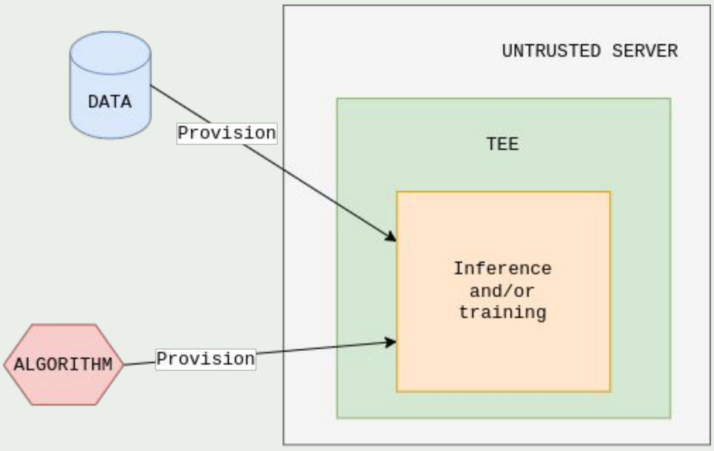
Cube AI

by Ultraviolet

Protecting LLMs in Secure Enclaves

Your AI is Now Protected!



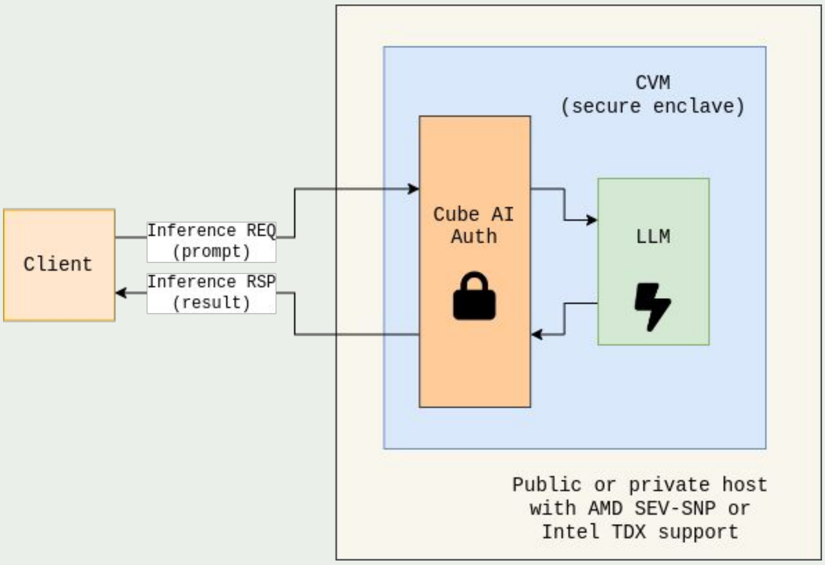
Confidential Computing

Confidential Computing and TEEs (Trusted Execution Environments) ensure data privacy and integrity by processing sensitive information in isolated and secure environments.

These technologies can protect AI by safeguarding data and algorithms during both model training and inference, preventing unauthorized access and tampering.

Cube AI

Cube AI is an open-source framework for securely deploying Large Language Models (LLMs) in privacy-sensitive applications using Confidential Computing. It leverages Trusted Execution Environments (TEEs) to protect user data and AI models, ensuring confidentiality and integrity during processing by isolating sensitive computations within secure enclaves.



