Federated learning to solve the data-sharing problem in radiation treatment planning

Andreas Hellander, Associate Professor, Division of Scientific Computing, Department of Information Technology, Uppsala University, Uppsala, Sweden

Fredrik Löfman, Head of Machine Learning, RaySearch Laboratories, Stockholm, Sweden

This project has the following main goals:

1. Improving Federated Machine Learning (FedML) methodology. FedML is a new class of distributed and decentralized optimization methods for training ML models while preserving data privacy.
2. Exploring how the privacy-enhancing method of differential privacy together with FedML affects convergence properties and how well it protects against inversion attacks.
3. Unlocking sensitive training data to improve deep learning organ segmentation and tumor segmentation for radiation treatment planning.

Radiation treatment (RT) planning software helps clinicians develop the complex treatment plans needed to accurately deliver radiation to cancer tumors while avoiding damaging tissue and organs. A critical part of the process is accurate segmentation of organs and tumors from 3D imaging of the patient (typically CT scans). Traditionally, this has been a manual and time-consuming step. Recently, automatic organ segmentation based on deep learning has shown great promise to improve both accuracy and segmentation speed [1]. However, unlike traditional methods such as ATLAS, deep learning segmentation relies critically on expert-annotated clinical data from different body sites to train the models. RaySearch’s product RayStation is the first RT software to implement deep learning segmentation and treatment planning. The proposed collaboration is a uniquely well suited use-case for advancing state-of-the-art in privacy-preserving AI. RaySearch is a leader in the application area and they have strong partnerships with many cancer clinics, facilitating real impact on cancer treatment.

Problem and opportunity:

Large amounts of training data in the form of volumetric images from patients are needed. However, training data is sensitive and located at different cancer clinics and hospitals. This data cannot be pooled for regulatory reasons. Today, models can be trained in isolation on patient data at individual clinics. If we could instead train a joint model over data at multiple clinics without risking exposing the data, the potential to improve segmentation results, and hence the radiation treatment planning process, is substantial.

Proposed solution:

We will implement, critically evaluate and improve training schemes based on Federated Machine Learning (FedML) [2,3]. FedML is a recently proposed approach for training joint ML models under strong input privacy requirements. In short, a model is trained by letting local models be incrementally updated on local, private data, and then combined into a global model using an aggregation scheme. Only parameters related to the actual model and optimization process are exchanged. Since training data is not shared at any stage of the process, input privacy is maintained. It can still be possible for an adversary in some cases to learn about the training data by systematically observing the output of the model. Here, differential privacy has been suggested as a solution. Differential privacy is a mathematically grounded idea in which controlled levels of noise is added to the input data or in select stages of the optimization process. In theory, it is then possible to bound the privacy leakage when using the model. However, it is not clear how to practically estimate these bounds, how to calibrate the noise levels during FedML training, or how the addition of noise influences the accuracy and convergence.
Interdisciplinary nature of the project:
The project needs expertise both in scientific computing, distributed computing and stochastic processes (Hellander) and in cancer radiation treatment, computer vision and machine learning (Löfman). The industry aspect of the collaboration is essential since this gives access to a realistic setting where privacy requirements are currently blocking pooling of training data.

Specific scientific aims
To date, FedML has shown very promising results on benchmark problems and datasets such as MNIST and CIFAR-10 [2], but it is still unclear how convergence and performance is impacted for more complex problems. A critical aspect is that data at different clinics cannot be assumed to be neither i.i.d nor balanced. As a result, the problem is not a distributed machine learning problem – care needs to be taken to develop training strategies that are efficient for irregular data distributions. Furthermore, most of the so far published algorithms for FedML have targeted consumer or IoT use cases where local models updates are computationally cheap and the amount of data transferred in each iteration relatively small. In this scenario one can afford thousands of communication rounds to reach convergence. The scenario we are targeting here is the opposite, and we will seek to optimize training schemes including balancing learning rates to fit this situation and to ensure robust results. Specifically we will:

1. Implement the federated learning algorithm Federated Averaging [2] for a state-of-the-art 3D U-Net segmentation model.
2. Critically assess performance, convergence and scalability and optimize the training scheme to minimize the number of iterations/communication rounds given a target accuracy.
3. Investigate how to optimally leverage differential privacy to protect against inversion attacks, seek robust and scalable methods to estimate the degree of privacy leakage, and understand how to calibrate the noise levels for a good tradeoff between convergence and privacy-protection.

