So machen Grazer Forscher künstliche Intelligenz sicherer und nachvollziehbarer

Zuletzt aktualisiert: 10. Februar 2020

Graz ist heute und morgen Europa-Hotspot in Sachen **künstlicher Intelligenz (Artificial Intelligence – AI)**. Es findet der Kickoff zum mit 4 Millionen Euro dotierten **COMET-Modul „DDAI – Data Driven Artificial Intelligence"** statt. Bei diesem steht eine verifizierbare und nachvollziehbarere AI im Fokus. Zu den Projektteams zählen unter anderem AVL List, Magna Steyr, AT&S und NXP aus der Steiermark.

Damit soll es für Unternehmen einfacher werden, Daten und Algorithmen zu verstehen und zu nutzen – bei maximalem Datenschutz. Am 11. Februar lädt das Know-Center zum ersten Mal zur internationalen AI-Fachkonferenz AI-KNOW, bei der sich die **weltweite Forschungselite** in der Alten Universität trifft.

Vor 20 Jahren, als das Know-Center gegründet wurde, war AI – wenn überhaupt – nur unter IT-Experten ein Thema. Heute ist das **Potenzial künstlicher Intelligenz** quer über alle Branchen hinweg bekannt. Das Know-Center hat sich Kompetenz aufgebaut, die wesentlich dazu beigetragen hat, dass das COMET-Modul „DDAI – Data Driven Artificial Intelligence" nach Graz geholt werden konnte. Das mit 4 Millionen Euro dotierte EU-Projekt wird 4 Jahre lang unter der Leitung des Know-Centers umgesetzt.

COMET Modul DDAI – Data Driven Artificial Intelligence

Kern des Moduls ist die Erarbeitung einer **theoretischen Basis für sichere Künstliche Intelligenz-Algorithmen**, die erklärbar und verifizierbar sind.

Daten sind „das neue Gold". Viele unterschiedliche Aspekte hindern Unternehmen aber daran, dieses Gold zu schürfen:

- Moderne datengetriebene AI ist hochkomplex.
- Der Weg von den Daten zum Analyseergebnis ist schwer verständlich und schwer verifizierbar.
- Ihre Anwendung erfordert Expertenwissen welches nicht in jedem Unternehmen verfügbar ist.
- Hinzu kommt, dass die Vertraulichkeit der Daten Unternehmenspartner daran hindert, Analyseergebnisse miteinander zu teilen.

Ziel des Moduls ist, an all diesen Punkten anzusetzen und sichere, **verifizierbare und erklärbare AI zu entwickeln** sowie ein Curriculum für Nutzer dieser AI zu erstellen, welches ein Verständnis für den Umgang mit und die Grenzen von AI schaffen soll.

Das Modul umfasst damit alle Stationen der Datenverarbeitungskette, von der zu verifizierenden Datenquelle, über kryptographische Verfahren zur sicheren Datenverarbeitung bis hin zum Nutzer der AI.

Industriepartner im Projekt sind AVL List, Magna Steyr, AT&S und NXP aus der Steiermark sowie das Blockchain-Unternehmen IoV42 aus England. Wissenschaftliche Partner sind die Universität Passau, die KU Leuven und die niederländische Universität Twente.

AI-KNOW – Internationale Vernetzung auf höchstem Niveau

Auf der AI-KNOW, der ersten Fachkonferenz für AI in Graz, präsentieren am 11. Februar 2020 führende internationale ExpertInnen ihre **Arbeiten und Visionen für die Zukunft der Künstlichen Intelligenz und des Maschinellen Lernens**. Themen sind:

1. Privacy-preserving Algorithmen
2. Neue Datenbank-getriebene Big Data Analysen
3. Artificial Intelligence
4. Visualisierungen und Informationstheorie

Die AI-KNOW ist die Folgekonferenz der I-KNOW, die von 2001 bis 2017 als Data Driven Future-Konferenz in Graz stattfand. Mit der AIKNOW bringen das Know-Center die internationale AI-Elite nach Graz und bieten damit den lokalen FachexpertInnen die Möglichkeit, sich über die weltweiten Entwicklungen in diesem Bereich zu informieren und zu vernetzen.

