COMET-Modul

S3AI
Security and Safety for Shared AI by Deep Model Design

Hauptstandort	Hagenberg, Linz; Oberösterreich
weitere Standorte	Leuven / Belgium , Cagliari / Italy
Thematische Schwerpunkte	S3AI wird die Grundlagen für den Aufbau sicherer kollaborativer künstlicher Intelligenzsysteme schaffen: Methoden zur Wahrung der Privatsphäre, Schutz vor feindlichen Angriffen und Garantien für das beabsichtigte Verhalten des Systems.

Anvisierte technologische Entwicklungen

Unser Ansatz basiert auf Methoden des Transfer Learning und sowie der algebraischen Geometrie unter Ausnutzung geometrischer Strukturen im Inputraum, die durch Deep-Learning-Modelle induziert werden. Als Ergebnis erwarten wir theoretische Frameworks und Analysewerkzeuge an der Schnittstelle von Mathematik, Deep Learning und Informationssicherheit bezüglich a) neuer DNN-Architekturen und damit zusammenhängender Lernstrategien zur Wahrung der Privatsphäre, b) neuer Abwehrstrategien gegen gegnerische Angriffe und c) neuer Methoden zur Beurteilung der Vertrauenswürdigkeit.

Ausgewählte Unternehmenspartner (Auszug: max. 10)

1. ENGEL AUSTRIA GmbH
2. kpibench GmbH
3. KEBA AG
4. RUBBLE MASTER HMH GmbH
5. KTM
6. AVI Systems GmbH
7. ONE LOGIC GmbH
8. PKE Holding AG
9. TissueGnostics GmbH
10. ventopay gmbh

Ausgewählte wissenschaftliche Partner (Auszug: max. 5)

1. Radon Institute of Computational and Applied Mathematics (RICAM) of Austrian Academy of Sciences
2. Research Institute for Symbolic Computation (RISC) at JKU (Linz)
3. Institute for Machine Learning at JKU (Linz)
4. Pattern Recognition and Applications Lab of University of Cagliari (Italien)
5. Dept. Elektrotechniek-ESAT/COSIC of the University of Leuven (Belgien)

Ausgewählte internationale Partner [1] (Auszug: max. 5)

1. Pattern Recognition and Applications Lab of University of Cagliari (Italien)
2. Dept. Elektrotechniek-ESAT/COSIC of the University of Leuven (Belgien)
3. ONE LOGIC GmbH (Deutschland)

Start des COMET-Moduls	Jänner 2020 (4 Jahre)
Mitarbeiterstand	9 VZÄ involviert (davon 8.5 VZÄ ForscherInnen)
Projektleitung	Priv.-Doz. Dr. Bernhard A. Moser
Kontakt/ COMET-Zentrum	SCCH (Software Competence Center Hagenberg GmbH) Softwarepark 21, 4232 Hagenberg, Austria + 43 50 343 office@scch.at; www.scch.at

[1] Unternehmens- und wissenschaftliche Partner mit Sitz außerhalb Österreichs

Das COMET-Modul wird im Rahmen von COMET – Competence Centers for Excellent Technologies – durch BMK, BMDW und mitfinanzierende Bundesländer gefördert. Das Programm COMET wird durch die FFG abgewickelt. >> www.ffg.at/comet