SUCCESS STORY

Know-Center | Know-Center GmbH – Research Center for Data-Driven Business & Big Data Analytics

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Center (K1)

Type of project: DDAI COMET Module

© Adobe Stock

SECURE EXCHANGE

SECURE DATA TRANSFER AND DATA PROTECTION OPENS THE DOORS FOR OPEN EXCHANGE IN SCIENCE AND INDUSTRY. COMPUTING WITH COMPLETELY ENCRYPTED DATA SHOWS TO BE TREND-SETTING

Transfer learning enables the training of reliable AI models, despite a small data pool – a very efficient method to still obtain accurate evaluations. An AI model is pre-trained with a large data set and the learned knowledge is transferred to the small data set. The pre-trained model does not have to be completely retrained but can deliver very accurate results with minor adjustments and even little data. However, a weak point here is data protection.

Sharing must be secure

From trained models, the training data can often be reconstructed with just a few steps. If, for example, a company wants to provide its suppliers with a pre-trained model for their own AI evaluations, there is a risk that the data used will become public. The Know Center has therefore developed the framework CrypotTL.

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

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at

CryptoTL
The framework combines transfer learning with homomorphic encryption, an encryption method that allows computations to be performed with completely encrypted data. This means that from the very beginning, computations are performed with completely encrypted data sets and models. CryptoTL not only protects the large data set for pre-training an algorithm or the algorithm itself, but also the small data set is only sent encrypted to the pre-trained model. This enables insights that would be out of reach for privacy reasons without this approach.

Data security on the device
In the model, the otherwise computationally intensive and rather inefficient homomorphic encryption is applied to only part of the algorithm. As a result, fast sub-second runtimes can be achieved on commercial devices such as notebooks. Thus, nothing stands in the way of CryptoTL's application in actual use cases.

Project coordination
Dr. Andreas Trügler, Know-Center
T +43 (0) 316 – 87330895
atruegler@know-center.at

Know-Center GmbH
Sandgasse 26
8010 Graz
T +43 (0) 316 – 87330895
office@know-center.at
www.know-center.at

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

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at