International Journal of Machine Learning and Cybernetics (2023) 14:2659–2670
https://doi.org/10.1007/s13042-023-01789-7

ORIGINAL ARTICLE

SecureFed: federated learning empowered medical imaging technique to analyze lung abnormalities in chest X-rays

Aaisha Makkar[1] · **KC Santosh**[2]

Received: 20 October 2022 / Accepted: 20 January 2023 / Published online: 14 February 2023

Abstract
Machine learning is an effective and accurate technique to diagnose COVID-19 infections using image data, and chest X-Ray (CXR) is no exception. Considering privacy issues, machine learning scientists end up receiving less medical imaging data. Federated Learning (FL) is a privacy-preserving distributed machine learning paradigm that generates an unbiased global model that follows local model (from clients) without exposing their personal data. In the case of heterogeneous data among clients, vanilla or default FL mechanism still introduces an insecure method for updating models. Therefore, we proposed SecureFed—a secure aggregation method—which ensures fairness and robustness. In our experiments, we employed COVID-19 CXR dataset (of size 2100 positive cases) and compared it with the existing FL frameworks such as FedAvg, FedMGDA+, and FedRAD. In our comparison, we primarily considered robustness (accuracy) and fairness (consistency). As the SecureFed produced consistently better results, it is generic enough to be considered for multimodal data.

Keywords Federated learning · Medical imaging · Security · Robustness · Chest X-ray

1 Introduction

1.1 Background and motivation

Shockingly, the global COVID-19 epidemic has resulted in roughly 257 million infections and 5.2 million fatalities around the world (as of 23rd November 2021) [37]. Coronavirus is a respiratory infection—identified in Wuhan (China) in December 2019—propagated across the world. It apprised as a pandemic for the complete world and its impact is still inspected in some of the world regions. This pandemic has proved dangerous to the front-line medical workers and health practitioners. Due to the contagious nature of COVID-19, timely, accurate, and faster diagnosis/screening is essential. Needless to mention, since the beginning, doctors/medical experts and scientists worked on exploring numerous methods of COVID-19 detection so further spread can be prevented.

Clinical testing primarily includes RT-PCR test in which a sample of sequence pathogen RNA is collected from virus specimens using a swab (inserted into the mouth or the nose). This collection of anti-bodies is done to know whether such anti-bodies of the infection entered the human body. Another popular approach is to investigate RNA sequences as it identifies antibodies that restrained pathogens and it requires FDA-sanctioned drugs to counter this virus. These clinical trials no doubt proved beneficial. However, these clinical procedures require medical experts and are time consuming, which in turn are expensive.

For COVID-19 and in the presence of adequate epidemic related data such as protein compositions RNA, serological reports, and pathological reports, doctors can diagnose at the earliest. In addition, image data can accurately clinical significance that is related to COVID-19 [27, 29, 30]. Based on our literature review, deep learning models or Deep Neural Networks (DNNs) demonstrated higher performance in detecting infectious disease. When it comes to public healthcare and pandemic management, early detection for COVID-19 clinical specimens is indeed a challenge. Early detection can help control further spreading [7, 26, 28]. Radiology

✉ Aaisha Makkar
a.makkar@derby.ac.uk

✉ KC Santosh
santosh.kc@usd.edu

[1] College of Science and Engineering, University of Derby, Kedleston Rd, Derby DE22 1GB, UK

[2] Applied AI Research Lab, Department of Computer Science, University of South Dakota, 414 E Clark St, Vermillion, SD 57069, USA

techniques such as Chest X-ray (CXR) also proved to be a reliable and cheaper medical imaging tool in understanding COVID-19 clinical manifestations. As mentioned before, it is widely accepted that chest radiography has low specificity for detecting relevant clinical abnormalities, despite the availability of numerous imaging modalities [32]. When diagnosing pulmonary abnormalities, healthcare professionals often screen CXRs. When it comes to mass screening and in resource-constrained regions, medical experts could possibly be complemented by machine learning CXR screening tools.

The rate of people contaminated with COVID-19 is not precise as their hospital settings and capacities are not transparent. Monitoring variations in the virus is being done by the WHO and its international networks of specialists to advise states/countries and the public of any adjustments that may be necessary to the variant and limit its spread. But it is worth noting how such important data is collected and secure. Testing is done at local healthcare centers and results are saved and transferred to WHO. Detecting the existence of disease has never been more important than it is today when it comes to performing mass screening. It then produces millions of data, but the procedure to secure this data is still challenging. This opens an opportunity to introduce SecureFed— a secure aggregation method—which ensures fairness and robustness in the Federated Learning (FL) settings.

1.2 Contributions and organization of the paper

This research work considers four key issues of FL: (a) security, (b) privacy, (c) robustness, and (d) fairness. To resolve these issues, we summarize them in three main contributions:

1. Training in FL settings could help provide security as well as privacy, and SecureFed provides a secure aggregation mechanism.
2. Our results demonstrated that SecureFed yields robustness and fairness in dealing with COVID-19 cases using CXRs.

The remaining of the paper is organized as follows. Section 2 discusses about the medical problem of COVID-19. It includes previous works and high-level comparison (among them), which helps draw shortcomings and/or research gap. Section 3 provides a conceptual idea on how we move on for a system design. We immediately provide basics of why federated is employed in Sect. 4. In Sect. 5, we explain the proposed framework titled "SecureFed," and it is composed of client (Sect. 5.1), server (Sect. 5.2), and aggregation method (Sect. 5.3). Results are provided in Sect. 6. It includes dataset description and experimental setup (Sect. 6.1), and results and merits that are related to SecureFed in medical imaging. As stated in our contribution, experimental results are primary focused on fairness, robustness, and security and privacy. Section 7 concludes the paper.

