Security and Privacy

2020/2021

Nuno Antunes, nmsa@dei.uc.pt

Assignment

November 20th @ 23:59

Objectives:

- Understand the advantages and limitations of homomorphic encryption and searchable encryption.
- Apply these techniques in the solution of concrete problems.

Exercise 1: Homomorphic Encryption

1. Select a dataset to use, from the folder "homomorphic" or one of your choice;
2. Select the homomorphic encryption library to use based on its capabilities and limitations of the libraries available;
3. Define an analysis model to apply to the data;
4. Explore up to how many elements you can process in your analysis;
5. Measure performance results for several sizes of the dataset;

Exercise 2: Searchable Encryption

1. Choose two different datasets to use. You can use two of the datasets available in the folder "searchable" or obtain your own dataset and confirm with me if it has the characteristics for this work.
2. Analyze the selected dataset and define which fields you will be defining as searchable and security sensitive.
3. Select the searchable encryption library to use, considering: the types of data you are planning to consider, how the data is organized.
4. For each dataset, prepare 3 versions of different sizes. (see way the "SNAP Memetracker" was used to generate 3 different versions).
5. Measure all the relevant times and compare the different datasets and versions of the datasets. Consider as relevant times at least: indexing time, searching time, etc.

Deliverable:

- A small report containing the results obtained;
- The complete sources developed and necessary for the results obtained;

Resources:

- Datasets: http://bit.ly/mecd-sp-a1