Federated Learning in Remote HealthCare: A Generalization as well as Personalization Perspective

K. Yadav

National Insititute of Technology, Kurukshetra

The growth of machine learning has brought about a revolutionary change in the field of drug discovery, gene sequencing, and health monitoring [1]. In health monitoring, a large amount of patient data needs to be collected, fed into a machine learning model, and trained. These data include patient name, patient medical history, patient address, age, etc. Due to the privacy of the people's individual data, they are no longer willing to share with the organizations who build this model. Additionally, countries such as the USA and UK are imposing strong regulations regarding the privacy of their people's data in exporting to other countries.

Using traditional machine learning in healthcare violates the privacy of people. To mitigate the privacy issue and extract knowledge from the data without exporting it to the server-side, federated learning has brought a very good impact on health care [2]. The architecture of federated learning based remote health monitoring system is presented in Figure 1. Federated learning consists of two aspects: server and client. At the client-side, there are various lightweight sensors attached to different parts of the body, such as the chest, right wrist, ankles, etc. These sensors are wirelessly connected by either Bluetooth or Wi-Fi to patient mobile devices. These sensors record medical readings, such as heartbeat rate, acceleration, sugar level, oxygen level, etc. From the server- side, a global deep learning model is sent to each mobile device where the medical readings are stored. The model is trained on the device data, and the weights of the model are updated. Weights from these devices are then sent to the server for aggregation. With the help of weight aggregation, individual devices learn from the data of other peer devices that participate in federated training. After a large number of federated training rounds, finally, the model converges; however, it takes a more number of rounds of federated training for the model to converge than that of traditional machine learning. The trained model then provides health monitoring by providing feedback in the form of medical reports, alerts, and suggestions. The advantage of federated learning over traditional learning is that it's data are updated on a very regular basis. Frequent data updation can detect rapidly evolving medical circumstances and provide suggestions accordingly.

Federated learning can help in providing generalized as well as personalized medical suggestions. A generalized medical suggestion is when during model training, the learning from all the devices is given equal weights. Let's consider a situation where a person has only high blood pressure and another person has high blood pressure, which leads to nausea, headache, bleeding. A generalized learning model will provide a medical suggestion to the person with only blood pressure that high blood pressure may sometimes lead to nausea and bleeding, and a way to prevent these further complications early.

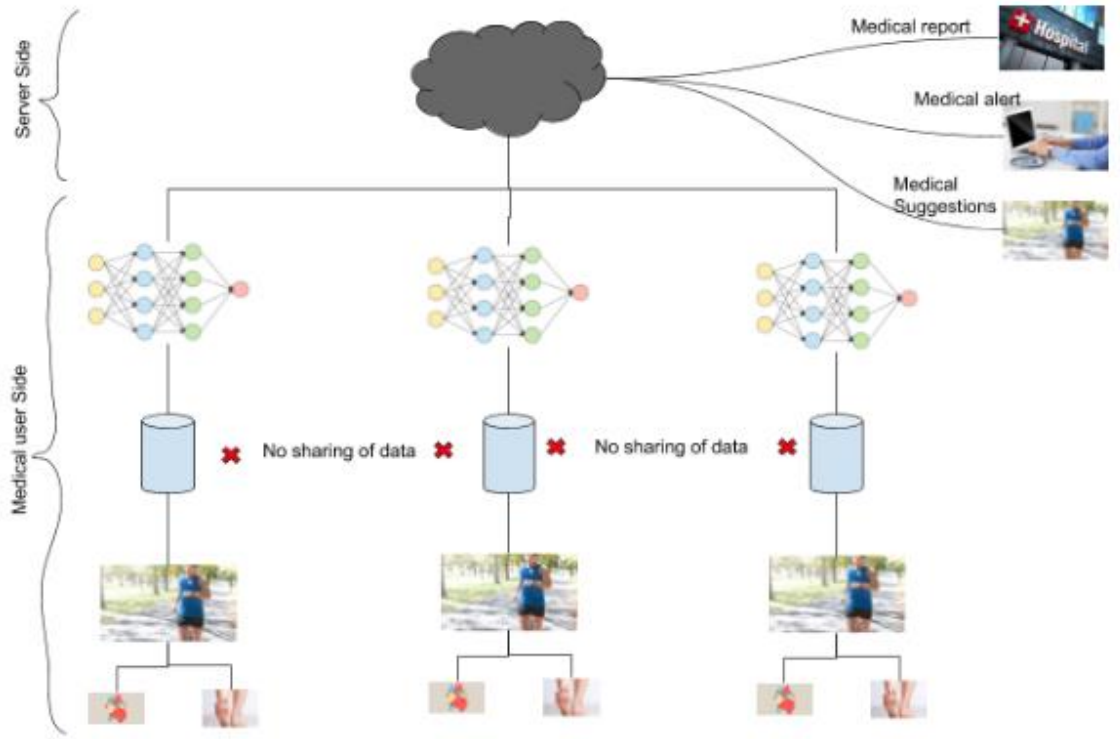

Fig 1: Architecture of federated learning-based remote healthcare system

In personalized learning, instead of giving equal weights to the updates from each device, a more specific model is created for each device by giving more weights to them. There can be a very novel medical condition to some people, such that this medical condition is not present in other people and requires special medical suggestions. To achieve this, a personalized model can be built with the help of multi-task learning.

Open research problems in federated learning

- Although, federated learning is not fully secured against privacy issues. During the exchange of weights, original data can be reconstructed from weights [3]. The reconstructed data may not provide all information; however, it may provide some useful information. Several efforts must be made to prevent this problem.
- When the dataset of medical records is created at the client-side, some clients may be malicious in nature and can inject poison data that degrades the performance of the global model [4]. A wide range of research is being carried out by numerous researchers worldwide to address these existing issues.

References

1. Bhardwaj, Rohan, Ankita R. Nambiar, and Debojyoti Dutta. “A study of machine learning in healthcare.” *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 2. IEEE, 2017.
2. Xu, Jie, et al. “Federated learning for healthcare informatics.” *Journal of Healthcare Informatics Research* 5.1 (2021): 1-19.

3. Geiping, Jonas, et al. “Inverting Gradients–How easy is it to break privacy in federated learning?.” *arXiv preprint arXiv:2003.14053* (2020).
4. Tolpegin, Vale, et al. “Data poisoning attacks against federated learning systems.” *European Symposium on Research in Computer Security*. Springer, Cham, 2020.