Ph.D. position in Computer Science
(36 months)

Title: Mitigating bias for collaborative and ethical learning on dynamic data.

Host laboratory: LISTIC, Université Savoie Mont Blanc, Annecy-le-Vieux, France.

Advisors: Prof. Alexandre Benoit
Dr. Faiza Loukil
LISTIC, Université Savoie Mont Blanc, Annecy-le-Vieux, France.

Description

Today, machine learning is applied in many fields to extract knowledge from data and guide increasingly complex decision-making processes, from search engines to disease diagnosis. Therefore, it is crucial to ensure that the predictions made by these approaches do not reflect discriminatory behavior towards certain populations, in the statistical sense, either at the level of the data or at the level of the individuals. One of the factors that can lead to erroneous decisions is learning bias. It is usually the consequence of using incomplete, flawed, or prejudicial data sets and models. These biases originate at the time of data collection. This collection can take different forms depending how the model is optimized. Traditional approaches optimize a model on a central server. This implies communicating and aggregating all the data created from potentially distant and distributed sources on this server. This approach raises communication costs and privacy issues. Although in this traditional configuration, bias reduction can be achieved by having access to all the data, it remains an open problem.

To counter these different problems, a collaborative approach has recently been introduced, called Federated Learning (FL). It allows local optimization of models, close to each data source. Through a collaborative process, local models share their model parameters to gain generalization capability and produce a more general model, without transmitting the data. By reducing communication costs and protecting private data by complying with the General Data Protection Regulation (GDPR), FL appears to be a very promising approach. On the other hand, bias issues need to be considered by taking into account the participation rate and data distributions of each participating model [1]. Furthermore, the privacy constraints imposed in federated learning do not allow the use of traditional bias mitigation techniques. Thus, although FL appears to be a major step forward in machine learning, the study of its biases remains an important scientific issue to be addressed.

The state of the art reports several approaches based on different types of bias mitigation techniques, including preventive and reactive techniques. However, these approaches remain incomplete, impose compromises, and focus on a global approach. Beyond these global issues, one of the purposes of federated learning is to build models adapted to hierarchically organized populations to generate not only a single general model, but also a set of intermediate models relevant to different groups of populations. On the other hand, it may be interesting that these intermediate models can be dynamic. *Questions then arise about the potentially dynamic construction of the hierarchy. Consistently, it is then necessary to address the problems of bias and privacy that this may cause.* Within this realistic framework, the state of the art does not report any work and is limited to propose global approaches [2][3].

The objective of this thesis is then to propose methods for detecting and eliminating both global and sub-population biases by taking into account the dynamic aspect of the data and the privacy constraints. Thus, this work aims at providing answers to the following scientific questions, whose order will guide the research program:

- How to define biases in federated learning models, and how to measure them ?
- What indicators should be defined to alert users in the design and production phases?
- What optimal methods for federated learning can be proposed to eliminate bias?
- What is the impact of this bias removal approach on convergence and efficiency as well as on the performance of the final models?
- How to implement these approaches in a real system for which the data are organized in a hierarchical way with constant evolution?

The recruited candidate will therefore be able to address these issues by relying first on reference data in the literature. Then, data from collaborations within the Solar Academy of the USMB or from remote sensing within the LISTIC could be integrated. On the aspects of computing resources, the recruited candidate will have access to the USMB MUST computing mesocenter.

Candidate Requirements: Ideally, the candidate is currently pursuing a Master's degree in research, or an engineering degree, ...) related to the field of Artificial Intelligence/Machine Learning. Knowledge in data engineering and particularly in distributed learning is required. Good skills in software development and mastery of programming languages (ideally Python) are essential. The candidate should be able to bring innovative ideas and to work in multidisciplinary teams.

Applications: Letter of motivation for the thesis and the theme.
Detailed CV.
M1 and M2 transcripts or equivalent.
Letter of recommendation if possible.

Contact: Dr. Faiza Loukil, faiza.loukil@univ-smb.fr.
Prof Alexandre Benoit, alexandre.benoit@univ-smb.fr.

References

1. Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., et al.: Advances and open problems in federated learning. Foundations and Trends® in Machine Learning **14**(1–2), 1–210 (2021)
2. Sattler, F., Müller, K.R., Samek, W.: Clustered federated learning. In: Proceedings of the NeurIPS'19 Workshop on Federated Learning for Data Privacy and Confidentiality. pp. 1–5 (2019)
3. Silva, A., Metcalf, K., Apostoloff, N., Theobald, B.J.: Fedembed: Personalized private federated learning. arXiv preprint arXiv:2202.09472 (2022)