Cybersicherheitsforschung der TU Darmstadt wird Teil des Private AI Collaborative Research Institute

11.12.2020 | Internationalisierung Deutschlands, Bi-/Multilaterales

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.

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.

Professor Ahmad-Reza Sadeghi, Leiter des System Security Lab und Sprecher des Profilbereichs Cybersicherheit (CYSEC) an der TU Darmstadt betont:

> *„Künstliche Intelligenz stellt eine wahre Goldmine für Cybersicherheitsforschung dar."*

Im Vordergrund seiner Forschungsarbeiten steht das sogenannte Federated Machine Learning, um exakte, vertrauenswürdige und sichere Algorithmen in Software und Hardware für KI zu etablieren.

Professor Thomas Schneider, Leiter des Fachgebiets Cryptography and Privacy Engineering (ENCRYPTO) erläutert:

> *„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."*

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.

Zum Nachlesen:

- intel: Newly Launched Private AI Collaborative Research Institute Funds First 9 Research Projects

Quelle: Technische Universität Darmstadt via IDW Nachrichten

Redaktion: 11.12.2020 von Mirjam Buse, VDI Technologiezentrum GmbH

Länder / Organisationen: Global

Themen: Information u. Kommunikation, Sicherheitsforschung

Zurück

Weitere Informationen