TODO

NEXT

DONE

Confidential Computing with Ma

Feb

Get introduced to enclave programming and system design.

Further Research on TPM enclaves.

Decide on technology stack and setup environnent.

C1 Diagram

Install Intel SGX SDK with Visual Studio

Test Sample Enclave code.

What modules are inside the enclave?

C2 Diagram
Platform backend

Mar

1. Deeper system design and point out the individual components .

2. init Documentation

MSC - What NN Modules in enclave?

ML - Implement NN

UI - UI Design of Encrypter and Main App

April

Implementation

1. Encrypter -CRY
2. Main App
3. NN Code Base tasks - NN
4. SGX Code Base - SGX
5. Documentation - MSC

Week -1

CRY - C++ file encryption CLI Module

CRY -Windows App Development Intro

CRY - C2 Diagram
Encryption Module

1. SGX Coding
2. Main App

achine Learning using Intel SGX

Dev Modules

Design, Docs and Misc. - MSC

- C1 Diagram
- C2 Diagram Platform backend
- C2 Diagram Encryption Module
- C3 Diagram
- Select Thesis Topic
- Decide on ML algorithm.
- Dataset streaming model?
- Install Intel SGX SDK with Visual Studio
- Decide on technology stack and setup environnent.
- What modules are inside the enclave?
- Test Sample Enclave code.
- Thesis Structure.

Machine Learning module -ML

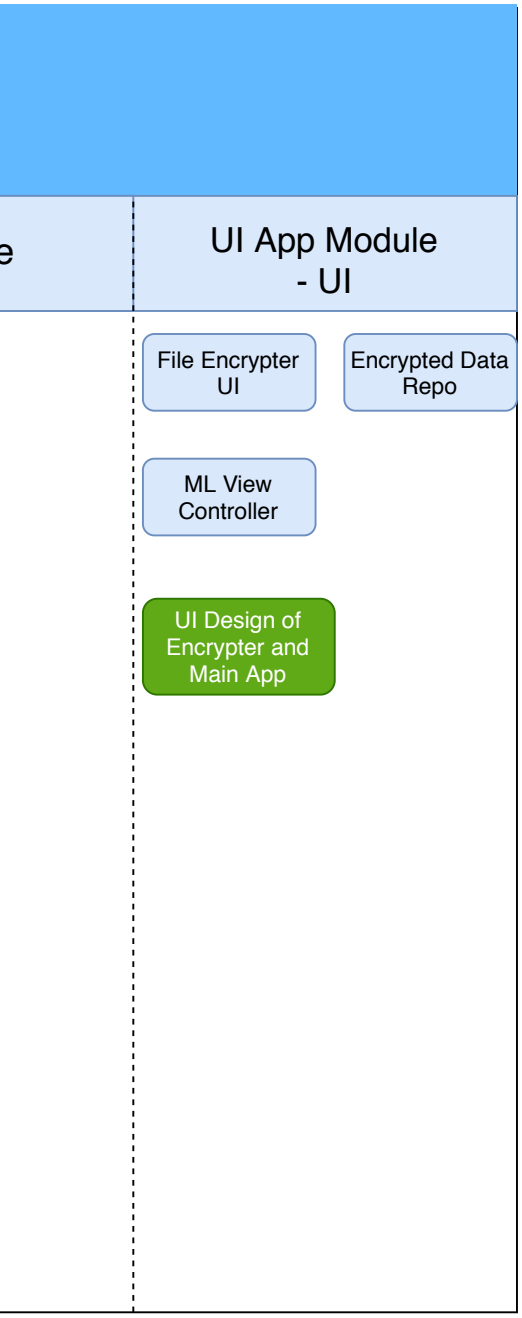
- KNN
- Distance Calculator
- Implement NN
- Identify the bridge Functions
- Init new Test dataset.
- Refine NN code into proper directories
- Split Train Data into multiple files.

Encrypt/Decrypt - CRY

- Decide on file encyption.
- C++ file CLI encryption Module
- C++ file CLI Decryption Module
- Windows App Development Intro
- Integrate Encryption CLI to main App

SGX Module - SGX

- NN as SGX APP design



Tech Stack

IDE : Visual Studio 2017 Enterprise

UI Design: Adobe XD

Encryption App :

- Encryption : 128 bit AES-GCM
- KDF: based on SHA-256
- Win32/C++ Application

Work Day Structure

- Update Kanban Board.
- Review TODOs
- Work on Tasks.
- Review/modify next day's tasks.