Confidential Computing in Distributed Systems

Vincent Cui

October 19, 2022

Background

One of the core elements of the digital age is data and information. Often times more data will lead to a more precise, and thus better usable, information. That is why it is in the interest of companies to share their data to compute information. But the problem is that this data is also valuable and could potentially include sensitive information. So how can a group of mutually distrusting parties efficiently collaborate in a privacy-preserving manner?

Assignment

This thesis shall explore the current state of confidential computing in general and in the context of distributed computing, discuss different problems that have to be overcome and investigate various concepts to apply confidential computing. Another objective will be to implement a proof of concept platform and define policies that will enable a group of distrusting parties to collaborate. This platform should be as privacy-preserving as possible while staying efficient. The thesis will also explain the compromises that will have to be made in order to balance efficiency and privacy-preservation. It will also clearly and transparently define trust relationships between the collaborators and the risks that arise in using the platform.

Plan

Phase	**Tasks**	**Time**
Research	Collect, sort, and organize literature	2 weeks
Concept	Create a concept that will be implemented	3 weeks
Implementation and Writing	Implement a proof of concept and writing the thesis	6 weeks
Correction	Checking literature and sources, proofreading, etc.	2.5 weeks
Submission	Printing and submitting the thesis	0.5 weeks
Buffer	Unplanned incidents	2 weeks
Sum		16 weeks