Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
A lightweight federated learning based privacy preserving 5G pandemic response network using unmanned aerial vehicles: A proof-of-concept

Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

PII: S1389-1286(21)00546-6
DOI: https://doi.org/10.1016/j.comnet.2021.108672
Reference: COMPNW 108672

To appear in: Computer Networks

Received date: 22 April 2021
Revised date: 8 November 2021
Accepted date: 30 November 2021

Please cite this article as: N. Nasser, Z.M. Fadlullah, M.M. Fouda et al., A lightweight federated learning based privacy preserving 5G pandemic response network using unmanned aerial vehicles: A proof-of-concept, Computer Networks (2021), doi: https://doi.org/10.1016/j.comnet.2021.108672.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2021 Published by Elsevier B.V.
Graphical Abstract

A Lightweight Federated Learning Based Privacy Preserving B5G Pandemic Response Network Using Unmanned Aerial Vehicles: A Proof-of-Concept

Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

Considered UAV-based B5G pandemic response network architecture exploiting heterogeneous links and federated learning.
Highlights

A Lightweight Federated Learning Based Privacy Preserving B5G Pandemic Response Network Using Unmanned Aerial Vehicles: A Proof-of-Concept

Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

- During the ongoing novel coronavirus disease (COVID-19) pandemic, much data are collected from mobile users for contact-tracing and other medical analytics purposes to both contain the pandemic and offer appropriate diagnostics and intervention, respectively. However, data privacy appears as a huge barrier to collecting data from the mobile users, given the complexity, heterogeneous Radio Access Technologies (RATs), and dynamically changing channel conditions of emerging 5G and beyond (B5G) networks. This paper addresses privacy-preserving challenges associated with the conventional data collection method and pushing the collected data to the cloud for analytics and emphasizes on the need for an alternative, distributed mechanism which addresses the privacy concern of the users.

- To provide a distributed privacy-preserving data collection and analytics framework at the same time, a federated learning-based framework is presented. This facilitates the exchange of wisdom of the underlying B5G mobile user data instead of explicitly sharing the raw data (e.g., location, mobility, health status, and so forth) with the central cloud.

- Asynchronous update of weights of local models is considered in the envisioned federated learning framework to significantly improve the B5G communication overheads. This facilitates lightweight decentralized model construction and execution at the resource-constrained mobile UEs and other distributed/local nodes (LNs).
A Lightweight Federated Learning Based Privacy Preserving B5G Pandemic Response Network Using Unmanned Aerial Vehicles: A Proof-of-Concept

Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouad, Asmaa Ali, Muhammad Imran

Abstract

The concept of an intelligent pandemic response network is gaining momentum during the current novel coronavirus disease (COVID-19) era. A heterogeneous communication architecture is essential to facilitate collaborative and intelligent medical analytics in the fifth generation and beyond (B5G) networks to intelligently learn and disseminate pandemic-related information and diagnostic results. However, such a technique raises privacy issues pertaining to the health data of the patients. In this paper, we envision a privacy-preserving pandemic response network using a proof-of-concept, aerial-terrestrial network system serving mobile user entities/equipment (UEs). By leveraging the unmanned aerial vehicles (UAVs), a lightweight federated learning model is proposed to collaboratively yet privately learn medical (e.g., COVID-19) symptoms with high accuracy using the data collected by individual UEs using ambient sensors and wearable devices. An asynchronous weight updating technique is introduced in federated learning to avoid redundant learning and save precious networking as well as computing resources of the UAVs/UEs. A use-case where an Artificial Intelligence (AI)-based model is employed for COVID-19 detection from radiograph images is presented to demonstrate the effectiveness of our proposed approach.
Keywords: 5G, Beyond 5G (B5G), federated learning, Unmanned Aerial Vehicle (UAV), pandemic, Artificial Intelligence (AI), edge computing.

1. Introduction

Recently, due to the devastating spread of the novel coronavirus (COVID-19) on a global scale [1, 2], researchers started exploring how to formulate intelligent pandemic response networks [3, 4]. Communication networks, particularly unmanned aerial vehicle (UAV)-integrated fifth generation and beyond (B5G) mobile networks, can be leveraged to construct agile pandemic response networks to disseminate pandemic recommendations, facilitate digital contact tracing, monitor the spread of the pandemic, and so forth. Incorporating intelligence into the UAVs using Artificial Intelligence (AI) techniques is, however, posing computational and privacy challenges. The surge of pandemic-related traffic will also lead to increasing the communication delay and overwhelm the backhaul links. Therefore, to construct an efficient UAV-based pandemic response network to complement the terrestrial cellular infrastructure for enhanced service coverage, collaborative learning by the UAVs [5] in a lightweight, as well as privacy-preserving manner, is essential.

Even though the drone resources for processing, memory, and battery have improved much recently, the UAVs are anticipated to still lack, in B5G networks, the resources to execute intelligent and coordinated learning based on the monitored and collected pandemic data of mobile users (UEs). Because maintaining privacy is a big concern for the acquired health data of the UEs, existing methods using explicit user reporting on their locations and pandemic data may not be directly adopted. It is worth clarifying the difference between the security and privacy of patient data. In the context of this paper, security typically implies safeguarding the data of the users/patients against unauthorized access of the information. On the other hand, the term privacy is harder to define since user-specific details (e.g., user/patient identity and other sensitive data) can also be secure data. In the context of our work, privacy focuses upon masking the user/patient-specific information. Thus, when the patients’ devices, referred to as UEs, communicate with the B5G terrestrial/aerial base stations (gNBs) and provide their raw radiograph images for pandemic data analytics, there are scopes for mapping back the
patient data to individual users and reveal their identities, whereabouts, living patterns, and so forth. The cloud-based analytics could also reveal certain information pertaining to the identification of the users [6]. The idea of this paper is to use an asynchronously updating federated learning framework to thwart such threats whereby the wisdom of the patients’ radiograph data are shared rather than the explicit images to train a central AI model without exposing the user-specific details in B5G networks. In this paper, by addressing the privacy challenge, we propose a collaborative learning method exploiting two-layer federated learning [7]. In our proposed technique, the general and specific weight parameters of the AI models locally learned in two layers (UEs and UAVs) are asynchronously updated to update the global AI model at the cloud, managed by hospitals and public health authorities. While reducing B5G network overheads, the proposed technique still allows the cloud to predict the appropriate pandemic features with reasonably high accuracy without the need to receive raw health data, locations, and other information of the UEs.

The key contributions of our work in this paper are outlined below.

1. To provide a distributed privacy-preserving data collection and analytics framework at the same time, a federated learning-based framework is presented. This facilitates the exchange of wisdom of the underlying B5G mobile user data instead of explicitly sharing the raw data (e.g., location, mobility, health status, and so forth) with the central cloud.

2. Asynchronous update of weights of local models is considered in the envisioned federated learning framework to significantly improve the communication overheads. This facilitates lightweight decentralized model construction and execution at the resource-constrained mobile UEs and other distributed/local nodes (LNs).

3. The need to seamlessly merge the asynchronously updating federated learning framework with the blockchain-enabled centralized aggregator is identified as an open research issue that will stimulate much work in the area of privacy-preservation of big medical data.

The remainder of the paper is structured as follows. Sec. 2 provides the related research endeavors for formulating pandemic response networks. Sec. 3 contains our considered network model, and then provides a formal problem description. Our proposed two-layer federated learning technique leveraging the asynchronous update of weights is delineated in Sec. 4. Sec. 5
presents the performance evaluation of our proposal based on a specific use-case. The future work and open research issues are discussed in Sec. 6. Sec. 7 concludes the paper.

