IronCore Labs Announces Breakthrough with Cloaked AI: Encrypted Training Data Makes AI Models Safe and Private

IronCore Labs' Cloaked AI now encrypts training data and models, ensuring AI privacy and security of production AI systems.

IronCore Labs: Lock Your-Data. Unlock Your AI.

BOULDER, CO, UNITED STATES, July 10, 2025 /EINPresswire.com/ -- IronCore Labs today announced powerful new capabilities for its existing Cloaked AI technology, extending its encrypted vector protection beyond search to also cover AI training data and models themselves. With this advancement, companies can train models using encrypted data that remains private, even to those building or hosting the models — and the models are only usable with the correct encryption key.

Traditional AI models are often trained on vast amounts of sensitive or proprietary data, creating serious risks of data leakage or theft. Cloaked AI eliminates this risk by applying approximate-distance-comparison-preserving encryption (DCPE) to vector embeddings. This allows data scientists to train accurate and performant models without ever exposing or risking the underlying data.

> Data used to train AI models is a liability if not handled securely."
>
> *Patrick Walsh*

"Data used to train AI models is a liability if not handled securely," said Patrick Walsh, CEO of IronCore Labs. "Cloaked AI encrypts the 'memory of AI', giving companies a way to build smarter models without compromising their users' privacy or their own sensitive information."

Models trained with Cloaked AI can operate normally, performing tasks like classification or prediction, but only respond to encrypted inputs that were encoded using the same key as the training data. This one-way encryption process ensures that models are not only secure from external threats, but also from internal misuse by engineers or admins.

Cloaked AI was initially designed to safeguard data stored in vector databases—a critical element of Retrieval Augmented Generation (RAG) workflows that is particularly vulnerable to embedding inversion attacks. With its new capabilities, Cloaked AI now extends its protection beyond vector databases, securing sensitive data both within RAG workflows and directly in AI models.

Cloaked AI is open source under the AGPL license and also available via commercial license as a software library. Developers can easily get started using the library in popular programming languages, and the IronCore team actively supports a growing community of users.

To learn more about Cloaked AI or try it out, visit the Cloaked AI product page. To learn more about encrypting training data and protecting models, download our Training AI Without Leaking Data White Paper.

About IronCore Labs

IronCore Labs is a leader in application-layer encryption and data privacy solutions for modern cloud and AI software. Its technology empowers organizations to build powerful, privacy-preserving AI and cloud applications by securing data at its most sensitive points — in use, in transit, and at rest. IronCore has a comprehensive platform with capabilities ranging from encrypted search and secure vector handling to multi-tenant SaaS BYOK patterns and AI model protection. By preventing data leakage and insider risk, IronCore helps businesses stay ahead of threats, meet global privacy regulations and adopt emerging technologies with confidence.

PR Liason
IronCore Labs
info@ironcorelabs.com
Visit us on social media:
LinkedIn
YouTube
X
Other