The thesis has the following tasks:

- Studying the state-of-the-art privacy-preserving machine learning frameworks, and focusing on deep learning framework since it's widely used in practice
- Investigating the existing approaches using TEEs to protect input data of machine learning systems
- Evaluating the proposed framework with micro-benchmarks and real-world datasets
- Investigating several differential privacy mechanisms that can be used in practice. For example, determining the epsilon value to protect the privacy of users
- Providing a detailed design of the secure and privacy-preserving framework using the building-blocks
- Implementing a prototype using Tensorflow/Pytorch for machine learning and SCONE for running with Intel SGX
- Evaluating the proposed system using micro-benchmarks and real-world datasets regarding throughput/latency, accuracy and privacy loss

This thesis will be written in English.

Betreuer:	Dr.-Ing. Do Le Quoc
Zweitgutachter:	Dr.-Ing. André Martin
Verantwortlicher Hochschullehrer:	Prof. Christof Fetzer
Institut und Lehrstuhl:	Systemarchitektur, Systems Engineering
Beginn am:	02.03.2020
Einzureichen am:	02.09.2020

Student	Betreuer	Verantwortlicher HSL