Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Expertise zu vertrauenswürdiger KI gewinnt

Teams aus der Cybersicherheitsforschung der TU Darmstadt erfolgreich

Darmstadt, 7. Dezember 2020. Zwei Forschungsteams der TU Darmstadt konnten in einem weltweiten Wettbewerb zu vertrauenswürdiger Künstlicher Intelligenz (KI) mit ihren Forschungsprojekten punkten und werden Teil des von den Unternehmen Intel, Avast und Borsetta initiierten Private AI Collaborative Research Institute.

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
joerg.feuck@tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Die Cryptography and Privacy Engineering Group unter Leitung von Professor Thomas Schneider und das System Security Lab unter Leitung von Professor Ahmad-Reza Sadeghi aus dem Profilbereich Cybersicherheit der TU Darmstadt überzeugten mit ihren Forschungsideen im Rahmen eines international ausgeschriebenen Wettbewerbs. Renommierte Universitäten waren aufgefordert, Forschungsideen für das von Intel, Avast und Borsetta initiierte Private AI Collaborative Research Institute einzureichen. Neun Forschungsteams, darunter zwei der TU Darmstadt, konnten sich im Konkurrenzfeld behaupten. Sie verstärken mit ihrer Expertise ab sofort die Forschungskooperation zu vertrauenswürdiger KI.

„Künstliche Intelligenz stellt eine wahre Goldmine für Cybersicherheitsforschung dar“, betont Professor Ahmad-Reza Sadeghi, Leiter des System Security Lab und Sprecher des Profilbereichs Cybersicherheit (CYSEC) an der TU Darmstadt. Im Vordergrund seiner Forschungsarbeiten steht das sogenannte Federated Machine Learning, um exakte, vertrauenswürdige und sichere Algorithmen in Software und Hardware für KI zu etablieren.

„Täglich werden enorme Datenmengen erzeugt, gesammelt und weiterverarbeitet. Wir benötigen neue Methoden der angewandten Kryptographie für Privatsphäre-schützende KI-Systeme, um so den Schutz sensibler Daten zu gewährleisten“, erläutert Professor Thomas Schneider, Leiter des Fachgebiets Cryptography and Privacy Engineering (ENCRYPTO). Sein Forschungsprojekt beschäftigt sich insbesondere mit Methoden zur sicheren Mehrparteienberechnung und der Anwendung von Hardware-beschleunigter Kryptographie im Kontext von dezentraler KI.

Die Kooperationspartner aus wissenschaftlicher Forschung und Industrie wollen unter dem Dach des Private AI Collaborative Research Institute Herausforderungen bewältigen, die durch die Ausbreitung von KI in nahezu alle Lebensbereiche und Industriezweige entstehen.

Das Private AI Collaborative Research Institute ist eine Forschungskooperation mehrerer Unternehmen. Das ursprünglich von Intel initiierte Zentrum baut sein Forschungspotenzial aus, indem es mit Avast, einem weltweit führenden Sicherheitsunternehmen, und Borsetta, einem Start-up für Edge-Computing,

eng zusammenarbeitet. Ziel ist es, mit der Förderung von Grundlagenforschung Technologien voranzubringen und zu entwickeln, welche die Sicherheit und das Vertrauen in dezentrale Künstliche Intelligenz (KI) stärken.

Internet:
https://www.intel.com/content/www/us/en/research/blogs/private-ai-collaborative-research-institute-launch.html

https://www.cysec.tu-darmstadt.de/cysec/index.de.jsp

Die Kooperationspartner:
Avast: www.avast.com
Borsetta: www.borsetta.io
Intel: www.intel.com

Kontakt:
System Security Lab
Prof. Dr.-Ing. Ahmad-Reza Sadeghi
E-Mail: ahmad.sadeghi@trust.tu-darmstadt.de
Tel.: +49 (0) 6151 16 – 25328

ENCRYPTO
Prof. Dr.-Ing. Thomas Schneider
E-Mail: schneider@encrypto.cs.tu-darmstadt.de
Tel.: +49 (0) 6151 16 - 27300

Über die TU Darmstadt
Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Internet und Digitalisierung, Cybersecurity, Energiesysteme, Kernphysik, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 312 Professorinnen und Professoren, rund 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie rund 25.200 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

www.tu-darmstadt.de

TECHNISCHE UNIVERSITÄT DARMSTADT

MI-Nr. 70/2020, Fröhlich/feu