> *Im Zuge der fortschreitenden Digitalisierung und den damit einhergehenden immer stärker wachsenden Datenmengen bedarf es auch einer vertieften Diskussion über die Möglichkeiten und den Einsatz von künstlicher Intelligenz. Das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie unterstützt daher die erste AI-KNOW in Graz, die sich diesem Thema mit international renommierten ExpertInnen widmet. Schon in der Vergangenheit war die vom Know-Center bzw. TU Graz unter der Leitung von Frau Prof. Stefanie Lindstaedt organisierte I-KNOW ein Garant für höchste Qualität und trug maßgeblich zur Sichtbarkeit der österreichischen Expertise auf diesem Gebiet bei.*

so Leonore Gewessler, Bundesministerin für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie.

COMET-Modul stärkt Standort und schafft Arbeitsplätze

> *Mit dem COMET-Modul zu Artificial Intelligence kann*
> *dieser Schwerpunkt am Know-Center in Graz gezielt ausgebaut werden."*

so *Henrietta Egerth* und *Klaus Pseiner*, Geschäftsführer der Österreichischen Forschungsförderungsgesellschaft FFG, die das Programm COMET abwickelt.

Die im Regierungsprogramm verankerte „Setzung von Forschungsschwerpunkten (gemeinsam mit Wirtschaft und Bildungssektor)" im Bereich AI wird am Know-Center gemeinsam mit Unternehmenspartnern und wissenschaftlichen Partnern aus dem In- und Ausland umgesetzt. Das Exzellenzzentrenprogramm COMET, das vom Bund (BMK und BMDW), Partnern aus der Wirtschaft und den Bundesländern getragen und finanziert wird, wird mit den Modulen entsprechend den Anforderungen zur Entwicklung neuer Technologien erweitert: So werden thematische Schwerpunkte wie etwa **Artificial Intelligence für Datenschutz** ermöglicht, der Standort gestärkt und zusätzliche Arbeitsplätze geschaffen.

Bindeglied zwischen Forschung und Wirtschaft

Rektor Harald Kainz über die Rolle der TU Graz:

> *Die TU Graz sieht sich als wesentlicher Träger der heimischen AI-Forschung. An unserer Universität beschäftigen sich aktuell über 200 Forschende in mehr als zehn Arbeitsgruppen mit AI. Das Thema AI ist heute auch in nahezu allen unseren Studienangeboten verankert. Für uns als Gesellschafter ist das Know-Center, als eine der europaweit führenden Forschungseinrichtungen für AI und Data-Driven Business, ein wichtiges Bindeglied zwischen Forschung und Wirtschaft. Viele unserer Institute wickeln Projekte gemeinsam mit dem Know-Center und mit externen Partnern ab. Das erhöht die Sichtbarkeit des Forschungsstandortes Graz in der internationalen AI-Community und stärkt die Außenwahrnehmung sowie den exzellenten Ruf der TU Graz im Bereich der Informations- und Kommunikationstechnologien.*

AI Fachwissen und internationales Netzwerk

Stefanie Lindstaedt, CEO und CSO des Know-Center und Institusvorstand des ISDS an der TU Graz zur Relevanz des Themas AI:

> *Es wird zwar heute immens viel über Big Data und AI geredet. Letzten Endes geht es aber darum, ins Umsetzen zu kommen und Geschäftsmodelle zu entwickeln, was wir in rund 150 Projekten jährlich auch laufend machen. Dazu braucht man einerseits Fachwissen und viel Erfahrung, aber auch ein starkes internationales Expertennetzwerk, das wir uns über 20 Jahre aufgebaut haben. Dadurch kennen wir auch die Entwicklungen in den anderen Ländern, etwa welche Start-ups dort gegründet werden oder woran man aktuell forscht. Zu uns kommen die Firmen, wenn sie Speziallösungen benötigen.*

Man sieht sich laut Lindstaedt als erste Anlaufstelle für Unternehmen, die einerseits das Potenzial ihrer Daten besser ausschöpfen wollen, oder aber Lösungen für konkrete Problemstellungen suchen – abseits von ‚Stangenprodukten. Mehr als 100 MitarbeiterInnen sind mittlerweile am Know-Center beschäftigt, wobei man sich sowohl als Dienstleister für Unternehmen, als auch als Ausbildungsstätte sieht, sowohl für Studierende als auch in Form von Trainings und Weiterbildungen für die Wirtschaft (z. B. der Know-Center Data Value Check oder der Kurs „AI Essentials", der gemeinsam mit der TU Graz angeboten wird).

