Student Assistant for the Security of Federated Learning

Federated Learning (FL) is an innovative approach to training Deep Neural Networks (DNNs) without sharing raw data. Instead of centralizing information, FL enables multiple parties to train models locally and only share model parameters—keeping sensitive data private. This method is widely used in applications like Google's GBoard (with over 5 billion installs), medical imaging for tumor detection in hospitals, and was even tested for health monitoring of NASA astronauts.

However, the decentralized nature of FL also makes it vulnerable to security threats, such as model poisoning, where attackers manipulate training data to degrade model performance. Our research focuses on developing strategies to detect and mitigate such threats, and we are looking for motivated student assistants to join our team!

Depending on your background and interests, you will:

- Design and analyze poisoning attacks that disrupt FL training (preventing model convergence).
- Implement and evaluate defenses against model poisoning.
- Enhance FL security by leveraging Trusted Execution Environments (TEEs).
- Compare and integrate state-of-the-art attack and defense techniques in FL.
- Contribute to the development of cutting-edge FL frameworks.

Prerequisites

- Good knowledge in computer security and Deep Learning
- Proficiency in Python
- Recommended: Experience with ML frameworks like PyTorch or TensorFlow.
- Good analytical and problem-solving skills.
- Ability to work independently and in a team.

Contact

If you are interested in this innovative research topic, contact Phillip Rieger and Kavita Kumari via info@trust.tu-darmstadt.de to learn more about it. Please include a brief overview of your study background and a transcript of records.

March 2025