

Untrusted machine

Distributed Application

app.py

Calculation
parameters

Calculation
result

SGX Enclave

trusted.py

Decrypt

Encrypted model

Gramine LibOS

Remote attestation

Decryption key

Intel® SGX Attestation Service
(external)

Verify remote
attestation

Trusted Machine

Key server