Besseres Verständnis für den Umgang mit AI

Meltdown, Spectre, Zombiload und Co: TU Graz und das Know-Center haben in letzter Zeit mehrfach gezeigt, dass sie in Sachen AI, Security und Privacy europaweit an vorderster Front mitspielen. Dieses Know-how und die starke internationale

Vernetzung des Know-Centers haben wesentlich dazu beigetragen, das DDAI-Modul nach Graz zu holen. Know-Center-CEO Lindstaedt über die Projektziele:

> *Nach 4 Jahre wollen wir die Basis für AI-Algorithmen haben, die erklärbar und verifizierbar sind und gleichzeitig die Privatsphäre schützen. Es soll den Nutzern dabei helfen, die Möglichkeiten und Grenzen der AI besser zu verstehen. Und es soll die Einstiegshürde für die Unternehmen und Personen drastisch herabsetzen, AI für die Analyse der eigenen Daten zu nutzen um sich damit Wettbewerbsvorteile zu sichern.*

Das Modul umfasst alle Stationen der Datenverarbeitungskette, von der zu verifizierenden Datenquelle, über kryptographische Verfahren zur sicheren Datenverarbeitung und bietet den Nutzern der AI eine bessere, weil nachvollziehbarere, Entscheidungsgrundlage.

Wie man AI verständlicher macht und die Privatsphäre schützt

Einer der führenden Forscher am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
und Areamanager für Data Security am Know-Center, *Christian Rechberger*, der auch federführend am DDAIModul mitarbeitet, erläutert die Herausforderungen des Projekts. Im Fokus steht, verifizierbare und erklärbare AI-Algorithmen zu entwickeln, die die Privatsphäre schützen. *Aber was heißt das nun konkret?*

Privatsphäre schützen:

Umso mehr Daten AI zur Verfügung hat, desto besser funktioniert sie. Im B2B-Bereich wäre der Datenpool, auf den die AI zugreifen kann, natürlich viel größer, wenn die Daten von unterschiedlichen Unternehmen zusammengefasst werden. Rechberger:

> *Oft ist das aber rechtlich und auch aus Gründen des Wettbewerbs nicht möglich. Kein Unternehmer will verständlicherweise, dass der Konkurrent seine Daten hat. Auch schiebt der Datenschutz aus gutem Grund hier Riegel vor. Die Kryptografie macht es aber möglich, gemeinsam mit einem Datenpool zu arbeiten, ohne die Daten der anderen entschlüsseln zu können. Sprich, man kann aus einem gemeinsamen Output lernen, ohne die einzelnen Datensätze zu lesen. Das sorgt für maximale Privatsphäre. Die Challenge dabei ist für uns noch, diese Verfahren effizienter und damit auch leistbarer für Unternehmen zu machen. Momentan wird das erst in Nischen eingesetzt.*

Erklärbarkeit und Verifizierbarkeit der künstlichen Intelligenz

> *Wie die AI arbeitet, ist derzeit nicht sehr transparent. Man bekommt ein Ergebnis, kann es aber schwer nachvollziehen. Im HR-Bereich kann das Ergebnis eine Empfehlung für eine Bewerberin bzw. einen Bewerber sein, nachdem die AI eine riesige Datenmenge analysiert hat. Das kommt aber gewissermaßen einer Blackbox-Entscheidung gleich. Wir wollen die Basis dafür liefern, dass man eine AI bauen kann, deren Entscheidungen nachvollziehbar sind.*

Die technische Herausforderung dabei ist, dass AI intern sehr komplexe Entscheidungswege hat. Man könnte diese zwar „einfach" alle darstellen, damit wären Laien aber völlig überfordert. „Die Challenge ist es, die Entscheidungswege so zu vereinfachen bzw. zusammenzufassen, dass sie verständlich werden."

AVL List: Großes Business-Potenzial mit AI

Einer der Industriepartner im DDAI-Modul ist AVL List. AI spielt für den langjährigen Partner des Know-Centers eine
zentrale Rolle. *DI Gerhard Schagerl*, Produktlinienmanager Data Intelligence bei AVL List:

> *Mit AI unterstützt AVL die Entwicklung von Antriebsstrang und Fahrzeugen. Darüber hinaus hilft AVL den Autoherstellern mit Methoden der Künstlichen Intelligenz, Probleme in den Fahrzeugen vorherzusagen, bevor diese auftreten, und auf Basis der Fehlervorhersagen auch gleich die richtigen Ersatzteile an die nächstgelegene Werkstätte zu versenden.*

Am DDAI-Modul beteiligt sich AVL List, „weil wir darin ein großes Potenzial sehen. Die Vertraulichkeit und der Datenschutz sind zentrale Punkte. Wir haben riesige Mengen von Daten aus unterschiedlichen Quellen, die nicht vermischt werden dürfen. Wenn wir effiziente Möglichkeiten zur Nutzung dieser Datenmengen hätten, würde sich ein enormer Mehrwert ergeben."