2. Related Work

In this section, we survey the recent related work from two perspectives, i.e., the relevant progress in theoretical and applied federated learning in the context 5G/B5G networks, and then review contemporary works on exploiting such federated learning frameworks to combat COVID-19.

First, we aim to capture the recent endeavors on federated learning theories and their applications in 5G and beyond communication networks. The federated learning concepts with privacy issues were discussed in the recent research works in [8, 9, 10, 11, 12]. While the research in [13] surveyed federated learning concepts in 5G/B5G mobile edge networks by considering communication overheads, resource assignment, privacy, and security, other researchers investigated the systems diversity, privacy concerns along with communication costs in federated learning environments [14, 15]. The work conducted in [16] exploited homomorphic encryption, secure multiparty computing, and differential privacy to provide privacy-preservation in federated learning. However, this work and similar surveys in [17, 18] did not address the privacy issues implied in federated learning frameworks. Federated learning applications in 5G networks, along with their emerging challenges for B5G communications, were discussed in [19]. Categorization and security analysis of federated learning setups were elaborated in [20] while the privacy robustness and efficiency in the presence of an adversarial server was considered in [21]. An extensive investigation on privacy preserving federated learning was carried out in [22] that identified the potential privacy leakage risks in federated learning. However, most of these works are theoretical in nature and do not offer QoS (e.g., bandwidth and delay improvement) along with the implied privacy that are required for B5G networks as explored in the coauthor’s earlier work in [23] by leveraging the theoretical findings on customizing federated learning with asynchronous temporal features in [24]. Based on these recent advancement of federated learning and their various variants, a taxonomy is presented in Table 1 to demonstrate the suitability of federated learning frameworks in B5G networks.

Next, we review the existing federated learning applications, with a focus on combating COVID-19. Indeed, federated learning has been conceptual-
Table 1: A taxonomy of related research work on federated learning techniques and scenarios depicting their suitability in 5G networks.

| Reference       | Federated learning technique and scenario                                                                 | B5G-ready? |
|-----------------|----------------------------------------------------------------------------------------------------------|------------|
| [14, 8, 12, 18, 20, 22] | Horizontal, vertical, and hybrid data partitioning and/or cryptographic, perturbative, and anonymization techniques for privacy | No         |
| [16, 17, 13, 15, 9, 21, 11] | Specific focus on privacy-preservation in federated learning setups without any wireless communication parameter | No         |
| [22]            | Privacy leakage scenarios with external and external attackers, active/passive attacks, inference attacks | No         |
| [24]            | Temporally asynchronous weight update of federated learning                                               | No         |
| [19, 23]        | Federated machine learning to address energy, bandwidth, delay and data privacy concerns in wireless communications by performing decentralized model training | Yes        |

ized to revolutionize the smart healthcare landscape recently [25] due to its potential in bypassing the need for centralizing or releasing patient data and raising regulatory, ethical, legal, and even technical challenges. However, the application of federated learning for combating COVID-19 was not considered in this work. The work in [26] raised the importance of respecting and protecting patients’ privacy while collecting their health data for COVID-19 identification. Their work used federated learning to train COVID-19 models and compared performances with popular AI models, including ResNet18, MobileNet, and COVID-Net. These models were also compared with a similar federated learning model presented in [27], focusing on chest X-ray and CT (computed tomography) scan images with normal and COVID-19 samples. A recent endeavor from NVIDIA attempted to construct AI models to predict oxygen needs without the need to share data and devise a generalizable model regardless of geographical location, patient population or data size [28]. The work in [29] identified the generalizability issue in building AI models to gain trust from both patients and clinicians and implemented the
unified CT-COVID AI diagnostic initiative (UCADI) framework for federated learning. This initiative allows any research institution or hospital with data and computational resources to contribute their local model parameters to enrich the centralized learning framework’s performance. In this way, the data heterogeneity problem, a key challenge in AI diagnostics in terms of patient diversity, diagnostic image resolution, number of cases, and so forth, is also implicitly considered. In this way, the participants worldwide using UCADI are anticipated to assist health practitioners in detecting COVID-19 patients robustly and reliably. However, the aforementioned methods share an inherent shortcoming in both the system model used and the manner in which the AI models are shared, which restrict the performance of the federated learning technique. For instance, using these methods, the patients may not be able to preserve their privacy because of the need to explicitly share their raw data with hospitals or clinics, which are assumed to secure and perform the federated learning on behalf of the patients. On the other hand, the distributed/transfer learning methods [30] also lead to an exchange of content-specific data (i.e., health data) since they require the UEs to collaborate. Furthermore, the existing applications of federated learning to address the COVID-19 pandemic are yet to explore whether an asynchronous model updating paradigm could be used to boost the learning performance with much-improved network overhead. To mitigate the UEs’ privacy concern and significantly reduce network overhead, a novel proactive method is urgently required in aerial as well as terrestrial base stations.

3. Considered System Model and Problem Formulation

Fig. 1 summarizes our considered B5G network scenario, which comprises an integrated aerial and terrestrial network. Several UAVs act as aerial base stations to complement the terrestrial base stations (gNBs) to collaboratively serve user equipment/entities or UEs with an improved service coverage. Typically the UEs represent mobile users such as patients with smartphones, wearables, fitness trackers, and other smart devices monitoring health. For simplicity, in the remainder of the paper, the term UE will refer to users-smartphones capable of training local AI models and establishing an uplink with the aerial/terrestrial base stations to exchange the AI model parameters. Further exploiting this scenario and based on our earlier work in [31], the system model is envisaged as a software defined network (SDN) which manages the data, control, and application planes, as depicted in Fig. 2. Us-
ing this approach, the SDN controller may virtualize network management algorithms as applications on commodity hardware having various computing resources, such as centralized processing units (CPUs), graphics processing units (GPUs), Baseband Unit (BBUs) pool, and other computing resources to carry out the computation of routing, link scheduling, and other network management tasks for terrestrial and aerial base stations. To summarize, this system model is considered to efficiently manage the integrated aerial and terrestrial links. The SDN can manage the deployment, link quality, and topologies of the UAVs to permit them to adaptively operate in heterogeneous radio access technology (RAT) environments. Thus, the network management is quite flexible and can be easily upgraded simply by updating the corresponding applications. Furthermore, to enhance the usage of the computing resources, optimal caching placement can be done on the drones to store AI models received from many UEs and carry out their own learn-
How to provide AI-native edge computing functionality in B5G resource-constrained UEs aimed to reduce communication delay with centralized cloud, without compromising user data-privacy?

Figure 2: Proposed system model illustrating the B5G network data, control, and application planes.

The considered communication system model is delineated from hereon based on [32]. During every transmission time round, UE-side local training model parameters are transmitted to the centralized aggregator via terrestrial base stations and/or UAVs to converge to an accurate AI model in a distributed manner. The improved AI model is then periodically shared with the UEs. For each time round, uplink and downlink transmission overheads considering channels with Additive White Gaussian Noise (AWGN) are assumed [33, 34]. The communication rounds are assumed to continue until the global model converges with a reasonable performance measure. Based
on the radiograph images collected, the most relevant images are selected by the centralized aggregator for caching at the serving terrestrial base stations and UAVs. Let the UE, terrestrial base station, and UAVs represent the distributed or local computing nodes, referred to as local nodes (LNs) for brevity. Let $d_i$ denote the transmission rate of $UE_i$, which can be estimated as:

$$d_i = Bln(1 + \frac{Pt_i g_i}{\zeta}),$$

(1)

where $B$, $Pt_i$, $g_i$, and $\zeta$ denote the transmission bandwidth of the serving LN, transmission power of $UE_i$, channel gain of $UE_i$, and background noise power, respectively. We assume the same radiograph data-size, $\theta$ for all UEs.

