Pressemitteilung

Eviden Deutschland koordiniert Forschungsprojekt zur Vertrauenswürdigkeit von KI und Machine Learning

Das Ziel: Holistisches KI-Framework für digitale Souveränität schaffen

München – 13. März 2025 – Eviden, ein Unternehmen der Atos Gruppe und führend in den Bereichen Digital, Cloud, Big Data und Sicherheit, leitet ein breit aufgestelltes Forschungsprojekt, dessen Ziel es ist, die Vertrauenswürdigkeit und Souveränität von Künstlicher Intelligenz (KI) und Machine Learning (ML) – Systemen zu verbessern.

Angesichts des raschen technologischen Fortschritts integrieren datenbasierte IT-Systeme zunehmend komplexe KI/ML-Komponenten - in kritischen Umgebungen können diese zu einer potenziellen Sicherheitsbedrohung werden. Eviden Deutschland geht diese Herausforderung in einem dedizierten Forschungsprojekt mit folgenden Projektpartnern an:

- dem Deutschen Forschungszentrum für Künstliche Intelligenz - DFKI
- dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie - FKIE
- dem Fraunhofer-Institut für Angewandte und Integrierte Sicherheit - AISEC
- dem Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme - IAIS
- dem Fraunhofer-Institut für Offene Kommunikationssysteme - FOKUS

Ziel der Forschung ist es, ein methodisches und technisches Framework zu entwickeln, das sowohl die End-to-End Konzeption, Umsetzung und den sicheren Betrieb von ML-basierten Systemen ermöglicht. Damit können Anwender KI-basierte Systeme äußerst zuverlässig, belastbar und souverän nutzen.

Im Bereich der Cybersicherheit müssen Behörden beispielsweise in der Lage sein, Bedrohungen klar zu erkennen und Lagebilder zu erstellen. Hier können KI-gestützte Lösungen helfen - zum einen, weil die Datenmengen für menschliche Analysten zu groß sind, zum anderen, weil KI-Lösungen sehr gut geeignet sind, um Muster zu erkennen. Wenn jedoch die Trainingsdaten für solche Lösungen "vergiftet" wurden, das heißt irreführende Informationen enthalten, sind KI-Lösungen auch nicht mehr in der Lage, entsprechende Bedrohungen zu erkennen.

Das Projekt verfolgt einen ganzheitlichen Ansatz, der die gesamte IT-Wertschöpfungskette und die darauf einwirkenden Bedrohungen und Risiken für alle Komponenten umfasst. Um das zu ermöglichen, wird das Framework Datentypen-unabhängig anwendbar konzipiert.

Das zugrundeliegende Bedrohungsmodell bildet neben der physischen Ebene des Gesamtsystems auch alle Prozesse des Softwarelebenszyklus ab. Eine offene Systemarchitektur mit maximaler Transparenz und der technisch modulare Aufbau ermöglichen eine kontinuierliche Weiterentwicklung, um auf die dynamischen Entwicklungen im Bereich des Machine Learnings zu reagieren.

Das Forschungsprojekt untermauert die etablierten Fähigkeiten von Eviden und hilft seinen Kunden, souveräne KI-Lösungen mit einem hohen Maß an Kontrolle über ihre KI-Umgebung bereitzustellen – einschließlich Anwendungen, Middleware, Daten, Modelle und Infrastrukturen. Als europäischer Marktführer für High Performance KI- und Cybersecurity Services gilt die Atos-Gruppe als europäischer Pionier für souveräne KI.

> **Dr. Tobias Nickchen, Gesamtprojektleitung bei Eviden Deutschland (Atos Gruppe) sagt:** „Das Forschungsprojekt greift die zentralen strategischen Erkenntnisse aus aktuellen Studien zu Sicherheit und Vertrauenswürdigkeit von KI auf. Dank der aufeinander abgestimmten Forschungsfelder stellen wir sicher, dass alle Aspekte der KI-Souveränität in ein ganzheitliches Framework eingehen. So können Anwender in kritischen Branchen von hochzuverlässigen KI-Systemen profitieren, die sie bei ihren wichtigen Entscheidungen unterstützen."

***

Über Atos

Atos ist ein weltweit führender Anbieter für die digitale Transformation mit ca. 82.000 Mitarbeitern und einem Jahresumsatz von zirka 10 Milliarden Euro. Als europäischer Marktführer für Cybersecurity sowie Cloud und High Performance Computing bietet die Atos Gruppe maßgeschneiderte, ganzheitliche Lösungen für sämtliche Branchen in 69 Ländern. Als Pionier im Bereich nachhaltiger Dienstleistungen und Produkte arbeitet Atos für seine Kunden an sicheren, dekarbonisierten Digitaltechnologien. Atos ist eine SE (Societas Europaea), die an der Börse Euronext Paris notiert ist.

Das Ziel von Atos ist es, die Zukunft der Informationstechnologie mitzugestalten. Fachwissen und Services von Atos fördern Wissensentwicklung, Bildung sowie Forschung in einer multikulturellen Welt und tragen zu wissenschaftlicher und technologischer Exzellenz bei. Weltweit ermöglicht die Atos Gruppe ihren Kunden und Mitarbeitern sowie der Gesellschaft insgesamt, in einem sicheren Informationsraum nachhaltig zu leben, zu arbeiten und sich zu entwickeln.

Über Eviden[1]

Eviden ist ein Technologieführer der nächsten Generation im Bereich der datengesteuerten, vertrauenswürdigen und nachhaltigen digitalen Transformation mit einem starken Portfolio an patentierten Technologien. Mit weltweit führenden Positionen in den Bereichen Advanced Computing, Security, KI, Cloud und digitale Plattformen bringt Eviden ein fundiertes Fachwissen für alle Branchen in über 47 Ländern mit. Mit 41.000 Talenten von Weltklasse erweitert Eviden die Möglichkeiten im Umgang mit Daten und Technologien über das gesamte digitale Kontinuum, heute und für kommende Generationen. Eviden ist ein Unternehmen der Atos-Gruppe mit einem Jahresumsatz von ca. 5 Milliarden Euro.

1Das Geschäft von Eviden umfasst die folgenden Marken: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, X-Perion. Eviden ist eine eingetragene Marke. © Eviden SAS, 2025.

Kontakt zur Presse

Eviden Germany GmbH | Lisa Ludewig | lisa.ludewig@eviden.com | +49 (0) 163 1669 790