**Project Title:** Secure and private machine learning inference in KNN-based recommenders

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

K-nearest-neighbors recommenders are efficient in making recommendations in highly dynamic applications with constantly changing data, such as social networks, news or user-generated video platforms.

Privacy, however, is a permanent concern, even at inference stage. Indeed, inference in KNN recommenders involves the access to sensitive data in the form of user profiles. Such profiles are composed by user ratings on items and may therefore leak users’ personal features or preferences.

To address the problem, this project aims at improving privacy in KNN-based recommenders at the inference step. More specifically, we will assume that a user-based KNN graph is established and we need to make sure that no personal information is leaked.

This will be achieved with the aid of Intel Software Guarded Extensions (SGX), a trusted executed environment that provides application enclaves with automatic memory encryption and other security features. In addition, we will investigate techniques such as differential privacy against statistical attacks on aggregated data and Byzantine fault tolerance against malicious legitimate users.

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

The intern is expected to build a user-based KNN recommender using the MovieLens dataset. The KNN graph is then supposed to be loaded in an SGX enclave for the inference step. This enclave will receive requests for recommendations form a user and will query the users’ K nearest neighbors for their profiles, before providing the recommendation. After this prototype is ready, we will move on for adding differential privacy techniques on the aggregated recommendation.

**EPFL machines with SGX capability will be used for implementing hardware enclaves. Development will be made using C, C++ and Python languages.**

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

**Short report about results achieved, source code and oral presentation.**