Institute for Machine Tools and Industrial Management (*iwb*)
TUM School of Engineering and Design
Technical University of Munich

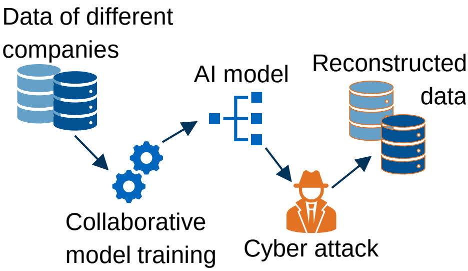
Model inversion attacks on AI models for condition monitoring

Starting point

The collection of machine data from multiple companies enables the training of generalizable condition monitoring models, which can then be used by the companies. However, as this data implicitly contains industrial secrets, federated learning is used for training. However, model inversion attacks still make it possible to reconstruct the training data and thus disclose a company's sensitive information. The lack of evidence to date as to whether federated learning is sufficient as a protective measure inhibits the participation of companies in such collaborative methods.

Task description

AI models for tool condition monitoring need to be trained using federated learning and then an attempt is to be made at reconstructing the original data. Methods such as generative adversarial networks will be used for this.



Requirements

Strong interest in machine learning, manufacturing technology and programming in Python

Contact

M. Sc. Daniel Piendl
Department of Machine Tools
Phone: +4989 / 289 15586
Daniel.Piendl@iwb.tum.de