BeeKeeperAI®

EscrowAI v1.5.1 System Capabilities

Overview

EscrowAI is a patented zero-trust, confidential computing platform for secure collaboration between algorithm developers and stewards of protected data. With EscrowAI, data remains within the data steward's secure environment and is made available for computation in a hardware-based Trusted Execution Environment (TEE) instance.

EscrowAI is protected by U.S. Patents 11,531,904 and 11,748,633.

Security

EscrowAI has the following important security features:

- **Data Stewards retain control of their data.** The Data Stewards' organizations retain full control of the data. With EscrowAI, data stays in the Data Steward's organizations' infrastructure.
- **Strong encryption protects data at rest, in transit, and in use.**
  Data is encrypted with AES-256-based ciphers and all network connections use TLS.
- **Data is protected in use.**
  Data and algorithms achieve high-isolation and memory encryption through hardware-based assurances. Secure attestation ensures the authenticity and integrity of the TEE execution environments.
- **Algorithm intellectual property is protected.**
  Algorithm owners retain protection of their intellectual property. Algorithm owners themselves encrypt their models, which are decrypted only in a TEE instance.

Confidential Computing Technology

EscrowAI offers the following types of confidential computing technologies. These technologies underlie the virtual machines (VMs) and other secure resources in the TEE instance that EscrowAI manages for you.

Confidential Containers in an Intel Software Guard Extensions (SGX) Enclave

EscrowAI offers Microsoft Azure's confidential containers that are based on Intel® Software Guard Extensions (Intel® SGX). SGX is a set of security-related instruction codes built into some Intel Central Processing Units (CPUs). On a hardware-based Trusted Execution Environment (TEE) instance, application code runs in private regions of memory, called *enclaves*, which are protected from all other processes running at higher privilege levels.

VM-isolated Confidential Containers on Azure Container Instances (CC ACI)

Confidential containers on Azure Container Instances are deployed in a container group with a Hyper-Visor isolated TEE, which includes a memory encryption key that is generated and managed by an AMD SEV-SNP capable processor. Data in use in memory is encrypted with this key to help provide protection against data replay, corruption, remapping, and aliasing-based attacks.

Included Functionality

Workflow
Organization Homepage with role-based Project listing.
Project collaboration workspaces.
Chat and notification within Projects.
Choice of Trusted Execution Environment, by Project.
Configurable workloads.
Algorithm containerization and build for TEE execution.
Encryption utility (local) for key generation, key wrapping, and data / algorithm encryption (AES256)
Push-button initiation of the workload in the TEE.
Automatic TEE decommissioning.
Within Development Plan communications.
Inference / Analytics standardized reporting.
Report content checking and enforcement policies.
Immutable version and transaction recording in Azure Confidential Ledger
Artifact preservation.
Run logging, monitoring, and error messaging.
Zero-trust & Security
Identity and access management: organization and role-based access
Single Sign On integration
All workloads process in Trusted Execution Environments
Attestation of Trusted Computing Base
End-to-end encryption for algorithm and data, including in process.
FIPS 140-2 HSM Key Manager (third party managed)
Memory isolation
Third-party application security testing

Customer Support
Onboarding service
Online Help Center 24/7
Online Issue reporting and tracking 24/7
Customer Service Response 8/5 (PT)