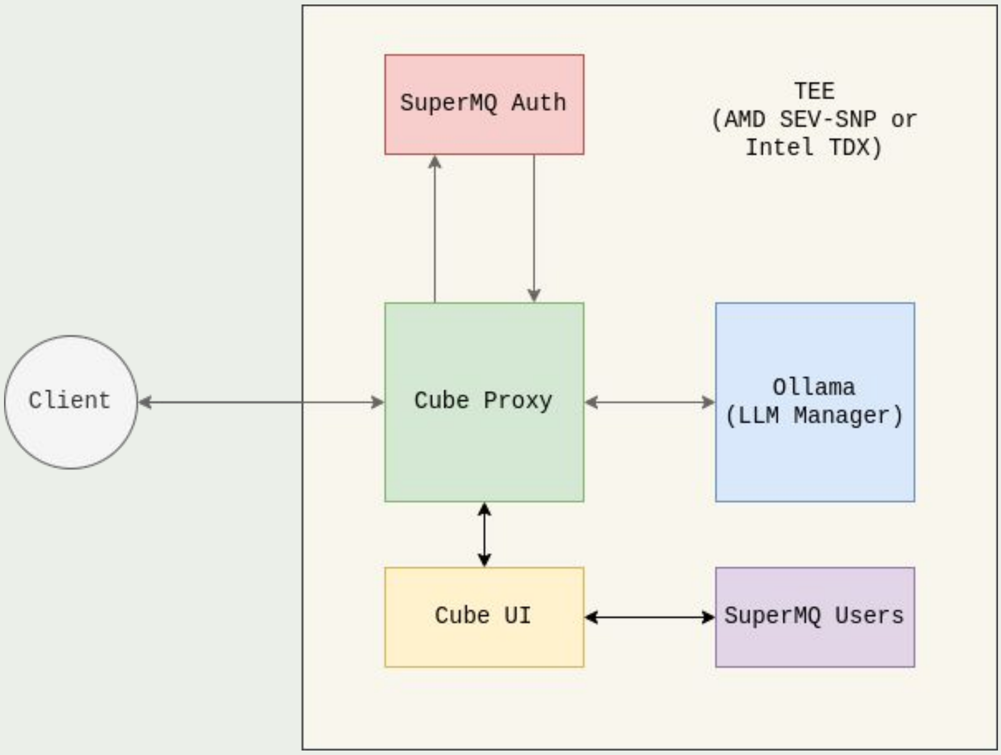
Deploy Any LLM

Cube AI empowers organizations to deploy **any Large Language Model (LLM)** securely and efficiently, integrating seamlessly with leading platforms like **Ollama and Hugging Face**.

With Cube AI, you can protect sensitive user prompts and data by leveraging Trusted Execution Environments (TEEs). This ensures that your AI applications not only perform optimally but also uphold the highest standards of confidentiality and security.

Whether you're working with pre-trained models or fine-tuning your own, Cube AI simplifies the deployment process, enabling secure, scalable, and compliant AI solutions for diverse applications.

How Cube AI Works



STEP 1: **User sends a prompt or query to the LLM** through an encrypted channel, ensuring the confidentiality of the request during transmission

STEP 2: **Cube Proxy authorizes the request** enforcing proper authorization and governance before forwarding it to the LLM

STEP 3: **The LLM processes the request securely within a Trusted Execution Environment (TEE)** and the result of the inference is returned to the client through the encrypted channel

Cube AI Use-cases

Healthcare

Process sensitive patient records securely and generate valuable insights for diagnostics and research without exposing private data. Cube AI ensures compliance with stringent healthcare privacy regulations.

Finance

Analyze confidential financial transactions, detect fraud, and produce secure financial reports with Cube AI's robust protections for sensitive data and computational integrity.

Customer Support

Deploy intelligent chatbots capable of handling sensitive user queries, providing personalized and private support, backed by Cube AI's secure data processing capabilities.

Enterprise AI

Build proprietary AI tools and workflows with confidence. Cube AI ensures the security of both proprietary models and sensitive enterprise data during AI development and deployment.

Cube AI Features

Secure Data: TEEs protect data and models during execution.

Remote attestation mechanism

Fine-grained access control (multi tenant, policies, ABAC/RBAC)

Model Agnosticism: Works with open-source and proprietary LLMs.

End-to-end encrypted traffic

Scalable: Handles large, high-performance AI workloads.

Easy Integration: APIs for seamless deployment.

Open-source, Apache-2.0 license

How Cube AI Is Developed

Ultraviolet, company behind Cube AI, is an active member of the Linux Foundation and the Confidential Computing Consortium

Cube AI is researched in 3 large-scale EU research projects funded by European Commission:

- CONFIDENTIAL6G -project that develops cryptographic quantum-resistant protocols and security proofs tools, libraries, mechanism and architectural blueprints for confidentiality in 6G
- TITAN EOSC - a software platform solution for confidential data collaboration & secure and privacy-preserving data processing
- ELASTIC - project that pioneers next-gen network orchestration, harnessing WebAssembly and Confidential Computing to ensure efficient, secure service delivery across 6G infrastructures

ULTRAVIOLET

Website: https://ultraviolet.rs

E-mail: info@ultraviolet.rs

Contact person: Drasko Draskovic, CEO (drasko@ultraviolet.rs)