Für Industrie relevante Anwendungsfälle

Die Rolle von AVL List und der anderen Industriepartner liegt beim DDAI-Modul darin, die für die Industrie relevanten, Anwendungsfälle einzubringen. Wesentlich ist für Schagerl die Verknüpfung der technischen Möglichkeiten bzw. die gemeinsame Forschung und Entwicklung. Der Manager kann bereits auf etliche erfolgreiche Kooperationen mit dem Know-Center verweisen.

> *Wir haben unter anderem ein Fahrer-Monitoring umgesetzt, bei dem Autofahrer mit vielen Sensoren vermessen wurden. Dieses Projekt ist mittlerweile in ein wirtschaftliches Vorhaben übergegangen.*

AVL List ist auch Sponsor der AI-KNOW Konferenz und der Know-Center Data Science Challenge – einem Format, um Nachwuchstalente zu finden – die im Februar 2020 bereits zum dritten Mal stattfindet. Die TeilnehmerInnen arbeiten an einer komplexen Problemstellung aus dem Bereich Data Science und maschinelles Lernen, es winken insgesamt 4.000 Euro Preisgeld. Die GewinnerInnen werden am 10. Februar 2020 auf der AI-KNOW ausgezeichnet.

AI-KNOW Speaker auf der ersten Fachkonferenz für AI in Graz

- **Ian Fischer**: Forscher für maschinelles Lernen bei Google Research, San Francisco. Information Theoretic Objectives, Generalization and Robustness
- **Maria Girone**: CTO am CERN OpenLab in der, Schweiz. Sie ist eine Expertin für globales Grid-Computing.
- **Volker Markl** ist ordentlicher Professor und Leiter der Gruppe Datenbanksysteme und Informationsmanagement (DIMA) an der Technischen Universität Berlin. Mosaics in Big Data
- **Michael Sedlmair** leitet eine Forschungsgruppe für Visualisierung und Virtual/Augmented Reality am Forschungszentrum VISUS der Universität Stuttgart. Machine Learning meets Visualization
- **Dimitar Jetchev** ist ein Kryptograph, CTO und Mitbegründer des Sicherheitsunternehmens INPHER mit Sitz
in New York City, San Francisco und Lausanne. Scalable Privacy-Preserving Computing with High Numerical Precision

Know-Center: Research Center for Data-Driven Business & Big Data Analytics am Campus Inffeldgasse in Graz

Das Unternehmen ist eines der führenden europäisches Forschungszentren für Data-Driven Business und AI und erste Anlaufstelle für Österreichs Wirtschaft. Seit 20 Jahren werden namhafte Unternehmen dabei unterstützt, Daten als Erfolgsfaktor zu nutzen. Das im Rahmen von COMET geförderte Kompetenzzentrum ist außerdem die führende Ausbildungsstätte für Data Scientists in Österreich. Qualifizierte AbsolventInnen von relevanten Studiengängen haben die Chance, neben der Arbeit an spannenden Projekten aus der Wirtschaft ihre Doktorarbeit zu verfassen. Neben COMET- und Auftragsforschung bietet das Know-Center eine Bandbreite an AI-Trainings für Firmen an.

European Innovation Space

Bereits zum dritten Mal wurde das Know-Center von der Big Data Value Association mit dem Label „European Innovation Space" ausgezeichnet. Mit der Anerkennung wird gewürdigt, dass Unternehmen als Trusted-Data-Inkubatoren darauf abzielen, datengetriebene Innovation in allen Wirtschaftsbereichen zu beschleunigen – sowohl in kommerzieller als auch in gemeinnütziger Absicht. Das Know-Center ist auch ein K1-Zentrum, das im Rahmen des Programms COMET – Competence Centers for Excellent Technologies – gegründet wurde.

Titelfoto Know-Center: vl. Christian Rechberger (Forscher Know-Center/TU Graz), Stefanie Lindstaedt (CEO und CSO des Know-Center), Harald Kainz (Rektor TU Graz), Gerhard Schagerl (AVL List)

Diese Themen könnten Dich auch interessieren: