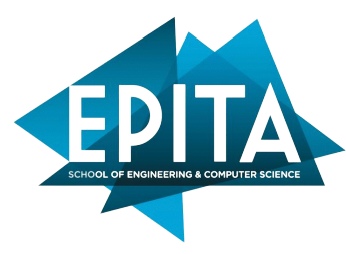
­



Federated Learning on Health Care Applications

Aida Zadinova, Ediz Emektas, Nataly Michail

EPITA, l'école des ingénieurs en intelligence informatique

**Federated Learning on Health Care Applications: A Literature Review**

**ABSTRACT**

Federated learning (FL) is a learning paradigm with which we seek to govern data and secure it such that user information is no longer linked to a specific person. This allows machine learning models to work on said data without having to worry about a user’s private information being leaked. ​​Data transferring processes for networks having multiple clients have always been open to vulnerabilities and privacy issues. It is not desired to gather all clients in distributed learning to share all the private data to the cloud or the central server. It is the main reason for the development of distributed learning architectures that could let the network use privately gathered data to train in a learning model locally. At this point, Federated Learning helps the network to enable clients to learn from a shared learning model altogether while having the data in a private position.

**INTRODUCTION**

Data-driven solutions have seen rapid growth in technology throughout recent years. With developing machine learning algorithms and advancements in artificial intelligence and deep learning, it has become increasingly apparent that there is a need for large amounts of data in order to properly make use of these technologies.

Thankfully, the availability of data has seen a massive increase these past few years. There are now several ways in which a company can collect information on their users, be it through their online activity, how often they check their phones, or even the extent of their mobility thanks to the widespread adoption of smartwatches. But with this new influx of data comes a higher demand for responsibility, specifically in how user data is handled. There is a lot of sensitive data floating around these databases from dates of birth to credit card information. The sensitivity of this information escalates when one refers to medical records. For some AI-based medical applications, the data required for the system includes very critical patient data, like in the example of computerized tomography (CT) or magnetic resonance imaging (MRI) data which can ultimately be used to reconstruct a patient’s face.

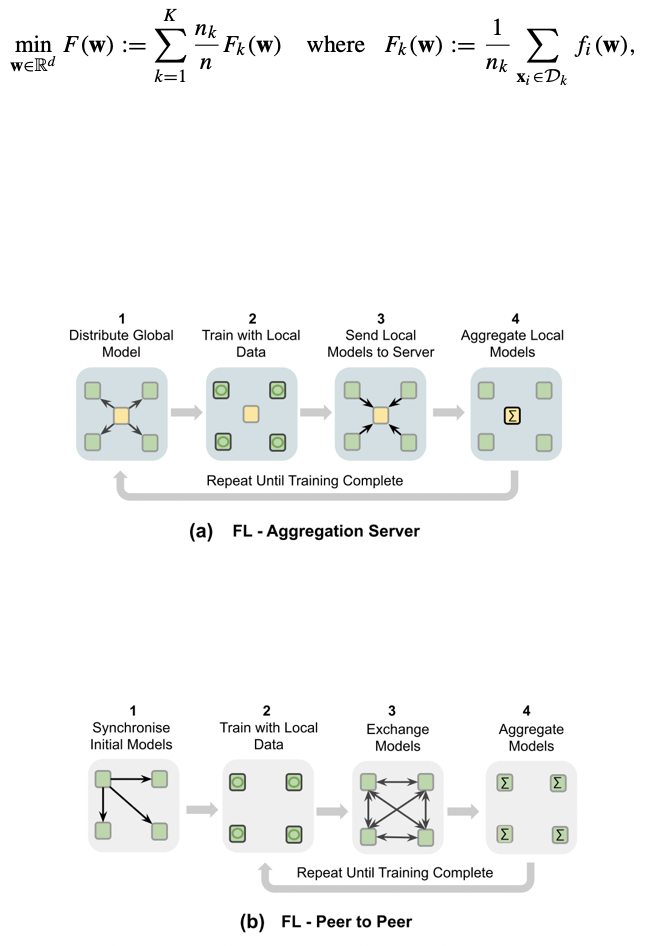
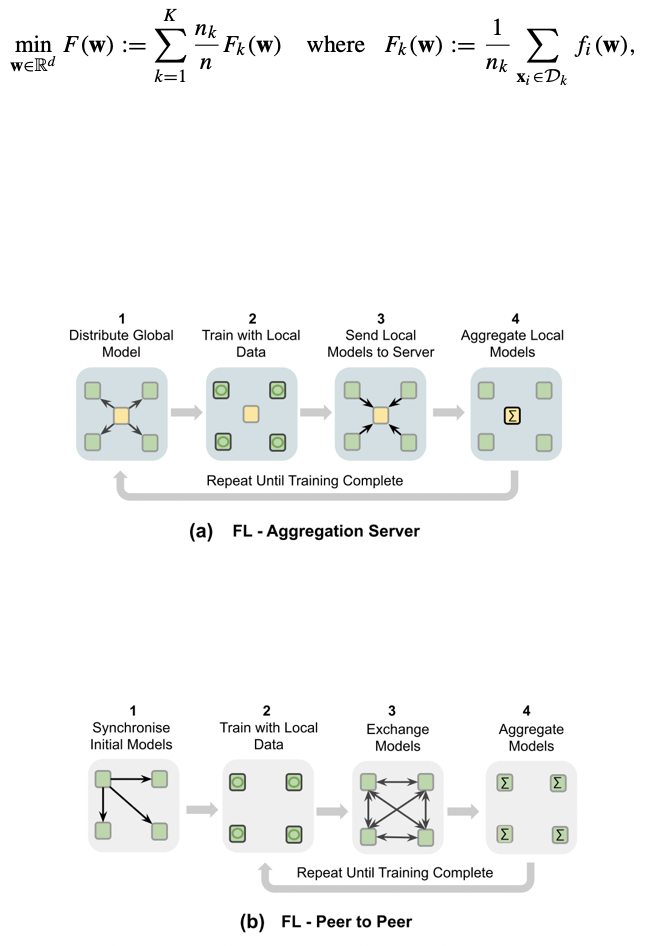
This is where federated learning comes in. FL allows healthcare applications to use their training models on patient data without seeing it. With FL, a model can gain insights into patient data without that data having to leave its original site. With this logic, any machine learning process would occur directly at the hospital in which the data resides and only the final results are known to the researcher. With that being said, FL still requires much development to enter the mainstream world of data analysis much of which will be discussed throughout this literature review.