2 Medical imaging: previous works and data

Healthcare data is integral to medical treatment. This crucial data could help in disease detection, prevention, and prediction. Nevertheless, the data should be collected either directly by the medical practitioners, or from the reliable sources (in the case of the year's data). The data can be in various forms and dimensions. For COVID-19, multimodal data is experimented for the last two years. Medical imaging is a technique for studying and forecasting covid-19's effects on the human body. With the use of Computerized Tomography (CT) and CXR images, healthy individuals and Covid-19 infected patients can be studied in parallel [16, 21, 27, 30]. Accurate visualization of CXR proved to be an effective measure to detect COVID-19 and it is one of the cost-effective tools for early detection of COVID-19 [5]. Although the screening of such method raised with exponential rise of COVID-19 cases, so as the follow-up and inspection time by the radiologist also increased. The datasets such as Mendeley, Larxel, and Corona Hack have been proved significant in validating the various COVID detection techniques [3]. Authors have developed various AI techniques for COVID-19 detection using CXR images, which can be classified into machine learning, deep learning, and federated learning [17].

2.1 Previous works

Authors [12] proposed a Convolutional Neural Network (CNN) to detect the COVID-19. Because pretrained CNN models are known to offer issues in practical applications, authors devised a small-sized CNN architecture. Authors employed a 12-class CXR dataset, with an 86% accuracy reported in their tests. Authors [41] It was discovered that lung nodules could be detected using Multi-Resolution CNN (MR-CNN), which was combined with patch-based MR-CNN to extract feature information. FAUC and R-CPM metrics were employed to assess performance, with results of 0.982 and 0.987 recorded, respectively. Authors [8] used an ensemble of five new deep-transfer-learning-based models to detect pneumonia in CXR images. Using their built ensemble deep model, the scientists reported a 96.4% accuracy rate. The AlexNet model was updated to detect lung anomalies from CXR pictures. Pneumonia was detected using a deep learning approach, according to the scientists. Classification accuracy reached 96% thanks to the use of a new "threshold filter" and a feature ensemble technique [6]. Covid-CAPS, a new modelling framework based on Capsule Networks that can handle small data sets, is presented. This

Table 1 Deep features for COVID-19 detection

Author	Description	Dataset (# of CXRs)	Accuracy
Loey et al. [15]	GAN model	COVID-19 (307)	80.60%
Panwar et al. [24]	Feature extractor	COVID-19 (392)	97.62%
Marques et al. [19]	Binary classification scheme	COVID-19 (2,482) CXR	96.00%
Panwar et al. [23]	CNN and transfer learning	1) COVID-10 (CXR, 526) 2) SARS-COV-2 (CT-scan, 2,482) 3) CXR (5,856)	95.61%
Serte et al. [31]	ResNet-50	Mosmed (1,110) and CCAP	90.00%
Ahsan et al. [2]	VGG16, MobileNetV2, InceptionResNetV2,ResNet50 ResNet101, and VGG19	CT (400) and CXR (400)	95.00%
Salvia et al. [13]	CNNs	CXR (2,908 from 450 patients)	98.00%

is important because of the rapid emergence of COVID-19 [1]. Using X-ray pictures as input, we found that COVID-CAPS outperforms earlier CNN-based models. Pre-trained deep-learning algorithms were used in conjunction with a robust technique proposed [9] to automatically diagnose COVID-19 pneumonia from digital CXR pictures and maximize detection accuracy. Several public databases were combined, and photos from recently published studies were also collected. There are 423 COVID-19 photos, 1485 viral pneumonia images, and 1579 images of normal CXR in the database. Image augmentation was utilized to train and test numerous pre-trained deep Convolutional Neural Networks using transfer learning techniques.Authors [35] proposed self-tuning PSO based convolution neural network (PSTCNN) that reduced human efforts to detect COVID-19. In [36], authors used wavelet entropy as a feature extraction method, where their proposed deep learning model (WE-SAJ) employed two-layer feed-forward neural networks (FNNs) for testing, and the adaptive Jaya algorithm for training. The first three instances of COVID-19 infection in France were examined [33]. Two people were diagnosed in Paris, while one person was diagnosed in Bordeaux. They were living in Wuhan, China, prior to contracting Covid-19 illnesses [4]. Table 1 summarises few deep learning techniques for the detection of COVID-19.

2.2 High-level comparison

Unlike previous studies, we propose federated learning to detect for the identification of COVID-19 using CXR images. Even though previous studies reported on the detection of multiple lung abnormalities such as Tuberculosis and Pneumonia, our study is COVID-19 versus normal (healthy) cases. However, there are few existing techniques of federated learning [18] for the detection of COVID-19.

1. *Liu et al.* (2020) presented an approach using federated learning for COVID-19 data training and conduct tests to confirm its efficacy. They also evaluated the results of four prominent models (MobileNet, ResNet18, MoblieNet, and COVIDNet) with and without the federated learning framework [14].
2. Authors [34] concentrated on the subject of COVID-19 imaging data privacy for illness diagnosis using computer vision and deep learning techniques. We explore how the differential privacy by design (dPbD) paradigm might improve data privacy in federated learning systems while still allowing for scalability and robustness.
3. For an automatic diagnosis of COVID-19, authors [25] used the developing idea of clustered federated learning (CFL). By developing a multi-modal ML model capable of diagnosing COVID-19 in both X-ray and Ultrasound imaging, the system is designed to intelligently analyze visual input at the edge. CFL is found to cope better with the divergence in data distribution from different sources than standard FL (i.e., X-ray and Ultrasound imagery).
4. Authors [39] suggested federated Learning on Medical Datasets Using Partial Networks (FLOP), in which the server and clients share just a partial model. Extensive tests using benchmark data and real-world healthcare tasks show that the method achieves comparable or better results while reducing privacy and security risks. Authors discovered that the FLOP algorithm can allow multiple hospitals to collaborate and effectively train a partially shared model without disclosing local patients' data on the COVID-19 dataset, which is of particular interest.
5. To detect COVID-19 infections, authors [40] suggested a unique dynamic fusion-based federated learning system for medical diagnostic picture processing. They create an architecture for medical diagnostic picture analysis using dynamic fusion-based federated learning systems. A dynamic fusion method is also described, which dynamically determines the participating clients based on their local model performance and schedules the model fusion based on the training duration of the participants.
6. By implementing a differential privacy solution at each hospital institution, authors [22] improved the privacy of federated COVID-19 data analytics. Furthermore, by decentralizing the FL process with a novel mining

