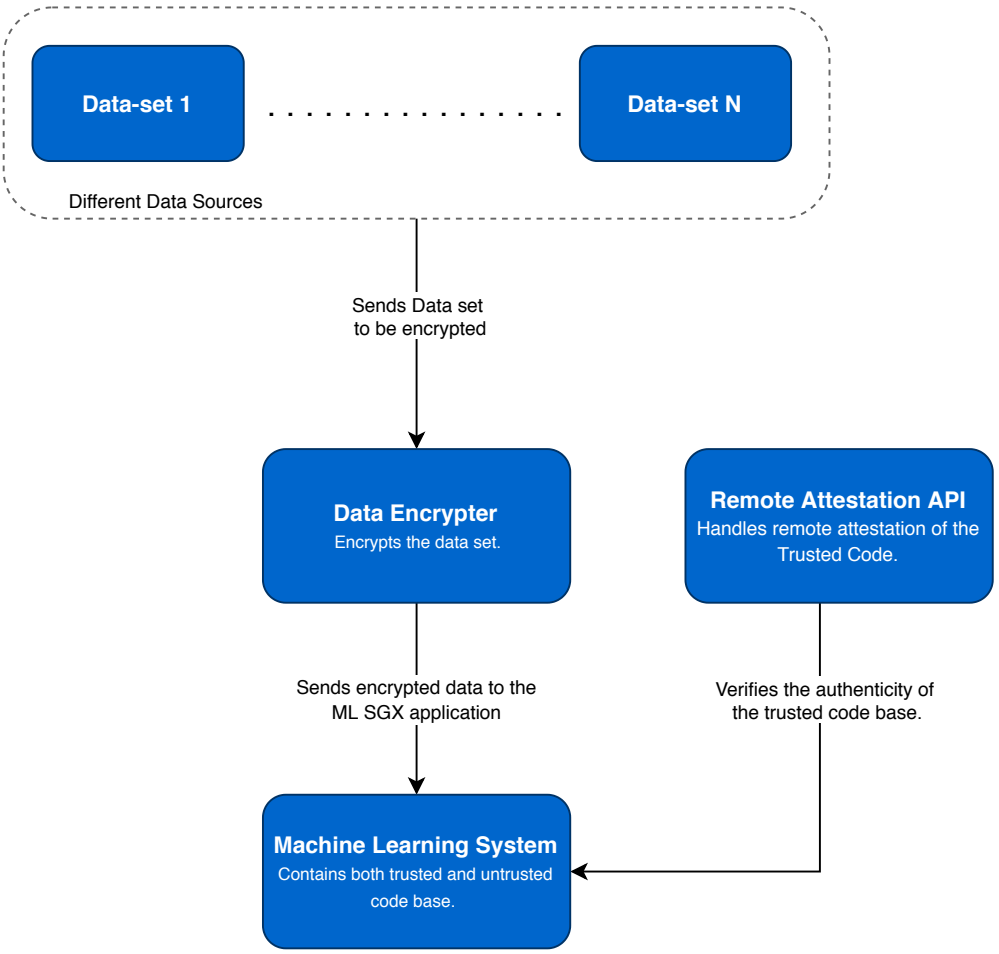
C4 Architecture
Confidential Computing with Machine Learning using Intel SGX

C1 Diagram



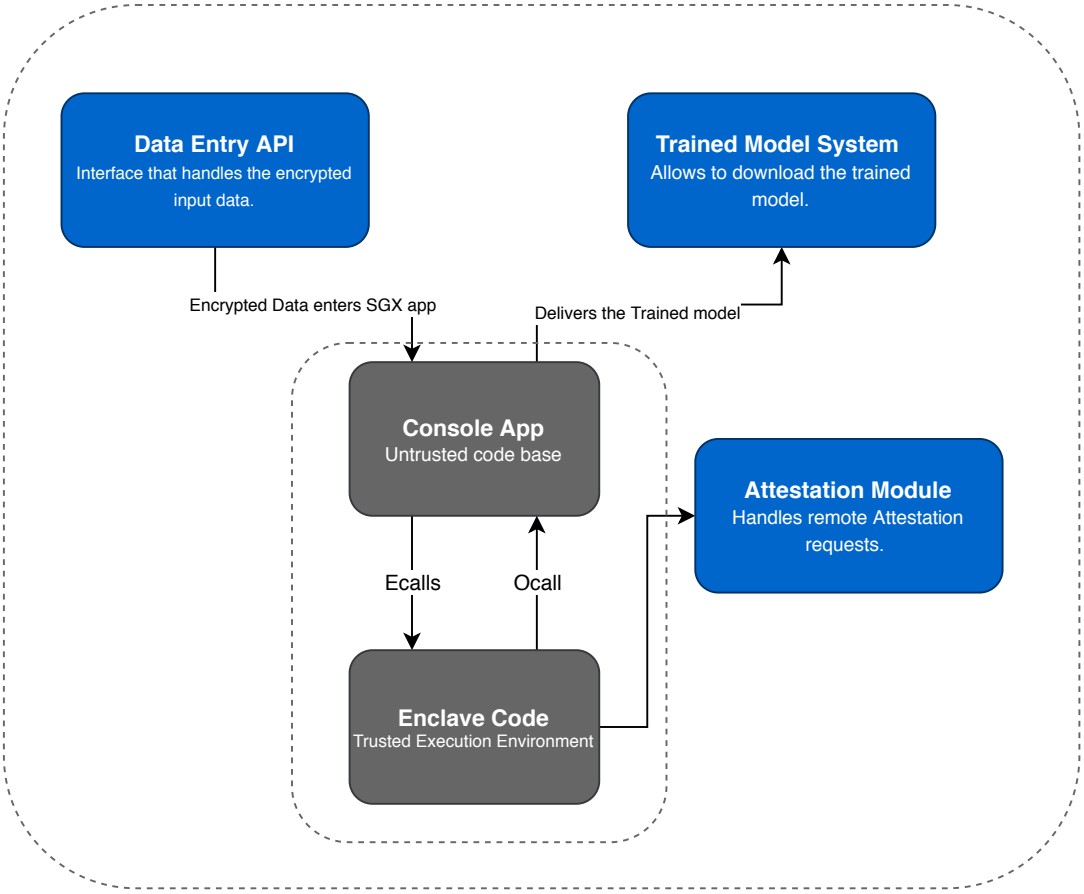
Components

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

C2 - Machine Learning System

Components

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



C3 - Enclave and Console Application

(KNN)

Components

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

Console Application
1. Performance Evaluator.