inpher

SecurAI

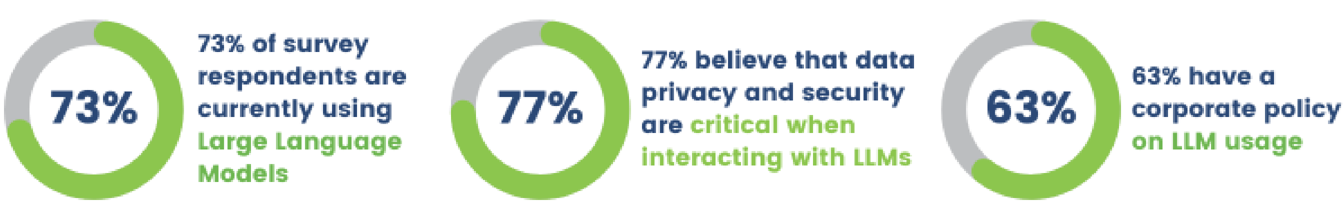
Leverage LLMs and generative AI privately, securely and with complete autonomy

Generative AI's Trust Problem

In the rapidly evolving landscape of generative Artificial Intelligence (AI), organizations are exploring applications to enhance productivity and unlock substantial business benefits. However, utilizing AI for applications like code development, content creation, anomaly detection, automation, healthcare analytics or personalization often involves handling sensitive data and intellectual property. The visibility of this data specifically through prompts and completions shared with a model service provider raises serious governance concerns, hindering organizations from fully leveraging AI capabilities.

Leveraging LLMs Securely

With Inpher SecurAI, organizations can harness the power of ChatGPT and other Large Language Models (LLMs) while ensuring privacy, compliance and trust. SecurAI also supports using Retrieval Augmented Generation (RAG) to provide specialized responses based on enterprise-specific data. SecurAI's solution leverages Trusted Execution Environments (TEEs) to address the privacy and security concerns that users contend with when trying to leverage open models where information might be susceptible to leakage and scrutiny by the hosting party.



Source: Inpher's 2023 survey on LLMs

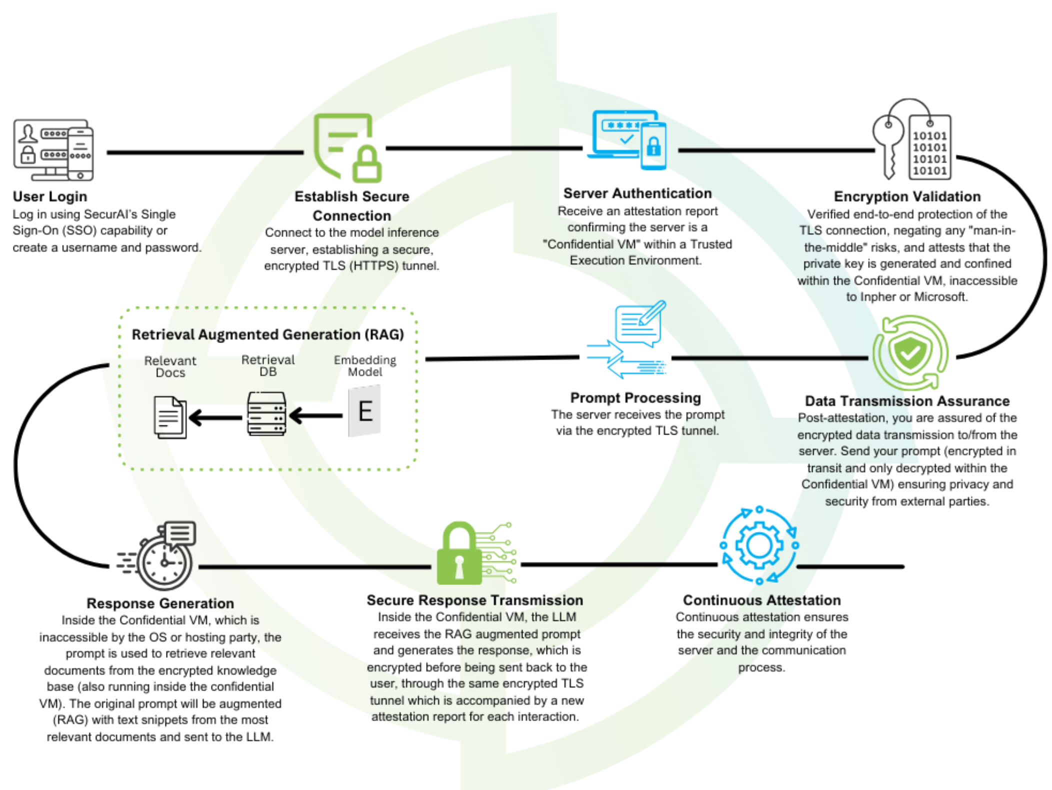
How SecurAI Works

SecurAI ensures security with a holistic model that combines hardware-based security measures, access controls, attestation, secure communication protocols, and proactive maintenance. At its core is the virtual machine (VM)-level TEE, a secure enclave where sensitive computations occur. The TEE employs hardware-based mechanisms to establish a foundation of trust, preventing unauthorized access and tampering. Secure boot processes, backed by cryptographic measures, ensure that the system initiates in a known, secure state.

The security model also incorporates attestation to verify the integrity of the VM. This involves generating cryptographic keys, producing attestation reports, and employing a secure channel for communication with remote verifiers. The attestation process serves as a continuous assurance mechanism, validating that the computing environment remains secure throughout its operation.

Secure communication protocols, such as attested transport layer security (TLS), protect data in transit. Encryption and secure key exchange mechanisms within these protocols add an additional layer of defense against eavesdropping and man-in-the-middle attacks.

If organizations wish to leverage RAG, the prompt can be used to retrieve relevant documents from the encrypted knowledge base, running inside the confidential VM. The original prompt will then be augmented with text snippets from the most relevant documents sent to the LLM.



Regulatory Compliance

Using a TEE aligns with regulatory and compliance requirements that mandate stringent data protection measures. By deploying LLMs in a secure enclave, optionally enhanced with RAG, organizations can demonstrate their commitment to maintaining the confidentiality and privacy of user inputs. The SecurAI model provides a multilayered defense that extends beyond conventional security protocols, safeguarding the integrity of the computation environment even in the presence of potential threats, such as malicious insiders or external attackers.

Your AI Security Partner

For organizations seeking to harness the predictive power of AI in a manner that aligns with ethical and regulatory demands, we invite you to experience the security and efficiency of SecurAI. In an era where data breaches are costly and trust is hard earned, partnering with Inpher means building your AI initiatives on a foundation of trust and reliability.

Inpher SecurAI – a revolutionary approach to leveraging LLMs, RAG and generative AI privately, securely and with complete autonomy.

About Inpher

Inpher, Inc. is the leader in privacy-enhancing computation that empowers organizations to collaborate on sensitive data seamlessly and securely across teams and borders. Inpher's award-winning platform employs machine learning and AI in order to remove data barriers and silos while delivering the highest level of trust and precision in even the most complex data collaboration initiatives. Founded by world-renowned cryptographers and engineers, Inpher has long been recognized as a pioneer in the fields of secure Multiparty Computation (MPC), Fully Homomorphic Encryption (FHE), Federated Learning (FL), and other combinations of privacy-enhancing technologies (PETs). Inpher continues to deliver enterprise ready capabilities and real-world examples.

For more information on Inpher, please visit us at inpher.io and follow us on LinkedIn and Twitter.

Try it for yourself today!
securai.inpher.io