approach for low running latency, authors propose a new FedGAN architecture based on blockchain for secure COVID-19 data analytics.

Table 2 summarizes how the proposed approach is different from the existing approaches.

Table 2 Summary: comparison of proposed work with existing literature

Authors	Aggregation	Dataset	Outcome
Liu et al. [14]	FL	CXR	ResNeXt (good performer)
Qayyum et al. [25]	Clustered FL	X-ray & Ultrasound	Improves F1 score (0.96)
Yang et al. [39]	FL with Partial Networks	Validated with 6 benchmark datasets	Reduces privacy and security
Zhang et al. [40]	Dynamic fusion-based FL with scheduled aggregation	CT scans and CXRs	Reduces communication overhead
Nguyen et al. [22]	Blockchain-based FedGAN	CXRs (COVID-19)	Improves accuracy (0.975)
Proposed work	FL – SecureFed	CXRs (COVID-19)	Achieves fairness and robustness

3 System model—a quick outline

Securing the huge COVID-19 testing data is a challenge. The causes, measures, and predictions by the WHO is done using the data. The procedure of communicating the testing data from the local health center to the WHO should be secure. Using computer-aided approaches, deep learning techniques contribute greatly to the state-of-the-art analysis for securing the data.

It is the fact to be accepted that deep learning models are trained with the data mainly consisting of patient personnel information as well as drug history. The privacy and security can be violated by training the models at the layer far from the device-end. The researchers have introduced many lite deep learning algorithms which can predict at edge (device-end) itself. This approach is known as federated learning, which proved to be more secure and efficient for medical equipment's, for training patient sensitive data. Using the approach of federated learning and edge computing, the trial is secured. The secure data sharing is supported to prevent from possible cyber attacks. The local dataset d is converted to f and is transmitted to WHO, and it can be mathematically expressed as:

$$f = \sum_{i=1}^{n} M_i * F_i. \tag{1}$$

The dataset is locally trained and contains the probability of COVID-19 infected patients/cases.

4 Federated learning

Processing medical data requires attention as they are sensitive due to confidential information such as phone number, address, and other personal credentials. For such a huge amount of data, data visualization could help understand more about the data trend. Training machine learning models at the server level could potentially lead to data leakage. In this scenario, there is demand of privacy preserving technique such as FL that trains the data at user-end. This means that such a self-training does not require data to be transferred to user-end (from server). The safe and accurate handling of COVID-19 data is essential. The data produced by the local hospitals/clinics need to be collected and sent to Central Health Organization (CHO). The major considerations under this situation are

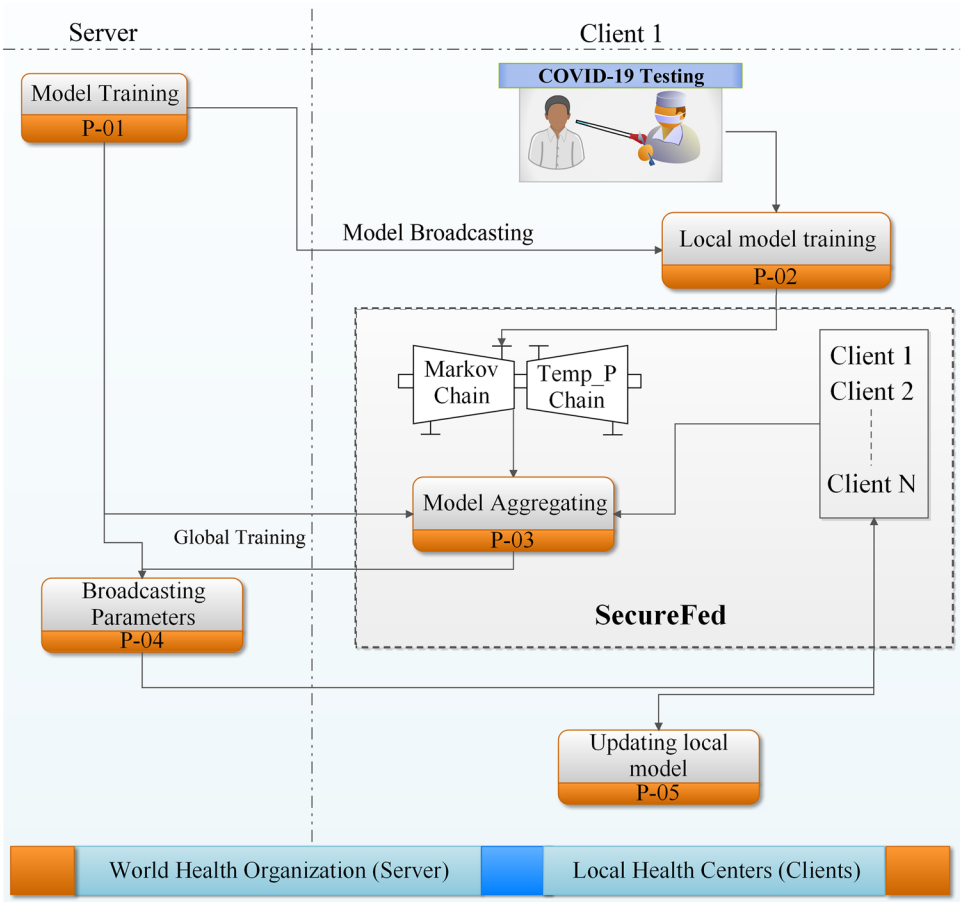

Fig. 1 Secure Federated Learning environment for aggregating the COVID-19 testing data

1. cost effective training at the local health center and
2. aggregating their corresponding results at the server, which is secure, robust, and accurate.

