SUCCESS STORY

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

Programm: COMET – Competence Centers for Excellent Technologies

Förderlinie: COMET-Zentrum (K1)

Projekttyp: DDAI COMET Modul

©Adobe Stock

AUSTAUSCH MIT SICHERHEIT

SICHERER DATENTRANSFER UND DATENSCHUTZ ÖFFNET DIE TÜREN FÜR DEN OFFENEN AUSTAUSCH IN DER WISSENSCHAFT UND INDUSTRIE. DABEI IST DAS RECHNEN MIT KOMPLETT VERSCHLÜSSELTEN DATEN ZUKUNFTSWEISEND.

Transfer Learning ermöglicht das Training verlässlicher KI-Modelle, trotz eines geringen Datenpools – eine sehr effiziente Methode, um in solchen Fällen trotzdem genaue Auswertungen zu erhalten. Dabei wir ein entsprechendes KI-Modell mit einem großen Datensatz vortrainiert und das gelernte Wissen auf den kleinen Datensatz transferiert. Das vortrainierte Modell muss nicht mehr komplett neu trainiert werden, sondern kann mit geringen Anpassungen und auch wenig Daten sehr genaue Ergebnisse liefern. Eine Schwachstelle ist hierbei jedoch wieder der Datenschutz.

Austausch muss sicher sein

Aus trainierten Modellen lassen sich die Trainingsdaten oft mit wenigen Schritten rekonstruieren. Sollte z.B. eine Firma ihren Zulieferern ein vortrainiertes Modell für ihre eigenen KI-Auswertungen zur Verfügung stellen wollen, besteht die Gefahr, dass die verwendeten Daten öffentlich werden. Das Know Center hat daher das Framework CrypotTL entwickelt.

CryptoTL

Das Framework kombiniert Transfer Learning mit homomorpher Verschlüsselung, einer Verschlüsselungsmethode, die es erlaubt mit komplett verschlüsselten Daten Berechnungen durchzuführen. Das bedeutet, dass von Beginn an mit komplett verschlüsselten Datensätzen und Modellen gearbeitet wird. CryptoTL schützt dabei nicht nur den großen Datensatz zum Vortrainieren

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

Bundesministerium Digitalisierung und Wirtschaftsstandort

Version 01/2020

eines Algorithmus oder den Algorithmus selbst, auch der kleine Datensatz wird nur verschlüsselt an das vortrainierte Modell geschickt. Dadurch werden Erkenntnisse ermöglicht, die ohne diese Herangehensweise aus Datenschutzgründen nicht greifbar wären.

Datensicherheit am Laufwerk

Im Modell wird die sonst rechenintensive und eher ineffiziente homomorphe Verschlüsselung nur auf einen Teil des Algorithmus angewandt. Dadurch können auf kommerziellen Geräten wie Notebooks schnelle Laufzeiten von unter einer Sekunde erreicht werden. CryptoTL's Anwendung bei tatsächlichen Use Cases steht somit nichts mehr im Wege.

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

Know-Center GmbH
Sandgasse 36
8010 Graz
T +43 (0) 316 87330801
office@know-center.at
www.know-center.at

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

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at