C4 Architecture
Confidential Computing with Machine Learning using Intel SGX

C1 Diagram

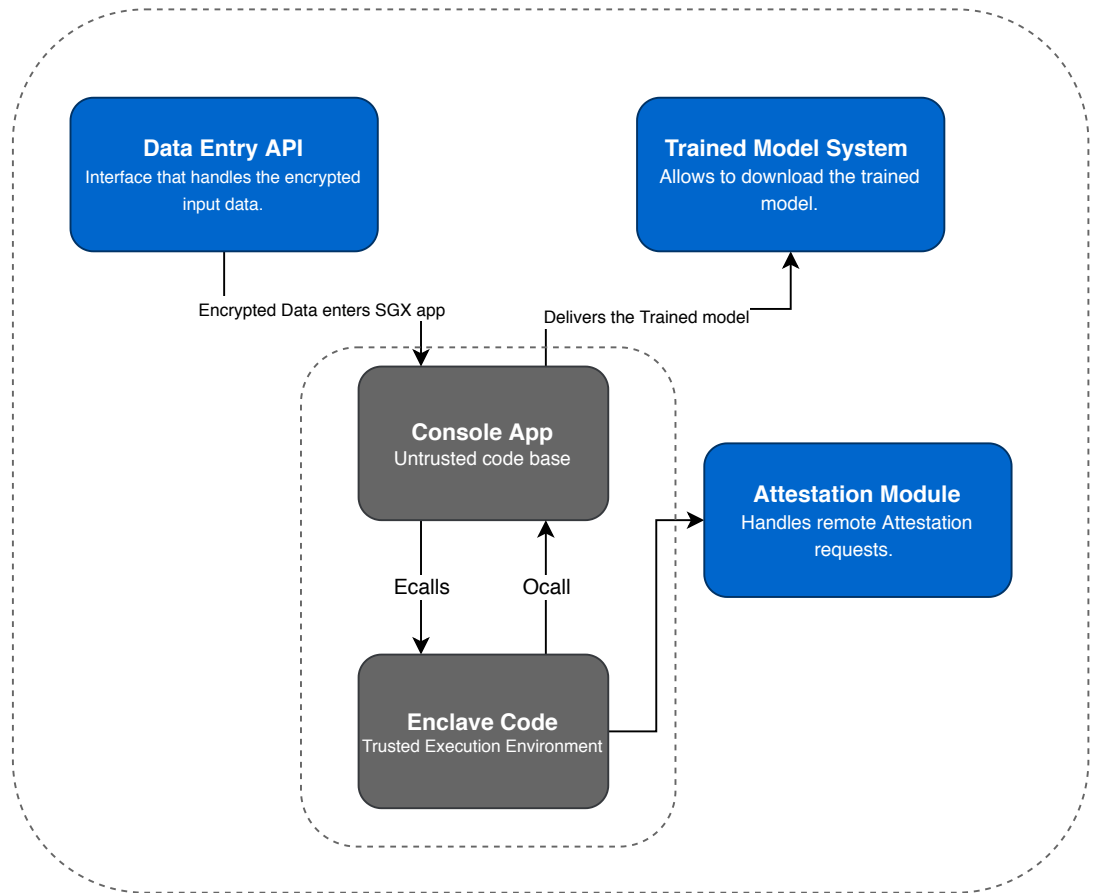**Data-set 1** . . . . **Data-set N**

Different Data Sources

Sends Data set
to be encrypted
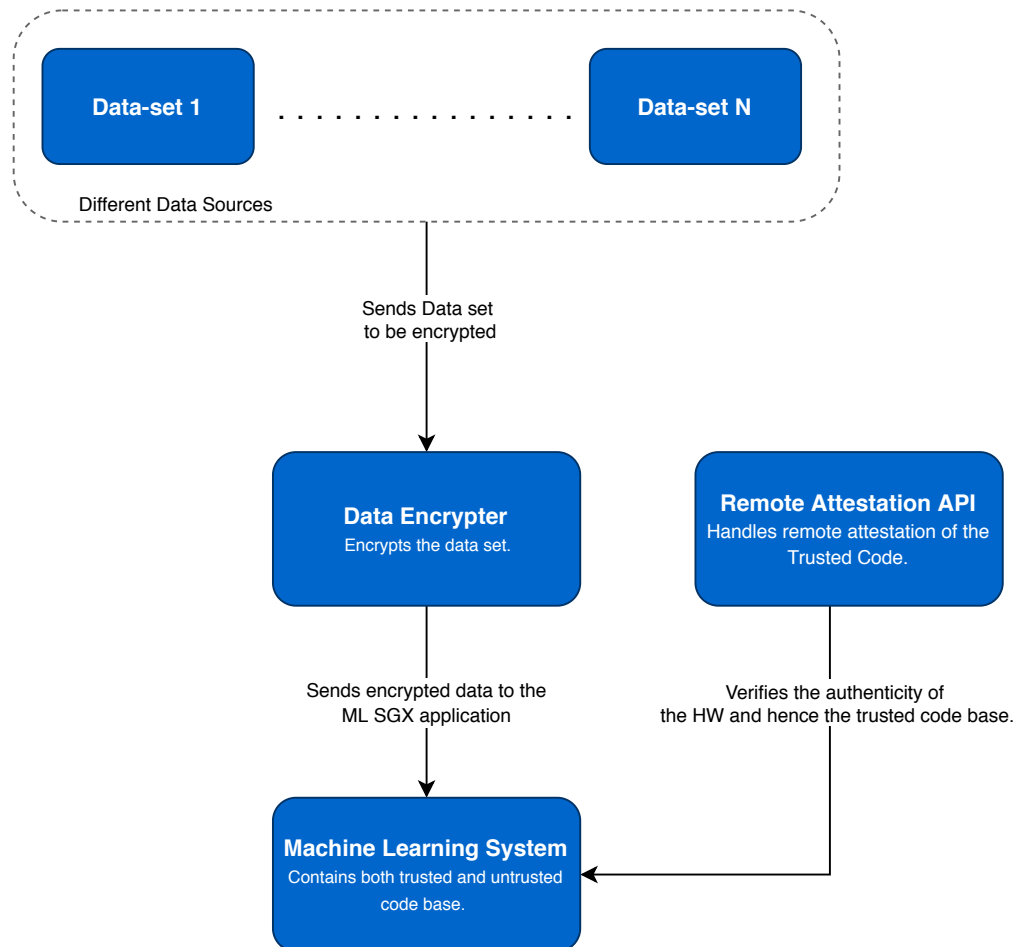
Components

1. Data sets
2. Encryption Module
3. Console App
4. Enclave code.
5. Remote Attestation

Data Encrypter
Encrypts the data set.

Remote Attestation API
Handles remote attestation of the
Trusted Code.

Sends encrypted data to the
ML SGX application

Verifies the authenticity of
the HW and hence the trusted code base.

Machine Learning System
Contains both trusted and untrusted
code base.

C2 - Machine Learning System

Components

1. Data Entry API
2. Trained Model System.
3. Console Application.
4. Attestation Module
5. Enclave Code

Data Entry API
Interface that handles the encrypted input data.

Trained Model System
Allows to download the trained model.

Encrypted Data enters SGX app

Delivers the Trained model

Console App
Untrusted code base

Attestation Module
Handles remote Attestation requests.