Following Fig. 1, we summarize the whole process of local training and aggregating the results within the scope of FL at the server. In Fig. 1, local centers collect the CXR, performs COVID-19 detection in and generate results. The federated model that is trained at the local healthcare system is updated with the results of COVID-19 detection using Chest X-Rays. The updated model updates are sent to CHO. The CHO then aggregates on the model based on local health centers.

Aggregation methods can be summarized as follows. Assume that $H(k)$ local healthcare centers collaborate to train a global model (WHO) with m (w) in a standard setting of federated learning. Specifically, the goal is to reduce the loss (as shown below):

$$\beta = \min(m) \sum_{H=1}^{H} \alpha H \lambda H(m), \tag{2}$$

where $\lambda H(m)$ is the loss function. This is FedAvg [20] based on stochastic gradient descent (SGD) optimiser for updating the local model. This method assumes the propositional distribution among all the clients. The term Auto FedAvg was coined to describe a new approach that extended the FedAvg. Aggregation weights can be designed in a more flexible manner than with FedAvg as the parameterized weights can be learned from data in a differentiable way [38].

In FedAvg, the weights must be specified in advance. Typical options include the size of each user's dataset and the user's 'importance.' This is how FedAvg works: A random subset of users is chosen for each round, and k epochs of local (full or minibatch) gradient descent are performed by each user.

Multi-objective minimization (MoM), multiple gradient descent (FedMGDA+) and existing FL algorithms are all extended in FedMGDA+. Authors [10] proved the convergence properties of the extended algorithm. This attempts by replacing average loss function to average loss function by:

$$\min_{w} \max_{\lambda \in \Delta} \lambda^T f(w) \equiv \min_{w} \max_{i=1,\ldots,m} .f_i(w). \tag{3}$$

Another method FedRAD, uses multivariate continuous probability distribution using discrete distribution among the clients, following non IID split. The notation used is:

$$f(Y;\alpha) = \frac{1}{A(\alpha)} \sum_{i=1}^{K} x_i^{a_i - 1}, \tag{4}$$

where $A(\alpha)$ refers to a normalized constant and rest of the equation works according to the gamma distribution.

Other methods such as Adaptive Federated Averaging (AFA) are focused on handling byzantine clients. Here, the concern is simulating and aggregating the COVID-19 data. So, within the region it is difficult to detect suspicious clients. In the proposed work, the attention is given to handle the medical data with appropriate approach.

5 Proposed framework: secureFed

The privacy preserving attributes of federated learning (FL), attracts medical domain to adapt it. The sensitive information of the patients is worth securing in case of COVID-19, where every day rises with the challenge of new variant. There exist different FL settings with various aggregation function. Let us consider a FL setting consisting of a server (WHO) and N clients. Every client C_i holds a dataset d_i. After the local training in order to optimise the loss, every client produces a vector v_i. Every vector produced by the N clients, is aggregated:

$$A \equiv \sum_{i=1}^{N} \frac{|D_i|}{|D|} v_i, \tag{5}$$

where v_i is the vector produced by the clients after the local training, the clients are ranging from 1 to N and A is the vector produced by aggregating the vectors by all the clients. Each client holds dataset d_i (see Eq.(5)), and server independently allocates parameters to each client. In Fig. 1, we present a complete overview on how it works; starting from parameter broadcasting to the aggregation process.

1. Model Training and Broadcasting (P-01): The server trains a threat model which is standard one for all the clients. The copy of standard model is sent to all the clients. In the proposed work, server refers to WHO and the clients are the local health centers. The threat model is trained with the parameters of dataset collected by the client.
2. Local model training (P-02): Once the model is available with all the clients, the clients can progress with training the threat model with the timely recorded images of the patients. The results of the tests are discussed with the patients and are then used for training. In the proposed work, there is no curtailment on time, for the local client to train the model. As it depends upon the region, and the pandemic situation, the rising cases may force the client (local health center) to train the model more swiftly.
3. Model Aggregating (P-03): The sensitive local information remains with the client and the vector produced by the local training is sent to the server. This process is free form as the response from every client is not fixed at a constant point. In our work, the vector produced by each C_i refers to the probability of positive COVID-19 cases, and the probability of negative COVID-19 cases. The information to be transmitted should not lead to data leakage. So, we propose new aggregate method, i.e., SecureFed (as discussed later in the Section), for secure aggregation by the server.
4. Broadcasting Parameters (P-04): Once the server performs aggregation, the global model is updated with the aggregated information. The aggregated parameters produced by the updated model are sent to N clients. In the proposed work, the parameters such as valid CT value, symptoms are broadcasted to all the clients (local healthcare center).
5. Updating local model (P-05): Once the updated parameters are received from the server, every client updates its model and the model get trained with the updated parameters. In the proposed work, every client (Healthcare center), updates the model with the updated parameters such as change in CT value, adverse symptoms to be considered, and new COVID variant.