Then, the transmission time, $T_{i_{Tx}}$, of a local model update with this data-size is expressed as:

$$T_{i_{Tx}} = \frac{\theta}{d_i}.$$  

(2)

Then, the time taken for one global iteration by $UE_i$, denoted by $T_{i_G}$ is given by:

$$T_{i_G} = log(\frac{1}{\epsilon_i})T_{i_L} + T_{i_{Tx}},$$

(3)

where $\epsilon_i$ refers to the local accuracy while $T_{i_L}$ denotes the computation time of a local iteration which will be described later. The caching entities of LNs are assumed to have finite storage. The LNs use their local learning models to make intelligent decisions on which radiographs should be cached. The cache is assumed to be able to store $m$ files of a constant size. Based on its local data, each LN is assumed to be able to independently calculate an update to the current global learning model and exchange the update to the centralized aggregator to aggregate a new global model. Each UE also trains a local dataset, which is generated from the radiographs, and can be co-trained with other structured data including different current activities, current location, contextual information derived from personal settings of mobile device sensors, and so forth. It is worth noting that each LN, particularly each UE, may have an individual context space. The local learning model in each UE and LN is based on Convolutional Neural Network (CNN) which will be described in Sec. 4. The local learning model update of $UE_i$ is impacted by the quality of its locally available data that can be expressed as the local accuracy, $\epsilon_i$. If the value of $\epsilon_i$ is high, we need to perform fewer local (as well as global) iterations bounded by $log(\frac{1}{\epsilon_i})$. This can be used to predict the content popularity more precisely and quickly. Now, we describe
the computation time of a local iteration, denoted by $T_{iL}$, in the local model training for $UE_i$ as follows:

$$T_{iL} = \frac{s_i c_i}{f_i},$$

where $s_i$ denotes the size of the local data of $UE_i$. The CPU cycle and number of CPU cycles needed to conduct the local model training with the sample-size $s_i$ are denoted by $f_i$ and $c_i$, respectively.

In the scenario presented in the preceding section, the small cell UEs, which are served by a terrestrial or aerial base station, participate in pandemic learning such as COVID-19 data collection regarding the user’s symptoms and vitals (e.g., temperature, heartbeat, blood oxygen saturation), travel history (e.g., through geolocation sensing), radiograph monitoring using emerging portable devices, and so forth. The users should not provide raw data to the aerial base stations or the cloud to avoid potential privacy breaches. In addition, the aerial base stations, despite their potential to extend 5G network coverage, are particularly useful for remote/rural locations and pandemic-affected sites where small cells are already prone to experiencing network congestion. Let us consider only those UAV nodes with sufficient energy budget during their flight. With the aforementioned scenario, the terrestrial and UAV base stations require a distributed methodology to learn pandemic features (e.g., COVID-19 symptoms, pneumonia classification using radiographs, and so forth) with privacy preservation to maximize the learning accuracy. Because the base stations lack a global view of UEs in various small cells, how they may leverage the proposed system model in Fig. 2 to perform decentralized machine learning without collecting the raw health data of the users arises a challenge. In this vein, the base stations collect the local training model from the UEs, and share this information with other base stations and then the cloud to further boost the decentralized training among UAVs. The cloud, upon receiving the locally trained models at the UE layer as well as the UAV layer, can then train a global model to arrive at a reasonable decision with significantly high accuracy. In other words, this is a two-layer federated learning problem. The objective is to minimize a loss function:

$$\min \sum_{i=1}^{N} \frac{S_i}{S} f_i(w, x_k, y_k),$$

where $f_i(w, x_k, y_k)$, $S_i$, and $S$ denote the loss function of $UE_i$, the sample size (locally monitored/acquired health data) of $UE_i$ and the training
samples used by the cloud. Every UE consists of a weight vector, $w$, which represents its locally trained AI model parameters using $x_k$ and $y_k$. The value of $f_i(w, x_k, y_k)$ increases with growing prediction error $(x_k^\top w - y_k)$. Therefore, the constraint $w_1 = w_2 = \ldots = w_k$ is needed to guarantee the convergence of global learning such that all UEs, UAVs, and the cloud can eventually derive the same AI model without explicitly exchanging the raw health data of UEs. Furthermore, in the context of the pandemic, there are two types of UEs considered in the considered system model, namely the individual UE type and the organizational UE type. The individual UEs do not have the capability of collecting certain information (e.g., X-ray images as mentioned) with their simple device type, and in this case the collected information constitutes their location, movement, body temperature, blood-oxygen saturation, and so forth. On the other hand, the organizational UEs such as a caregiver’s system (e.g., a hospital EMR system) or biomedical equipment with IoT capability are assumed to have the capability of sensing/acquiring other information such as X-ray images as presented in the performance evaluation scenario.

To summarize, the research challenge is to design a technique so that (1) each UE is capable of training a shared global model with its local model update based on its data, and (2) each UE shares its updated local model with the cloud through the aerial base stations to revise/update the global model. Similarly, the aerial base stations confront their own local model training problem to predict UEs’ pandemic patterns and participate in second-level federated learning with the global model. Until the loss function is minimized and/or the global model accuracy is deemed reasonable, this distributed training process needs to continue. Therefore, how to design such a decentralized technique with reduced network overhead and privacy-preservation property can be regarded as the main research problem of our work in this paper.

4. Proposed Asynchronous Updating Federated Learning for Pandemic Response Network

The fundamental idea of our proposal is to allow the UEs, constrained by small computational capacity, to train and build localized AI models based on the monitored health data of the user. The UEs participate in the first layer of federated learning to make this possible. Furthermore, the AI model parameter exchange of our proposed system, as shown in Fig. 2, orchestrates a
Terrestrial small cell base station (TSC<sub>k</sub>)
Aerial base station (UAV<sub>j</sub>)
SINR with TSC<sub>k</sub> is lower than threshold
Congestion at TSC<sub>k</sub>
Train initial global AI model
Hospital cloud
Sense pandemic/disease symptoms and relevant features using sensors and wearables
Mobile/rural UEs lacking terrestrial service (UE<sub>i</sub>)
Cannot exchange models with TSC<sub>k</sub>
Request for AI model when SINR with UAV<sub>j</sub> is acceptable
Initialize local model with vector w, control flag checkShallow = true, minibatch size B, epochs e
Use stochastic gradient descent (SGD) with learning parameter η
Send shallow model parameters because checkShallow = true
Send small-sized shallow model parameters because checkShallow = true
Set checkShallow = false
Send large-sized deep model parameters because checkShallow = false
Aggregate received models to revise global model to share with terrestrial and aerial Base stations
Updated global model receiving interval
Updated global model
Figure 3: Proposed algorithm.
proactive pandemic feature learning algorithm leveraging a second-layer federated learning with the collaboration of UAVs to acquire pandemic model-specific information from the UEs of small cells when the terrestrial base stations are either congested or unable to provide service coverage to UEs due to geographical barriers (e.g., in rural/remote locations). To discover the hidden features from complex pandemic/health data, we utilize a customized convolutional neural network (CNN) to build the AI model at UEs, UAVs, and the cloud [35, 36]. For the UE-generated local AI models, shallow and dense layers are considered to be smartly scheduled for transmission to the serving aerial base station to reduce network overhead. This approach is different from the traditional federated averaging [7], where the parameters of the entire deep neural network are updated at a single shot. This traditional model update process results in large communication overheads. On the other hand, an asynchronous parameter update methodology, inspired by the work in [37, 30] may deal with this problem as follows. The shallow layer (general) parameters acquire general features of the pandemic while the deep layer parameters, big in size, capture specific features regarding specific symptoms and context information of the users. Consequently, the shallow layer weights can be updated and exchanged more often compared to deep layer-parameters. This asynchronous weight updating methodology is shown in the algorithmic steps of Fig. 3.

