Intelligent Healthcare with Federated Learning: A Brief Investigation

Hengjie Ma[a]
Data Science and Big Data Technology with Contemporary Entrepreneurialism, Xi'an Jiaotong-Liverpool University, Suzhou, China

Keywords: Federated Learning, Machine Learning, Healthcare, Medical.

Abstract: Intelligent healthcare is an emerging field that leverages technologies such as wearable Internet of Things (IoT) devices and deep learning to analyze various types of medical data, including traditional records, medical images, and sensor data from wearables. These innovations facilitate more accurate diagnosis and personalized treatment. However, they also raise significant privacy concerns, as sensitive data collected from devices like smart speakers and IoT wearables may be vulnerable to breaches. Federated Learning (FL) offers a promising solution by allowing data to remain on local devices while sharing only model updates with a central server. This method enhances privacy and reduces the risks associated with transferring personal medical data. This paper summarizes some of the recent research outcomes in this field, including a brief introduction to the federated learning algorithm and its variants, a privacy-preserved medical data processing model SCALT, different FL-IoMT architectures according to data partition, a clustered federated learning based multimodal COVID-19 diagnosis model and voice recognition-based Alzheimer's disease detection ADDetector. However, challenges such as data heterogeneity and hardware limitations remain, requiring further algorithmic improvements and specialized hardware development. As FL holds the potential to revolutionize healthcare, enabling safer, more efficient processing of medical data while protecting patient privacy, this paper gives this brief review to investigate the current outcomes of this field and gives out.

1 INTRODUCTION

Intelligent healthcare is one of these days' emerging fields. This technology usually combines the usage of wearable Internet of Things (IoT) devices and deep learning methods to utilize the healthcare data analysis and treatment from a variety of types of data including regular medical records, e.g., Electrocardiogram (ECG), medical image data, gene data and data collected from wearable IoT devices (Sun & Wu, 2022; Kumar & Singla, 2021), other types of data that is not from medical inspections while could be processed through deep learning methods, e.g., voice based neural diseases diagnostic (Li et al., 2021).

However, with large numbers of healthcare data collected for intelligent healthcare model training, this technology soon faces some limitations. According to Li et al. (Li et al., 2021), voice-based Alzheimer's Disease detection implemented on smart speakers would involve recording voices from users' home environment, indicating a serious privacy problem. Medical data collected from wearable IoT devices used for training these models have the same privacy issues as illustrated by Thilakarathne et al., as those data typically have a strong connection with a specific personnel, which centralized cloud computing could lead to potential data leakage. Furthermore, traditional centralized cloud computing requires other infrastructure to provide smart service, consuming more resources and less efficient compared to if this intelligent could be implement on device-side, which would enable real-time processing (Guo et al., 2022). In this case, many emerging studies combine the Federated Learning (FL) algorithm to give these issues a potential solution. Instead of centralized cloud computing, FL processes data on the local client and then send a new iteration of model back to the server for aggregation, preventing the potential of sensitive data leakage caused by data transferring. Based on the implementation of FL, edge-computing is more important as the model would be trained natively, as

[a] https://orcid.org/0009-0003-4218-7707

Ma and H.
Intelligent Healthcare with Federated Learning: A Brief Investigation.
DOI: 10.5220/0013527500004619
In *Proceedings of the 2nd International Conference on Data Analysis and Machine Learning (DAML 2024)*, pages 516-520
ISBN: 978-989-758-754-2

a result edge intelligent could be achieved (Akter et al., 2022). This could enable some IoT health data sensors to provide intelligent services to the users directly, rather than relying on a specified platform, which contributes to energy efficiency according to Akter et al (Akter et al., 2022). Considering that the development of intelligent healthcare would be greatly rely on large amounts of data as deep learning algorithms seems gradually plays a more important role in smart healthcare, involving FL would contribute to balance data collection and privacy protection. Besides, since no sensitive data transferred in this process, this enables facilities including hospitals and medical institutions to share the training results, so that the final aggregated model would generally perform better compared to the models from only one institution (Kumar & Singla, 2021). Hence, FL provided an essential opportunity for training outcomes to be shared, while keeping all the data stored and processed natively.

