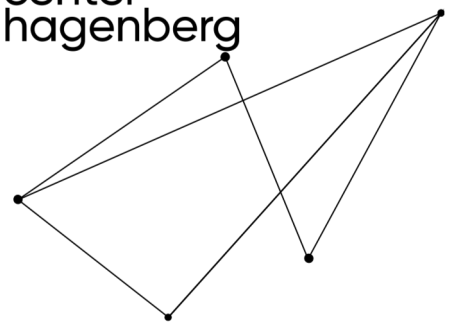
scch { software competence center hagenberg }



scch { }

KI-SIGS / PetAI

Privacy Secured Explainable and Transferable AI

Lukas Fischer

www.scch.at
lukas.fischer@scch.at

SCCH is an initiative of JKU JOHANNES KEPLER UNIVERSITY LINZ

Bundesministerium Digitalisierung und Wirtschaftsstandort

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

FFG Forschung wirkt.

PetAI / KI-SIGS: Überblick

scch { }

Ziel: Ein Methoden- und SW-Framework für Machine Learning zum Schutz privater Daten unter Wahrung von Erklärbarkeit und Transferierbarkeit (Ethische KI)

Anwendung: KI-Space für intelligente Gesundheitssysteme

Partner: norddeutsche Universitäten und Unternehmen

Laufzeit: Laufzeit 27 Monate

KI·SIGS
SPACES FÜR INTELLIGENTE GESUNDHEITSSYSTEME

https://projekte.ffg.at/projekt/3817537
https://www.scch.at/data-science/projekte/detail/KI-SIGS

Bilaterale Kooperation / Integration

scch { }

PetAI
Privacy Secured Explainable and Transferable AI

iAuge {
AP 310 Homecare Augendiagnostik
}

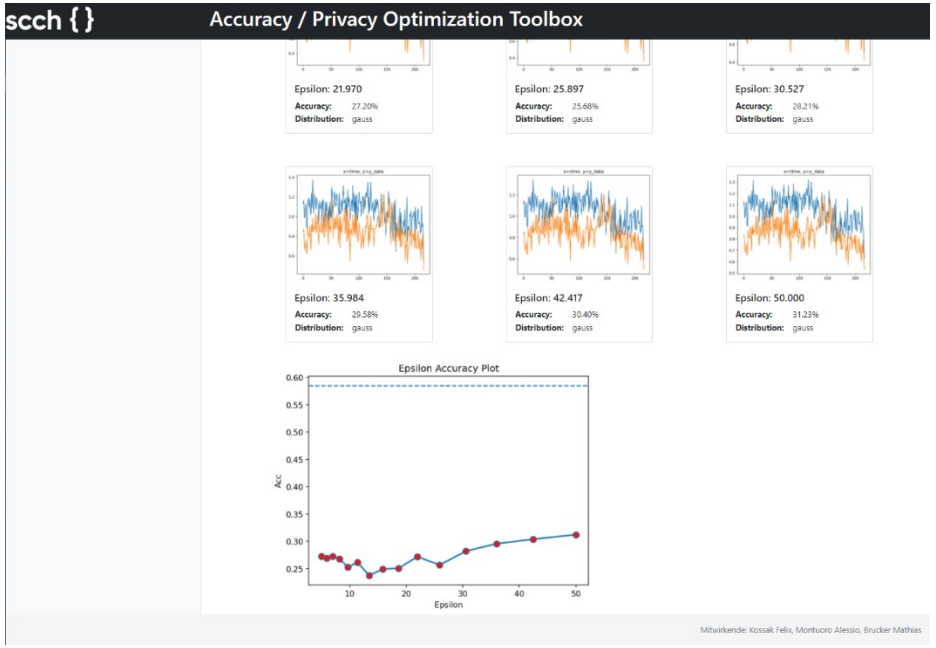
KI·SIGS
SPACES FÜR INTELLIGENTE GESUNDHEITSSYSTEME

RIDIMP {
AP 330 Risikoindikatoren für cardiopulmonale Dekompensation auf Intensivstationen durch Monitoring von Vitalparametern
}

Businessmodelle

scch { }

Softwaresystem zur numerischen Analyse des Kompromisses zwischen Schutz der Trainingsdaten (durch Hinzufügen von Rauschen, quantifiziert durch Berechnung der Privacy Leakage) und finaler Modell Performanz



- Bewusstsein Schaffen für „Schwächen“ von KI Systemen
- „Zwischen-Layer“ zum Schutz der Privatsphäre in ML/KI Systemen
- Adversarial Attacks auf KI Systeme (auch in Richtung KI Zertifizierung)
- XAI – Erklärbare und interpretierbare KI Systeme

Apache Airflow

mlflow