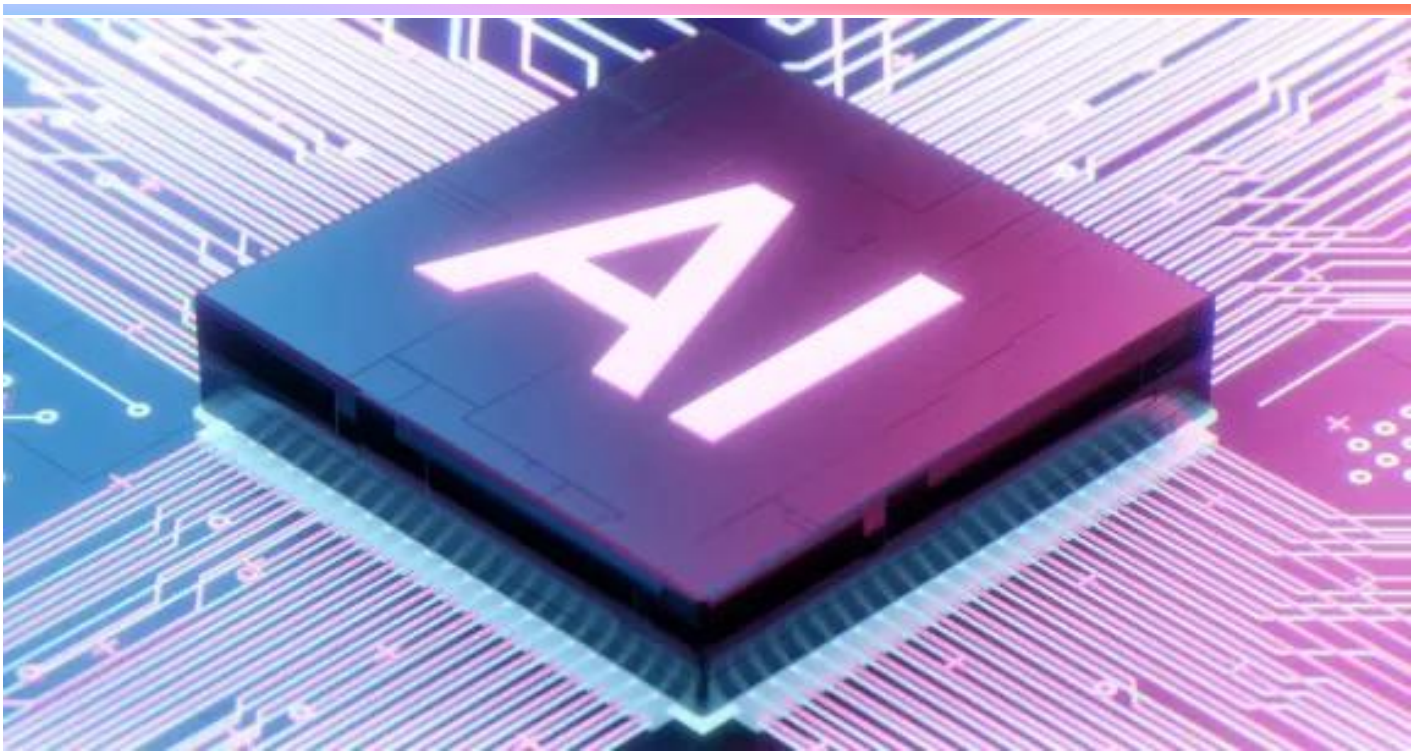


The ZEE project: building trustworthy AI in the supply chain

02 July 2025, 11:59

Henrique Cabral

The ZEE project: building trustworthy AI in the supply chain

Supply chains today are more interconnected and vulnerable than ever. From global pandemics to geopolitical disruptions, the ability to predict and adapt quickly has become essential. But digital solutions like supply chain digital twins, virtual replicas that simulate the entire logistics chain, face a major obstacle: data sharing. Companies hesitate to share sensitive data and intellectual property, even when transparency could unlock significant gains.

That is the core challenge we tackle in the **Zero-Data Exchange for Engineering (ZEE) project**. ZEE brings together industrial partners Ahlers, Globis, and Nallian, supported by our expertise at Sirris in secure, distributed AI and system architecture. Our goal: to research a reference architecture enabling secure, privacy-preserving data exchange in complex supply chain environments, making digital twins both practical and trustworthy.

Privacy-Preserving AI Innovations

In the project, we are researching advanced AI techniques that allow companies to collaborate without exposing their raw data.
In transport logistics, together with Globis, we explored predictive models that forecast when goods will be ready for pickup, improving the ability of carriers to reserve capacity and reduce bottlenecks. To protect data privacy, we researched two approaches:

- **Synthetic data generation**: Anonymized datasets that retain the statistical properties of the original data can be created via machine learning algorithms. This allows training predictive models without risking exposure of sensitive details, leveraging techniques that guarantee differential privacy.
- **Federated learning**: Instead of sharing raw data, models are trained locally on each company's data. Only the model parameters are shared and combined into a global model, ensuring that sensitive data stays within the company's premises.

For warehouse management and in collaboration with Ahlers, we investigated methods to forecast outgoing warehouse orders weeks in advance. Here, we developed federatable algorithms based on multi-branch LSTM networks that can fuse heterogeneous data sources with different temporal granularity, like historical orders and socio-economic and geographical indicators into high-quality forecasts. The model predicts future stock movements per product and customer, empowering more agile and sustainable warehouse operations.

At airports, cargo handling is a fragmented, multi-stakeholder process with limited visibility. Together with Nallian, we are advancing their framework by applying machine learning to predict cargo handling times dynamically. Using historical data, our models help optimize slot reservations for offloading goods, reducing delays and improving resource usage.

Building the Foundations: Security and Architecture

Ensuring secure and controlled access to data and algorithms is critical, we designed a hybrid access control system combining Role-Based and Attribute-Based Access Control (RBAC and ABAC), supported by a modular policy enforcement layer. This allows dynamic, fine-grained access decisions based on roles, attributes, and contextual policies. The solution is identity-provider agnostic and integrates with platforms such as Microsoft Entra ID (formerly Azure AD), while supporting Single Sign-On (SSO) for usability.

Additionally, we designed a shared data space architecture compatible with federated learning and synthetic data workflows. This ensures secure coordination, distributed training, and protection of both data and models. Traceability back to original data sources, support for data standardization, owner consent, and integrity assurance are built in, providing a robust foundation for secure and trustworthy cross-domain data sharing.

Conclusion

By combining privacy-preserving AI with robust security architecture, the ZEE project paves the way for resilient, transparent, and efficient supply chains. It shows that with the right technology, companies can unlock the benefits of digital twins, without sacrificing their data.

Building trustworthy AI solutions for industry, together

Discover how companies collaborate around AI, data, and (cyber)security in a data-driven R&D ecosystem. Explore the ZEE project, focusing on privacy-aware **AI solutions for industrial supply chains** compliant with regulations like NIS2.

Read more about the event

Authors



Henrique Cabral