Currently, the study of implementing FL on intelligent healthcare has a range of outcomes, with many of these already being able to be introduced to practice. Sun and Wu (Sun et al., 2022) introduced SCALT, an efficient privacy-protective FL-based medical sensor data classification system. Li et al. (Li et al., 2021) developed a voice-based Alzheimer's disease (AD) detection system deployed on smart speakers with FL for privacy protection. In the meantime, with the continuous development and growth of FL algorithms and edge-computing hardware, intelligent healthcare now has a relatively firm platform and infrastructure to be further developed. This study will give a review of recent research outcomes in the field of Federated Learning and intelligent healthcare. The organization of this article is as follows. Section 2 introduces current methods of implementing FL algorithms on intelligent healthcare, Section 3 discusses current hurdles and possible future developments, and Section 4 concludes the whole paper.

2 METHOD

2.1 Introduction to Federated Learning

FL shown in Figure 1 is a distributive deep learning algorithm where only locally trained models will be sent back to the central server for aggregation, as the training data will be kept on the local devices. This algorithm was developed to reduce the privacy risks since it prevents data from being transmitted between devices and the cloud (McMahan et al., 2017). With the further development of FL, there comes with a range of variants including FedAvg, which performs stochastic gradient descent locally with a server for model aggregation, and FedProx, which modifies FedAvg and adds a proximal term μ, providing that FedProx performs more robustly in heterogeneous networks (Li, Sahu et al., 2020). FL is currently widely deployed especially on edge-computing devices including mobile phones and IoT hardware, providing features containing input predictions, photo processing and Optical Character Recognition (OCR) without violating privacy.

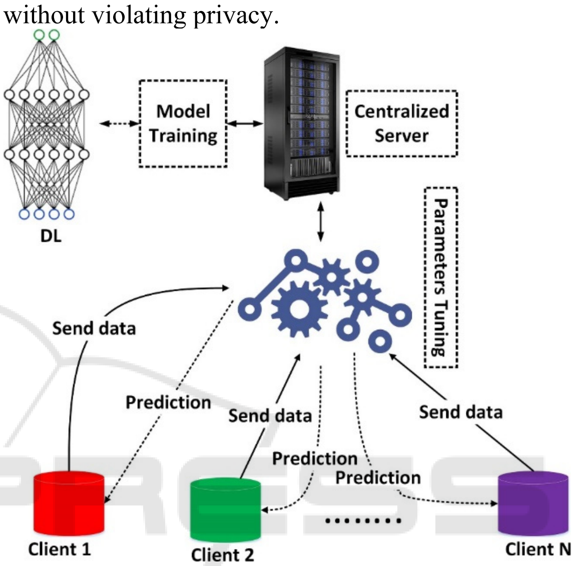

Figure 1: The workflow of Federated Learning (Ullah et al., 2023).

2.2 Federated Learning Based Healthcare Data Analysis

2.2.1 SCALT

Federated Learning concept could be implemented onto IoMT devices, provide a better privacy protection while processing the patients' health information. A system named SCALT (Sun & Wu, 2022) is proposed to deploy on edge devices including wearables and cell phones. Those devices will collect health data including ECG, heart rate, body temperature and so on. Then those data will be processed by SCALT, generate the result to assist the doctor's decision. During this process, the local model will be trained on edge devices using locally collected dataset. The training process of SCALT first denoise the collected dataset by wavelet transform, then it will be reconstruct and segment into short slices. Each slice will then be normalized and extract the feature. Since SCALT is mainly used on edge devices with limited computing power, it uses a lightweight 1-D CNN network. The extracted slice features will then be classified using per-class classifier (PCC). The use of PCC allows SCALT to adapt different tasks as a PCC could be simply added for a new class. An original SCALT model will be initially trained on the cloud, then distribute to edge devices for local training. By implementing FL, only new parameters will be required to send back to the cloud server, avoiding the exposure of original health sensor data.

2.2.2 FL-IoMT

Another study done by Thilakarathne et al. (Thilakarathne et al., 2022) also introduced FL-IoMT architecture. This study categorized FL into three different types according to their data partition architecture: vertical FL (VFL), horizontal FL (HFL) and federated transfer learning (FTL). In a HFL case the local databases are with the same feature space but different sample spaces, while a VFL case is an inversion of HFL. In a FTL case the local databases will have different feature spaces and sample spaces. The study also divided the architecture into two categories with respect to whether the network is centralized or decentralized. A centralized FL network, according to Thilakarathne et al., is usually for protect the privacy and security of the training dataset, as the decentralized network will not mandatorily require a central server to aggregate each local model. In this case peer-to-peer (P2P) communications will be introduced between each client for model exchanges. By applying FL architecture, researchers could access to datasets which may contain sensitive medical information safely, which could also accelerate the improvement of algorithms as mentioned by Thilakarathne et al. FL could also be implemented in medical imaging processing and analysis. Thilakarathne et al. provides that computer vision algorithms with FL could be used for tumor segmentation and computed tomography (CT) and magnetic resonance imaging (MRI) image diagnosis.

