SafeLiShare Introduces Revolutionary ConfidentialAI™ LLM AI Governance Platform Empowered by Secure Enclave

Eliminate AI poisoning, model evasion and extraction attack vectors across the LLM and AI pipelines

MORRISTOWN, NEW JERSEY, UNITED STATES, June 14, 2023 /EINPresswire.com/ -- SafeLiShare, Inc, a leading provider of cutting-edge data privacy and AI security solutions, proudly announces the launch of its industry-first ConfidentialAI™ Governance Platform. Powered by secure enclave technology, this groundbreaking platform enables organizations to enforce access policies while maintaining the utmost confidentiality during AI model training, inferencing, and retraining processes. SafeLiShare's innovative solution revolutionizes the way confidential computing is utilized, offering multiparty model sharing and bringing Model to Data in strict data residency and compliance scenarios.

Traditionally, organizations have faced challenges when it comes to preserving the privacy and confidentiality of their sensitive data during AI operations. SafeLiShare's ConfidentialAI™ Governance Platform addresses these concerns by leveraging secure enclave technology, which ensures that sensitive information remains fully protected, even during processing. By encapsulating AI workloads in secure enclaves, SafeLiShare enables organizations to enforce access policies and encryption in use that guarantee confidentiality throughout the entire AI lifecycle.

According to a recent Gartner survey, it was found that 41% of organizations have encountered an AI privacy breach or security incident, highlighting the growing concern. With the proliferation of third-party algorithm models and data, the risk of adversarial attack vectors is on the rise, leading to an expanding attack surface. Given these circumstances, it becomes crucial to implement effective governance and security measures to safeguard against such attacks on AI models and data access.

What sets SafeLiShare apart from other solutions is its ability to facilitate multiparty model sharing. Organizations can securely collaborate and share AI models with trusted partners while ensuring the privacy of their proprietary algorithms and data. This capability is particularly valuable for industries that require strict compliance measures and data residencies, such as healthcare, finance, and government sectors.

"We are excited to introduce the ConfidentialAI™ Governance Platform to the market," said

Shamim Naqvi, CEO and Co-Founder of SafeLiShare, Inc. "We understand the critical importance of data privacy and compliance in today's AI adversarial attack landscape. With SafeLiShare, organizations can harness the power of AI while maintaining complete control and confidentiality over their models and data pipelines."

SafeLiShare's ConfidentialAI™ Governance Platform offers the following key features:
- Secure Enclave Technology: Utilizes state-of-the-art secure enclave technology to protect sensitive data and algorithms during AI operations.
- Access Policy Enforcement: Enforces stringent access policies to ensure confidentiality throughout the AI lifecycle, including model training, inferencing, and retraining.
- Multiparty Model Sharing: Enables secure collaboration and sharing of AI models among trusted partners, maintaining data privacy and confidentiality.
- Bring Model to Data Approach: Supports bringing compute to data, ensuring compliance with strict data residency regulations, and avoiding data transfers.

SafeLiShare invites organizations to explore the power of its ConfidentialAI™ Governance Platform and experience the benefits of secure and confidential AI operations. For more information and to request a demo, please visit https://safelishare.com/solution/confidential-ai/ or contact ai@safelishare.com.

About SafeLiShare, Inc:
SafeLiShare, Inc is a leading provider of advanced data privacy and AI governance solutions based in Morristown, New Jersey. The company is committed to helping organizations protect sensitive data and maintain privacy throughout the LLM and AI lifecycle. SafeLiShare's innovative ConfidentialAI™ Governance Platform, powered by secure enclave technology, enables multiparty model sharing and supports compute-to-data scenarios in strict data residency and compliance environments.

Cynthia Hsieh
SafeLiShare, Inc.
+1 408-869-6277
media@safelishare.com
Visit us on social media:
Twitter
LinkedIn
YouTube