**FEDERATED LEARNING VS LEARNING ON A CENTRALISED DATA LAKE**

In order to better understand how and why an FL model would serve as a better alternative to data lakes, the two images below show two different FL server models, aggregation servers and peer-to-peer servers.

Image a) depicts the FL aggregation server. In it, data in the training nodes (shown as green squares) receive a global model from the global server (yellow square) that trains the local data and sends back a partially trained model to the central server for aggregation. The process is then repeated until training is complete.

Image b) showcases the peer-to-peer model that instead allows each training node to exchange its own partially trained model with the rest of the nodes and each node does its own aggregation on the data received.



However, for centralized training, each site (hospital for example) must donate all the data to a central data lake allowing data scientists to extract whichever records they need for their own independent training.

**CONSIDERATIONS WHILE APPLYING FEDERATED LEARNING IN HEALTHCARE**

*Data heterogeneity*

Medical data is extremely diverse, random, and biased. When extracting large amounts of data from different hospitals, it is important to note that. For instance, Obermeyer et al. found that one of the more popular algorithms used to determine enrolment in specific health programs assigned the same level of risk to African Americans and healthier caucasian patients. This is due to an increased diversity of data sources. Most algorithms assume independently and identically distributed data (IID) that can be used without biasing which is often not the case.

*Privacy and security*

The level of privacy protection that FL offers highly exceeds any techniques used in today’s machine learning models. But that doesn’t mean it doesn’t come with its trade-offs. In general, the cost of securing patient data can mean a decrease in the performance of these techniques which could, in turn, affect the accuracy of the output. However, there are two types of FL collaboration that participants can use:

* Trusted: where all parties are trusted and are obliged to follow a collaboration agreement. This essentially removes any threats of data leakage or extraction or corruption of the model.
* Non-trusted: when a collaboration agreement cannot be achieved, to eliminate any dangers, advanced model submission encryption, secure authentication, action traceability, differential privacy, and other approaches are used instead.

*Traceability and accountability*

As opposed to centralized training, FL requires multi-party computations from each node which can differ in hardware, software, and networks. This means that there needs to be a method in which all parties are held accountable after the training process by measuring how much each participant contributed to the computational resources they consumed as well as the quality of data they used. This is especially true for non-trusted federations. Traceability would show each participant’s data access history as well as their training configurations during training.

*System architecture*

Usually, medical sites are equipped with state-of-the-art computational resources and good, reliable networks. While this may help facilitate the training steps, it comes with its own problems. Compromised data integrity is an issue that is dealt with by designing secure encryption methods or scheduling the nodes to better distribute computational power.

*Unlabeled Data*

Large-scale systems containing huge amounts of data points can be challenging to handle. To be able to process through each row of the datasets, each data point has to be labeled and ordered in the same order. However, the data points in the real world use cases can be unlabeled or labeled in the wrong way. This issue will cause a complex problem in detecting each client’s very specific data.

*Asynchronous Federated Model/Data/Client*

As the ordered and labeled data matters, the association between the data points has a significant impact on the predicted results. This problem might occur on the model, data, and over the client end. The progress of the complete system will depend on the slowest step, the least performant point always decides the total performance of the Federated system.

