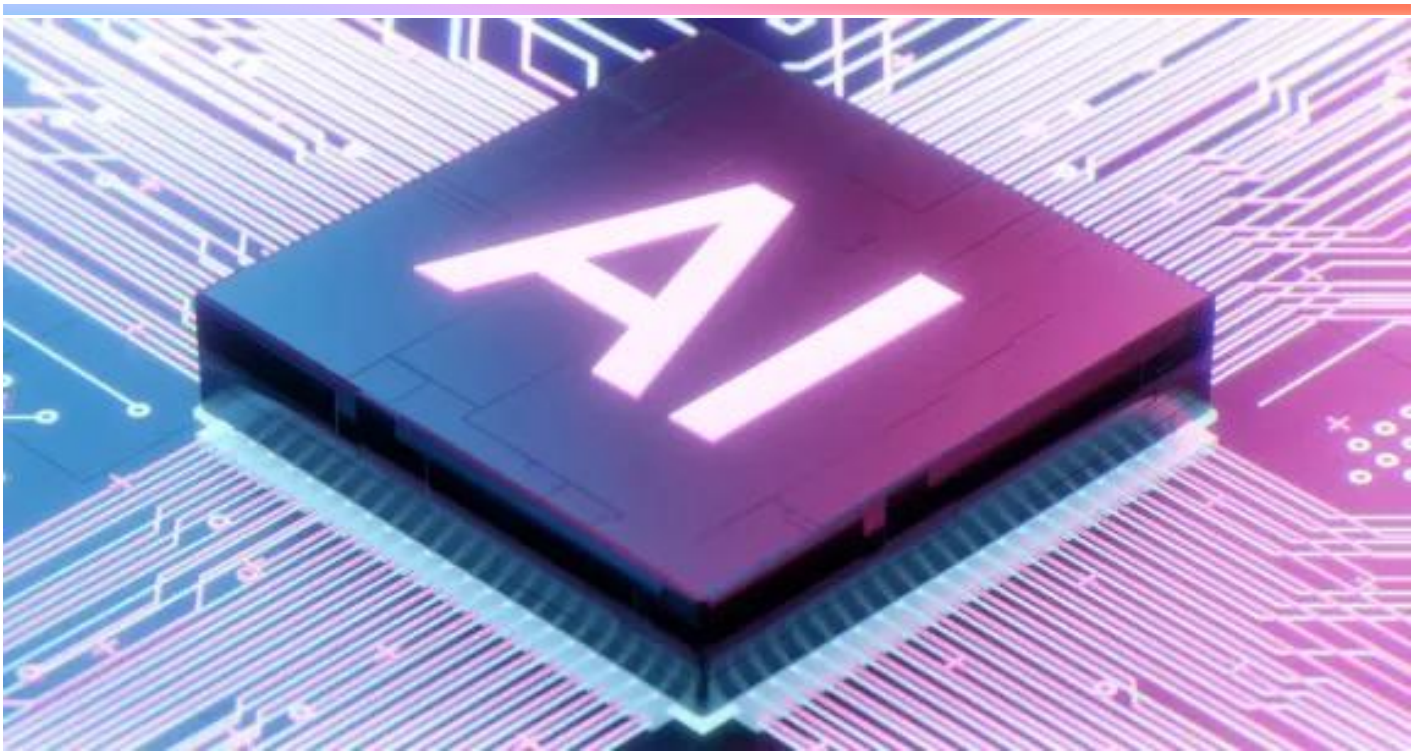


Le projet ZEE : construire une IA digne de confiance dans la chaîne d'approvisionnement

02 juillet 2025, 12:17

Henrique Cabral

Le projet ZEE : construire une IA digne de confiance dans la chaîne d'approvisionnement

Aujourd’hui, les chaînes d’approvisionnement sont plus interconnectées et vulnérables que jamais. Dans un contexte marqué par les pandémies mondiales et les perturbations géopolitiques, la capacité à anticiper et à s’adapter rapidement est devenue essentielle. Mais les solutions telles que les jumeaux numériques de la chaîne d’approvisionnement, des répliques virtuelles qui simulent l’ensemble de la chaîne logistique, se heurtent à un obstacle majeur : le partage des données. Les entreprises hésitent à partager leurs données sensibles et leur propriété intellectuelle, même lorsque la transparence pourrait déboucher sur des gains significatifs.