Federated Machine Learning
Simply speaking, training a FedML model proceeds by model updates on private data nodes, then weights are averaged by a server forming a global model (schematic figure inline). Care needs to be taken to balance local model training with global synchronization to avoid poor convergence and to minimize communication rounds. FedML differs from standard distributed learning/optimization in that data cannot be assumed to be balanced across nodes or low-latency high-throughput networking between nodes. During 2017 and 2018, Google Research presented an approach to FedML based on TensorFlow targeting mobile devices [2,3]. Other efforts include the open source project OpenMined and Tensorflow federated. Intel in collaboration with the University of Pennsylvania recently demonstrated a real-world case for FedML based on biomedical imaging [4]. In our group at UU we are currently working on various aspects of FedML such as new federated ensemble methods and schemes to measure individual member contributions in a scalable fashion. In collaboration with our spin-off company Scaleout Systems (www.scaleoutsystems.com) we are developing FEDn, an open source distributed framework for hierarchical FedML. FEDn is used in both industrial and academic collaborations in the AI Sweden collaboration.

Delimitations and feasibility
FedML is a new technique in the research community. The project focuses on gaining a more complete understanding of key properties of the federated optimization schemes under statistical heterogeneity (non-IID data partitions), with and without the addition of the privacy-enhancing technique of differential
privacy. FedML has also attracted major interest in the computer security domain. Systems security [7] will not be a focus in this project, although it would be a critical part of an enterprise-grade FedML system. We will also collaborate with Scaleout Systems on open source codes which reduces the risk of extensive software development and allows the PhD student to focus on the more theoretical and algorithmic aspects of the problem.

Impact

The project will demonstrate a novel way to solve the problem of gaining access to larger amounts of training data in a regulated sector. If successful the collaboration will demonstrate a new way of improving the organ segmentation step in a radiation treatment planning pipeline with large potential impact on cancer therapy. The insights gained will translate to many areas where ML is used and data is sensitive, private or too large to collect in a central storage. The project goes beyond state-of-the art in the science domain by:

1. Providing insight into the convergence, accuracy and efficiency of FedML for complex real-world application. This advances state-of-the-art in FedML.
2. Improved performance of federated training schemes under unbalanced and non-IID data scenarios.
3. An improved understanding of how privacy-enhancing techniques such as differential privacy influences the accuracy and convergence of the optimization process, for non-trivial models.

Supervisors, research environment and collaboration plan

The student will be enrolled in the PhD program in Scientific Computing, at the division of Scientific Computing, department of Information Technology. The division of scientific computing contributes 25% co-funding and the plan is that RaySearch contributes with 25%.

Andreas Hellander (main advisor) is Associate Professor in Scientific Computing at the Department of Information Technology, Uppsala University (hosting institution). He leads the research group Integrative Scalable Computing Laboratory, focusing on the interface of scientific computing, machine learning and distributed systems. He runs a number of projects with funding from SSF, VR and NIH. Hellander’s existing CIM PhD student Fredrik Wrede graduates in June 2020, before the start of the proposed project.

Fredrik Löfman (co-advisor) is Head of Machine Learning at RaySearch Laboratories. He holds a PhD in optimization with specialization in Radiation Therapy from KTH (2008) and has experience from various roles in R&D, project management and machine learning. Löfman contributes with a deep domain knowledge in radiation treatment planning and in machine learning.

The student will work in close collaboration with the machine learning department at RaySearch. To facilitate this, he or she will be offered to spend up to one day/week at RaySearch offices in Stockholm. In addition, we will hold monthly team-wide meetings online or at UU. The student will also collaborate with the software developers at Scaleout Systems on open source codes for federated learning.

References