SECURE AND PRIVATE USER-BASED KNN RECOMMENDER

THE ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE (EPFL)

45 days (27.06.2022-28.08.2022)

Elif Cemre Durgut

Computer Science and Engineering

PROJECT OBJECTIVE & EXPECTATIONS

Nowadays, many commercial websites use recommender systems which help them to increase their profits and helps users to pick items between thousands of them. Collaborative filtering is one of the most popular recommenders which makes recommendation based on user profile similarities. However, this method creates a privacy threat since it reaches user profiles and their preferences. This problem can be solved by using Software Guarded Extensions (SGX) by Intel which provides trusted enclaves to process profile information while preserving privacy. It is aimed at centralized K-nn recommender that uses Intel SGX and measuring the overhead of using SGX. It is expected that the overhead of SGX will be little.

OUTCOMES

1. Secure and private user based collaborative filtering K-nn recommendation system is developed and accessible on GitLab.
2. The latency-throughput tests of SGX and non-SGX servers are written with the cases of 10, 100 and 1000 requests being sent at a time.
3. As a result, it is found that the average time taken per request increases as the total number of requests increases.
4. The comparison of non-SGX and SGX systems is ongoing.