Federal Ministry
Republic of Austria
Climate Action, Environment,
Energy, Mobility,
Innovation and Technology

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

FFG
Promoting Innovation.

COMET Module

S3AI

Security and Safety for Shared AI by Deep Model Design

Main location	Hagenberg, Linz, Upper Austria
Other locations	Leuven / Belgium , Cagliari / Italy
Research programme	S3AI will provide the foundations required to build secure and safe shared artificial intelligence systems: methods for privacy preservation, protection against adversarial attacks and guarantees for the system's intended behavior.

Planned realisation and outcomes

Our approach is based on transfer learning and algebraic geometry by exploiting geometric structures (tessellation) in the input space induced by deep learning models. As outcome we expect theoretical frameworks and analysis tools at the intersection of mathematics, deep learning and information security regarding a) novel DNN architectures and related learning strategies for privacy preserving collaborative AI, b) novel defense strategies against adversarial attacks, and c) novel measures of confidence.

Selected company partners (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

Selected scientific partners (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 (Italy)
5. Dept. Elektrotechniek-ESAT/COSIC of the University of Leuven (Belgium)

Selected international partners [1] (max. 5)

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

Start of the COMET Module	January 2020 (4 years)
Number of personnel	9 (FTE) are involved (8.5 FTE are scientists)
Project management	Priv.-Doz. Dr. Bernhard A. Moser
Contact/ COMET Centre	SCCH (Software Competence Center Hagenberg GmbH) Softwarepark 21, 4232 Hagenberg, Austria + 43 50 343 office@scch.at; www.scch.at

[1] Partners with headquarters outside Austria

The COMET Module is funded within COMET – Competence Centers for Excellent Technologies – by BMK, BMDW as well as co-financing federal provinces. The COMET programme is managed by FFG. >> www.ffg.at/comet