self-ensembled co-training framework that is taught by both limited labeled data and massive amounts of unlabeled data. In order to increase the variety of unsupervised data, it constructed a co-training system made up of two collaborative models, wherein the models learn from and teach each other utilising anticipated pseudo-labels of the other's training examples. The work [36] proposed better categorise lung infections, and a new context-aware neural network is presented. Particularly, the autofocus and panoramic modules are made to extract specifics and semantic knowledge, as well as to capture the long-range dependencies of the setting from both the peer level and the cross-level. By illustrating the structural connection between foreground and background, a unique architectural consistency rectification is also suggested for calibrating. The work [37] proposed to train the segmentation network using only flawed annotations, with the training set consisting of both a small, high-quality set of expert-annotated images and a much larger, lower-quality set of annotations made by non-experts. It presented a method for training segmentation networks to handle noisy labels, which should prevent labels of varying quality from compromising the segmentation model. To learn independently from the precise and imprecise annotations, it developed devise a Divergence-Aware Selective Training (DAST) technique in which a divergence-aware noisiness score distinguishes between highly and moderately noisy annotations. The work [38] proposed a segmentation-based COVID-19 classification network, dubbed SC2Net, which is suggested for efficient identification of COVID-19 from chest x-ray (CXR) images in an effort to address these concerns. A COVID-19 lung segmentation network (CLSeg) and a spatial attention network (SAN) make up the SC2Net (SANet). the CLSeg is used to isolate the lung area in the CXR, which helps to reduce noise from the image's surroundings. A lot of studies were proposed for the segmentation of COVID-19 infections [42]-[45], but they all assume that the input data share the same distribution or acquisition settings.

B. Multi-site Based Approaches for Disease Diagnosis

Federated Learning (FL): Commonly, FL could be realized via one of two schemas. First, the training is performed in every site of data (e.g. hospital or institution) utilizing the corresponding private CT scans; so, the transfers are just performed for model parameters This has been investigated in several studies [13-17]. Second, employing encryption procedures to permit benign transportation among various data sources [13]. Accordingly, the specifications of the patients' data are not released or become accessible by any party. This study emphasizes the former schema to address the challenge of aggregating e satisfactory amount of CT images. In addition to data aggregation, annotating infection in 2d/3D CT scan necessitate experienced radiologists which could be handled by the partnership between clinical societies. Nevertheless, sharing CT data to federal locations is still subject to tons of probable lawful and technical problems [14], particularly among intercontinental organizations. In view of this, multi-site DL based on unshared patient data was studied for the first time in [17]. Later, Li et al [18] experimentally investigated privacy-protection (PP) problems via a sparse vector method and inspected data imbalance using weights sharing mechanism. We observed that FL has not been explored for the randomization technique for PP and DA challenges. Thus, we propose to investigate these issues in this paper.

Domain adaption (DA): The primary goal of domain adaptation (DA) is to transfer the information obtained from one domain (a source domain) to another (a target domain). Therefore, a deep learning network is given further training using data from the source domain in order to familiarise it with a data set that was generated from a different target domain. Unsupervised DA techniques have received a lot of research over the years[19]. Nevertheless, these works could not meet the necessities of FL situations where the data are locally kept and could not be public, which cumber the acclimatable methods in conventional domains since they need access to both target and source data [20]. Thus, federated DA (FDA) has been lately introduced [21],[22] to address these issues. This paper proposes to integrate two techniques of the FDA for multi-institution infection area segmentation from CT scans of COVID-19 patients. The work [39] presented an approach for model construction that avoids the need to transfer private information between the source and the target domains. The label-rich source domain could be used by the target domain party without disclosing any of the target domain's private information. the work moved the common practice of domain adaptation into a distributed network where multiple nodes share a single global server and model. Further, a homomorphic encryption (HE) technique was implemented to safeguard data in transit and at rest. The work [40] proposed to tackle this under-researched but realistic cross-silo federated DA problem, where the party of the target domain is deficient in both samples and features, it introduces a unique federated adversarial DA approach (PrADA). To handle the feature-scarce problem, it employed vertical federated learning with a feature-rich party, while the sample-scarce problem was addressed with adversarial DA from a sample-rich source party to a sample-scarce target party. To draw on domain

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

knowledge, PrADA partitioned the feature space into several subspaces, each of which contains highly informative features, and then learn a high-order feature with semantic significance from each subspace. The work [41] develops DA, Source HypOthesis Transfer (SHOT), to train the destination domain's feature extraction component by adapting the destination input variables to the static source categorization module. To guarantee that the target characteristics were intuitively matched with the characteristics of unobserved source information using the same assumption, SHOT made use of both knowledge maximization and self-supervised learning for the image retrieval unit learning.

3. METHODOLOGY

A. Foundation of privacy-protection Federated Learning

This section articulates multi-site segmentation and quantification of COVID-19 infection without sharing patients' CT scans in an FL system. Following, we present the randomization technique for PP. Lastly, we discuss the specifics of training this FL for PP.

1) Problem Formulation

Given matrix D_i represent the CT data held by the site (i.e. institution or hospital) i . State N sites $\{S_1, \ldots . S_N\}$ seeking to train their DL models by combining their corresponding CT data $\{D_1, \ldots , D_N\}$. For the COVID-19 analysis from CT scans, typically, the number of scans that exist at each site is not enough to build and train an efficient DL approach. Traditionally, this issue could be solved by joining all data in a single site and employing $D = \{D_1 \cup D_2 \ldots . \cup D_N\}$ for the purpose of training M_{joinly}. Simultaneously, the part of these CT data may be annotated, and others will be unannotated. For convenience, the feature space is represented as X , the ground truth (GT) space is denoted as Y, and the sample identity space is represented as I. Hence, the $X, Y, and\ I$ establish the entire dataset. In the scenario of multi-site COVID-19 lesion segmentation, D_i is CT data aggregated from the institution S_i; whereas X is the acquired CT features and with the ground truth Y that are used to segment and quantify the infection area. In this configuration, the datasets have a common feature space yet their samples differ. For instance, heterogeneous sites possess diverse patients. Nevertheless, the CT features get extracted and learned from the identical learning pipeline. Consequently, the data distribution could be formulated by equation (1).

$$X_i = X_j, \quad Y_i = Y_j, \quad I_i = I_j \; \forall D_i D_j \; i \neq j \qquad (1)$$

which is a type of horizontal FL in which a variety of datasets exhibit a huge feature intersection while they have a trivial sample space intersection [14].