Algorithm 1 Threat model: Client-side training

Input: Chest X-Ray image data
Require: learning rate, loss function, epochs
Output: Categorical vectors and states: COVID-19/Non-COVID-19

procedure LOCAL_UPDATE_MODEL(w)
  $w_t = w$ [Comment: Initializing local model]
  $x_i = \frac{x_i - \hat{\mu}\beta}{\sqrt{\hat{\sigma}_\beta + \varepsilon}}$ [Comment: Forming mini-batches using Gradient Descent algorithm]
  for $i = 1$ *to* n **do**
    Set $i \leftarrow i + 1$
  end for
  Training x_i in CNN [Comment: Training with the mini-batches]
  for $x = 1$ *to* n **do**
    Update model
  end for
end procedure

5.1 Threat model: client

To detect COVID-19 cases, we used Neural Network (NN) using CXRs. This NN is firstly trained by the server and a copy of model is sent to all the clients. This network is trained at client side as a threat model. The targeted output is the probabilities produced by the model to detect the probability of COVID-19/Non-COVID-19. As there are two classes of output, so categorical cross entropy loss is simulated. The activation function used is soft-max method for classification. In the proposed work, the CXR are processed by the neural network by following Mini-Batch Gradient Descent algorithm. The convolutional layers of filter of size 3×3 with a stride of 1 is used, whereas the max pool layer is composed of filter 2×2 with the stride of 2 (*ref.* 1).

5.2 Threat model: server

The server maintains the global model which is circulated to the N number of Clients. Once the client (Healthcare center) trains and updates the local model, the updates by all the clients are aggregated. The clients work in free form manners, i.e., are not restricted to update the local model. However, the timely response is expected. The server then updates the global model with the aggregated model. The updated results are saved and analyzed. After the screening of results by the medical experts, the global model is again updated if any changes are required. The updated model is then again shared with the clients.

5.3 Aggregation method: secureFed

The new aggregation method to be used by the server is proposed in this work and named as SecureFed. The idea behind this method is that the Google search engine uses the Markov model to find the probability that the user would select the web page. Similarly, when each client produces the probability vectors of the test results that whether the patient is COVID affected or not, it is also added to the Markov chain. Once the present state of vector is added to the chain, the temporary prediction is stored in temp matrix which is used by the server during aggregation. The chain keeps on updating by the clients, two matrices are maintained, one by the original vectors produced after the local training and the other temp matrix being developed during immediate prediction by the markov chain.

Markov chains are stochastic models developed by Andrey Markov that show the likelihood of a series of events occurring given the prior event's state. The page rank algorithm (e.g, Google's search engine) determines which links to show first. This model uses the observations to forecast an approximation of future events using maths. The Markov chain process two vectors:

Table 3 Dataset distribution among the clients

Dataset	COVID-19 (2358)		Healthy (1583) [11]		Pneumonia (4273) [11]	
Clients	Images	Size	Images	Size	Images	Size
10	100	350 MB	50	25 MB	50	67.5 MB
20	200	700 MB	100	50 MB	100	135 MB
30	300	1050 MB	150	75 MB	150	200 MB
50	500	1750 MB	250	125 MB	250	350 MB
100	1000	3500 MB	500	250 MB	500	700 MB
Total	2100	7000 MB	1050	525 MB	1050	1500 MB

1. Initial state vector: The initial vector is provided by the server as the record to capture the initial vectors computed by the local client after training.
2. Transition vector: This vector represents the probability transitions, as the two state, i.e., 0 and 1 are recorded after local training of each mini batch. In the proposed work, 1 denotes COVID-19 affected patient.

The Markov chain is produced by gathering the local trained vectors of each client as: $M_C = \sum_{i=1}^{n}[a_i]$, where a_i is the probability vector produced by a client. Markov_C is the Markov chain produced by the summation of probability vectors by all the clients. The predicted chain, Temp_C is the immediate prediction when the probability vector a_i enters the Markov_C:

$$\text{Temp}_C(C_{n+2} = i \mid C_n = j) = \sum_{K=1}^{n} P(C_{n+2} = i \text{ and } C_{n+1} = k \mid C_n = j). \tag{6}$$

These matrices are then used by the server for the global training. The predicted matrix (Temp_C) is identified and normalized. The aggregated results after global training are sent as the updated model to the clients.

6 Results and discussion

The proposed federated learning framework processes the medical images for the detection of COVID-10/Non-COVID-19 cases. The client is the healthcare center which records the CXR and performs the local training using the threat model (which is standard model for all the clients provided by the server). After the local training the results are sent using the method of Markov chain, named as SecureFed. The Markov chain

