Privacy-Preserving application using Homomorphic Encryption on NLP algorithms

Jose Contreras (jose.angel.contreras.gedler@ut.ee)

Karlos Taaniel Lillem'e (email@ut.ee)

March 31, 2023

Description

Privacy is a critical concern in various applications, particularly in NLP, where sensitive data is often involved. For instance, medical records contain confidential information that can be analyzed by NLP to predict a patient's disease. However, to maintain privacy, the data should not be shared with the NLP algorithm. Similarly, businesses may wish to predict customer sentiment through NLP while keeping the data confidential. Homomorphic encryption offers a solution by enabling encrypted data to undergo operations without decryption, thereby allowing NLP algorithms to be performed on encrypted data without compromising privacy. Our project will implement a homomorphic encryption scheme to conduct NLP algorithms on encrypted data, ensuring data privacy.

More formally, we can define HE as follows: Let E be an encryption scheme, and K be a key space. Then, E is a homomorphic encryption scheme if there exists a function f such that for all $x, y \in \mathbb{Z}$ and all $k \in K$, we have that $E_k(f(x, y)) = f(E_k(x), E_k(y))$.

The function f is called the homomorphic operation.

A similar work can be found here: encrypted_sentiment_analysis. For the implementation, we will use the library concrete-numpy.

Data

We will use the following datasets:

Evaluation

One method to evaluate the performance of a homomorphic encryption scheme is to messure the accuracy of the predictions over encrypted data and compare it with the accuracy of the predictions over plaintext data. We can also messure the time it takes to perform the predictions. We expect that the time it takes to perform the predictions over encrypted data is higher and also that the accuracy is lower. However, we expect that the accuracy is still high enough to be useful.