Title: Robust Decentralized Learning

Context: Machine learning plays a central role in many applications, and the increasing adoption of decentralized solutions, combined with dependability requirements, necessitates that learning tasks be carried out in a decentralized manner. In such settings, nodes in the system can assume multiple roles: performing learning on their local data while also aggregating the computational results of other nodes.

In this context, we aim to achieve **confidentiality**, ensuring that private local data is not leaked while providing a practical solution.

Objective: The goal of this internship is to explore **Multi-Party Computation (MPC)** in a **Federated Learning** context, in an **adversarial** environment, to assess the feasibility and effectiveness of these MPC approaches in ensuring confidentiality, while keeping the learning task effective.

Our team has previously conducted an exploratory study on MPC in the Federated Learning context, in a weak adversarial model (Honest But Curious). The initial global system is composed of n processes and up to fraction of them can be faulty. To improve performance, we proposed a solution where the n processes are organized in clusters, which raises the question of what is a **tolerated distribution of faulty processes among the clusters**.

The successful candidate will join the **Laboratory for Trustworthy, Smart, and Self- Organizing Information Systems (LICIA)** at CEA LIST, working in a multicultural, multidisciplinary environment with opportunities to collaborate with external researchers.

Methodology: The intern will be responsible for the following tasks:

1. Become familiar with attacks in Federated learning
2. Conduct a state-of-the-art review of cluster based solutions in the presence of faulty processes.
3. Definition and analyze different approaches for cluster distribution.
4. Become familiar with the MPC solution developed in the laboratory.
5. Implement the diffrent cluster distribution approaches.
6. Evaluate and compare the performance of the different configurations.

Commissariat à l'énergie atomique et aux énergies alternatives
Institut List | CEA Paris-Saclay (Nano-INNOV)
91191 Gif-sur-Yvette Cedex - FRANCE
list.cea.fr

Requirements:

- **Background in computer science or a related field**, with a focus on privacy-preserving technologies, or machine learning.
- Strong **programming skills** in languages commonly used for cryptographic or machine learning tasks (e.g., Python, C++).
- Experience with **distributed systems**, **federated learning**, or **byzantine faults** is a plus.
- Ability to **work independently** and **collaborate** in a research-driven environment**.**
- Comfortable working in English, essential for documentation purposes.

Required Specialization: Computer Science

Resources (experiments, analysis methods, others...): destributed systems, programming languages, machine learning, data privacy, fault tolerance.

Desired Level: Master's degree (Bac +4/5) - Master 2 Internship

Duration: 6 months

Defense clearance level required (AS minimum): AS

Desired Education: Engineering/Master's degree

Possibility of continuing with a PhD: Yes

Internship Location: CEA, Saclay Nano-Innov Center, 91191 Gif-sur-Yvette

Contacts: Alexandre Rapetti alexandre.rapetti@cea.fr