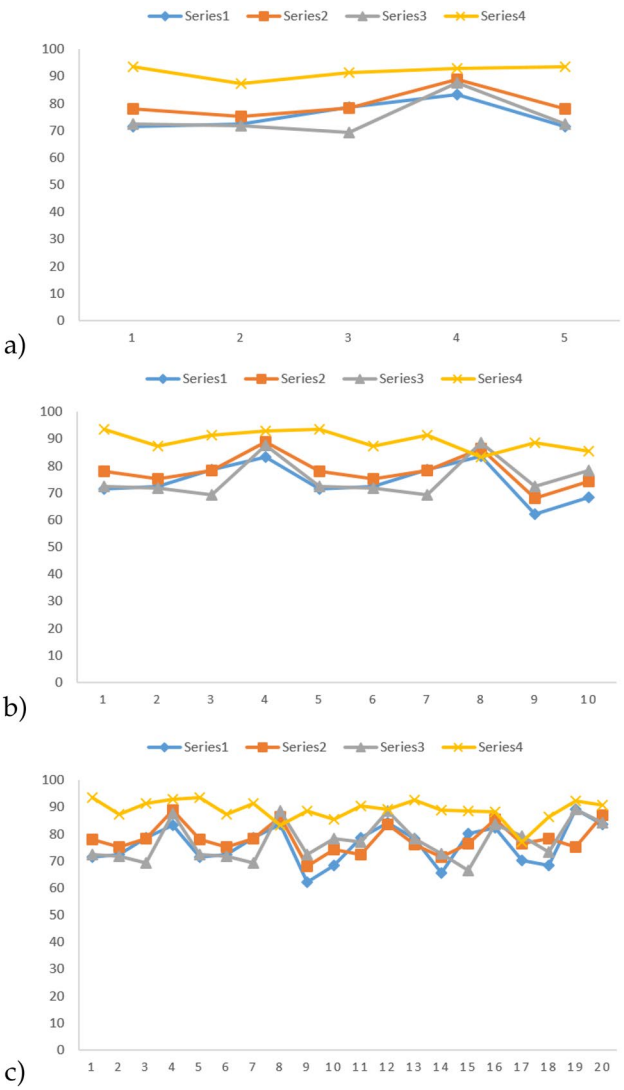

Fig. 2 Comparison of SecureFed(Series 4) with FedAvg (Series 1), FedMGDA+ (Series 2), and FedRAD (Series 3) along different settings of a) five clients, b) 10 clients, and b) 20 clients

Table 4 Performance of SecureFed to detect COVID-19 positive cases

10 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	69.67%	72.05%	71.62%	78.1%	72.3%	73.4%
FedMGDA+	65.3%	68.8%	72.3%	75.1%	71.9%	77.4%
FedRAD	56.43%	81.8%	78.7%	78.4%	69.4%	81.4%
SecureFed	84.4%	81.6%	83.4%	88.74%	87.6%	82.8%
20 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	79.11%	72.05%	71.62%	78.1%	72.3%	73.4%
FedMGDA+	65.3%	68.8%	72.3%	75.1%	71.9%	77.4%
FedRAD	56.43%	81.8%	78.7%	78.4%	69.4%	81.4%
SecureFed	82.3%	84.5%	83.6%	86.34%	88.5%	83.4%
30 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	55.46%	60.23%	62.24%	68.0%	72.45%	78.46%
FedMGDA+	56.4%	61.6%	68.24%	74.32%	78.2%	75.41%
FedRAD	58.23%	68.2%	78.7%	72.3%	77.2%	80.36%
SecureFed	83.3%	82.4%	84.2%	83.54%	88.7%	89.2%
50 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	73.2%	71.5%	78.22%	76.12%	78.23%	72.64%
FedMGDA+	65.2%	73.2%	65.7%	71.41%	72.6%	78.94%
FedRAD	65.33%	83.2%	80.17%	76.34%	66.34%	78.64%
SecureFed	82.24%	84.6%	82.3%	85.32%	83.5%	88.2%
100 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	69.22%	70.1%	70.12%	76.33%	79.09%	77.2%
FedMGDA+	62.22%	63.2%	68.3%	78.21%	73.3%	76.4%
FedRAD	62.44%	68.3%	89.3%	75.3%	89.2%	77.23%
SecureFed	82.2%	89.3%	83.5%	86.98%	84.2%	88.9%

collects the results the results of local model by each client, which is aggregated by the server. The proposed approach focuses on the problem of handling the complex medical data for processing and predicting. Below is the discussion of experiments being performed for the validation of proposed approach.

6.1 Dataset and experimental setup

To validate the proposed approach, it is essential to have a balanced dataset. To obtain the collection of COVID-19 Medical images, three distinguish datasets[1][2][3] are being combined. The dataset of healthy and pneumonia patients is collected for non-COVID medical images. Table 3 provides detailed information about the dataset with respect to different numbers of clients (for our experimental setup).

6.2 SecureFed in medical imaging

In this section, we discuss on the usefulness of the proposed system, SecureFed. In what follows, we take fairness, robustness, and security and/or privacy into account.

Fairness: The fairness of the system in the settings of federated learning is ensured by model broadcasting. With this step, the clients receives the standard threat model, which allows to train the CXR images irrespective of patient's age, illness or sex. The threat model processes the input medical images with same scale. The timely updations by the server also guarantees that the updated model is synchronised with all the clients, which maintains the effect of SecureFed on the medical images. The fairness is evaluated by the effect of SecureFeb on the different size of clients. In Fig. 2, four methods FedAvg

[1] https://github.com/agchung/Figure1-COVID-chestxray-dataset.

[2] https://github.com/agchung/Actualmed-COVID-chestxray-dataset.

[3] https://www.kaggle.com/datasets/tawsifurrahman/covid19-radiography-database.

Table 5 Performance of SecureFed to detect COVID-19 negative cases

10 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	62.34%	73.30%	78.3%	76.4%	76.2%	79.3%
FedMGDA+	62.2%	69.3%	76.6%	68.3%	78.3%	72.04%
FedRAD	56.43%	81.8%	78.7%	78.4%	69.4%	81.4%
SecureFed	94.4%	81.6%	83.4%	88.74%	87.6%	82.8%
20 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	69.67%	72.05%	71.62%	78.1%	72.3%	73.4%
FedMGDA+	65.3%	68.8%	72.3%	75.1%	71.9%	77.4%
FedRAD	65.34%	85.5%	73.2%	77.86%	71.12%	83.3%
SecureFed	92%	90.8%	82.1%	84.78%	89.9%	86.9%
30 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	69.67%	72.05%	71.62%	78.1%	72.3%	73.4%
FedMGDA+	65.3%	68.8%	72.3%	75.1%	71.9%	77.4%
FedRAD	56.43%	81.8%	78.7%	78.4%	69.4%	81.4%
SecureFed	84.4%	81.6%	83.4%	88.74%	87.6%	82.8%
50 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	53.23%	65.32%	55.2%	67.8%	69.90%	76.2%
FedMGDA+	61.3%	72.7%	86.3%	54.3%	54.7%	64.5%
FedRAD	74.45%	62.6%	72.1%	79.2%	82.1%	82.3%
SecureFed	91.2%	92.3%	88.8%	82.4%	87.9%	88.9%
100 Clients	Accuracy			Prediction		
Ratio	30:70	40:60	50:50	30:70	40:60	50:50
FedAvg	64.72%	78.29%	68.54%	76.23%	78.2%	78.7%
FedMGDA+	63.2%	65.3%	71.5%	78.2%	72.2%	76.2%
FedRAD	55.22%	82.2%	75.6%	78.4%	70.2%	81.2%
SecureFed	82.2%	88.3%	82.7%	86.45%	87.4%	81.01%

