

CASE STUDY



AI in a World of User-Owned Data

EXECUTIVE SUMMARY

The Institute for Experiential AI and Inrupt are proving that businesses can indeed responsibly leverage user data for impactful AI solutions that help customers and the business. By rapidly applying state of the art large language models (LLMs) to Inrupt's Solid platform architecture, the companies are enabling businesses to create privacy-first generative AI applications that deliver personalization at scale. In fact, the LLMs on Solid's platform achieve higher levels of personalization and performance than traditional LLMs and hold a number of other key advantages for businesses. The work has enormous potential in industries such as financial services, retail, health care, and more.

THE CHALLENGE

Inrupt was founded by World Wide Web inventor Tim Berners-Lee to rebalance the digital landscape by putting personal data back into the hands of users. The company believes in AI's potential to drive new offerings and personalization, but it lacked the in-house resources to integrate the latest AI technology into its privacy-oriented **Solid architecture**, which allows organizations to securely host digital wallets for their customers or citizens and includes identity management, access control, and universal standards for data.

To create powerful AI applications that work with the user-owned data central to Inrupt's system, the company partnered with the Institute for Experiential AI's **AI Solutions Hub** (AISH) to produce a new kind of generative AI solution as innovative as the Solid infrastructure it was built on.





A COLLABORATIVE APPROACH

Members of the **AI Solutions Hub** had to invent a technique for leveraging AI that was compatible with the innovative ways that data is stored and managed in Inrupt's Solid architecture. None of this was straightforward. When data is managed by the users, the fundamental ways AI applications access and use data changes dramatically.

After the AISH team underwent training on Inrupt's Solid architecture, Inrupt explained the mission: To take data from a user's Solid Wallet and get it into the context window of a large language model in a way that provides full traceability on what happens to that data to confirm it's never sent anywhere else.

After exploring several different frameworks, the AISH team quickly built a novel interface between Solid and one of the latest open-source LLM technologies. The team was then able to demonstrate that generative AI solutions could achieve personalization without relying on centralized stores of millions of people's data. The work was presented at an Inrupt conference in August of 2023.

“Northeastern University was an expert partner in the fast-moving landscape of open source AI. Their eagerness to learn and apply the power of Solid ensured that we could quickly prove the value of Active Wallet™, Solid's user-centric data storage delivering uniquely safe AI. Our successful proof of concept paved the way for Inrupt to release Active Wallet™, which is being applied across multiple industry use cases.”

— John Bruce, CEO & Co-Founder,
Inrupt

**Interested in how AI can help
your organization?**

Schedule a strategy session today:
ai.northeastern.edu/partner-with-us



A NEW PATH FORWARD FOR AI

The highly personalized LLM platform works with data stored in Inrupt's Solid Wallet, paving the way for generative AI applications to work in the world of user-owned data. AISH experts also showed Inrupt examples of how the architecture worked, including in a natural language movie recommender.

The solution showed the potential to build highly-personalized generative AI applications in ways that preserve user control of data and privacy, for instance by ensuring user data won't be used to train future models.

Furthermore, by using an individual's Solid Wallet data, the LLMs have several key advantages over generic LLMs. Namely, the LLMs offer a closer fit between the model and its use cases because of its understanding of the user and clearly defined application scope.

THE PROMISE OF PRIVACY-FIRST AI

Privacy-first AI holds enormous potential in industries such as financial services, retail, and health care. It could be used for applications like global health portals built off of data shared by citizens, or to provide personalized product recommendations based on each user's interests.

The project aligns closely with the Responsible AI work done at the Institute for Experiential AI. Indeed, techniques such as federated learning, data governance, bias, and consent are all things our institute's experts think about on a daily basis.

“Businesses shouldn't have to hand over their users' data to get value from AI applications. By combining Inrupt's decentralized data ecosystem with our approach to building AI solutions for real business problems, we're showing that using privacy-preserving Responsible AI to drive value for customers is a reality, and at scale.”

— **Usama Fayyad, Senior Vice Provost for AI and Data Strategy, Senior Advisor to the President & Inaugural Director of the Institute for Experiential AI, Northeastern University**