Owing to the rules and policies, each clinical organization is unable to share data. An FL scheme is a training schema in which the institutions S_i to cooperatively train a particular model M_{FED} without disclosing their data. In the scenario of our problem, we undertake a centralized computation server. All of the institutions (sites) use the same DL architecture for the segmentation task. The model is trained locally at every institution and the training parameters regularly get updated and transferred to the centralized server. An arbitrary noise ε is applied to the joint parameters to protect the data from reverse anatomization leakage. As soon as the server all parameters reach the server, it epitomizes and upgrades them and broadcast the new parameters to the contributing institution.

2) Threat Model

The "honest but curious" computer or other components in the IoMT system could be the adversary that is taken into consideration here. The central controller and endpoints that are participating in federated learning will faithfully adhere to the training session that was developed for them, and they might not knowingly inject intentionally misleading information into the learning experience. They are, however, interested in the confidential data stored on a targeted system and may be able to deduce this information from the information that is supplied throughout the learning phase. When the training process is being carried out, the adversary might also take the form of a passive outer attacker who tracks the diagnosis tasks in the IoMT system. Primary individual data are stored locally in federated learning, which offers some sort of security against the invasion of privacy. On the other hand, local model changes are communicated throughout each cycle, and these updates are trained on confidential CT data. If adversaries have access to shared model upgrades, they are able to conduct model resonance attacks to rebuild the CT data or use affiliation inference attacks to deduce if a data record was in the raw training database. Both of these attacks require the adversaries to recreate the raw training examples. Therefore, maintaining data locally and just communicating model upgrades does not offer the appropriate security for the person's privacy. Instead, we need to establish stringent privacy guarantees in order to defend ourselves against the threats that have been described.

3) Privacy-protection distributed learning

The basic FL system comprises two main phases in distributed optimization: first, the local upgrade. Second, the server communication. The loss function used for training the segmentation network at any institution n is the dice Loss.

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

$$L_{dice} = \frac{1}{N}(1 - DC) \quad (2)$$

$$DC = \frac{2|\hat{Y} \cap Y|}{|\hat{Y}| + |Y|} = \frac{2\sum_{i=1}^{n}\sum_{j=1}^{m}\hat{z}_{ij} \cdot y_{ij} + \varepsilon}{\sum_{i=1}^{n}\sum_{j=1}^{m}\hat{z}_{ij}^2 + \sum_{i=1}^{n}\sum_{j=1}^{m}y_{ij}^2 + \varepsilon} \quad (3)$$

where $z_i$and y_i correspondingly represent the model prediction and GT for input x_i. the entire training set is arbitrarily selected from the feature space $X_n$with and GT space Y_n. Randomization technique for privacy-protection
In DP, we talk about how algorithms operating on large datasets can ensure the privacy of personal information. A differentially private technique is one in which the addition of a unified view to the data does not significantly alter the results of the method.
The primary motivation behind DP is the ability to investigate the attributes of data in its entirety without disclosing any personal information. To ensure that an attacker is unable to determine whether a given individual is present or absent from the data, DP involves introducing noise into either statistical queries or the actual dataset. When using DP as originally specified in [45], consumers must have faith in the data producer because they are entrusting the data administrator with their accurate information. As it is submitted by users, the data is saved on the main server. However, neither the data curator nor the data scientist can be trusted. So, prior to answering statistical questions from 3rd parties, the data administrator employs DP to mess with the training dataset. Centralized DP refers to this specific method of deploying DP. The term "centralized DP" arises from the belief that different from the local DP that will be detailed later on, the disturbance is done primarily by the data curators.

For convenience, this study refers to a method that fulfills DP by ϵ -DP [29], in which ϵ indicates privacy leakage. Prior to delivering the description of an ϵ -DP method, it is essential to define the notion of compassion of a certain query function f and the adjoining databases.
Given that D^n representing the realm of all databases, termed universal database, the database $D \in D^n$ and databased $D' \in D^n$ can be declared as adjoining if D *and* D' vary in a single instance, such that the addition or elimination of a single instance of D return D'. More, the compassion of a certain query function $f: D^n \to \mathbb{R}^d$, *mapping* D *and* D' to a real number can be defined as the highest value by which f varies when one instance is included or eliminated from any of the databases:

$$\Delta_f = \max_{D,D'} ||f(D) - f(D')||_1. \quad (4)$$

wherever $||\cdot||$ signifies the ℓ1 norm.

A randomization method M is dubbed ϵ -DP if for all adjacent database $D, D' \in D^n$, as well as $S \subseteq Y$, when the following condition is applied

$$Pr[\,h\,(D) \in S] \leq e^{\epsilon}\, Pr\,[\,h\,(D') \in S], \quad (5)$$

whereas Y denotes a group of all conceivable outputs. This implies that the outcome of method M applied to D resembles the outcome obtained once applying M to D'. The minimum value of ϵ denotes the ideal amount of privacy is assured. It's important to note that a DP technique can be created by combining two DP processes, a process called composition. This definition describes the composition principle.
Given M_1 denoting $\epsilon_1 - DP$ method and M_2 denoting $\epsilon_2 - DP$ system, the composition of them can be characterized by $M_{1,2} = (M_1, M_2)$ is an $(\epsilon_1{+}\epsilon_2)$ -DP. Assuring the privacy of the FL gradient is one such tangible result made possible by DP, according to the composition theory. For instance, suppose a Florida client processes the gradient with a delta DP method before transmitting it to the centralised server. The composition theory stated that in j iterations, the DP method will lead to the (j× ϵ) DP method. To rephrase, privacy breach was ϵ at the first epoch and j×ϵ after k iterations.

