Innovationswettbewerb KI & Cybersicherheit Baden-Württemberg (2022)

Projektsteckbrief

Software zur datensicheren Nutzung von Künstlicher Intelligenz in der Industrie



Baden-Württemberg
Ministerium für Wirtschaft,
Arbeit und Tourismus

Worum geht es: Bislang sind KI-Anwendungen in Industrie und produzierendem Gewerbe noch nicht weit verbreitet. Ein bedeutendes Hemmnis sind Risiken für die Datensicherheit, da bei Cloud-basierten KI-Anwendungen oftmals sensible Fertigungsdaten mit Dritten geteilt werden müssen. Ziel des Innovationsprojektes ist die Entwicklung einer neuartigen Software-Lösung, die diese Risiken durch eine sichere Edge-to-Cloud-Architektur und den Einsatz von Verschlüsselungstechnologien minimiert.

Durchgeführt von: i-flow GmbH, Schömberg

Innovationswettbewerb KI & Cybersicherheit Baden-Württemberg

In künstlicher Intelligenz (KI) steckt viel Potenzial für innovative Produkte, Dienstleistungen und Geschäftsmodelle – und zwar quer durch alle Branchen. Das eröffnet Firmen aus Baden-Württemberg neue Chancen für Wertschöpfung und Wachstum. Wettbewerbsvorteile entstehen insbesondere dann, wenn KI-Knowhow gezielt mit Branchenwissen kombiniert wird, um neuartige Lösungen zu schaffen.

Zugleich wird in einer zunehmend digital vernetzten Welt der wirksame Schutz vor Cyberangriffen immer wichtiger. Deshalb hat das Wirtschaftsministerium Baden-Württemberg einen Innovationswettbewerb ausgeschrieben, mit dem Unternehmen bei der Entwicklung von neuartigen Produkten und Dienstleistungen zur Abwehr von Cyberangriffen gefördert werden. Im Fokus der geförderten Projekte stehen Innovationen, bei denen KI-Technologien zum Einsatz kommen oder die dazu dienen, KI-Systeme sicherer zu machen.

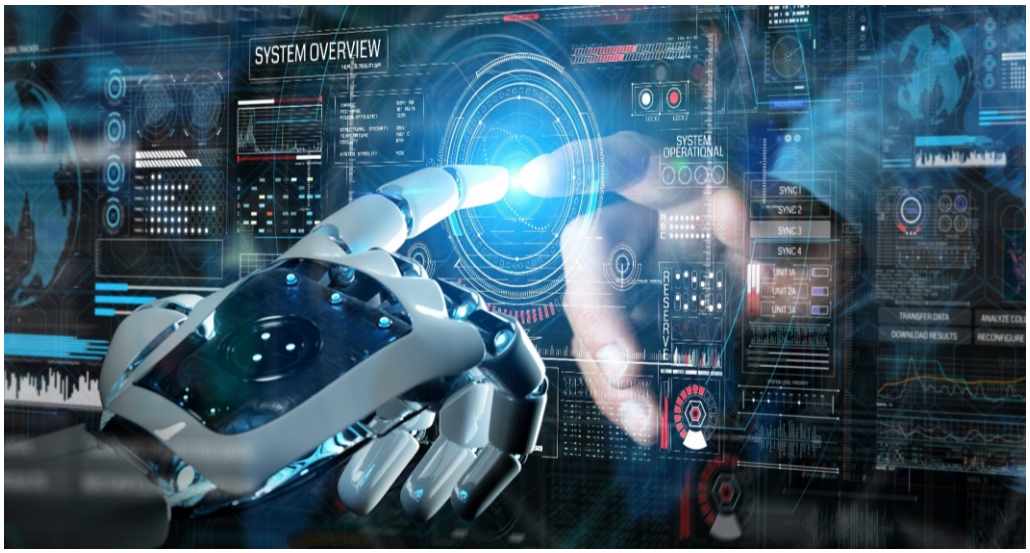
Der Innovationswettbewerb KI & Cybersicherheit ist eine Maßnahme im Rahmen des Aktionsprogramms KI für den Mittelstand des Ministeriums für Wirtschaft, Arbeit und Tourismus Baden-Württemberg.