(Series 1), FedMGDA+ (Series 2), FedRAD (Series 3), and SecureFed (Series 4) are compared, where SecureFed outperforms. Moreover, in Fig. 2b and c, SecureFed maintained its performance even when we increase client's size.

Robustness: This is to ensure that the proposed approach outperforms than other existing aggregation methods, when applied to medical imaging. We experimented the proposed approach of aggregation over the different datasets. We considered 5 cases, 10 clients, 20 clients, 30 clients, 50 clients, and 100 clients. We perform the statistical test that concluded that the proposed method not only helped in aggregation but the better prediction as well. The same experiments are being with other aggregation methods but the results (in comparison to the proposed scheme) does not show any contribution towards the prediction. The testing data and the training data is divided into different portions to prove the robustness of the proposed approach. Different number of clients are experimented using various methods such as FedAvg, FedMGDA+, FedRAD, and SecureFed. Starting from 10 clients (to 100 clients), on a various train/test dataset distributions, SecureFed performed better. Interestingly, it holds true in predicting both cases: positive (Table 4) and negative (Table 5).

Security and privacy: The principle in this work is to adopt the nature of federated learning which takes care that the medical images are processed at the client itself. The privacy is maintained as only the results after the local training (Probability of COVID/non-COVID patients) are transferred from the various clients to the server. The security is maintained as the method SecureFed aggregates and produces the matrices (Markov and temp).

7 Conclusion

In this article, we have proposed a novel federated learning (FL) based aggregation approach to improve privacy, fairness, and robustness. This approach proved to be beneficial and secure platform for the detection of COVID-19. The

proposed research work is validated using Chest X-ray of 2100 positive cases. The results proved that the proposed work (SecureFed) outperforms the existing COVID-19 detection approaches as a robust, secure and privacy preservation scheme. Further, we have compared the SecureFed with the existing aggregation methods in FL frameworks such as FedAvg, FedMGDA+, and FedRAD. The experiments are conducted by considering different ratios of training and testing dataset. The resultant figures prove that the SecureFed outperforms. Soon, we are planning to integrate the proposed aggregation method in different FL settings.

Author Contributions A Makkar conceptualized the study and its methodology. KC Santosh discussed on its merits on the application of medical imaging data (chest X-ray). A Makkar wrote the original draft and KC Santosh reviewed, revised, and finalized the manuscript.

Funding Not applicable.

Availability of supporting data Not applicable.

Declarations

Conflict of interest There are no potential conflicts of interest reported by any of the authors.

Ethical approval and consent to participate This article does not include any human participant studies conducted by any of the authors

Human andanimal ethics This study did not include any human subjects or animals

Consent for publication This article contains no identifying information, so it is inapplicable