The proposed framework relax the above definition of privacy to $(\epsilon, \delta) - DP$ by including a preservative factor, δ, in the above formula to acquire the privacy shield of the Gaussian distribution. A randomization method M is dubbed ϵ -DP if for all adjacent database $D, D' \in D^n$, as well as $S \subseteq Y$, when the following condition is applied

$$Pr[\,h\,(D) \in S] \leq e^{\epsilon}\, Pr\,[\,h\,(D') \in S] + \delta, \quad (6)$$

whereas Y denotes a group of all conceivable outputs. The understanding of a method M satiates $(\epsilon, \delta) - DP$ is this method is $\epsilon - DP$ but with the possibility δ. $(\epsilon, \delta) - DP$ is suggested to alleviate the privacy outflow for ϵ-DP in the case of composition, as ϵ -DP is closed under composition. $(\epsilon, \delta) - DP$ offers reduced collective loss below composition. $(\epsilon, \delta) - DP$ is not applicable in the situation somewhere S is a singleton collection. It is important to note

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

that if we want to escape the worst-case situation of always compromising the privacy of a proportion of the dataset, then ought to be small relative to the size of the collection S.
Here, we detail the various probability distributions that have been proposed in the literature and that meet $(\epsilon, \delta) - DP$. We also describe the nature of the noise, the state of relevant apps, and some example deployments.
Laplace LDP**: it** is the most applied methodology in research studies because its suitability to any form of data and it involves of injecting noise taken from the endless Laplace distribution

$$M(D) = f(D) + Lap(0, \frac{\Delta_f}{\epsilon}). \quad (7)$$

Gaussian LDP: It fulfills the concept of the new form of -DP, which is f-DP, and it supports the controllability of the privacy constraint in the compilation.

$$M(D) = f(D) + \mathcal{N}(0, \frac{\Delta_f^2}{\epsilon^2}), \quad (8)$$

Geometric LDP: It is utilized in the process of incorporating discrete noise into the outcome of a query function for data types that are integer-valued.

$$M(D) = f(D) + \Delta, \quad (9)$$

$$P(\Delta = \delta) = \frac{1-e^{-\epsilon}}{1+e^{-\epsilon}} e^{-\epsilon|\delta|} \quad (10)$$

Binomial LDP: It is utilised in the process of incorporating discontinuous noise into the outcome of the query function.

$$M(D) = f(D) + (Z - Np)s \quad (11)$$

B. Domain Adaption for FL-based segmentation.

Despite the improved and efficient privacy realized by FL, there is an extra challenge in segmenting the COVID-19 infection from CT scans that have a heterogeneous data distribution, which causes domain shift between different institutions [15]. The key notion here is that the DA techniques could improve the segmentation performance of multi-site data in a FL configuration, and that keep efficient even if the noises are applied for PP, particularly for the institutions whose data distributions are completely varied from other institutions. Thus, we present two DA techniques: 1) Assortment of Specialists (AoS), output level adaptation, and 2) Adversarial DA (ADA) technique, in which the adaptation performed at the level of learned knowledge representation.

1) An assortment of Specialists (AoS)

The AoS technique (sometimes called a mixture of experts) [25], [26] is used to tentatively syndicate experienced specialists for processing input samples. In the field of DL, specialists are the DL models. So, the AoS layer of the segmentation models acts as a trainable gating architecture that automatically allocates gated parameters to integrate several models. Hence, all sections of the large model containing all specialist models and the AoS layer are trained cooperatively through back-propagation. Combining the outputs of a jointly trained universal model and a domain specialist was investigated for DA in [14]. To improving over this work [14], we propose to apply the beforementioned randomization technique in the AoS technique. Every contributing institution has an autonomous set of annotated training samples that they want to retain privately, acquired from a particular distribution. These contributors work together to construct a universal segmentation model while maintaining private, DA specialist models. Hence, the weighted mean of the output of all of these models (i.e. universal and specialists) are used as a final segmentation result. The parameters are updated using AoS architecture [14], [25], thereby the gradient descent can be employed for model training. unambiguously, assume having input sample $x \in X$, the segmentation of the universal model $y_g = \boldsymbol{f}_{\bar{W}}(\boldsymbol{x})$, learned by Algorithm 1. In the segmentation scenario. Concurrently, the institutional model $f_{\phi i}$ that has identical architecture. The institutional model is regularly trained and its output $y_l = f_{\phi i}(x)$ is calculated without incorporating privacy-relevant noise. The final segmentation of sample i is calculated with equation (6).

$$\hat{y} = a_i(x) y_g + (1 - a_i(x)) y_p \quad (12)$$

While the parameter $a_i(x)$ represent the gating operation of AoS, which is computed as $a_i(x) = \sigma(\psi_i^T \cdot x + b_i)$, where σ denotes the sigmoid operation, and ψ_i and b_i represent the learned parameters through training in FL schema.

2) Federated Domain Generalization

In FL configurations, the CT scans were institutionally kept for protecting their privacy. For the DA challenge, we aim to generalize from heterogeneous source domains to the shared domain space of target data. Owing to restrictions

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

imposed in sharing data in FL schema, it is impossible to train a specific segmentation model that could use both the source and target domain concurrently. To tackle this problem, a novel adversarial alignment technique [14] that proposes two components (i.e. 1) institutional domain-relevant feature extractor; 2) universal discriminator through segmentation models and separated the optimization procedure into two autonomous stages.

The primary objective of our adversarial adaptation is to decrease the distance between the source and target interpretations $\left(M_s(X_t), M_t(X_t)\right)$. Once this objective is achieved, the source model can be effeceintly applied yo the target space. In our framework, the Maximum Mean Discrepancy (MMD) is adopted to estimate the statistical divergence between target and source domains as follows:

$$\min_{S,T} \left\| \frac{1}{n_s} \sum_{x_i \in \boldsymbol{X}^s} S^T x_i - \frac{1}{n_t} \sum_{x_j \in \boldsymbol{X}^t} T^T x_j \right\|_F^2 . \tag{13}$$

Then,we follow joint distribution analysis (JDA) [22] to decrease the restrictive distribution shift across two domains as follow:

$$\min_{S,T} \left\| \frac{1}{n_s^{(c)}} \sum_{x_i \in \boldsymbol{X}^{s,(c)}} S^T x_i - \frac{1}{n_t^{(c)}} \sum_{x_j \in \boldsymbol{X}^{t,(c)}} T^T x_j \right\|_F^2 . \tag{14}$$

