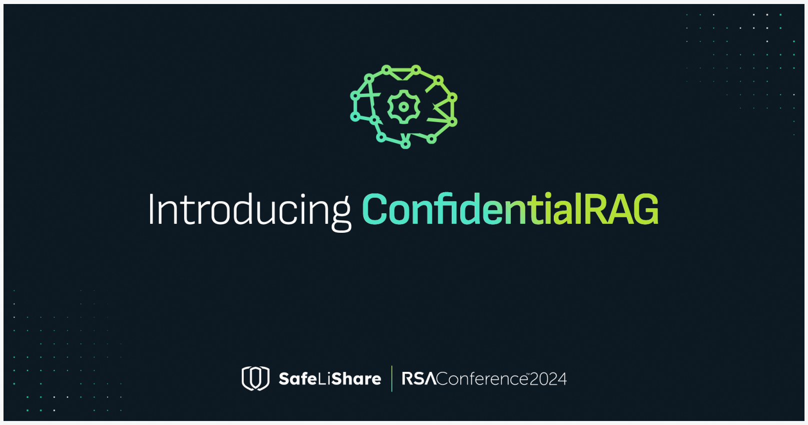
EINPRESSWIRE

SafeLiShare unveils ConfidentialRAG Private Beta at RSAC 2024, featuring Microsoft Azure OpenAI Service for LLM Apps

Ground LLM RAG workflow in the organizations' owned data, vector databases, or knowledge graphs and bolster data security and privacy for enterprises.



Introducing ConfidentialRAG

SafeLiShare | RSAConference2024

SafeLiShare ConfidentialRAG Private Beta Announcement at RSAC2024

SafeLiShare

MORRISTOWN, NEW JERSEY, UNITED STATES, May 6, 2024 / EINPresswire.com/ -- SafeLiShare, a pioneer in delivering innovative solutions for data security and privacy in AI ecosystems, is thrilled to unveil the private beta of ConfidentialRAG® at RSA Conference 2024. This groundbreaking API solution is tailored to provide the simplest no-code approach for securing Large Language Models (LLMs) utilizing the Retrieval Augmented Generation (RAG) architecture, particularly when integrated with Microsoft's Azure OpenAI Service. ConfidentialRAG is poised to address the critical needs of enterprises with assets in sectors such as critical infrastructure, fintech, healthcare, and government applications.

SafeLiShare ConfidentialRAG ensures the confidentiality of every prompt with end-to-end protection. Cloud service providers cannot access queries, responses, chat history, or any login information, guaranteeing the privacy of your enterprise. The solution enhances responses by employing runtime encryption to shield enterprise private data within a trusted execution environment. It ensures the confidentiality of shared knowledge bases and assets, bolstering cybersecurity, data loss prevention (DLP), and input/output security. This preview version aims to fortify the protection of private data, a paramount concern for modern enterprises.

SafeLiShare ConfidentialRAG provides content filtering for enterprise LLM policies that filter out hallucinations, copyright materials, malicious executables, inaccurate contents, and unwanted outputs. The output filter is situated in SafeLiShare ConfidentialAI for RAG, an encrypted enclave that cannot be jailbroken or subjected to backdoor leaks.

> “SafeLiShare ConfidentialRAG is easy to integrate for data aggregators' LLM foundation with cloud-native confidential enclave to define the boundary for Needl.ai RAG to connect, curate, and converse.”
>
> *Vikram Srinivasan, CEO of needl.ai*

With SafeLiShare ConfidentialRAG, the privacy impact assessments are straightforward since LLMs are trained in a fully encrypted enclave. It provides a security compliance audit trail and verification of user data security, privacy, and protection in hosted OpenAI LLM environments.

The platform offers accessible robust REST APIs, facilitating seamless onboarding for tasks such as similarity search, vector database access, and tokenization for input/output filtering. It efficiently manages enclave-based authentication and key management for secure data access, incorporating parameterized access for heightened security. Additionally, an enclave-based log ensures access verification and compliance audit, allowing users to monitor data plane and control plane activities effectively.

Policy-driven identity access to enterprise private data is seamlessly managed, ensuring an easy way to house conversation AI engine using Azure OpenAI services to ensure RAG computation is fully encrypted with advanced DLP.

Designed for enterprise LLM RAG applications handling sensitive private data, ConfidentialRAG emerges as a vital tool in fortifying AI deployments against evolving threats.

The RSA Conference, renowned as the premier cybersecurity event globally, provides an ideal platform for SafeLiShare to introduce ConfidentialRAG to the cybersecurity community. Visitors to the SafeLiShare booth located at ESE / Early Stage Expo, situated at Moscone Center South Room 205, will have the opportunity to experience firsthand the power and capabilities of ConfidentialRAG.

Shamim Naqvi, CEO of SafeLiShare, expressed enthusiasm about the public beta release, stating, "ConfidentialRAG represents a significant leap forward in our mission to empower enterprises with secure and compliant AI deployments. By leveraging Azure OpenAI Service and adding advanced confidentiality features, ConfidentialRAG offers the utmost protection for sensitive private data located in Data Lakehouse, ERP, and CRM systems, ensuring trust and regulatory adherence in AI workloads."

Vikram Srinivasan, CEO of needl.ai, also praised SafeLiShare's ConfidentialRAG, saying, "SafeLiShare ConfidentialRAG is easy to integrate for data aggregators' LLM foundation with cloud-native confidential containers to define the boundary for Needl.ai RAG to connect, curate, and converse with enterprise' applications, web sources, and regulatory sources with enterprise-class confidentiality and privacy control at petabyte scale, especially important for enterprises in Financial services, consulting, legal, and pharmaceutical industries."

John Kindervag, Strategic Advisor for SafeLiShare, emphasized the importance of zero-trust principles in safeguarding sensitive data within AI environments. "Zero trust principles become more critical than ever to protect sensitive data within AI environments. Conversational AI leaks concern events where sensitive data input into an LLM is unintentionally exposed, underscoring the urgency for solutions like ConfidentialRAG leveraging validated execution environment to prevent sensitive data from unintentionally leaving the enterprise network by managing user permission in LLMs and encryption in use while in memory."

ConfidentialRAG offers a comprehensive array of features tailored to meet the stringent security and compliance requirements of enterprise environments.

For press inquiries and interviews regarding ConfidentialRAG private beta and SafeLiShare's innovative solutions, please contact press@safelishare.com.

About SafeLiShare: SafeLiShare is a leading provider of advanced solutions for data security and privacy in AI environments. With a focus on confidential computing and trusted execution environments, SafeLiShare empowers enterprises to safeguard sensitive information, mitigate risks, and maintain compliance in AI-driven applications. Learn more at www.safelishare.com.

Contact:
Press Contact: press@safelishare.com
Private Beta Contact: ConfidentialRAG@safelishare.com
Website: www.safelishare.com

Media Hotline
SafeLiShare Inc.
email us here
Visit us on social media:
Twitter
LinkedIn
YouTube