![inpher logo] 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 or cloud 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 Large Language Models (LLMs) while ensuring privacy, compliance and trust. 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.
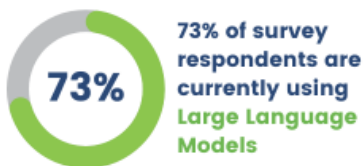
Regulatory Compliance

Using a TEE aligns with regulatory and compliance requirements that mandate stringent data protection measures. By deploying LLMs in a secure enclave, 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.

73% — 73% of survey respondents are currently using Large Language Models

77% — 77% believe that data privacy and security are critical when interacting with LLMs

63% — 63% have a corporate policy on LLM usage

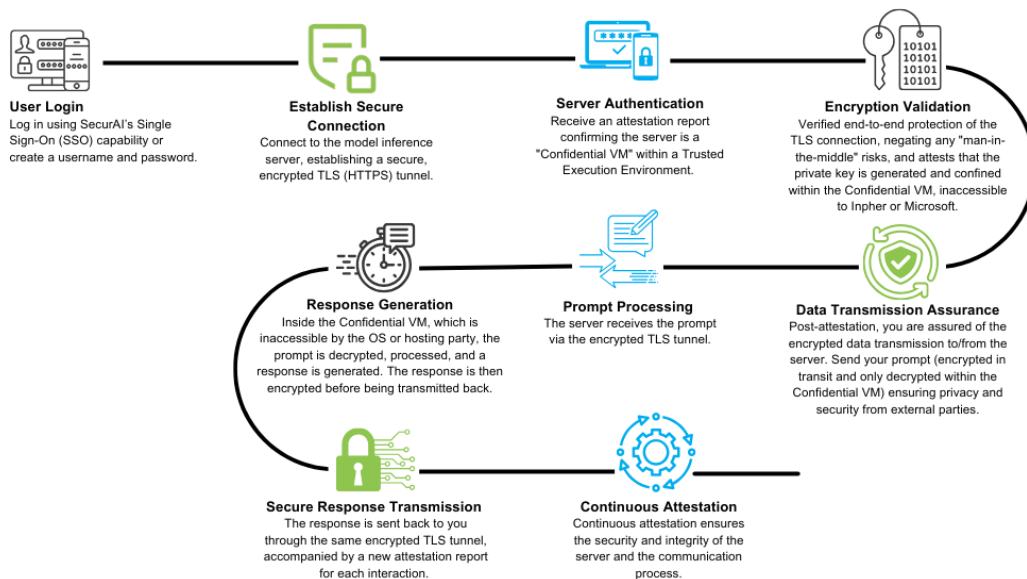Source: Inpher's 2023 survey on LLMs

inpher.io

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.

User Login
Log in using SecurAI's Single Sign-On (SSO) capability or create a username and password.

Establish Secure Connection
Connect to the model inference server, establishing a secure, encrypted TLS (HTTPS) tunnel.

Server Authentication
Receive an attestation report confirming the server is a "Confidential VM" within a Trusted Execution Environment.

Encryption Validation
Verified end-to-end protection of the TLS connection, negating any "man-in-the-middle" risks, and attests that the private key is generated and confined within the Confidential VM, inaccessible to Inpher or Microsoft.

Response Generation
Inside the Confidential VM, which is inaccessible by the OS or hosting party, the prompt is decrypted, processed, and a response is generated. The response is then encrypted before being transmitted back.

Prompt Processing
The server receives the prompt via the encrypted TLS tunnel.

Data Transmission Assurance
Post-attestation, you are assured of the encrypted data transmission to/from the server. Send your prompt (encrypted in transit and only decrypted within the Confidential VM) ensuring privacy and security from external parties.

Secure Response Transmission
The response is sent back to you through the same encrypted TLS tunnel, accompanied by a new attestation report for each interaction.

Continuous Attestation
Continuous attestation ensures the security and integrity of the server and the communication process.

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

About Inpher

Inpher, Inc. is the leader in privacy-enhancing computation that empowers organizations to harness the potential of AI securely and with trust. Inpher makes privacy-preserving machine learning easy, enabling organizations to unlock the value of sensitive data across teams, organizations, and geographies without moving it. For organizations seeking to leverage new generative AI technologies such as ChatGPT, Inpher SecurAI ensures privacy and compliance. 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).

Try SecurAI