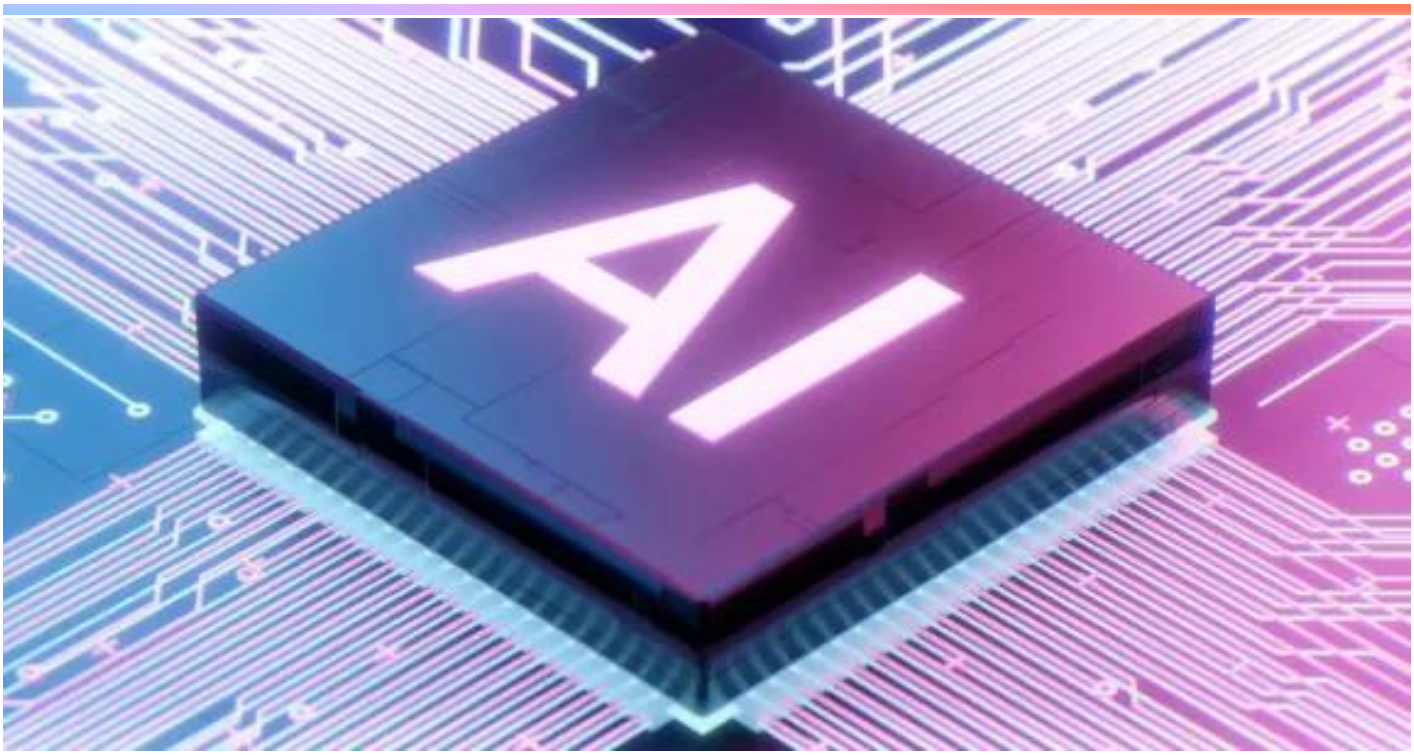


Het ZEE-project: bouwen aan betrouwbare AI in de toeleveringsketen

02 juli 2025, 09:03

Henrique Cabral

Het ZEE-project: bouwen aan betrouwbare AI in de toeleveringsketen

De huidige toeleveringsketens zijn sterker met elkaar verbonden en kwetsbaarder dan ooit. Tegen een achtergrond van wereldwijde pandemieën en geopolitieke onrust is het vermogen om snel te voorspellen en bij te sturen essentieel geworden. Tegelijkertijd kampen digitale oplossingen, zoals een ‘digital twin’ van de toeleveringsketen, met een groot obstakel: die virtuele replica's vereisen immers dat bedrijven hun gegevens delen. En hoewel die transparantie vaak aanzienlijke voordelen kan opleveren, aarzelen bedrijven om hun gevoelige gegevens en intellectuele eigendom ter beschikking te stellen.

Dat is de belangrijkste uitdaging die we aangaan met het **ZEE-project**, voluit ‘**Zero-Data Exchange for Engineering**’. ZEE verenigt de industriële partners Ahlers, Globis en Nallian in een veilige, gedistribueerde AI- en systeemarchitectuur, ondersteund door de expertise van Sirris. Ons doel: een referentiearchitectuur uitwerken die binnen complexe toeleveringsketens garant staat voor een veilige gegevensuitwisseling met behoud van de privacy, zodat digital twins zowel praktisch als betrouwbaar worden.