Ecalls

Ocall

Enclave Code
Trusted Execution Environment
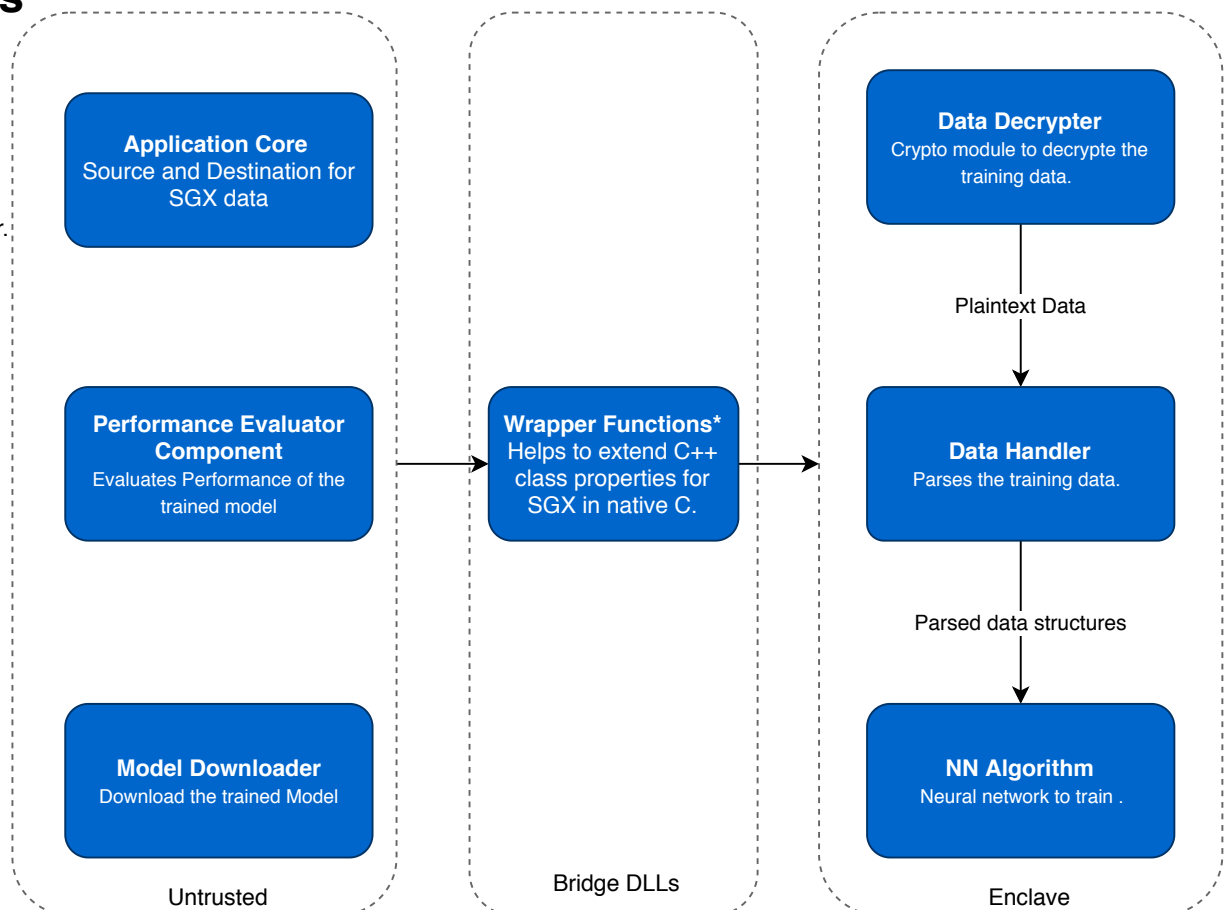

C3 - Enclave and Console Application
(Neural Network)

Components

Enclave Code
1. Data Decypter.
2. Data Handler.
3. ML Algorithm

Console Application
1. Performance Evaluator.

Application Core
Source and Destination for SGX data

Data Decrypter
Crypto module to decrypt the training data.

Plaintext Data

Performance Evaluator Component
Evaluates Performance of the trained model

Wrapper Functions*
Helps to extend C++ class properties for SGX in native C.

Data Handler
Parses the training data.

Parsed data structures

Model Downloader
Download the trained Model

NN Algorithm
Neural network to train .

Untrusted

Bridge DLLs

Enclave

* Most of the ECalls are made using wrapper functions.

Class Diagram
(Neural Network)