Abstract for thesis Federated learning by Martin Georgiu

The remarkable advancements in machine learning in recent years have been unprecedented, yet the constant need for more and more data to train artificial neural networks (ANNs) remains. In sectors such as healthcare, it is unrealistic to aim to create one single dataset that would consolidate all the information about patients from various hospitals. When training ANNs, the data cannot leave the hospital, and therefore any ANN training can be executed solely locally on the given hospital's data. Federated learning (FL) is a novel approach that can be used in such settings, maintaining the system's privacy without compromises. In this thesis, we are comparing FL against other approaches striving for the same objective, diving into the security of FL and investigating concrete strategies for FL. Lastly, we've created a fully working open-source example of skin spot analysis trained using FL, which can also be easily extended and used with other datasets.