For perfect federated domain adaptation, the proposed framework instantaneously decrease the change in both the marginal and the conditional distribution between sources and targets. This way, the objective distance function can be formulated as follow:

$$\begin{aligned} &\min_{S,T} \left(\left\| \frac{1}{n_s} \sum_{x_i \in \boldsymbol{X}^s} S^T x_i - \frac{1}{n_t} \sum_{x_j \in \boldsymbol{X}^t} T^T x_j \right\|_F^2 \right. \\ &\left. + \left\| \frac{1}{n_s^{(c)}} \sum_{x_i \in \boldsymbol{X}^{s,(c)}} S^T x_i - \frac{1}{n_t^{(c)}} \sum_{x_j \in \boldsymbol{X}^{t,(c)}} T^T x_j \right\|_F^2 \right). \end{aligned} \tag{15}$$

In ur framework, we divide representations are into the source, M_s, and target spaces, M_t . Then, adversarial learning is applied on the M_t, while keeping the distribution source data invariant. This notion could be equivalent to the GAN model whereas the actual data distribution is kept unaffected and the gernator learn to effecintly generate samples. Hence, optimizing the distance between the source and target can be ragrded as a problem of minimizing adversarial functionalities, in which non-saturating GAN loss is used as the objective of adversarial leaning:

$$\begin{aligned} \min_{M_s,C} L_{cls}(X_s, Y_s) &= \mathbb{E}_{(x_s,y_s)\sim(X_s,Y_s)} \\ &\quad - \sum_{k=1}^{K} \mathbb{I}\,[k \\ &\quad = y_s]\, log\; C(M_s)x_s)) \end{aligned} \tag{16}$$

$$\begin{aligned} &\min_{\mathrm{D}} \mathrm{L_{advD}}(\mathrm{X_s}, \mathrm{X_t}, \mathrm{M_s}, \mathrm{M_t}) = -\mathbb{E}_{\mathrm{x_s}\sim\mathrm{X_s}}[\mathrm{logD}(\mathrm{M_s}(\mathrm{X_s}))] - \mathbb{E}_{\mathrm{x_t}\sim\mathrm{X_t}}[\log\left(1 - \mathrm{D}\left(\mathrm{m_t}(\mathrm{x_t})\right)\right] = \\ &\min_{\mathrm{M_s},\mathrm{M_t}} \mathrm{L_{advM}}(\mathrm{X_s}, \mathrm{X_t}, \mathrm{D}) = -\mathbb{E}_{\mathrm{x_t}\sim\mathrm{X_t}}\left[\mathrm{logD}\left(\mathrm{M_t}(\mathrm{x_t})\right)\right] \end{aligned} \tag{17}$$

Once the training of the FL model is combined with an alignment component, the divergence between both domains (i.e. source and target) could be reduced. By performing domain adaptative training, the following formula is optimized:

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

$$E'^{(\theta_f,\theta_y,\theta_d)} = \frac{1}{n}\sum_{i=1}^{n} L_y\left(G_y\left(G_f(x_i;\theta_f);\theta_y\right),y_i\right) - \lambda\left(\frac{1}{n}\sum_{i=1}^{n} L_d\left(G_d\left(G_f(x_i;\theta_f);\theta_d\right),d_i\right) + \frac{1}{n}\sum_{i=n+1}^{N} L_d\left(G_d\left(G_f(x_i;\theta_f);\theta_d\right),d_i\right)\right) \quad (178)$$

whereas $G_f(x_i;\theta_f)$ denote a feature extraction model with θ_f as the learning parameter. The term $G_y(.;\theta_y))$ denote the class prediction model with θ_y denoting the parameter. Similarely, the $G_d(.;\theta_d)$ denote the domain prediction model with parameter θ_d. Each of the above component act as follows. The learning parameters are updated to reach the lowest loss value for both feature extraction and classification models, while keeping the parameters domain classifier fixed. Then, the loss value of domain classifier is optimized by fixing the learning parameters of both the feature extraction and classification models. This can be mathematically expressed as follow:

$$(\theta_f',\theta_y') = argmin_{\theta_f,\theta_y} E(\theta_f,\theta_y,\theta_d') \qquad \theta_d' = argmax_{\theta_d} E(\theta_f',\theta' y,\theta_d) \quad (189)$$

With μ denoting the learning rate, and λ denoting the adaptation paramete, the gradient computationi is updated as follows:

$$\theta_f \leftarrow \theta_f - \mu\left(\frac{\partial L_y^i}{\partial \theta_f} - \lambda\frac{\partial L_d^i}{\partial \theta_f}\right) \qquad \theta_y \leftarrow \theta_y - \mu\left(\frac{\partial L_y^i}{\partial \theta_y}\right) \qquad \theta_d \leftarrow \theta_d + \mu\left(-\lambda\frac{\partial L_d^i}{\partial \theta_d}\right) \quad (20)$$

4. Experiments and Analysis

A. Dataset Description

In order to assess the performance of the proposed HS-nCov-Net on heterogeneous multi-source data, we select three publicly available 2019nCov CT datasets. First, the COVID-19-CT-Seg dataset [28], which comprises twenty public 2019nCov CT volumes from the Coronacases Initiative and Radiopaedia with more than 1,800 annotated slices—in our experiments, we refer to this dataset as DS1. Second, we use a 50 CT volume published in the MosMedData dataset [29], which was aggregated from the municipal hospitals in Moscow, Russia—in our experiments we refer to this data as DS2. The third is a larger dataset, BIMCV COVID-19+ [30], which consists of 163 CT volumes aggregated from 1,311 patients—we refer to this data as DS3.

B. Evaluation metrics

Inspired by the extensively used approaches for evaluation of segmentation techniques, we assess the segmentation performance of proposed model using two complementary metrics: the dice similarity coefficient (DSC) is a region-based metric utilized to evaluate region overlap (see Eqs(2-3)), and boundary-based normalized surface dice (NSD) [28] is employed to measure the resemblance between model outcome and the GT surfaces with itemized tolerance τ. For both measures, higher values indicate improved segmentation outcomes, and 100% represents the segmentation outcome identical to GT. Let $G;\ S$ symbolize GT and the model outcome, correspondingly.

$$NSD = \frac{2|\partial S \cap B_{\partial S}^{\tau}| + 2|\partial S \cap B_{\partial G}^{\tau}|}{|\partial S| + |\partial G|} \quad (19)$$

where $B_{\partial S}^{\tau}$ and $B_{\partial G}^{\tau}$ designate the border area of GT and segmentation surface at τ tolerance, and are expressed as

$$B_{\partial S}^{\tau} = \{x \in R^3 | \exists x \in \partial S,\ \widehat{\|x - \hat{x}\|} \le \tau\}, \quad (2220)$$