First, we discuss the local model update at \( UE_i \) in Fig. 3. The proposed algorithm has three inputs: the UE identifier \( i \), the weight vector of the UE-generated model \( w \), and a control flag \( \text{checkShallow} \). The collected health data of the pandemic and context information are split into mini-batches, and \( B \) represents the mini-batch size. \( \epsilon \) denotes the epoch of the local model. The control flag \( \text{checkShallow} \) is exploited to select whether all the layers or the shallow layers will be updated. Stochastic Gradient Descent (SGD) is used \( w = w - \eta * \nabla l(w; b) \). Here, \( \eta \) and \( b \) refer to the learning rate and minibatch, respectively. On the other hand, the aerial base station, \( \text{UAV}_j \), polls the UEs by initializing a clock, in synchronization with the UEs and the cloud. \( \text{UAV}_j \) receives the timestamp for each of the UEs it serves. Then, \( \text{UAV}_j \) starts a temporary buffer. Using the timestamp information, \( \text{UAV}_j \) makes a decision to execute either the shallow or deep parameters update. Then, for each round, the UAV polls its served UEs (\( UE_i \) to \( UE_k \) where \( i \) is an index between 1 and \( k \)) and receives the relevant parameters from \( UE_i \) given the current timestamp and the \( \text{checkShallow} \) control variable. Next, \( \text{UAV}_j \) appends the parameters received from \( UE_i \) to the buffer. After
polling all the UEs, this buffer contains the information of shallow-only or complete weight vector parameters for the UEs served by that UAV. As shown in Fig. 3, the shallow-only/deep parameters are sent during the flag switch interval, which is considered to be much smaller than the updated global model receiving interval of each UE. The content of the buffer is then sent to the cloud. UAV \( j \) also locally executes its deep learning structure for predicting pandemic trends in collaboration with the neighboring UAVs. Then, the UAV continues to poll the UAVs again in the same manner until the model accuracy becomes reasonable.

At the cloud-end, the temporally weighted aggregation occurs over multiple communication rounds [37]. The timestamps for general and specific weights/parameters are initialized. The federated learning takes place in each round \( T \), which is split into \( \Delta \) time-slots. Before each round, the cloud exchanges the timestamp list it initialized for each UE to the serving base station. Then, for each round \( T \), the time-slots which are in \( \delta \) (the set of time-slots during which specific parameters are fetched from UEs), the control variable \( \text{checkShallow} \) is set to true. A participating subset of the clients is randomly selected per round. The specific and general parameters are fetched from each base station. Thus, the aggregation is performed to update the shallow and deep parameters (\( w_g \) and \( w_s \), respectively).

Based on these steps, we present the two algorithms for our envisioned asynchronous federated learning model for privacy-preserving COVID-19 screening, namely Algorithms 1 and 2. The global and local AI models, constructed at the cloud and aerial base station/terrestrial base station/UE, respectively, are facilitated by either a custom ANN (artificial neural network) model or a customized CNN model developed in our earlier work to carry out a centralized COVID-19 prediction [38].

First, we describe Algorithm 1 used for training the initial global AI model. This algorithm accepts the set of all available UAVs, terrestrial small cell base stations (TSCs), and UEs. The objective of the algorithm is to return \( M_g \), the trained global model. The algorithm parameters are initialized in step 1. The elements of the set of all the local or distributed nodes (i.e., the distributed learning agents in terms of the deployed UAVs, TSCs, and UEs), referred to as \( LN \), is iterated through steps 3 to 5. Thus, the parameters obtained from the distributed nodes can be aggregated. The aggregated parameters are then shared with the distributed nodes by the cloud. Learning continues until the learning performance in terms of loss is improved compared to a pre-determined threshold, \( (\text{min} \text{loss}) \), in step 7 of Algorithm 1.
Algorithm 1: Centralized asynchronous learning at the hospital cloud that aggregates the learning parameters.

**Input**: Set of all local nodes $LN$ (UAVs, TSCs, and UEs), $\text{min}_\text{loss}$ (performance threshold)

**Output**: $M_g$ (global trained model)

1. $M_g \leftarrow \emptyset$
2. while true do
   3. for $u=1$ to length($LN$) do
   4. update $M_g$ by aggregating the received parameters ($W_u$) from $LN_u$
   5. end
   6. $\text{curr}_\text{acc} \leftarrow$ access the current performance of global model $M_g$
   7. if ($\text{curr}_\text{loss} \leq \text{min}_\text{loss}$) then
   8. break
   9. end
10. end
11. return $M_g$

Next, Algorithm 2 is presented to execute the distributed learning on the LN’s side. The inputs of the algorithm consist of $u$, $\Delta$, $T$, and $\lambda$. Throughout the first three steps, the required parameters related to the algorithm and the local model ($M_u$) is set to selected values. Following this, a binary parameter, referred to as the contextual switch and denoted by $cs_u$, is set to false. In the subsequent step, the data size of each radiograph data is evaluated by setting the instance and feature sizes as $d_r$ and $d_c$, respectively. Then, the new data is loaded and standardized as:

$$Z = \frac{(X_u - \bar{X}_u)}{\sigma_u},$$

where $X_u$ indicates the data after performing resizing, $\bar{X}_u$ denotes the mean value of the data, and $\sigma_u$ refers to the standard deviation.

Step 9 of Algorithm 2 signifies that the training process at each LN takes place over $t = 1$ to $t = T$ iterations, where $T$ denotes the number of time-steps during which the whole process at each LN is executed once. After $\Delta$ time rounds, when the condition for setting the switches on is verified in step 10, the contextual switch ($cs_u$) is set to true. Then, an alert is triggered.
Algorithm 2: Learning at the local nodes LN's.

Input: $u$ (the current LN), $\Delta$ (time round), $T$ (total number of iterations), $\lambda$ (deep parameter exchange rate, $0 < \lambda < 1$)

1. initialize model: $M_u \leftarrow \emptyset$
2. choose the values for hyperparameters such as epochs ($\eta$), batch-size ($B$), activation function ($\Omega$)
3. initialize timestep $u$ to 0 and send to cloud
4. $cs_u \leftarrow$ false
5. $d_r, d_c \leftarrow$ initialize data dimension
6. $X_u \leftarrow$ load new data
7. $X_u \leftarrow$ resize $X_u$ by adopting the dimension ($d_r, d_c$) and then applying standardization
8. $X_u \leftarrow$ update by utilizing standardization defined in Eq. (6)
9. for ($t=1$ to $T$) do
10. \hspace{1em} if ($t \bmod \Delta = 0$) then
11. \hspace{2em} $cs_u \leftarrow$ true
12. \hspace{2em} generate automatic alert for turning on the physical switch
13. \hspace{2em} $block_u \leftarrow$ store data access information
14. \hspace{2em} $M_u \leftarrow$ update the model of LN$_u$ by adopting the model hyperparameters (e.g., $\eta$, $B$, $\Omega$)
15. \hspace{2em} if $cs_u = true$ then
16. \hspace{3em} $t$ is assigned to timestep$_u$
17. \hspace{3em} $W_u \leftarrow$ extract local weights of $\lambda$ from $M_u$
18. \hspace{3em} transmit $W_u$, $block_u$, and timestep$_u$ to the cloud
19. \hspace{3em} $cs_u \leftarrow$ false
20. \hspace{3em} generate automatic alert for turning off the physical switch
21. \hspace{2em} else
22. \hspace{3em} $W_u \leftarrow$ extract local weights of $(1 - \lambda)$ from $M_u$
23. \hspace{3em} transmit $W_u$ to the cloud
24. \hspace{2em} end
25. end
26. delete $X_u$ from storage