AI-innovaties met behoud van de privacy

In dit project bestuderen we geavanceerde AI-technieken die bedrijven in staat stellen om samen te werken zonder hun ruwe gegevens te grabbel te gooien.

In de transportlogistiek onderzochten we samen met Globis voorspellende modellen die schatten wanneer goederen klaar zullen zijn om opgehaald te worden. Zo kunnen transporteurs beter de juiste capaciteit reserveren en knelpunten voorkomen. We namen twee benaderingen onder de loep om de privacy van hun gegevens te beschermen:

- **Gesynthetiseerde gegevensgeneratie**: met algoritmen voor machinaal leren kunnen er geanonimiseerde datasets worden aangemaakt die de statistische eigenschappen van de oorspronkelijke gegevens behouden. Zo kunnen voorspellende modellen worden getraind zonder het risico te lopen dat gevoelige gegevens worden vrijgegeven. Daarbij wordt gebruik gemaakt van technieken die de differentiële privacy garanderen.
- **Federatief leren**: in plaats van onbewerkte gegevens te delen, worden modellen lokaal getraind met de gegevens van elke onderneming. Alleen de modelparameters worden gedeeld en gecombineerd tot een globaal model, zodat gevoelige gegevens binnen het bedrijf blijven.

Wat magazijnbeheer betreft, bestudeerden we in samenwerking met Ahlers methoden om uitgaande magazijnorders weken van tevoren te voorspellen. Daartoe ontwikkelden we federatieve algoritmen op basis van multi-branch LSTM-netwerken die heterogene gegevensbronnen met verschillende tijdgranulariteit kunnen samenvoegen tot hoogwaardige voorspellingen. Denk bijvoorbeeld aan eerdere orders en sociaaleconomische en geografische indicatoren. Het model voorspelt toekomstige voorraadbewegingen volgens product en klant, waardoor magazijnoperaties flexibeler en duurzamer verlopen.

Op luchthavens is vrachtafhandeling een gefragmenteerd proces met diverse belanghebbenden en een beperkte zichtbaarheid. Samen met Nallian verbeteren we hun raamwerk door machinelearning toe te passen om vrachtbehandelingstijden op dynamische wijze te voorspellen. Met behulp van historische gegevens helpen onze modellen slotreserveringen voor het lossen van goederen te optimaliseren, vertragingen te beperken en het gebruik van middelen te verbeteren.

De basis: beveiliging en architectuur

Om een veilige en gecontroleerde toegang tot gegevens en algoritmen te garanderen, hebben we een hybride toegangscontrolesysteem ontwikkeld: het combineert rol- en attribuut-gebaseerde toegangscontroles (RBAC en ABAC) en wordt ondersteund door een modulaire laag om dit beleid af te dwingen. Zo draagt het bij tot dynamische en nauwkeurige toegangsbeslissingen op basis van rollen, attributen en contextueel beleid. De oplossing is onafhankelijk van de identiteitsaanbieder en werkt samen met platformen zoals Microsoft Entra ID (voorheen Azure AD), terwijl het ook Single Sign-On (SSO) ondersteunt om de gebruiksvriendelijkheid te garanderen.

Daarnaast ontwierpen we een architectuur voor gedeelde gegevensruimten, die compatibel is met federatief leren en synthetische gegevensworkflows. Dat resulteert in een veilige coördinatie, gedistribueerde training en bescherming van zowel gegevens als modellen. De traceerbaarheid

naar de oorspronkelijke gegevensbronnen, de ondersteuning van gegevens-standaardisering, de toestemming van de eigenaar en de integriteitsgarantie zijn ingebouwd, waardoor een robuuste basis wordt gelegd om gegevens veilig en betrouwbaar te delen tussen verschillende domeinen.

Conclusie

Door privacybeschermende AI te verenigen met een robuuste beveiligingsarchitectuur maakt het ZEE-project de weg vrij voor veerkrachtige, transparante en efficiënte toeleveringsketens. Het laat zien dat bedrijven, mits gebruik van de juiste technologie, echt hun voordeel kunnen doen met digital twins zonder hun gegevens op te offeren.

Bouw mee aan betrouwbare AI voor de industrie

Kom naar het Sirris Brokerage Event en ontdek hoe bedrijven samenwerken rond AI, data en (cyber)security binnen een datagedreven R&D-landschap. Centraal staat het ZEE-project, dat inzet op betrouwbare **AI-oplossingen voor industriële toeleveringsketens**, met respect voor privacy en regelgeving zoals NIS2.

Lees meer over het event

Auteurs



Henrique Cabral