**Project Title:** K-NN Movie Recommendation System using SGX (not very coverage?)

**Project Description :**  
State the objectives clearly and concisely in 150 to 200 words.

In the scope of the project, the intern is expected to build a K-nearest Neighbor to make user-based movie recommendations by comparing user profiles’ similarity in MovieLens dataset.

To provide better privacy, the model should be decentralized.

Then it is expected to run the user-information on Software Guarded Extensions (SGX) which is a trusted executed environment by Intel that provides encrypted enclaves to secure the application.

However, Intel has removed support for SGX on new generation processors on client side recently. To compensate the privacy vulnerability for users who do not have SGX on their machines and to prevent untrusted devices from lowering the model accuracy, the intern is expected to improve the model such that it is Byzantine fault tolerant. I am not quite sure how?

Making recommendations based on other similar users’ profiles poses a privacy thread since one has the potential to identify the similar users by analyzing his/her own recommendations. Therefore, the next step of the project is to add differential privacy by adding noise to the data by considering the accuracy and privacy trade-off.

The project can be summarized as building K-nn model, decentralization of the model, applying on SGX, adding BFT and finally DP if time allows.

**Suggested Method/Tool/Techniques(s) of Approach :**

**Machines will be used at EPFL IC Cluster with CPU Intel(R) Xeon(R) E-2288G CPU @ 3.70GHz and OS Ubuntu 20.04.4 LTS (GNU/Linux 5.11.0-20-generic x86\_64).**

**Python will be used to build K-nn model for movie recommendations with the help of Numpy, Pandas, SciPy and Sklearn. C/C++ will be used in SGX enclaves on Visual Studio.**

**The dataset is MovieLens by grouplens.org.**

**Results And Deliverables Expected(from company's perspective) :**

**The overhead caused by SGX will be measured.**

**The intern is expected to deliver the code and make a presentation at the end of the project.**