The Investigation Related to Application of Federated Learning's in Chest X-ray Detection

Haotian Tan *

Information Security, Shanghai Jiao Tong University, Shanghai, China

* Corresponding author: thtfinal@sjtu.edu.cn

Abstract. Following the global emergence of COVID-19 in 2020, the significance of Chest X-ray detection has grown exponentially as it plays a crucial role in diagnosing respiratory conditions. Concurrently, the evolving federated learning framework has been progressively integrated into the medical field, particularly in conjunction with Chest X-ray detection. This integration reflects a promising trend in enhancing collaborative diagnostic capabilities and leveraging collective knowledge across diverse medical institutions. Based on this background, this article provides a thorough review of medicine detection related federated learning frameworks and federated models, summarizes the characteristics and methods of federated models that have been widely used in various experiments in recent years, discusses and analyzes their advantages and disadvantages, and compares their performance with existing other machine learning models. In conclusion, the federated model outperforms non-federated machine learning models when it comes to analyzing Chest X-ray images and predicting symptoms. Lastly, this article outlines potential risks and offers improvement suggestions for the implementation of federated learning in chest X-ray detection.

Keywords: Federated Learning, Information Security, Chest X-ray.

1. Introduction

The COVID-19 epidemic from 2019 to 2022 permanently harmed public health and the economy. Similar illnesses, such as COVID-19 variations, continue to pose a hazard to human health today. As a result, a more effective and efficient method of identifying the infection's focal point is required. Medical detection has been deeply transformed by the combination of traditional detection methods and machine learning frameworks. However, using machine learning to diagnose illnesses will unavoidably result in some patient privacy being compromised, which is a major risk to data security. Federated learning sticks out in this context as a potentially useful way to improve medical information security.

Google made the first mention of federated learning (FL) in 2016 [1]. The aforementioned distributed machine learning system aims to maximize the effectiveness of artificial intelligence models while simultaneously protecting data privacy, security, and legal compliance. Furthermore, FL is superior to conventional frameworks in a number of ways: (1) Protection of Privacy. Without transferring raw data, federated learning enables model training on local devices or servers. To protect data privacy, only model updates are communicated instead. (2) Dispersion of power. Federated learning works well in decentralized situations because it minimizes the need for a centralized server and keeps the data on local devices. The possibility of unwanted access can be reduced in this way.

Federated learning models are frequently combined with deep learning networks in real applications due to their superior prediction capability [2-5]. Federated learning models not only guarantee a higher level of information security but also provide equal or even better performance than models solely based on single-institutional data. Federated learning involves incorporating local data into a global model without requiring users to transmit data to a single centralized server. The model is trained locally on each device instead, and the resultant parameter updates are aggregated by computing their average value before being uploaded back to the device [6]. In recent years, federated learning has been widely used in Chest X-ray (CXR) image recognition because CXR proved to be a fast and cost-effective way to COVID-19 screening [7]. Furthermore, lung infections including COVID-19 can all be detected by CXR, without the need for specific reagents. Therefore,

reviews on federated learning applications in CXR detection should be concluded, which also indicates the theme of this paper.

The paper will be organized into different sections. In Section 2, this paper will discuss various methods and prevalent applications of FL in detail. Section 3 will cover the current progress of FL in CXR screening and detection, along with the limitations and challenges of FL use in these fields. Finally, in Section 4, this paper will present the conclusion and potential future work.

2. Overview of Federated Learning Methods in Chest X-ray Detection

2.1. Definition

Federated Learning is a technique that involves distributing machine learning models to various devices that have independent datasets. The goal is to train the models across multiple devices while keeping the datasets private and secure. Its definition is as follows: defining N data owners $\{U_1, \dots, U_N\}$, and they have their dataset $\{D_1, \dots D_N\}$. In the framework of FL, every data owner collaborates to train one model M_{FED} without leaking any data to other data owners. In addition, the accuracy of M_{FED}, denoted by V_{FED}, is close to that of a model trained with all the data together, denoted by V_{SUM}. The absolute difference between V_{FED} and V_{SUM} should be lower than a non-negative real number δ [8].