To activate an optional, physical switch. Next, in step 14, the data access information for LN$_u$ is stored in a dedicated block ($block_u$). The local model
is trained by adopting the selected hyperparameters in step 15 of Algorithm 2. Steps 16 to 21 are executed while flag $cs_u$ is true. Through these steps, the local weight ($W_u$) with shallow parameters and relevant access and time-step information ($\text{block}_u$, $\text{timestep}_u$) are shared with the cloud. The parameter $\alpha$ refers to the rate of the deep parameters exchange. The parameter $\text{timestep}_u$ holds the iteration information when the deep parameter exchange with the cloud occurs. Through steps 20 and 21, $cs_u$ is set to false. This is done to avoid unauthorized transmissions. Furthermore, an on-display alert is generated at the LN for the LN manager to turn off the physical switch until the next time round commences. If $cs_u$ is false, the shallow parameters of $(1 - \alpha)$ ratio from the local model ($M_u$) are shared with the cloud. On completion of the training over $T$ time-steps, the already employed data ($X_u$) is permanently removed from the cache to prevent possible breaches of user data in the future.

From hereon, we analyze the convergence performance of the proposed asynchronously updating federated learning to address the original optimization problem. The centralized aggregator transmits the model parameters $g = w$ to LNs to initialize and train their respective localized AI models. The UEs, TSCs, and UAVs selectively exchange shallow-only and deep parameters using Algorithm 2 such that the update of each LN's local model parameter $w_i$ depends on the global model $g$ while the update of the global model $g$ relies on all LNs' local federated learning models. The update of the local model $w_i$ depends on the learning algorithm such as Gradient Descent, Stochastic Gradient Descent (SGD), or Randomized Coordinate Descent (RCD). The update of the global model $g$ is obtained as \( \sum_{i=1}^{N} K_i w_i \). The update of LN$i$’s local model $w_i$ at time $t$ is expressed as:

$$w_{i,t+1} = g_t - \eta \sum_{k=1}^{S_i} \nabla f(g_t, x_{ik}, y_{ik}), \quad (7)$$

where $\eta$ denotes the learning rate and $\nabla f(g_t, x_{ik}, y_{ik})$ represents the gradient of $f(g_t, x_{ik}, y_{ik})$ with respect to $g_t$.

Assuming that $F(g) = \frac{1}{N} \sum_{i=1}^{N} \sum_{k=1}^{S_i} f(g, x_{ik}, y_{ik})$ and $F_i(g) = \sum_{k=1}^{S_i} f(g, x_{ik}, y_{ik})$, the update of global model $g$ at time $t$ can be given by:

$$g_{t+1} = g_t - \eta(\nabla F(g_t) - \lambda). \quad (8)$$

Here, $\lambda = \frac{\sum_{i=1}^{N} K_i a_i w_i C(w_i)}{\sum_{i=1}^{N} K_i a_i C(w_i)}$, where $C(w_i)$ is 1 if a resource block is assigned to LN$i$ for transmitting its local model parameters with sufficient
transmit-energy. Then based on the work [39], the federated learning algorithm converges to an optimal global model $g^*$ after the learning steps in Algorithm 2. Interested readers may view the proof of the expected convergence rate in [39].

5. Performance Evaluation

To synthesize the dataset required for experiments, DJI Matrice 300 RTK drone with URUAV GRAPHENE 6S 22.2V 6000mAh 100C Lipo Battery XT90 [40] having an energy capacity of 133.2Wh has been considered in this work. This battery is commonly used for heavy-duty tasks such as local AI model training. The drone has a flight time of 15 minutes which is considered enough to offload information from mobile UEs not having access to TSCs due to lack of infrastructures or overburdened TSCs. Up to 10 drones are considered in the simulation. In other words, the number of LNs is varied between 2 to 10 in the conducted simulations.

To demonstrate the performance of our envisioned asynchronously updating federated learning model, a public repository of X-ray images with COVID-19, pneumonia, and normal chest X-ray images is employed. Compared to the existing work dealing with small datasets, we prepared a large and robust dataset by merging four different existing datasets consisting of Posteroanterior (PA) chest X-rays based on the coauthors’ earlier work in [38]. It is worth noting that the hyperparameter tuning of the underlying ANN and CNN models was done in our earlier work [38]. As for the hyperparameter tuning of our presented federated learning setup, the tuning of deep/shallow parameter exchange ratio/interval is considered for hyperparameter optimization. According to the underlying AI model, two variations of the proposed asynchronously updating federated learning models are simulated based on ANN and CNN, which we refer to as Fed-ANN and Fed-CNN, respectively, for clarity. Furthermore, we define the iteration and time round for evaluating the performance of our proposal. An iteration refers to the number of times the whole process runs (e.g., the local training for the LNs and exchanging parameters). On the other hand, a time round consists of multiple iterations, after which the cloud is updated with the deep weights. In other words, an iteration is an atomic unit relative to the time round. For instance, if the number of iterations is 20 and the number of time rounds is 5, then for the 5th, 10th, 15th, and 20th iteration, the deep model update is triggered in our proposed approach while the shallow model parameter
update takes place during the other iterations. The number of iterations was set to 20, considering the learning loss converged in all considered cases. For all the simulations, the epoch-size and batch-size were set to 50 and 16, respectively. The exponential linear unit (ELU) was employed as the activation function, while Adagrad was used as the optimizer to select and regularly update a preconditioned stochastic gradient descent smartly. For the Fed-ANN model, a fully connected layer followed by the output layer was considered. On the other hand, the Fed-CNN model consists of three convolution layers, followed by three fully connected layers and the output layer.

Table 2 demonstrates the comparison of Fed-ANN and Fed-CNN models for 2 to 10 LN in 10 vari 10 varing time rounds during the learning phase. The Fed-ANN's best accuracy is 92.88%, which takes 27 iterations to converge, requiring 15 time rounds. On the other hand, Fed-CNN requires 50 iterations and yields a higher COVID-19 prediction accuracy (94.83%), consuming only 10 time rounds.

Fig. 4 compares the learning accuracy and loss of the Fed-ANN and Fed-CNN architectures over different time rounds varying from 5 to 20. Notice from Fig. 4a that both models’ learning accuracy is over 90% at the fifth time round. Both the variations of our proposal gain higher accuracies with the increasing number of time rounds. However, the Fed-CNN model exhibits superior performance for all the time rounds. This is also illustrated in learning loss, in terms of the mean squared error (MSE), in Fig. 4b.

Next, the impact of iterations on the learning loss performances of Fed-ANN and Fed-CNN is investigated in Fig. 5. Both Fed-ANN and Fed-CNN demonstrate improvement in the learning with an increasing number of iterations. However, the Fed-CNN model shows a much faster convergence trend, indicating its viability as the candidate deep learning technique for the proposed federated learning framework.

In Fig. 6, we compare the required execution time and memory requirement for the training phase for the proposed Fed-ANN and Fed-CNN models. While these overheads incurred by Fed-ANN are lower than that of the Fed-CNN model during training, the accuracies in the testing phase between these models as well as the centralized benchmark algorithm [38] are found to be quite similar, as demonstrated in Table 3. Thus, there is a slight tradeoff between the accuracy and overhead between our proposal’s two variations (i.e., Fed-ANN and Fed-CNN), which demonstrates Fed-CNN as the most suitable technique for the COVID-19 detection task.