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

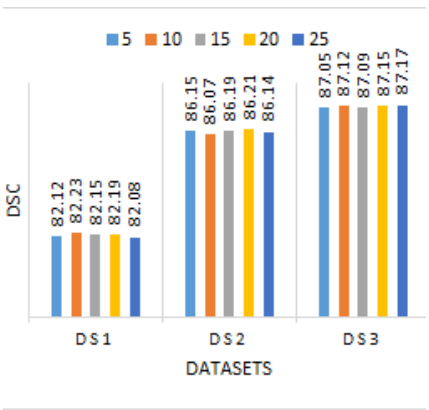

Fig. 1. The impact of interaction stride on the performance

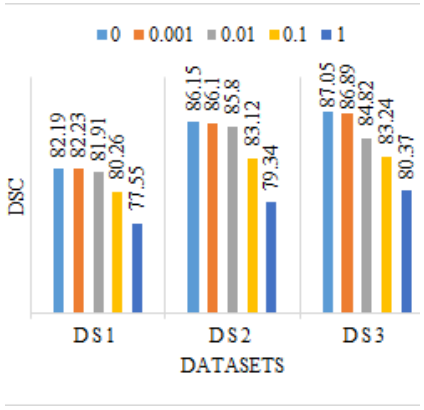

Fig. 2. The impact of gaussian noise degree on the performance

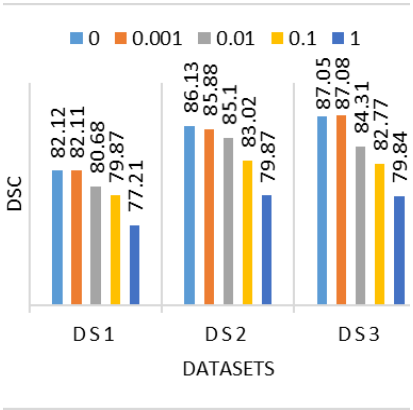

Fig. 3. The impact of Laplace noise degree on the performance

$$B_{\partial G}^{\tau} = \{x \in R^3 | \exists x \in \partial G, \quad \widehat{\|x - \hat{x}\|} \leq \tau\}$$

The acceptance is calculated by estimating the difference between two diverse radiologists. The key advantage of presenting NSD is disregarding the slight edge deviations due to a small number of inter-observer mistakes that are inevitable and frequently not clinically pertinent when segmenting targets by radiologists.

C. Implementation Setup and Analysis

The standard U-Net [25] is employed as the segmentation network. The outputs of the U-Net are a segmentation map indicating the COVID-19 infection regions. The dice loss is used as the cost function. 5-fold cross-validation is adopted for training. The segmentation network is optimized using Adam optimizer while initializing the learning rate to be 1e-3 which is decreased by 0.5 after every 25 epochs and is stabilized after $75 - th$ epoch. Through all epochs, an institutional upgrade is carried out several times depending on the interaction stride τ as a replacement for of one-time upgrade. 100 is selected to be the number of steps used per epoch.

The impact of interaction pace: since the interaction speed is often expensive and laborious, we experiment and analyze the impact of varying the interaction stride on segmentation performance. For determining the optimal interaction stride τ, we perform this experiment without applying any noise to the shared parameters. The segmentation result presented in Fig. 1 demonstrates that there is no noteworthy difference between the dice scores when the τ changed from $5\ to\ 25$.

The impact of randomization technique: as discussed earlier, the randomization technique is applied to defend against contrary attack, where the inferring data could be recovered based on the private model parameters s, given institutional model parameters; so, we experiment with the effect of applying these techniques on the segmentation performance. The key reason for such an experiment is that the institutions might need to determine the privacy degree they are required to keep, and this will reverberate in the degree of generated noise. In the experiment of the gaussian technique, where α represents the degree of noise, we change its value through the interval [0.001,1], to evaluate its impact on the performance, as presented in Fig. 2. it could be noted that there is a trade-off between the degree of noise and the segmentation DSC. In the experiment of the Laplace technique, where α denotes the scale factor, we changed its value through the interval [0.001,1], and calculated the DSC for each value, as shown in Fig. 3. Like gaussian experiments, it is notable that there is a trade-off between the privacy (noise) level and the segmentation performance (i.e. DSC). More specifically, once the degree level reaches the highest $\alpha = 1$, conforming to the highest degree of privacy, segmentation performance significantly degrades.

D. Comparative Analysis

In order to validate the efficiency and the effectiveness of the proposed FL framework (FL-Cov) for finetuning the COVID-19 segmentation performance of multi-institutional CT data, we propose to compare the FL-Cov approach (with $\tau = 15$ and $\alpha = 0.01$) against four different learning schemas that are non-federated in nature, and they are

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

Table I. Quantitative results (mean ± standard deviation) for 2019ncov lesion segmentation using different learning schemas.

	DSC↑				NSD↑			
Methods	***DS1***	***DS2***	***DS3***	***Total***	***DS1***	***DS2***	***DS3***	***Total***
Cross-DS1	-	84.3±15.1	81.3±11.1	82.80±13.10	-	81.8±14.8	80.3±17.5	81.05±16.15
Cross-DS2	82.3±11.4	-	86.9±14.3	84.60±12.85	80.1±14.5	-	87.2±10.7	83.65±12.60
Cross-DS3	83.4±10.2	86.8±10.4	-	85.10±10.30	81.8±14.6	85.3±9.3	-	83.55±11.95
Independent	82.1±8.9	86.1±9.9	87.1±8.9	85.10±9.23	80.9±10.3	84.9±11.1	87.1±11.5	84.30±10.97
Ensemble	82.9±10.2	85.9±11.4	88.1±9.7	85.63±10.43	80.3±8.7	84.1±9.7	88.1±10.5	84.17±9.63
FL-Cov	85.4±10.2	88.7±8.8	**91.8±8.3**	88.63±9.10	83.9±9.3	87.8±12.2	89.8±9.7	87.03±10.40
FL-Cov-AoS	87.1±6.8	**89.4±5.2**	89.8±8.2	88.77±6.73	82.4±11.3	**89.7±8.1**	**90.0±6.5**	87.37±8.63
FDG	**88.8±6.5**	88.8±6.4	90.7±8.1	89.43±7.00	**84.9±8.4**	88.6±8.7	89.9±6.5	87.80±7.87
Blend	85.3±13.3	87.7±11.1	89.5±12.8	87.50±12.40	82.6±7.1	86.8±12.9	88.8+5.1	86.07±8.37