2.3 Federated Learning Based Edge Diagnosis

2.3.1 Clustered Federated Learning

A study conducted by Qayyum et al. (Qayyum et al., 2022) focused on multi-model edge diagnosis of COVID-19 using FL. As proposed by Qayyum et al., traditional methods of diagnosing COVID-19 usually only use one modality and without FL, some FL-based methods still use single modality to diagnose. Considering deploying ML at the edge could easily face privacy issues, along with data heterogeneity, communication costs and other challenges.

Considering those challenges, Qayyum et al. (Qayyum et al., 2022) proposes a chest image classification model using multiple sources based on Clustered Federated Learning (CFL). The two clusters are two medical facilities with one of them have clients with X-ray images, another have clients with Ultrasound images. Local training will be performed at those two facilities, then send the weights updates to central server to aggregate the multimodal model. In addition, as noted by this study, conventional FL could not train a single multi-modal.

For the dataset, they first convert the X-ray and Ultrasound images into gray-scale image, then resize to 256×256. Those resized images will then be normalized for training. Adam optimizer was used during their training process. The study compared the performance of CFL multimodal model and conventional FL multimodal model with specialized conventional FL model. As shown by the study, the CFL model performs better compares to conventional FL methods, and it could also confirm that a collaboratively trained model is able to recognize the test images without having explicit knowledge about all these modalities.

2.3.2 ADDetector

Another study completed by Li et al. proposed a FL based privacy-preserving smart healthcare system named ADDetector that could be deployed onto smart speakers and use users' voice input to detect whether the user has AD. They designed this system to be easy to deploy, high efficiency and privacy preserving, and FL is relatively suitable for those requirements (Li et al., 2021).

The ADDetector, as mentioned by Li et al. (Li et al., 2021), is constructed by three layers: user layer, detection layer and the cloud layer. The data collection model was used in the user layer, prompt the user to provide voice samples for AD detection. The detection process will extract features from both acoustic and linguistic aspects. Then the data will be processed by the FL-based decision module and assign the features to detection clients, and then optimize the AD classification by interacting between clients and the cloud. By implementing FL network, those raw data could be processed at user level, avoiding transferring voice records containing the users' home environment and personal voice to the cloud. Finally, they use the Asynchronous Privacy-Preserving Aggregation Module for model aggregation, as well as ensuring the integrity of the interaction between clients and the cloud.

For the performance, they utilized the ADReSS Challenge dataset for testing. When using 3 clients in the FL network, ADDetector have an accuracy of 81.9% under Laplace-based DP protection and cryptography-based scheme, and it takes 711.55ms per user detection on a desktop system, which considered acceptable in the smart home scenario. Further study by them shows that the most time-consuming stage is feature generation (97.9% of total time), proving that the privacy-preserving schemes by this study are time efficient. For real world scenarios, the model proposed by them maintains an accuracy of 78%, demonstrating the effectiveness and robustness of ADDetector.

3 DISCUSSION

As more studies concentrate on FL implementation on intelligent healthcare, there do have more approaches for medical data processing and disease diagnosis based on different modal of data. However, there still some hurdles on the way to overcome. As the FL models will mainly be trained locally, which means the dataset would mainly come from the edge device, usually varies a lot compared to centralized training as centralized training would usually use pre-made high quality datasets, while edge devices may not be able to perform this selection process on the dataset. As a result, this heterogeneity would cause the aggregated model's performance to vary from device to device, so do the training process. This would require improving the FL algorithm to adapt such varying environments or design the original model to be client-specific to minimize the issue (Qayyum et al., 2022).

Another issue would be potential impacts of data heterogeneity in the system. This would become more significant when involving model sharing between medical authorities, as a well-trained model from hospital A might have a decreased performance when using data inputs from hospital B. Although as mentioned above, FedProx model would help to minimize the impact of data heterogeneity, however considering the application is in the field of healthcare, this issue might still require the development of FL algorithm to further improve the overall performance of the models under data heterogeneous conditions, which is considered common in realistic implementation.