Finally, Fig. 7 shows how our proposed asynchronous weight update
Table 2: Performance comparison of federated learning architectures for a varying number of users and time rounds (learning phase).

| Number of LNs | Fed-ANN | Fed-CNN | Fed-ANN | Fed-CNN |
|---------------|---------|---------|---------|---------|
|               | Time round | Iterations to converge | Accuracy | Loss | Time round | Iterations to converge | Accuracy | Loss |
| 2             | 15       | 6       | 0.8968  | 0.0629 | 10       | 6       | 0.9477  | 0.0293 |
| 4             | 10       | 10      | 0.9038  | 0.0599 | 10       | 16      | 0.9456  | 0.0314 |
| 6             | 10       | 16      | 0.9157  | 0.0561 | 5        | 27      | 0.9468  | 0.0309 |
| 8             | 10       | 26      | 0.9208  | 0.0527 | 10       | 31      | 0.9444  | 0.0320 |
| 10            | 15       | 27      | **0.9288** | 0.0507 | 10       | 50      | **0.9483** | 0.0290 |

![Figure 4: Accuracy over time rounds.](a) Accuracy over time rounds. ![Figure 4: Loss over time rounds.](b) Loss over time rounds.

The method reduces the network overhead. In this case, 20 rounds are considered, which are enough to demonstrate the overhead reduction performance. Notice that with the larger deep parameter rates, a more overhead reduction is possible by performing more generic parameter exchanges from the local model using the LN to the cloud and only transferring the specific parameters after a relatively high number of time rounds.

6. Future Directions and Open Issues

In this section, we highlight the open issues and the benefits that the proposed approach has in the B5G context, and then describe the future directions to introduce further security/privacy augmentations that were beyond the scope of the current work.
As discussed in Section 2, only few federated learning techniques started to focus on considering the QoS improvement issue along with privacy-preserving federated learning that is critical for B5G network users in UAV-served tiny cells where competition for bandwidth will be immense despite the high bandwidth capacity. The proposed work provides a proof-of-concept demonstrating how asynchronously updating weights of the locally trained...
Figure 7: Overhead reduction for the federated learning asynchronous update method over different time rounds and deep parameter exchange ratios.

Table 3: Performance comparison among diverse AI methods (testing phase).

|               | Accuracy | Precision | Recall | F1-score |
|---------------|----------|-----------|--------|----------|
| Centralized deep learning Benchmark | 0.94630 | 0.94513 | 0.94352 | 0.94433 |
| Fed-ANN       | 0.91914 | 0.91763 | 0.91914 | 0.91419 |
| Fed-CNN       | 0.93891 | 0.93773 | 0.93891 | 0.93557 |

depth and shallow models can be efficiently scheduled to significantly reduce the overhead reduction while attaining reasonable execution time and memory use as well as achieving high learning accuracy. This is particularly important for emerging health applications for distributed processing and analytics on users’ electronic health records, locations, and biomedical image data as demonstrated in the COVID-19 usecase in this paper. The opportunistic use of the temporal synchronization in a smart manner, thus, enlarges the scale of training data with resource-constrained and highly mobile B5G mobile under dynamically changing RAT conditions, and at the same time, protects the privacy of the user data.

As an open research issue, we provide a theoretical argumentation, in a high-level manner, describing possible integration of the Blockchain technol-
ogy and/or methods to enable Blockchain-based applications with the proposed asynchronously updating federated learning framework. This is due to the fact that the security of local parameters, the learning quality, and the varying computing and communication resources, remain unexplored topics in the existing federated learning schemes [41] including our proposal. Blockchain is an advanced technology which has modified the ways to store, exchange, and record the data using a public ledger so that the transactions are immutable [42, 43, 44]. On the other hand, the aim of federated learning is somewhat limited to applications orchestrated by the centralized aggregator as demonstrated in Algorithm 1. Hence, the robustness of the centralized aggregator relies upon the secrecy performance and resiliency of the central server. In other words, the aggregator may act as a single-point-of-failure by jeopardizing the entire federated learning framework [45]. Furthermore, despite the local data from LNs not being shared explicitly in their original format, knowledgeable adversaries may approximate the raw data reconstruction during the aggregation process [45]. Thus, privacy leakage may occur during model aggregating by outsider threats [46]. Also, concealing the COVID-19 training data may present the malicious users with an opportunity to inject backdoors into the trained model [45, 47]. Researchers are recently considering adversarial models whereby an attacker may be able to inject backdoors to the trained model during federated learning, and then can leverage the backdoor to make the model misclassify at a later time. In the future, how more seamless integration between asynchronous federated learning and blockchain should be integrated needs to be carefully investigated to avoid the aforementioned open research issues. Furthermore, this work can be considered as proof-of-concept and can be extended toward other pandemic monitoring given that the dataset is available from public health agencies and other relevant organizations at the national level.

Next, because of the heterogeneous resources and capabilities of different RATs and UEs in B5G networks, the selection of participating nodes (e.g., a mobile UE as opposed to a more powerful UAV node or a even more powerful terrestrial gNB) may have a dominating impact on the performance and convergence-time of federated learning. Furthermore, in the global model aggregator/server-side, initialization level of the global model and fine-tuning parameters such as the duration for each iteration, as well as duration for local model exchange for deep/shallow parameters, need to be taken into account in the future.
7. Conclusion

In this paper, we highlighted the importance of formulating an intelligent pandemic response network, particularly during the ongoing pandemic of COVID-19. We presented a drone-based heterogeneous computing system model to support the patient/user entities or user equipment (UEs), which have the capability of collecting their health data but are not bound to sharing the collected data with the drones/other base stations to be delivered to the central cloud managed by the public health authority and/or other hospitals. Instead, they share the wisdom with the network entities in more frequent, small-sized locally trained shallow model parameters and infrequent, heavy deep, or specific model parameters regarding their monitored health data. On the other hand, the UAVs poll each UE systematically, exchange them further with other UAVs, and forward the models to the cloud. They also help, in addition to terrestrial base stations, to deliver the updated global model to the UEs. Using this smart technique, the user data’s privacy is inherently respected, and the network overhead is significantly reduced. Through the performance evaluation on a particular use-case using X-ray images containing COVID-19, pneumonia, and normal samples, the effectiveness of two variants of our proposed asynchronously updating federated learning approach demonstrated the effectiveness as a viable pandemic response network methodology.

Acknowledgment

Authors would like to thank AlFaisal University for funding and supporting this work through the Internal Research Grant IRG21207.

References

[1] Z. Fadlullah, M. M. Fouda, A. S. K. Pathan, N. Nasser, A. Benslimane, Y. D. Lin, Smart IoT solutions for combating the COVID-19 pandemic, IEEE Internet of Things Magazine 3 (3) (2020) 10–11. doi:10.1109/MIOT.2020.9241464.

[2] T. Tazrin, M. M. Fouda, Z. M. Fadlullah, N. Nasser, UV-CDS: An energy-efficient scheduling of UAVs for premises sterilization, IEEE Transactions on Green Communications and Networking (2021). doi:10.1109/TGCN.2021.3074536.
[3] COVID watch | pandemic response network.
URL https://pandemicresponsenetwork.org/

[4] COVID-19 pandemic response network - full text view.
URL https://clinicaltrials.gov/ct2/show/NCT04320862

[5] F. Tang, Z. M. Fadlullah, B. Mao, N. Kato, F. Ono, R. Miura, On a novel adaptive UAV-mounted cloudlet-aided recommendation system for LBSNs, IEEE Transactions on Emerging Topics in Computing 7 (4) (2019) 565–577. doi:10.1109/TETC.2018.2792051.