Table II. statistical significance of the proposed FV-Cov against other learning schemas using DSC and NSD measures

Methods	***DS1***	***DS2***	***DS3***
DSC			
Independent	0.0091	0.0099	0.0032
Ensemble	0.0091	0.0211	0.0274
Blend	0.0612	0.0398	0.0475
NSD			
Independent	0.0184	0.0009	0.0032
Ensemble	0.0204	0.0011	0.0115
Blend	0.0581	0.0473	0.0421

summarized as follow. First, the segmentation network is trained and tested on each institutional data separately (**independent**); second, the segmentation network is trained on data from the specific institution and tested on CT data from another institution (**Cross**); third, all of the data from different institutions are aggregated together in a single location and used for training and testing (**Blend**); fourth, an ensemble DL framework is constructed utilizing the private models at diverse institutions (**Ensemble**). The Ensemble schema takes the mean of outcomes of an **independent** schema that is trained inside the institution and a Cross schema that is trained using data from different institutions. Independent and *Cross* schemas usually protect the privacy of CT data, yet they cannot include the data of other institutions. The Blend schema utilizes the entire CT data from various institutions, yet it cannot protect the privacy of the data. The segmentation performance of Blend schema is anticipated to gain much improvement compared to FL-Cov as it makes use of a complete set of CT data.

In an attempt to achieve fair performance comparison, we propose to select the optimal parameters for diverse learning schemas by changing the network as slightly as conceivable. Bearing in mind the heterogeneity of the data distribution, we attempted to employ the DA techniques discussed in the previous section to finetune the segmentation performance of *FL-Cov*. Accordingly, combining the AoS technique with the FL-Cov framework shapes the *FL-Cov-AoS* schema in which a private segmentation model is trained concurrently with the public federated network. On the other hand, integrating the proposed FL-Cov with a generative adaption form an additional schema called FDG schema, in which four discriminators network D employed to differentiate whether the CT scans of COVID-19 originated from the same domain or a different one. As a consequence of applying the randomization techniques in *FL-Cov*, the generated feature representation was distorted by the gaussian noises $\varepsilon_n\ (0, 0.01\sigma)$ is transferred to act as input for the discriminators D. The universal network was the concatenation of the generator G and the segmentation network SG. The parameters of the private $G\ and\ C$ only shared with the universal network. In the beginning, we train the $G\ and\ SG$ models for 10 epochs and broadcast the generative loss presented in equation (8). Following, the entire framework is trained using the same settings employed for FL-Cov training.

The comparative segmentation results are introduced in Table 3. Where the training data used in the *Cross* schema are written as 'Cross-<dataset site>'. The test result on the training dataset is not reported as the whole data from this site is used for training. More, taking into account performing the test on CT scans from the remaining institutions, thus we did not report a standard deviation (std) for Cross learning experiments. The segmentation results for the remaining schema are stated in the form of 'mean (std)'. According to the comparison between average DSC and NSD, we spotlight the optimal DSC and the optimal NSD score in Table I. It could be noted that the *Cross-learning* schema realizes higher DSC and NSD values compared to the independent schema when the amount of training data is lesser. This observation is clearly obvious for training on DS1 data. On the other hand, when the Cross-training was performed on the DS3 data,

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

the performance gets improved by 1.3% and 0.7% over the Independent learning schema on DS1 and DS2 respectively. Besides, the DSCs and NSDs of the *Ensemble* schema are not improved enough compared to the segmentation results of independent schema, possibly because the ensemble learning schema might not take the advantage of the decisions taken by a variety of segmentation networks (i.e. private models) and negatively impair the predictive capability.

With respect to FL-Cov, the average DSCs show great improvements (DS1:2%, DS2:2%, DS3:5%) over the Cross-learning schema for every institution. Also, it significantly achieves great DSC improvements (2%-5%) over both Independent and Ensemble schemas. Similarly, the average NSDs achieved by FL-Cov present significant improvements (DS1:2.1%, DS2:2.5%, DS3:25%) over the Ensemble learning. Also, the NSD of FL-Cov is greatly improved (2%-3%) over the Independent and Ensemble schemas. Moreover, compared to FL-Cov, the FL-Cov-AoS improved the DSC on DS1 and DS2 by 1.7% and 0.7% respectively; yet it reduced the DSC of DS3 by 1%. Similarly, the NSD of FL-Cov-AoS gets improved by 1.9% and 0.2% on DS2 and DS3 respectively, however, it gets decreased by 1.5%. Furthermore, the FDG improves the DSC by 3.4% on DS1 and realizes equal and less DSC on DS1 and DS2 correspondingly. The NSD of FDG gets improved by 1% on both DS1 and DS2 and attains comparable value on DS3 compared to the FL-Cov. The observed behavior of the DA technique might be reasoned by or depending on the distribution of data at different institutions. Finally, we experiment with the statistical significance of the FV-Cov compared to different Learning schemas using paired t-test, and the calculated p-values are presented in Table II. Where the p-value <0.05 means that the model is statistically significant. It could be seen that all of the p-values are less than 0.05 except for the Blend schema on DS1. This could possibly be caused by the small size of DS1.

E. Discussions

Though according to the experimental trial that demonstrates that the interaction stride, used to regulate the number of times the parameters of the private and universal networks get upgraded, did not influence the segmentation performance, we are unable to conclude that the stride parameter is unrelated. Extra wide-ranging stride values need to be scrutinized based on the underlying application. Also, we employed applied methods to study the PP technique. Nevertheless, the sympathy of the mapping function $h: D \rightarrow \mathbb{R}^m$, the U-Net in our situation, is problematic to approximate. Thus, we could not directly specify the limit ϵ. Later research [14] also established Laplace and Gaussian noise higher than a particular degree might be a perfect protection from data recovery invasion. Based on certain datasets or applications, it is possible to experimentally approximate an appropriate noise degree according to the attacking viewpoint too. Additionally, through our experiments, the averaging strategy is employed to calculate the model's outcomes in the Ensemble learning schema. For realizing improved performance in Ensemble schema, further innovative ensemble approaches can be employed, like a forest of randomization trees. We used the traditional U-Net as a segmentation network, further improved DL segmentation models can be investigated too.