There are three main types of Federated Learning [9]. Vertical Federated Learning is used when multiple parties hold different features of the same data, such as different patient attributes in the case of medical institutions. Horizontal Federated Learning is employed in situations where various institutions hold data of a similar nature but with unique data samples. Federated Transfer Learning emphasizes the enhancement of the model's applicability by allowing it to transfer knowledge from one domain to another.

2.2. Federated Models Used for Chest X-ray Detection

Experiments have been carried out to evaluate different federated models in CXR detection, combining Federated Learning with CXR to guarantee the security and privacy of patients' data while providing accurate detection and disease prediction. Some particular models will be presented as follows.

2.2.1. EXAM Model

Built upon a clinical decision support model [10], the EXAM model incorporates CXR images, along with clinical and medical data, as its inputs [11]. The model utilizes a comprehensive set of 20 features, comprising 19 electronic medical record (EMR) features and 1 CXR feature. To extract features from CXR images, a multiple-layer convolutional neural network known as ResNet34 is utilized. The FL method was employed to train the model with the client-server fusion of EMR and CXR features. When the dataset was relatively small, global FL models outperformed locally trained models by around 16% [11].

2.2.2. Dynamic Focused Federated Model

In the dynamic-focused federated learning approach, models with poor performance, especially those with high training loss, are emphasized. This technique differs from other federated methods because of the introduction of the dynamic factor q and the structure of iteration [12]. During global iterations, clients train the model with their local training sets. After uploading the parameters and training loss, the factor q will be updated and utilized as the next iteration's new input. Additionally, unlike FedAvg [1], which directly averages all the local parameters to generate the global parameter, the aggregation of local parameters in dynamic-focused federated learning considers the loss proportion. Dynamic focused federated learning achieves faster convergence and slightly higher accuracy than FedAvg.

2.2.3. Decision-making Based Federated Learning Network (DMFL_Net)

DMFL_Net is convenient for reducing communication costs associated with the transmission of parameters and improving communication efficiency. With the help of local models, DMFL_Net can select clients to take part in the model combination process [13]. During each round of model updates, with the exception of the first round, every client is allocated a timer to monitor their average training duration. If a client fails to finish the training process within the designated timeframe, they will be excluded from the aggregation process. If none of the clients can complete the training, the aggregation for that round will be skipped [14].

2.2.4. Other Federated Existing Models

Federated Learning can not only be used to create new machine learning models but also to improve the performance of existing ones. Various experiments have been conducted to compare the convergence speed, training loss, and accuracy of different models with and without the federated learning network. In one of these experiments, COVID-Net, ResNet18, and some other networks were combined with federated learning. When trained with the same parameters, ResNet18 demonstrated superior accuracy and faster convergence compared to other tested models [7,15].

3. Discussion

The concept of federated learning has garnered attention, particularly when utilized in conjunction with chest X-ray imaging and detection technology amidst the COVID-19 pandemic. While the technology is in its early developmental phases, its potential for advancing disease detection and safeguarding patient privacy through artificial intelligence is substantial.

The application of federated learning, a machine learning technique, is becoming increasingly popular in the medical field, particularly in X-ray imaging and detection. Its privacy-preserving approach enables model training without sharing patient data, ensuring data confidentiality. Furthermore, it resolves the issue of isolated data storage and promotes the development of shared models without requiring local data. With access to independent data from different hospitals, federated learning can expand the size of the sample for model training and enhance its accuracy. This empowers clinicians to gain early insights into effective methods of treating patients, based on models that are trained on a diverse range of sources [16].

Despite improvements in data security, federated learning still carries many limitations in X-ray detection and disease prediction. The accuracy of federated models is closely linked to data quality and standardization. On one side, there is an imbalance in the availability of non-shared data from different hospitals, potentially resulting in reduced model performance on specific datasets. On the other side, the reliance on distributed device networks can introduce a substantial communication overhead in federated learning methods.