[6] S. Sakib, M. M. Fouda, Z. M. Fadlullah, N. Nasser, On COVID-19 prediction using asynchronous federated learning-based agile radiograph screening booths, in: 2021 IEEE International Conference on Communications (ICC), 2021.

[7] K. Bonawitz et al., Towards federated learning at scale: System design, ArXiv abs/1902.01046 (2019). arXiv:1902.01046.

[8] J. hua Li, Cyber security meets artificial intelligence: a survey, Frontiers of Information Technology & Electronic Engineering 19 (2019) 1462–1474.

[9] H. C. Tanuwidjaja, R. Choi, K. Kim, A survey on deep learning techniques for privacy-preserving, in: X. Chen, X. Huang, J. Zhang (Eds.), Machine Learning for Cyber Security, Springer International Publishing, Cham, 2019, pp. 29–46.

[10] A. Wang, C. Wang, M. Bi, J. Xu, A review of privacy-preserving machine learning classification, in: X. Sun, Z. Pan, E. Bertino (Eds.), Cloud Computing and Security, Springer International Publishing, Cham, 2018, pp. 671–682.

[11] D. Zhang, X. Chen, D. Wang, J. Shi, A survey on collaborative deep learning and privacy-preserving, in: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 2018, pp. 652–658. doi:10.1109/DSC.2018.00104.

[12] L. Lyu, H. Yu, Q. Yang, Threats to federated learning: A survey, CoRR abs/2003.02133 (2020). arXiv:2003.02133.
URL https://arxiv.org/abs/2003.02133

25
[13] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. T. Niyato, C. Miao, Federated learning in mobile edge networks: A comprehensive survey, IEEE Communications Surveys & Tutorials 22 (2020) 2031–2063.

[14] Q. Li, Z. Wen, B. He, A survey on federated learning systems: Vision, hype and reality for data privacy and protection, ArXiv abs/1907.09693 (2021).

[15] T. Li, A. K. Sahu, A. S. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, IEEE Signal Processing Magazine 37 (2020) 50–60.

[16] Z. Li, V. Sharma, S. P. Mohanty, Preserving data privacy via federated learning: Challenges and solutions, IEEE Consumer Electronics Magazine 9 (3) (2020) 8–16. doi:10.1109/MCE.2019.2959108.

[17] G. Kaissis, M. R. Makowski, D. Rückert, R. F. Braren, Secure, privacy-preserving and federated machine learning in medical imaging, Nature Machine Intelligence 2 (2020) 305–311.

[18] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2) (Jan. 2019). doi:10.1145/3298981. URL https://doi.org/10.1145/3298981

[19] S. Niknam, H. S. Dhillon, J. H. Reed, Federated learning for wireless communications: Motivation, opportunities, and challenges, IEEE Communications Magazine 58 (2020) 46–51.

[20] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, H. Yu, Federated learning, Synthesis Lectures on Artificial Intelligence and Machine Learning 13 (3) (2019) 1–207. arXiv: https://doi.org/10.2200/S00960ED2V01Y201910AIM043, doi: 10.2200/S00960ED2V01Y201910AIM043. URL https://doi.org/10.2200/S00960ED2V01Y201910AIM043

[21] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawit, Z. Charles, G. Cormode, R. Cummings, R. G. L. D’Oliveira, H. Eichner, S. El Rouayheb, D. Evans, J. Gardner, Z. Garrett, A. Gascón, B. Ghazi, P. B. Gibbons, M. Gruteser, Z. Harchaoui,
C. He, L. He, Z. Huo, B. Hutchinson, J. Hsu, M. Jaggi, T. Javid, G. Joshi, M. Khodak, J. Konecný, A. Korolova, F. Koushanfar, S. Koyejo, T. Lepoint, Y. Liu, P. Mittal, M. Mohri, R. Nock, A. Özgür, R. Pagh, H. Qi, D. Ramage, R. Raskar, M. Raykova, D. Song, W. Song, S. U. Stich, Z. Sun, A. Theertha Suresh, F. Tramèr, P. Vepakomma, J. Wang, L. Xiong, Z. Xu, Q. Yang, F. X. Yu, H. Yu, S. Zhao, 2021.

[22] X. Yin, Y. Zhu, J. Hu, A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions, ACM Comput. Surv. 54 (6) (Jul. 2021). doi:10.1145/3460427. URL https://doi.org/10.1145/3460427

[23] Z. M. Fadlullah, N. Kato, Hcp: Heterogeneous computing platform for federated learning based collaborative content caching towards 6g networks, IEEE Transactions on Emerging Topics in Computing (2020) 1–1 doi:10.1109/TETC.2020.2986238.

[24] Y. Chen, X. Sun, Y. Jin, Communication-efficient federated deep learning with asynchronous model update and temporally weighted aggregation, CoRR abs/1903.07424 (2019). arXiv:1903.07424. URL http://arxiv.org/abs/1903.07424

[25] N. Rieke et al., The future of digital health with federated learning, NPJ Digital Medicine 3 (Sep. 2020). doi:10.1038/s41746-020-00323-1.

[26] W. Zhang et al., Dynamic fusion based federated learning for COVID-19 detection, ArXiv abs/2009.10401 (2020). arXiv:2009.10401.

[27] B. Liu, B. Yan, Y. Zhou, Y. Yang, Y. Zhang, Experiments of federated learning for COVID-19 chest X-ray images, ArXiv abs/2007.05592 (2020). arXiv:2007.05592.

[28] M. Flores, Triaging COVID-19 patients: 20 hospitals in 20 days build AI model that predicts oxygen needs, The Official NVIDIA Blog (Oct. 2020). URL https://blogs.nvidia.com/blog/2020/10/05/federated-learning-covid-oxygen-needs/

[29] B. Ikiz, A pandemic AI engine without borders, Stanford HAI (Aug. 2020).
[30] Z. M. Fadlullah, N. Kato, HCP: Heterogeneous computing platform for federated learning based collaborative content caching towards 6G networks, IEEE Transactions on Emerging Topics in Computing (2020). doi:10.1109/TETC.2020.2986238.

[31] B. Mao, Z. M. Fadlullah, F. Tang, N. Kato, O. Akashi, T. Inoue, K. Mizutani, Routing or computing? the paradigm shift towards intelligent computer network packet transmission based on deep learning, IEEE Transactions on Computers 66 (11) (2017) 1946–1960. doi: 10.1109/TC.2017.2709742.

[32] J. Kang, Z. Xiong, D. Niyato, H. Yu, Y. Liang, D. I. Kim, Incentive Design for Efficient Federated Learning in Mobile Networks: A Contract Theory Approach, ArXiv abs/1905.07479 (2019). arXiv:1905.07479.

[33] N. Nomikos, E. T. Michailidis, P. Trakadas, D. Vouyioukas, H. Karl, J. Martrat, T. Zahariadis, K. Papadopoulos, S. Voliotis, A UAV-based moving 5G RAN for massive connectivity of mobile users and IoT devices, Vehicular Communications 25 (2020) 100250. doi:10.1016/j.vehcom.2020.100250.

[34] L. Xiang, L. Lei, S. Chatzinotas, B. Ottersten, R. Schober, Towards power-efficient aerial communications via dynamic multi-UAV cooperation, ArXiv abs/2001.11255 (2020). arXiv:2001.11255.

