

Invitation to the Oral Examination – Department CS

For the occasion of his examination for a Doctoral Degree,

Mr. Reza Nasirigerdeh, M.Sc.

will present his dissertation entitled

Efficient Federated and Privacy-preserving Machine Learning

on **24.10.2024** at **10:00 h**

Attendance to the presentation is open to the public.

The presentation will be in English.

The candidate, all members of the Examination Committee, and authorized examiners of the TUM School of CIT are invited to the presentation and subsequent oral examination.

The presentation and subsequent examination will take place in a hybrid manner. **In person** at the **TUM School of CIT, Boltzmannstr. 3, room 01.07.014** and via **Zoom** under the following link:

<https://tum-conf.zoom-x.de/j/65456037837?pwd=KQ386kOtvhH1WCXU7JuDaBsOOEHGzU.1>

Meeting-ID: 654 5603 7837

Kenncode: 105765

Examination committee:

Chair: **Prof. Dr. Ing. Pramod Bhatotia**

First Examiner: **Prof. Dr. Daniel Rückert**

Second Examiner: **Prof. Dr. Hamed Haddadi**

Garching, the **16th of October 2024**

Abstract:

We first show that the regression and neural network models trained in a federated fashion can achieve optimal utility independent of data distribution across clients. Next, we introduce a new normalization method called KernelNorm, and illustrate that kernel normalized models can enhance not only utility but also communication and privacy simultaneously in federated, differentially private, and differentially private federated learning environments.