It is important to note that while data security has improved overall in federated learning, it cannot solve all medical data security issues. In the process of federated learning, some information is shared. If opponents can observe each update of the federated model (especially parameter updates), they can increase the risk of data leakage through reverse engineering [6]. Furthermore, deliberately designed data can be used for data poisoning, which will pollute the datasets and interfere with the training process.

4. Conclusion

This paper provides a comprehensive review of Federated Learning, its background, characteristics, and definition, with a particular focus on its application in CXR Detection. The first section of the paper offers a detailed introduction to Federated Learning, covering its history, the advantages it provides over traditional machine learning, and its suitability for privacy-sensitive data. The definition and working of Federated Learning are also explained in detail. In the next part, the paper provides a thorough analysis of various federated models used in CXR disease detection. The

models' structures, including their architectures, training methods, and optimization algorithms, are presented and analyzed in detail, highlighting their advantages and limitations. This paper delves into the realm of Federated Learning's use in CXR detection, accentuating its superiority over centralized learning, while tackling potential hazards. It further encapsulates the present advancements and typical applications, underscoring the significance of safeguarding both the model and data. In conclusion, the paper puts forth promising research avenues like enhancing communication efficiency and fortifying the system against possible attacks.

References

[1] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data. Artificial intelligence and statistics. PMLR, 2017: 1273 - 1282.

[2] Qiu, Y., Wang, J., Jin, Z., Chen, H., Zhang, M., & Guo, L. Pose-guided matching based on deep learning for assessing quality of action on rehabilitation training. Biomedical Signal Processing and Control, 72, 2022, 103323.

[3] Kaastra, I., & Boyd, M. Designing a neural network for forecasting financial and economic time series. Neurocomputing, 10(3), 1996, 215 - 236.

[4] Yurochkin, M., Agarwal, M., Ghosh, S., Greenewald, K., Hoang, N., & Khazaeni, Y. Bayesian nonparametric federated learning of neural networks. In International conference on machine learning (pp. 7252 - 7261), 2019, PMLR.

[5] Zhu, H., & Jin, Y. Multi-objective evolutionary federated learning. IEEE transactions on neural networks and learning systems, 31(4), 2019, 1310 - 1322.

[6] Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. NPJ digital medicine, 2020, 3 (1): 119.

[7] Feki I, Ammar S, Kessentini Y, et al. Federated learning for COVID-19 screening from Chest X-ray images. Applied Soft Computing, 2021, 106: 107330.

[8] Yang Q, Liu Y, Chen T, et al. Federated machine learning: concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10 (2): 1 - 19.

[9] Mammen P M. Federated learning: Opportunities and challenges. arXiv preprint arXiv:2101.05428, 2021.

[10] Musen M A, Middleton B, Greenes R A. Clinical decision-support systems. Biomedical informatics: computer applications in health care and biomedicine. Cham: Springer International Publishing, 2021: 795 - 840.

[11] Dayan I, Roth H R, Zhong A, et al. Federated learning for predicting clinical outcomes in patients with COVID-19. Nature medicine, 2021, 27 (10): 1735 - 1743.

[12] Li Z, Xu X, Cao X, et al. Integrated CNN and federated learning for COVID-19 detection on chest X-ray images. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2022.

[13] Malik H, Naeem A, Naqvi R A, et al. DMFL_Net: A Federated Learning-Based Framework for the Classification of COVID-19 from Multiple Chest Diseases Using X-rays. Sensors, 2023, 23 (2): 743.

[14] Zhang W, Zhou T, Lu Q, et al. Dynamic-fusion-based federated learning for COVID-19 detection. IEEE Internet of Things Journal, 2021, 8 (21): 15884 - 15891.

[15] Liu B, Yan B, Zhou Y, et al. Experiments of federated learning for covid-19 chest x-ray images. arXiv preprint arXiv: 2007. 05592, 2020.

[16] Xu J, Glicksberg B S, Su C, et al. Federated learning for healthcare informatics. Journal of Healthcare Informatics Research, 2021, 5: 1 - 19.