Cybersicherheit als Voraussetzung für den erfolgreichen Einsatz von KI in der Produktion

KI-Anwendungen sind im verarbeitenden Gewerbe bei weitem noch nicht so stark verbreitet wie in anderen Branchen. Für einen erfolgreichen, möglichst breiten Einsatz von KI in der Produktion sind neben einer ausreichender Menge und Qualität von Daten, robusten Algorithmen sowie der Nutzung von Cloud Computing für das Training von KI-Modellen vor allem folgende Aspekte entscheidend, für die im Rahmen dieses Projektes eine industrietaugliche Lösung entwickelt werden soll:

- eine sichere Edge-to-Cloud-Architektur, in der KI-Modelle mit Maschinendaten aus dem Feld sicher trainiert und evaluiert werden können und die ein sicheres Deployment von trainierten KI-Modellen an die Maschinen ermöglicht.
- ein hohes Maß an Datensicherheit, so dass im Falle eines erfolgreichen Cyberangriffes auf die Unternehmens-Netzwerke kein oder nur ein möglichst minimaler Schaden verursacht wird.

Das Mehr an Sicherheit beim Training der KI-Modelle und im Betrieb der KI-Anwendungen soll dazu beitragen, bisher vorhandene Sicherheitsbedenken in Unternehmen auszuräumen und so dem verstärkten Einsatz von KI in der Produktion den Weg zu ebnen.



Verschlüsselung und ausgefeilte Edge-to-Cloud-Architektur verbessern Sicherheit und Datenverfügbarkeit

Im Unterschied zu herkömmlichen Konzepten für den KI-Einsatz im verarbeitenden Gewerbe soll eine Lösung entwickelt werden, bei der die Fabrik-Edge (Feldebene) weitestgehend und sicher von der Cloud-Umgebung abgekoppelt ist. Der Anteil der Cloud-Nutzung wird dabei auf das aus Latenz-Gründen notwendige Minimum reduziert, nämlich auf die Vorbereitung der Trainingsdaten und das Training des KI-Modells.

Um auch in diesen Phasen ein Maximum an Sicherheit zu ermöglichen, ist zusätzlich eine homomorphe Verschlüsselung der Daten vorgesehen, bevor diese in die Cloud geschickt werden. Dadurch kann eine Interpretation und Nutzung der Daten durch Dritte ausgeschlossen werden.

Insbesondere der Ansatz der Daten-Verschlüsselung ist bei diesem Ansatz gänzlich neu – und entscheidend, um die Sicherheit durchgängig zu gewährleisten und den Missbrauch der Daten wirksam zu verhindern.

Darüber hinaus ermöglicht die Verschlüsselung der Daten den Maschinenbauunternehmen, Daten mehrerer Kunden zu kombinieren und so größere Datensätze für das Training der Modelle zu erzeugen. Eine ausreichende Menge an Trainingsdaten ist ausschlaggebend für die Robustheit von KI-Modellen. Dies stellt insbesondere für kleinere Maschinenbauunternehmen, die tendenziell weniger Maschinen im Feld haben, eine große Herausforderung bei der Entwicklung von innovativen KI-basierten Zusatzfunktionen und Services dar. Von der Lösung können daher sowohl Maschinen- und Anlagenbauer wie auch deren Kunden profitieren.

Kontakt

i-flow GmbH
Christoph Sauerborn
Timo Vormweg
Ulmenstraße 3, 75328 Schömberg
christoph.sauerborn@i-flow.io
timo.vormweg@i-flow.io

Gefördert durch

Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg
Postfach 10 01 41
Schlossplatz 4 (Neues Schloss)
70001 Stuttgart
Tel: 0711 123-2869
Fax: 0711 123-2871
pressestelle@wm.bwl.de
www.wm.baden-wuerttemberg.de

Projektwebsite und weitere Informationen

https://i-flow.io

Quellenhinweis

S. 1, © sakkmesterke, istockphoto.com
S. 2, © knssr, stock.adobe.com
S. 3, © sdecoret, stock.adobe.com
S. 4, © panuwat, stock.adobe.com

Weitere Informationen zum Innovationswettbewerb finden Sie auf der
Website der Initiative Wirtschaft 4.0 Baden-Württemberg

Baden-Württemberg
Ministerium für Wirtschaft,
Arbeit und Tourismus

Initiative Wirtschaft 4.0 BW