We discovered that DA techniques are not permanently an advantageous addition to the FL-Cov. According to the performance results shown in Table I, we observe that DA techniques enhance the segmentation performance for some institutions yet not all. The reason for this could be that the present network upgrading policy is not ideal. according to this, we intend to first investigate the distribution of the latent representations of diverse institutions and followingly determine whether to employ the proposed FDG or not. Contrary to the FL-Cov where few numbers of contributors (institutions) exist, other FL systems, like Apple or Google writing recommenders, in which there exist a million FL contributors. Thus, the number of FL contributors could have an influential role here, particularly when the averaging policy is employed to upgrade the universal network. Integrating a furtherly improved network-election mechanism and upgrading policy might potentially assist in avoiding the inclusion of erroneous private networks in updating procedures.

5. CONCLUSIONS AND FUTURE WORK

This study introduces a privacy-protection framework for multi-institution COVID-19 infection segmentation by integrating two randomization techniques into a federated learning scheme. To tackle the problem of heterogeneity of data distribution at every institution, two techniques (i.e. AoS and generative domain adaption) are introduced to empower the performance of federated architecture. The segmentation performance has confirmed the benefit of utilizing the FL framework for multi-institution segmentation with no need for sharing CT data in comparison with other approaches. Also, the results show that the domain adaption help finetuning the FL model. In addition, the presented FL framework could be generalized to be a medical imaging tool for segmenting the disease lesions, especially those with a limited amount of data. For future improvements, there are several directions to be explored. First, experiment with the proposed framework on different medical images and different diseases. Second, the proposed framework could be extended to be trained in a semi-supervised manner to enable learning from unlabeled CT scans. A third direction is to integrate the proposed FL-Cov or FDG framework on the internet of medical things environment.

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

REFERENCES

[1] C. Wang, P. W. Horby, F. G. Hayden, and G. F. Gao, "A novel coronavirus outbreak of global health concern," *The Lancet*, vol. 395, no. 10223, pp. 470–473, Feb 2020.

[2] C. Huang, Y. Wang et al., "Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China," *The Lancet*, vol. 395, no. 10223, pp. 497–506, Feb 2020.

[3] T. Ai, Z. Yang et al., "Correlation of chest CT and rt-pcr testing in coronavirus disease 2019 (COVID-19) in China: A report of 1014 cases," *Radiology*, vol. 2019, p. 200642, Feb 2020.

[4] X. Ouyang, J. Huo, L. Xia, F. Shan, J. Liu, Z. Mo, *et al.*, "Dual-Sampling Attention Network for Diagnosis of COVID-19 from Community Acquired Pneumonia," *IEEE Transactions on Medical Imaging*, 2020.

[5] H. Kang, L. Xia, F. Yan, Z. Wan, F. Shi, H. Yuan, *et al.*, "Diagnosis of coronavirus disease 2019 (covid-19) with structured latent multi-view representation learning," *IEEE transactions on medical imaging*, 2020.

[6] X. Wang, X. Deng, Q. Fu, Q. Zhou, J. Feng, H. Ma, *et al.*, "A Weakly-supervised Framework for COVID-19 Classification and Lesion Localization from Chest CT," *IEEE Transactions on Medical Imaging*, 2020.

[7] J. Wang, Y. Bao, Y. Wen, H. Lu, H. Luo, Y. Xiang, *et al.*, "Prior-Attention Residual Learning for More Discriminative COVID-19 Screening in CT Images," *IEEE Transactions on Medical Imaging*, 2020.

[8] Z. Han, B. Wei, Y. Hong, T. Li, J. Cong, X. Zhu, *et al.*, "Accurate Screening of COVID-19 using Attention Based Deep 3D Multiple Instance Learning," *IEEE Transactions on Medical Imaging*, 2020.

[9] D.-P. Fan, T. Zhou, G.-P. Ji, Y. Zhou, G. Chen, H. Fu, *et al.*, "Inf-Net: Automatic COVID-19 Lung Infection Segmentation from CT Images," *IEEE Transactions on Medical Imaging*, 2020.

[10] W. Xie, C. Jacobs, J.-P. Charbonnier, and B. van Ginneken, "Relational modeling for robust and efficient pulmonary lobe segmentation in ct scans," *IEEE transactions on medical imaging*, 2020.

[11] Abdel-Basset, M., Chang, V., Hawash, H., Chakrabortty, R.K. and Ryan, M., 2021. FSS-2019-nCov: A deep learning architecture for semi-supervised few-shot segmentation of COVID-19 infection. *Knowledge-Based Systems*, *212*, p.106647.

[12] L. Zhou, Z. Li, J. Zhou, H. Li, Y. Chen, Y. Huang, *et al.*, "A Rapid, Accurate and Machine-agnostic Segmentation and Quantification Method for CT-based COVID-19 Diagnosis," *IEEE Transactions on Medical Imaging*, 2020.

[13] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, pp. 50-60, 2020.

[14] Xiaoxiao Li, Yufeng Gu, Nicha Dvornek, Lawrence H. Staib, Pamela Ventola, James S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," *Medical Image Analysis*, vol. 65, 2020.

[15] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, pp. 1-19, 2019.

[16] N. Lewis, H. Gazula, S. M. Plis, and V. D. Calhoun, "Decentralized distribution-sampled classification models with application to brain imaging," *Journal of neuroscience methods*, vol. 329, p. 108418, 2020.

[17] Guan, H., Liu, Y., Yang, E., Yap, P.T., Shen, D. and Liu, M., 2021. Multi-site MRI harmonization via attention-guided deep domain adaptation for brain disorder identification. *Medical Image Analysis*, *71*, p.102076.

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

[19] E. Ahn, A. Kumar, M. Fulham, D. Feng, and J. Kim, "Unsupervised Domain Adaptation to Classify Medical Images using Zero-bias Convolutional Auto-encoders and Context-based Feature Augmentation," *IEEE Transactions on Medical Imaging*, 2020.

[20] Y. Zhang *et al.*, "Collaborative Unsupervised Domain Adaptation for Medical Image Diagnosis," in *IEEE Transactions on Image Processing*, vol. 29, pp. 7834-7844, 2020, doi: 10.1109/TIP.2020.3006377.