References

1. Afshar P, Heidarian S, Naderkhani F et al (2020) Covid-caps: A capsule network-based framework for identification of covid-19 cases from x-ray images. Pattern Recogn Lett 138:638–643
2. Ahsan MM, Nazim R, Siddique Z, et al (2021) Detection of covid-19 patients from ct scan and chest x-ray data using modified mobilenetv2 and lime. In: Healthcare, Multidisciplinary Digital Publishing Institute, p 1099
3. Alghamdi H, Amoudi G, Elhag S, et al (2021) Deep learning approaches for detecting covid-19 from chest x-ray images: A survey. IEEE Access
4. Alqudah AM, Qazan S, Alquran H, et al (2020) Covid-2019 detection using x-ray images and artificial intelligence hybrid systems. https://doi org/1013140/RG 2(16077.59362):1
5. Bhalla N, Pan Y, Yang Z et al (2020) Opportunities and challenges for biosensors and nanoscale analytical tools for pandemics: Covid-19. ACS Nano 14(7):7783–7807
6. Bhandary A, Prabhu GA, Rajinikanth V et al (2020) Deep-learning framework to detect lung abnormality-a study with chest x-ray and lung ct scan images. Pattern Recogn Lett 129:271–278
7. Bhapkar HR, Mahalle PN, Dey N et al (2020) Revisited COVID-19 mortality and recovery rates: Are we missing recovery time period? J Medical Syst 44(12):202. https://doi.org/10.1007/s10916-020-01668-6
8. Chouhan V, Singh SK, Khamparia A et al (2020) A novel transfer learning based approach for pneumonia detection in chest x-ray images. Appl Sci 10(2):559
9. Chowdhury ME, Rahman T, Khandakar A et al (2020) Can ai help in screening viral and covid-19 pneumonia. IEEE Access 8:132,665-132,676
10. Hu Z, Shaloudegi K, Zhang G, et al (2020) Fedmgda+: Federated learning meets multi-objective optimization. arXiv preprint arXiv:2006.11489
11. Kermany D, Zhang K, Goldbaum M, et al (2018) Labeled optical coherence tomography (oct) and chest x-ray images for classification. Mendeley data 2(2)
12. Kesim E, Dokur Z, Olmez T (2019) X-ray chest image classification by a small-sized convolutional neural network. In: 2019 scientific meeting on electrical-electronics & biomedical engineering and computer science (EBBT), IEEE, pp 1–5
13. La Salvia M, Secco G, Torti E et al (2021) Deep learning and lung ultrasound for covid-19 pneumonia detection and severity classification. Comput Biol Med 136(104):742
14. Liu B, Yan B, Zhou Y, et al (2020) Experiments of federated learning for covid-19 chest x-ray images. arXiv preprint arXiv:2007.05592
15. Loey M, Smarandache F, Khalifa M, NE (2020) Within the lack of chest covid-19 x-ray dataset: a novel detection model based on gan and deep transfer learning. Symmetry 12(4):651
16. Mahbub MK, Biswas M, Gaur L et al (2022) Deep features to detect pulmonary abnormalities in chest x-rays due to infectious diseasex: Covid-19, pneumonia, and tuberculosis. Inf Sci 592:389–401. https://doi.org/10.1016/j.ins.2022.01.062
17. Makkar A, Ghosh U, Rawat DB et al (2021) Fedlearnsp: preserving privacy and security using federated learning and edge computing. IEEE Consumer Electronics Magazine 11(2):21–27
18. Makkar A, Kim TW, Singh AK, et al (2022) Secureiiot environment: Federated learning empowered approach for securing iiot from data breach. IEEE Transactions on Industrial Informatics
19. Marques G, Agarwal D, de la Torre DI (2020) Automated medical diagnosis of covid-19 through efficientnet convolutional neural network. Appl Soft Comput 96(106):691
20. McMahan B, Moore E, Ramage D, et al (2017) Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics, PMLR, pp 1273–1282
21. Mukherjee H, Ghosh S, Dhar A et al (2021) Deep neural network to detect COVID-19: one architecture for both CT scans and chest x-rays. Appl Intell 51(5):2777–2789. https://doi.org/10.1007/s10489-020-01943-6
22. Nguyen DC, Ding M, Pathirana PN, et al (2021) Federated learning for covid-19 detection with generative adversarial networks in edge cloud computing. IEEE Internet of Things Journal
23. Panwar H, Gupta P, Siddiqui MK et al (2020) A deep learning and grad-cam based color visualization approach for fast detection of covid-19 cases using chest x-ray and ct-scan images. Chaos, Solitons & Fractals 140(110):190
24. Panwar H, Gupta P, Siddiqui MK et al (2020) Application of deep learning for fast detection of covid-19 in x-rays using ncovnet. Chaos, Solitons & Fractals 138(109):944
25. Qayyum A, Ahmad K, Ahsan MA, et al (2021) Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. arXiv preprint arXiv:2101.07511
26. Santos MS, Soares JP, Abreu PH et al (2018) Cross-validation for imbalanced datasets: avoiding overoptimistic and overfitting approaches [research frontier]. ieee ComputatioNal iNtelligeNCe magaziNe 13(4):59–76

27. Santosh K (2020) Ai-driven tools for coronavirus outbreak: Need of active learning and cross-population train/test models on multitudinal/multimodal data. J Medical Syst 44(5):93. https://doi.org/10.1007/s10916-020-01562-1
28. Santosh K (2020) COVID-19 prediction models and unexploited data. J Medical Syst 44(9):170. https://doi.org/10.1007/s10916-020-01645-z
29. Santosh K, Ghosh S (0) Covid-19 versus lung cancer: Analyzing chest ct images using deep ensemble neural network. International Journal on Artificial Intelligence Tools 0(ja):null. https://doi.org/10.1142/S021821302250049X
30. Santosh K, Ghosh S (2021) Covid-19 imaging tools: How big data is big? J Medical Syst 45(7):71. https://doi.org/10.1007/s10916-021-01747-2
31. Serte S, Demirel H (2021) Deep learning for diagnosis of covid-19 using 3d ct scans. Comput Biol Med 132(104):306
32. Speets AM, van der Graaf Y, Hoes AW et al (2006) Chest radiography in general practice: indications, diagnostic yield and consequences for patient management. Br J Gen Pract 56(529):574–578
33. Stoecklin SB, Rolland P, Silue Y et al (2020) First cases of coronavirus disease 2019 (covid-19) in france: surveillance, investigations and control measures, january 2020. Eurosurveillance 25(6):2000,094
34. Ulhaq A, Burmeister O (2020) Covid-19 imaging data privacy by federated learning design: A theoretical framework. arXiv preprint arXiv:2010.06177
35. WANG W, PEI Y, WANG SH, et al (2019) Pstcnn: Explainable covid-19 diagnosis using pso-guided self-tuning cnn
36. Wang W, Zhang X, Wang SH et al (2022) Covid-19 diagnosis by we-saj. Systems Science & Control Engineering 10(1):325–335
37. WHO (2021 (accessed November, 2021)) Covid report. https://covid19.who.int
38. Xia Y, Yang D, Li W, et al (2021) Auto-fedavg: Learnable federated averaging for multi-institutional medical image segmentation. arXiv preprint arXiv:2104.10195
39. Yang Q, Zhang J, Hao W, et al (2021) Flop: Federated learning on medical datasets using partial networks. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, pp 3845–3853
40. Zhang W, Zhou T, Lu Q et al (2021) Dynamic-fusion-based federated learning for covid-19 detection. IEEE Internet Things J 8(21):15,884-15,891
41. Zuo W, Zhou F, Li Z et al (2019) Multi-resolution cnn and knowledge transfer for candidate classification in lung nodule detection. Ieee Access 7:32,510-32,521