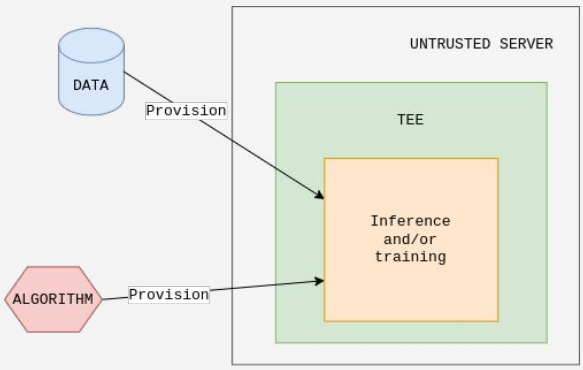
Prism AI

by Ultraviolet

Platform for Confidential Computing and Secure Collaborative AI

Your AI is Now Protected!



Confidential Computing

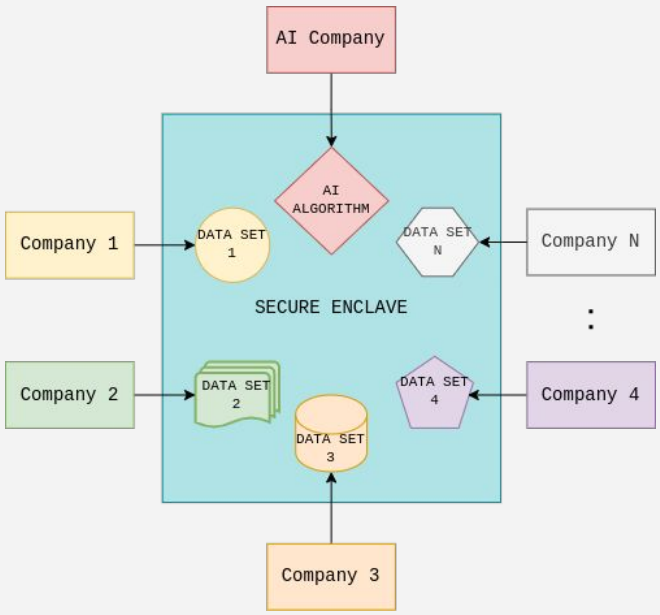
Confidential Computing and TEEs (Trusted Execution Environments) ensure data privacy and integrity by processing sensitive information in isolated and secure environments.

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

Prism AI Platform

Prism AI utilizes Confidential Computing and TEEs for secure execution of algorithms on combined datasets from multiple parties.

Data is protected by TEEs from everyone, including host and service providers, ensuring that participants cannot see each other's data; only the Result Recipient receives the processed results, with data never leaving the secure enclave and remaining invisible to participants throughout the computation.

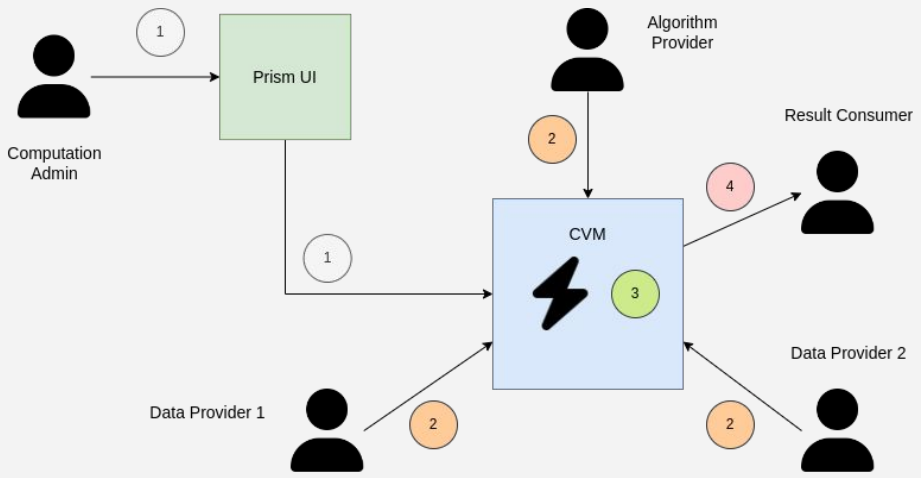


Intuitive and Easy to Use

Prism AI excels in user-friendliness with an **intuitive UI** that simplifies navigation and operation. It offers effortless **Confidential VM (CVM) provisioning** and deployment, complemented by streamlined tools for seamless integration into existing workflows.

The platform also supports easy and secure user management, **collaborative workspaces**, and straightforward **computation definitions** and sharing, making complex tasks accessible and manageable.

How Prism AI Works



STEP 1: **User creates the Computation** and defines Computation characteristics and participants (Program Providers, Data Providers and Result Consumers). When Computation is started, secure VM (TEE) will be dynamically provisioned and prepared for use (hardware and runtime enablement)

STEP 2: **Program and Data Providers upload programs and datasets** into the enclave using CLI over secure connection, after attesting the validity of the enclave using remote attestation mechanism

STEP 3: **Program is executed over combined dataset** (following the instructions in the Computation manifest). This execution is coordinated by an in-enclave Agent, once all artifacts defined in Computation manifest are received inside the enclave via secure connection.

STEP 4: **Result is sent to the Result Consumer user** (defined in the Computation manifest) after the algorithm completed the execution inside the enclave

Prism AI Use-cases

Healthcare

Healthcare, a sector with highly sensitive data, can be revolutionized by AI on combined datasets. Prism AI is used in large-scale EU project TITAN, where medical partners Inserm France, Charité Berlin hospital and UEF are exchanging confidential AI algorithms and data for pediatric care.

Finance

Confidential Computing secures sensitive financial data by processing it in protected enclaves, preventing unauthorized access. This enables financial institutions to use advanced analytics and AI on encrypted data, enhancing fraud detection, risk management, and customer insights while ensuring regulatory compliance.

Industry

Confidential Computing secures sensitive industrial data by processing it in protected enclaves, preventing unauthorized access. This enables companies to use advanced analytics and AI on encrypted data, optimizing production, enhancing predictive maintenance, and improving supply chain management while ensuring data integrity and compliance.

Government

Confidential Computing secures sensitive government data by processing it in protected enclaves, preventing unauthorized access. This allows agencies to use advanced analytics and AI on encrypted data, enhancing decision-making, improving public services, and ensuring data privacy and compliance.

Prism AI Features

- Computation definition and management
- Remote attestation mechanism
- Fine-grained access control (multi tenant, policies, ABAC/RBAC)
- Intuitive user interface
- Secure VM provisioning, managing and monitoring
- End-to-end encrypted traffic
- Hardware abstraction layer and runtime inside the secure enclaves for workload execution
- Pluggable computation backends
- In-enclave Agent - execution scheduler and coordinator
- Multiple workload runtime support (Python, Docker, Wasm, binary, …)
- Cloud-native deployment
- CLI & SDK
- Small memory footprint and fast execution
- Open-source Core (Cocos AI)

How Prism AI Is Developed

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

Prism 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)