[21] S. Zhao, B. Li, X. Yue, Y. Gu, P. Xu, R. Hu, *et al.*, "Multi-source domain adaptation for semantic segmentation," in *Advances in Neural Information Processing Systems*, 2019, pp. 7287-7300.

[22] L. Song, C. Ma, G. Zhang, and Y. Zhang, "Privacy-Preserving Unsupervised Domain Adaptation in Federated Setting," *IEEE Access*, vol. 8, pp. 143233-143240, 2020.

[23] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "Local differential privacy for deep learning," *IEEE Internet of Things Journal*, 2019.

[24] K. Chaudhuri, J. Imola, and A. Machanavajjhala, "Capacity bounded differential privacy," in *Advances in Neural Information Processing Systems*, 2019, pp. 3474-3483.

[25] O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional networks for biomedical image segmentation," in MICCAI. Springer, 2015, pp. 234–241.

[26] D. J. Shah, "Multi-source domain adaptation with mixture of experts," Massachusetts Institute of Technology, 2019.

[27] D. Peterson, P. Kanani, and V. J. Marathe, "Private federated learning with domain adaptation," *arXiv preprint arXiv:1912.06733*, 2019.

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022

[28] J. Ma, Y. Wang, X. An, C. Ge, Z. Yu, J. Chen, et al., "Towards Efficient COVID-19 CT Annotation: A Benchmark for Lung and Infection Segmentation," arXiv preprint arXiv:2004.12537, 2020.
[29] S. Morozov, A. Andreychenko, N. Pavlov, A. Vladzymyrskyy, N. Ledikhova, V. Gombolevskiy, et al., "MosMedData: Chest CT Scans With COVID-19 Related Findings Dataset," arXiv preprint arXiv:2005.06465, 2020.
[30] M. de la Iglesia Vayá, J. M. Saborit, J. A. Montell, A. Pertusa, A. Bustos, M. Cazorla, *et al.*, "BIMCV COVID-19+: a large annotated dataset of RX and CT images from COVID-19 patients," *arXiv preprint arXiv:2006.01174*, 2020.
[31] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu and V. Chang, "Trustworthy and Intelligent COVID-19 Diagnostic IoMT Through XR and Deep-Learning-Based Clinic Data Access," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15965-15976, 1 Nov.1, 2021, doi: 10.1109/JIOT.2021.3055804.
[32] 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," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9603-9610, 15 June15, 2021, doi: 10.1109/JIOT.2020.3013710.
[33] T. Kitrungrotsakul et al., "Attention-RefNet: Interactive Attention Refinement Network for Infected Area Segmentation of COVID-19," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 7, pp. 2363-2373, July 2021, doi: 10.1109/JBHI.2021.3082527.
[34] Y. Zhang, Q. Liao, L. Yuan, H. Zhu, J. Xing and J. Zhang, "Exploiting Shared Knowledge From Non-COVID Lesions for Annotation-Efficient COVID-19 CT Lung Infection Segmentation," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 11, pp. 4152-4162, Nov. 2021, doi: 10.1109/JBHI.2021.3106341.
[35] C. Li et al., "Self-Ensembling Co-Training Framework for Semi-Supervised COVID-19 CT Segmentation," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 11, pp. 4140-4151, Nov. 2021, doi: 10.1109/JBHI.2021.3103646.
[36] R. Wang, C. Ji, Y. Zhang and Y. Li, "Focus, Fusion, and Rectify: Context-Aware Learning for COVID-19 Lung Infection Segmentation," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 1, pp. 12-24, Jan. 2022, doi: 10.1109/TNNLS.2021.3126305.
[37] S. Yang et al., "Learning COVID-19 Pneumonia Lesion Segmentation From Imperfect Annotations via Divergence-Aware Selective Training," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 8, pp. 3673-3684, Aug. 2022, doi: 10.1109/JBHI.2022.3172978.
[38] H. Zhao et al., "SC2Net: A Novel Segmentation-Based Classification Network for Detection of COVID-19 in Chest X-Ray Images," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 8, pp. 4032-4043, Aug. 2022, doi: 10.1109/JBHI.2022.3177854.
[39] L. Song, C. Ma, G. Zhang and Y. Zhang, "Privacy-Preserving Unsupervised Domain Adaptation in Federated Setting," in IEEE Access, vol. 8, pp. 143233-143240, 2020, doi: 10.1109/ACCESS.2020.3014264.
[40] Y. Kang, Y. He, J. Luo, T. Fan, Y. Liu and Q. Yang, "Privacy-preserving Federated Adversarial Domain Adaptation over Feature Groups for Interpretability," in IEEE Transactions on Big Data, 2022, doi: 10.1109/TBDATA.2022.3188292.
[41] J. Liang, D. Hu, Y. Wang, R. He and J. Feng, "Source Data-Absent Unsupervised Domain Adaptation Through Hypothesis Transfer and Labeling Transfer," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 11, pp. 8602-8617, 1 Nov. 2022, doi: 10.1109/TPAMI.2021.3103390.
[42] W. Ding, M. Abdel-Basset, H. Hawash and O. M. Elkomy, "MT-nCov-Net: A Multitask Deep-Learning Framework for Efficient Diagnosis of COVID-19 Using Tomography Scans," in IEEE Transactions on Cybernetics, doi: 10.1109/TCYB.2021.3123173.
[43] M. Abdel-Basset, H. Hawash and V. Chang, "FV-Seg-Net: Fully Volumetric Network for Accurate Segmentation of COVID-19 Lesions from Chest CT Scans," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3146175.
[44] K. Shankar, Fuzzy Clustering and Classification based Iris Recognition: A Medical Application, American Journal of Business and Operations Research, Vol. 1, No. 1, 2020: 19-27 doi: https://doi.org/10.54216/AJBOR.010102
[45] Reem Atassi , Fuad Alhosban , Milan Dordevic, A New Data Fusion Model for Medical Image Encryption in IoT Environment, Fusion: Practice and Applications, Vol. 8, No. 1, 2022 : 16-26 doi : https://doi.org/10.54216/FPA.080102

Doi: https://doi.org/10.54216/JISIoT.070201
Received: May 28, 2022 Accepted: December 26, 2022