C’est précisément ce défi que nous relevons avec le **projet Zero-Data Exchange for Engineering (ZEE)**. Le projet ZEE réunit les partenaires industriels Ahlers, Globis et Nallian, soutenus par l’expertise de Sirris en matière d’architecture système et d’IA sécurisée et distribuée. Notre objectif est de rechercher une architecture de référence permettant un échange de données sécurisé préservant leur confidentialité dans des environnements de chaîne d’approvisionnement complexes, afin de rendre les jumeaux numériques à la fois pratiques et fiables.

Des innovations pour une IA qui préserve la confidentialité des données

Dans le cadre de ce projet, nous étudions des technologies d'IA avancées qui permettent aux entreprises de collaborer sans exposer leurs données brutes.

Dans le domaine de la logistique des transports, nous avons exploré avec Globis des modèles prédictifs prévoyant quand les marchandises seront prêtes pour l'enlèvement, permettant ainsi aux transporteurs d'optimiser la réservation de capacité et de réduire les goulets d'étranglement. Pour protéger la confidentialité des données, nous avons étudié deux approches :

- **La génération de données synthétiques** : des ensembles de données anonymisées qui conservent les propriétés statistiques des données originales peuvent être créés au moyen d'algorithmes d'apprentissage automatique. Cette approche permet d'entraîner des modèles prédictifs sans risquer d'exposer des détails sensibles. Elle s'appuie sur des méthodes qui garantissent une confidentialité différentielle.
- **L'apprentissage fédéré** : au lieu de partager les données brutes, les modèles sont entraînés localement sur la base des données de chaque entreprise. Seuls les paramètres du modèle sont ensuite partagés et combinés en un modèle global, ce qui garantit que les données sensibles ne sortent pas de l'entreprise.

En ce qui concerne la gestion des entrepôts, en collaboration avec Ahlers, nous avons étudié des méthodes permettant de prévoir les commandes sortantes plusieurs semaines à l'avance. Pour ce volet, nous avons développé des algorithmes fédérables basés sur des réseaux LSTM multibranches capables de fusionner des sources de données hétérogènes avec une granularité temporelle différente, comme des commandes historiques et des indicateurs socioéconomiques et géographiques, afin d'obtenir des prévisions de haute qualité. Le modèle prédit les futurs mouvements de stock par produit et par client, permettant un fonctionnement plus agile et durable des entrepôts.

Dans les aéroports, la manutention du fret est un processus fragmenté et impliquant de multiples parties prenantes, dans un contexte de visibilité limitée. Avec Nallian, nous travaillons à résoudre cette problématique en utilisant l'apprentissage automatique pour prédire de manière dynamique les temps de manutention du fret. En utilisant des données historiques, nos modèles permettent d'optimiser les réservations de créneaux horaires pour le déchargement des marchandises, réduisant ainsi les retards et améliorant l'utilisation des ressources.

Poser les bases : sécurité et architecture

Puisqu'il est indispensable de garantir un accès sécurisé et contrôlé aux données et aux algorithmes, nous avons conçu un système de contrôle d'accès hybride combinant le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC), soutenu par une couche modulaire d'application des politiques. Ce système permet de prendre des décisions dynamiques et précises en matière d'accès sur la base des rôles, des attributs et des politiques contextuelles. La solution ne dépend pas des fournisseurs d'identité et s'intègre à des plateformes telles que Microsoft Entra ID (anciennement Azure AD), tout en prenant en charge l'authentification unique afin de simplifier l'expérience utilisateur.

En outre, nous avons conçu une architecture d’espace de données partagé compatible avec l’apprentissage fédéré et les flux de données synthétiques. Cette architecture garantit une coordination sécurisée, un entraînement distribué et la protection à la fois des données et des modèles. La traçabilité jusqu’aux sources de données d’origine, la prise en charge de la normalisation des données, le consentement du propriétaire et l’assurance de l’intégrité sont intégrés, ce qui constitue une base solide pour un partage de données sécurisé et digne de confiance entre les domaines.

Conclusion

En associant une IA qui préserve la confidentialité des données à une architecture de sécurité robuste, le projet ZEE ouvre la voie à des chaînes d’approvisionnement résilientes, transparentes et efficaces. Le projet montre qu’avec la bonne technologie, les entreprises peuvent exploiter les avantages des jumeaux numériques sans avoir à sacrifier leurs données.

Participez au Sirris Brokerage Event et façonnez l’avenir d’une IA fiable pour l’industrie

Découvrez comment les entreprises collaborent autour de l’IA, des données et de la (cyber)sécurité dans un écosystème R&D axé sur les données. Explorez le projet ZEE, qui développe des **solutions IA** respectueuses de la vie privée pour les **chaînes d’approvisionnement industrielles**, conformes aux réglementations telles que la directive NIS2.

En savoir plus sur l'événement

Auteurs



Henrique Cabral