*Dropped Clients*

In the Federated Network, the appearance of each client end is presumed as available. But in practice, any client can go offline for several reasons such as connectivity issues and broken hardware. A large amount of dropped clients can undoubtedly cause accuracy issues which directly affect the performance and reliability of the Federated Learning system. The developed Federated architecture needs to be solid on client drops over the network and has to have anticipated scenarios for such problems, in both the network and the model wise.

**CONSENSUS IDEA**

Data transferring processes for networks having multiple clients have always been open to vulnerabilities and privacy issues. It is not desired to gather all clients in distributed learning to share all the private data to the cloud or the central server. It is the main reason for the development of distributed learning architectures that could let the network use privately gathered data to train in a learning model locally. At this point, Federated Learning helps the network to enable clients to learn from a shared learning model altogether while having the data in a private position.

Federated Learning is generally considered to be an effective privacy-first learning solution for participants to conduct collaborative model training. However, a malicious participant could exploit the process to gain access to other participants' sensitive information. In addition, by using Federated Learning’s common model, attackers can not only explode the entire learning system but also disguise the trained model and launch attacks to achieve malicious goals.

While on the other hand, communication expenses are important issues that need to be resolved before implementing Federated Learning on a large scale. Especially, modern Federated models have high inference accuracy but they are becoming more complex with millions of parameters. Therefore, slow upload speeds on mobile devices can hinder efficient Federated Learning implementation. Federated Learning does not guarantee privacy in the presence of malicious attacks or for server aggregations. Therefore, recent studies have clearly pointed out that malicious participants are present in Federated Learning systems and they can derive private information about other participants directly from shared parameters. Still, Federated Learning needs to consider privacy and security issues even if it is one of the most convenient options that can be selected on large-scaled architectures.

**FURTHER CONSIDERATIONS**

One of the main considerations of Federated Learning is the reliability of the algorithm used. Algorithms try to find balanced parameters to decrease the central model gatherings. It can be pointed out more as a shared optimization issue. The studies that have been done so far suggest analysis and evaluations of the consistent limits of the gradient slide-based Federated Learning for multiple and non-multiple-sided loss functions are significant research directions. As in the existing studies on the branch covering the topic, most of the assurances are bounded to limitations such as the curve of the loss function used.

Federated Learning is a noticeable player in the game and has an increasingly important aspect in many of the applications. Especially, in healthcare, mobile predictions, and transportation systems. Most current research on Federated Learning applications ignores implementation challenges and focuses primarily on integrated training in learning models. In addition to the research aspects, Federated Learning-based algorithms need to decide about the challenges mentioned in the review (data heterogeneity, privacy and security, etc.). Beyond, Federated models also need to consider the special issues connected to the architecture model in which the Federated algorithm will be tuned in. Especially, for the applications where the timing performance matters.

**OPEN QUESTIONS**

*Data quality*: most healthcare systems struggle with data overload and inefficiency. Data acquired from many sources is of varying quality, and there is no universal data standard. When unclean data is mistakenly utilized as samples, the analyzed findings appear to be useless.

*Incorporating expert knowledge*: Watson for Oncology, a tool that uses IBM's natural language processing engine to summarize patients' electronic health information and search the massive database behind it to advise doctors on treatments, was unveiled in 2016. Unfortunately, some oncologists believe they can trust their own judgment more than Watson's recommendations.

*Incentive mechanism*: a rising number of smartphone healthcare apps are compatible with wearable devices thanks to the internet of things and a range of third-party websites. Self-interested mobile or other wearable devices may be hesitant to engage in federal learning assignments without well-designed incentives, which will stifle the development of federated learning.

**CONCLUSION**

After carefully considering all the challenges that come with federated learning (including data heterogeneity, privacy and security, traceability and accountability, and system architecture), it becomes clear that the benefits greatly outweigh the downsides. FL ultimately protects an individual’s identity by ensuring that their personal data is not visibly connected to their medical data.

**REFERENCES**

Nicola Rieke, J. H.-H. (2020). The future of digital health with federated learning. npj Digit. Med., 119.

Jie Xu, B. S. (2021). Federated Learning for Healthcare Informatics. Journal of Healthcare Informatics Research, 5.

Tian Li, A. T. (2019). Federated Learning: Challenges, Methods, and Future Directions. 21.

Qiang Yang, Y. L. (2019). Federated Machine Learning: Concept and Applications. ACM

Transactions on Intelligent Systems and Technology.

Eugene Bagdasaryan, A. V. (2019). How To Backdoor Federated Learning.

Wei Yang Bryan Lim, N. C.-C. (2020). Federated Learning in Mobile Edge Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 2031-2063.

Mingzhe Chen, Z. Y. (2022). A Joint Learning and Communications Framework for Federated Learning over Wireless Networks.