Besides the algorithm itself, the performance bottlenecks of the hardware are another potential hurdle. Considering this technique has a strong connection with IoT devices, it is a necessity that FL models should be designed to be efficient, drawing a little amount of computing power while still maintain an acceptable accuracy. This would require the optimization and possibly specialized models to focus on a certain objective to reduce the overall performance consumption, or the improvement of IoT hardware to allow running higher performance models with no significant higher consumption of power.

While besides those difficulties, the future of FL based network on healthcare is still bright. For the FL algorithm itself, the original FedAvg algorithm would simply drop those clients who could not reach the required local steps, causing the system could easily be disrupted by the heterogeneity inside the network. While improved FL algorithms including FedProx and Scaffold (Karimireddy et al., 2020) avoids to do so and use certain computations to add correction onto the local updates from each client, in this way optimized the speed and robustness of the training process.

In the meantime, those improved FL algorithms also perform better on heterogeneous data compared to the original FedAvg. According to Li et al., FedProx would have a significantly improved training loss in normal data heterogeneous conditions and could converge in extreme data heterogeneous conditions compared to FedAvg, which would not converge in this case. This made FL based medical models more applicable, since real world data would have some heterogeneity, it is considered essential for a medical model to maintain a certain accuracy in heterogeneous conditions.

The development of IoT devices also supported to solve the performance bottleneck. With more efficient chips developed and the appearance of deep learning specified processors including Neural network Processing Unit (NPU) and Tensor Processing Unit (TPU), low power IoT devices were able to process high performance models efficiently, eventually improving the overall accuracy of the model while only requiring a little amount of power, making the actual large-scale application to be possible.

4 CONCLUSIONS

This paper summarized some of the recent methods and implementations of Federated Learning in intelligent healthcare. The paper briefly introduced the mechanism of FL and one improved FL method: FedProx. The paper reviewed two methods: SCALT and FL-IoMT architecture, and two edge diagnosis implementations: edge COVID-19 diagnosis and ADDetector. Currently the implementation of FL models helped to provide a privacy-preserved way for better data processing and earlier diagnosis, however those methods would require further validation to build trust among users, or be verified by medical authorities to be used for realistic applications. Those methods would need to be utilized for better performance with reduced hardware cost, which also requires to combine with the development of FL algorithm itself.

REFERENCES

Akter, M., Moustafa, N., Lynar, T., & Razzak, I. 2022. Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. IEEE Journal of Biomedical and Health Informatics, 26(12), 5805-5816.

Guo, K., Chen, T., Ren, S., Li, N., Hu, M., & Kang, J. 2022. Federated learning empowered real-time medical data processing method for smart healthcare. IEEE/ACM Transactions on Computational Biology and Bioinformatics.

Karimireddy, S. P., Kale, S., Mohri, M., Reddi, S., Stich, S., & Suresh, A. T. 2020. Scaffold: Stochastic controlled averaging for federated learning. In International Conference on Machine Learning (pp. 5132-5143). PMLR.

Kumar, Y., & Singla, R. 2021. Federated learning systems for healthcare: perspective and recent progress. In Federated Learning Systems: Towards Next-Generation AI (pp. 141-156).

Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q., & Shen, X. 2021. A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics, 18(3).

Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. 2020. Federated optimization in heterogeneous networks. Proceedings of Machine Learning and Systems, 2, 429-450.

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. 2017. Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics (pp. 1273-1282). PMLR.

Qayyum, A., Ahmad, K., Ahsan, M. A., Al-Fuqaha, A., & Qadir, J. 2022. Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge. IEEE Open Journal of the Computer Society, 3, 172-184.

Sun, L., & Wu, J. 2022. A scalable and transferable federated learning system for classifying healthcare sensor data. IEEE Journal of Biomedical and Health Informatics, 27(2), 866-877.

Thilakarathne, N. N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R. K., & Shafiq, M. 2022. Federated learning for privacy-preserved medical internet of things. Intelligent Automation & Soft Computing, 33(1), 157-172.

Ullah, F., Srivastava, G., Xiao, H., Ullah, S., Lin, J. C. W., & Zhao, Y. 2023. A scalable federated learning approach for collaborative smart healthcare systems with intermittent clients using medical imaging. IEEE Journal of Biomedical and Health Informatics.