Karlsruher Institut für Technologie

Institute of Biomedical Engineering

IBT

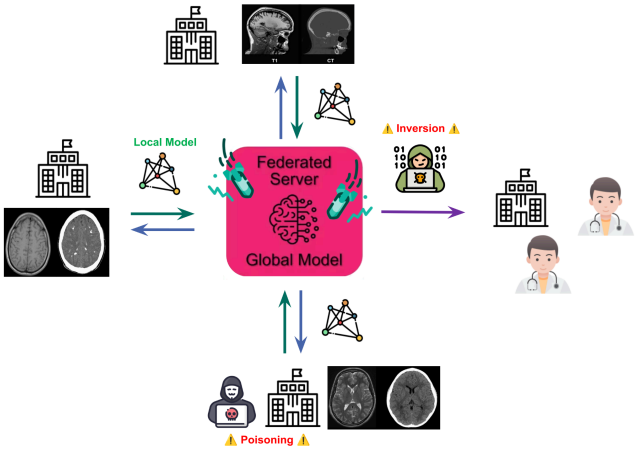
Bachelor/Master Thesis

Validating the Privacy of a Decentralised MRI to sCT Translation Framework through Security Attacks

M. Sc. Ciro Benito Raggio

Motivation

Federated Learning (FL) is an innovative approach to train artificial intelligence models that can be particularly useful in the medical field, where privacy is of critical importance. Although FL offers many privacy benefits by allowing models to be trained without centralising data, it also introduces new vulnerabilities. Several types of attacks can compromise both the integrity of the model and the privacy of personal information. A FL framework that decentralises the training of a model for the translation of Magnetic Resonance Imaging (MRI) images into synthetic Computed Tomography (CT) scans was built in the last months. A preliminary assessment of the methodology indicated its feasibility for implementation in a clinical context.



How can this federated approach be validated to ensure the protection of patient confidentiality, thereby enabling its deployment in real-world settings?

Student Project

The aim of this project is to validate the security of the existing architecture by simulating with specific tools and analysing various types of security attacks, including model inversion attacks, poisoning, Byzantine, and DDoS. The analysis will focus on the resilience of the architecture, thus contributing to the understanding of vulnerabilities and proposing practical solutions to improve security in the medical field.

Notes

- Python or programming knowledge is a plus. Knowledge of medical imaging is a plus.
- All missing skills will be integrated during the first period of the thesis with dedicated sessions and goals.
- The student will have the opportunity to learn how to manage a project with SCRUM and GitFlow methodologies.

Research Area

Medical Imaging for Modeling and Simulation

Project

Decentralised approaches to training AI models in healthcare

Orientation

Privacy preserving, Software Programming, Simulation

Course of studies

Electrical Engineering and Information Technology, Biomedical Engineering, Computer Science

Starting Date

As soon as possible

Contact person

M. Sc. Ciro Benito Raggio
Geb. 30.33, Raum 508
Fritz-Haber-Weg 1 76131
Karlsruhe
eMail ciro.raggio@kit.edu