[35] N. Q. K. Le, E. K. Y. Yapp, H.-Y. Yeh, ET-GRU: Using multi-layer gated recurrent units to identify electron transport proteins, BMC Bioinformatics 20 (1) (Jul. 2019). doi:10.1186/s12859-019-2972-5.

[36] Y. Xu, Q. Kong, Q. Huang, W. Wang, M. D. Plumbley, Convolutional gated recurrent neural network incorporating spatial features for audio tagging, arXiv abs/1702.07787 (2017). arXiv:1702.07787.

[37] Y. Chen, X. Sun, Y. Jin, Communication-efficient federated deep learning with asynchronous model update and temporally weighted aggregation, arXiv abs/1903.07424 (2019). arXiv:1903.07424.
[38] S. Sakib, T. Tazrin, M. M. Fouda, Z. M. Fadlullah, M. Guizani, DL-CRC: Deep learning-based chest radiograph classification for COVID-19 detection: A novel approach, IEEE Access 8 (2020) 171575–171589. doi:10.1109/ACCESS.2020.3025010.

[39] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, S. Cui, A joint learning and communications framework for federated learning over wireless networks, arXiv abs/1909.07972 (2019). arXiv:1909.07972.

[40] URUAV GRAPHENE 22.2V 6000mAh 100C 6S Lipo Battery XT90 Plug for RC Racing Drone, URL https://www.uruav.com/URUAV-GRAPHENE-22-2V-6000mAh-100C-6S-Lipo-Battery-XT90-Plug-for-RC-Racing-Drone-p-506.html.

[41] Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Blockchain and federated learning for 5G beyond, IEEE Network 35 (1) (2021) 219–225. doi:10.1109/MNET.011.1900598.

[42] S. Kothari, T. Tazrin, D. Desai, A. Parveen, M. M. Fouda, Z. M. Fadlullah, On securing electronic healthcare records using hyperledger fabric across the network edge, in: Secure Edge Computing, CRC Press, 2021, pp. 155–176. doi:10.1201/9781003028635-12.

[43] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, W. Alasmary, Smart parking system with privacy preservation and reputation management using blockchain, IEEE Access 8 (2020) 150823–150843. doi:10.1109/ACCESS.2020.3016945.

[44] S. K. Radha, I. Taylor, J. Nabrzyski, I. Barclay, Verifiable badging system for scientific data reproducibility, Blockchain: Research and Applications (2021) 100015doi:10.1016/j.bcr.2021.100015.

[45] C. Ma, J. Li, M. Ding, L. Shi, T. Wang, Z. Han, H. Poor, When federated learning meets blockchain: A new distributed learning paradigm, ArXiv abs/2009.09338 (2020). arXiv:2009.09338.

[46] T. Li, A. K. Sahu, A. S. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, IEEE Signal Processing Magazine 37 (3) (2020) 50–60. doi:10.1109/MSP.2020.2975749.
[47] H. B. Desai, M. S. Ozdayi, M. Kantarcioglu, Blockfla: Accountable federated learning via hybrid blockchain architecture, CODASPY '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 101–112. doi:10.1145/3422337.3447837.
Nidal Nasser (Senior Member, IEEE) received the Ph.D. degree from the School of Computing, Queen’s University, Kingston, ON, Canada, in 2004. He is currently a Professor of Software Engineering with the College of Engineering, Alfaisal University, Saudi Arabia. He worked with the School of Computer Science, University of Guelph, Guelph, ON, Canada. He was the Founder and the Director of the Wireless Networking and Mobile Computing Research Lab, University of Guelph. He is currently the Founder and the Director of the Telecommunications Computing Research Lab, Alfaisal University. He received several outstanding research awards as well as several best paper awards.

Mostafa M. Fouda (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID, USA. He also holds the position of an Associate Professor with Benha University, Egypt. His research interests include cyber security, machine learning, blockchain, IoT, 6G networks, and smart grid communications. He is an Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and an Associate Editor of IEEE ACCESS.

Zubair Md Fadlullah (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He is currently an Associate Professor with the Computer Science Department, Lakehead University, and a Research Chair of the Thunder Bay Regional Health Research Institute, Thunder Bay, ON, Canada. He was an Associate Professor with the Graduate School of Information Sciences, Tohoku University from 2017 to 2019. His main research interests span over the cyber–physical system layers in sensing, communication, and computing problems and elegant solutions.

Dr. Asmaa Ali received her B.Sc. and M.Sc. in Electrical Engineering from Kuwait University, State of Kuwait, in 2000 and 2004, respectively. She received another M.Sc. in Engineering System and Computing from the University of Guelph, Guelph, Ontario, Canada, in 2015. She completed her Ph.D. in the School of Computing at Queen’s University, Kingston, Ontario, Canada, in 2020. She received the Best Paper Award at the IEEE International Conference on Smart Applications, Communications, and Networking (SmartNets 2019). Her current research interests are computer vision and pattern recognition, communication, robotics, control system, engineering analysis, artificial intelligence, machine/deep learning, data science, and wireless sensor network.

Muhammad Imran is an assistant professor in the College of Computer and Information Science, King Saud University. His research interests include mobile ad hoc and sensor networks, WBANs, IoT, M2M, multihop wireless networks, and fault-tolerant computing. He has published a number of research papers in peer reviewed international journals and
conferences. His research is financially supported by several grants. He is serving as a Co-Editor-in-Chief for EAI Transactions on Pervasive Health and Technology. He also serves as an Associate Editor for the Wireless Communication and Mobile Computing Journal (Wiley), the Inderscience International Journal of Autonomous and Adaptive Communications Systems, Wireless Sensor Systems (IET), and the International Journal of Information Technology and Electrical Engineering. He has served/serves as a Guest Editor for IEEE Communications Magazine, IJAACS, and the International Journal of Distributed Sensor Networks. He has been involved in a number of conferences and workshops in various capacities such as a Program Co-Chair, Track Chair/Co-Chair, and Technical Program Committee member. These include IEEE GLOBECOM, ICC, AINA, LCN, IWCMC, IFIP WWIC, and BWCCA. He has received a number of awards such as an Asia Pacific Advanced Network fellowship.
AUTHORSHIP STATEMENT

Manuscript title: A Lightweight Federated Learning Based Privacy Preserving Pandemic Response Network Using Unmanned Aerial Vehicles: A Proof-of-Concept

Authorship contributions

Category 1
Conception and design of study: Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

acquisition of data: Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda

analysis and/or interpretation of data: Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

Category 2
Drafting the manuscript: Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran

Category 3
Approval of the version of the manuscript to be published (the names of all authors must be listed):

Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran;
This statement is signed by all the authors (a photocopy of this form may be used if there are more than 10 authors):

| Author’s name (typed) | Author’s signature      | Date       |
|-----------------------|-------------------------|------------|
| Nidal Nasser          | Nidal Nasser            | Sept 1, 2021|
| Zubair Md Fadlullah    | Zubair Md Fadlullah      | Sept 1, 2021|
| Mostafa M. Fouda      | Mostafa M. Fouda        | Sept 1, 2021|
| Asmaa Ali             | Asmaa Ali               | Sept 1, 2021|
| Muhammad Imran        | Muhammad Imran          | Sept 1, 2021|
Conflict of Interest and Authorship Conformation Form

Please check the following as appropriate:

✓ All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.

✓ This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

✓ The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript

  o The following authors have affiliations with organizations with direct or indirect financial interest in the subject matter discussed in the manuscript:

| Author’s name | Affiliation |
|---------------|-------------|
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |