MIT CSAIL Alliances

Dynamo AI

Case Study

Dynamo AI

Written by Audrey Woods

In a world of booming generative AI applications, business leaders across the economy worry that they need to incorporate AI or risk falling behind. However, there are many factors to consider before designing, using, and/or launching AI systems, including security, privacy, hallucinations and legal compliance. Between increasing regulation and shifting consumer expectations, it's more important than ever for companies to be aware of and address the risks at every level of their evolving AI stack.

MIT CSAIL Startup Connect member Dynamo AI aims to help companies navigate this change with a suite of products designed to offer end-to-end privacy, security, and compliance solutions. Broken into three pillars of AI-focused support—DynamoEval, DynamoEnhance, and DynamoGuard—Dynamo AI seeks to support the democratization of AI technologies by making them accessible, reliable, and safe to implement.

GETTING THEIR START

As CEO and Co-Founder Vaikkunth Mugunthan tells it, Dynamo AI began as the last chapter of his PhD thesis at MIT. When he first started his graduate studies under CSAIL Principal Research Scientist Lalana Kagal, he was focused on theoretical privacy. But when a CSAIL Alliances poster session landed him a summer internship with JPMorgan, he was introduced to federated learning, which trains AI by sharing the model itself instead of sharing data, thereby offering valuable privacy guarantees. There was a pressing industry demand for this technology, especially in finance and healthcare, and the interest he experienced made him confident enough to launch the company in 2021.

While Dynamo AI was originally focused only on providing a "plug and play" tool for federated learning—in fact the company's original name was DynamoFL—the team soon realized that there were many other aspects of AI implementation that customers were concerned about. New AI-related laws emerging around the world, the risks, both known and unknown, of launching AI systems, and the ongoing process of protecting users and companies from those who might misuse AI programs either intentionally or not were all issues that Mugunthan realized Dynamo AI could help with. Therefore, in late 2023 and early 2024, the company pivoted from a focus exclusively on federated learning to a broader, more comprehensive set of features designed to assist companies in both designing and launching safe and compliant AI systems.

Now Dynamo AI is partnering with Fortune 500 businesses to test their tools in various industry functions. They went through the YCombinator startup accelerator and got "the first interview on the first day," Mugunthan says, and the company has since gone on to raise $19.4 million. Their two different TechCrunch features—one in 2022 and one in 2023—each brought a fresh wave of publicity that helped grow the company to where it is today, with 45 employes and customers such as Lenovo, Qualcomm, and Aisin. As a self-described "research-heavy" company, Dr. Mugunthan explains how their priority is to "hire masters or PhDs from the best schools" and become the most trusted name in the field of AI support.

DYNAMO AI: SECURING THE AI STACK

When explaining the need that Dynamo AI aims to meet in the industry, Head of Growth and Strategic Partnerships Kavi Arora says, "if we really want to democratize these technologies in different GenAI-based consumer-focused, internally focused applications, and agent focused applications, there are a many risks that exist in privacy, security, and hallucinations." Dynamo AI, he explains, is "addressing the need for privacy, security, and compliance throughout that AI stack [by] testing applications for risks, remediating those risks, and then real-time guardrailing applications as they go into production." These services fall into three main "modules:" DynamoEval, DynamoEnhance, and DynamoGuard.

DynamoEval evaluates LLMs and generative AI programs as they're being designed to make sure a given program complies to emerging regulatory standards. Providing automated stress testing, DynamoEval generates the needed documentation for regulatory audits and checks a system's weaknesses in privacy, security, and hallucination. DynamoEnhance offers support at the next phase of development, fixing and remediating the identified risks. This module offers several easy-to-use techniques to improve privacy (such as federated learning), mitigate hallucinations, and bolster program safety. And finally, DynamoGuard supports AI programs going into production by creating real time guardrails that are customizable in natural language, for every organization's bespoke policies. "For example," Arora says, "multiple financial services institutions are deploying internal chatbots leveraged by different portfolio managers. We're enabling them to create guardrails where you can allow certain levels of portfolio managers to drive certain types of insights and others to not." That level of granularity helps businesses enforce governance policies, prevent misuse, and easily audit their LLMs.

Taken altogether, Dynamo AI's various modules offer a platform for enabling secure, private, hallucination-free, and regulation-compliant AI models.

THE CSAIL CONNECTION

One thing Dr. Mugunthan makes clear is how much he attributes his success to Lalana and CSAIL. From the very beginning, it was Dr. Kagal's encouragement that inspired him to take a chance and apply to MIT, and he describes his time at CSAIL as "a fantastic experience."

"I really enjoyed the collaborative nature of projects," he says, highlighting his ability to get a minor from Harvard and his deep roots in the CSAIL community.

For Dr. Mugunthan, his link to CSAIL is more than nostalgic; it's a pivotal part of his company's strategy. He says through MIT, "we have access to the best talents in the world," an advantage he's used to hire some of the PhDs the company now employs. Dynamo AI is also planning to launch internships and create a Dynamo AI ambassador program with CSAIL, which would deepen this connection. Dr. Mugunthan adds, "I wouldn't have been at this stage [without CSAIL], so I want to give it back as well."

Beyond recruitment, Dynamo AI is utilizing their connection with CSAIL Alliances to maximize the company's exposure and vet potential business partners. Dr. Mugunthan has been invited to present at several Alliances conferences, which has led to "a good number of client leads" and helped Dr. Mugunthan understand specifically which companies were interested. "We were able to tailor our product toward what they needed," he explains, which helped Dynamo AI create even more market traction. Because of that, he's eager to take part in future CSAIL Alliances events.

"CSAIL Alliances has been super helpful," Dr. Mugunthan says, calling Sr. Client Relations Coordinator Philip Arsenault "a fantastic friend of mine."

LOOKING FORWARD

When asked what they're focused on next, Dr. Mugunthan and Arora explain that Dynamo AI is now looking to expand the company's reach into new sectors, exploring how their suite can be applied to different industries. With the AI market growing in nearly every economic sector, Dynamo AI hopes to use this momentum to their advantage and support positive technological change.

Dr. Mugunthan says the end goal for Dynamo AI is "to make sure that when it comes to privacy preserving machine learning, the first company that comes to anyone's mind is us." With that in mind, Dr. Mugunthan calls his association with MIT an "added advantage," showing clients that Dynamo AI has the best people on the job.