Preliminary Implementation Study Plan

Version: 1.0

Prepared by:

Sienna Gaita-Monjaraz

Tania Alam

Carlo Leiva

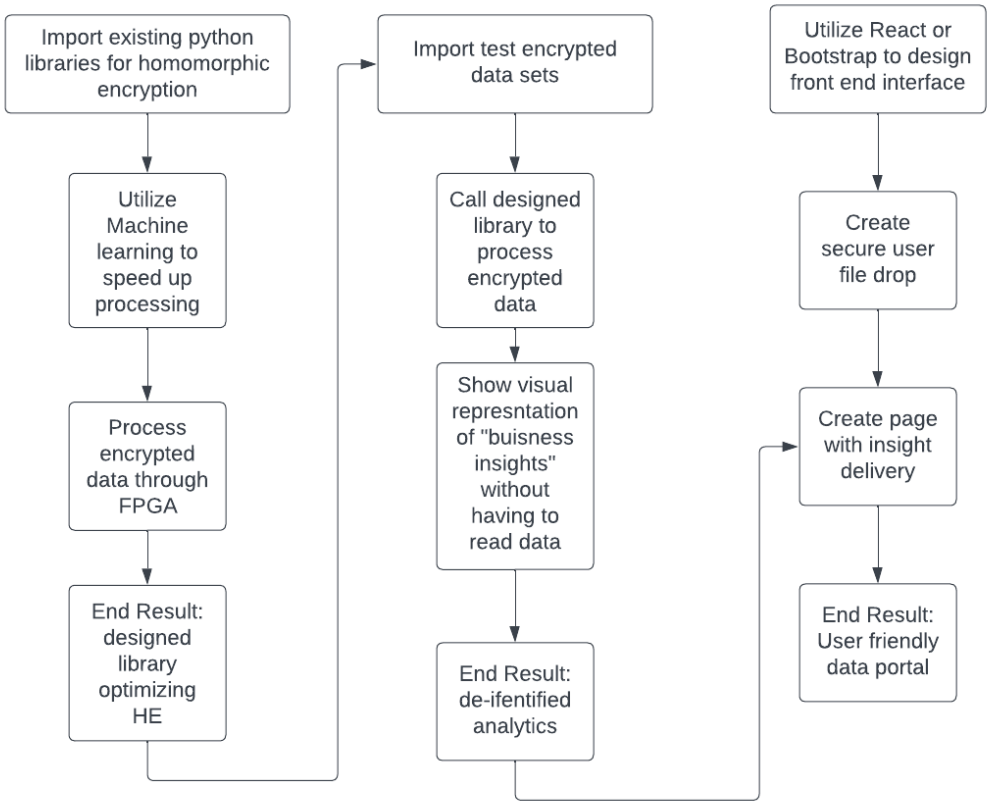
Aleysha Sierra Santiago

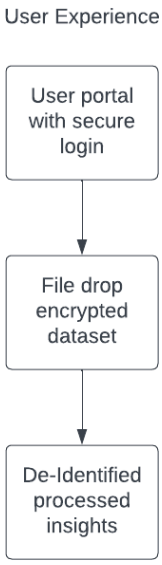
Dien Tran

Florida Atlantic University

November 9th, 2023

Flow of project creation





Aleysha Sierra Santiago: FPGA implementation

My role for this is hardware implementation, I chose the nexys A7 FPGA over using a GPU because they are highly customizable and can be programmed at the hardware level to implement specific algorithms. I am planning to use VHDL to tell the FPGA about its role and purpose, then I will integrate it with the python library. This component is being used as the driver for the hardware acceleration.

Carlo and Dien

Carlo and Dien would be implementing the front end using either react/JS or Angular/TS. We would be connecting the Homomorphic and Textual libraries to the front end. We hope to create a nice and well-thought-out front end that will allow for users to have a nice and easy experience.

Carlo will be implementing symmetrical encryption, Public Key Infrastructure (PKI) and the Secure Multiparty Computation (SMPC) on textual data. In this cryptographic approach, a secret key is generated using a secure algorithm, and this key is then exchanged securely between the communicating parties. This will be done using a library called “cryptography. Fernet” to streamline this process. We will implement this in our textual data library which will be worked on by both Carlo and Dien.

Tania

My primary responsibility for this project is in the software aspect and leveraging machine learning algorithms to conduct data analysis on the data. I will then present the insights through user-friendly visuals such as graphs, while ensuring that the sensitive data remains encrypted and hidden from the

user's view. This relates to the overall project as I will be using the library overlooked by Sienna and the visualization will be shown in the front-end, implemented by Carlo and Dien.

Sienna

In leading the homomorphic encryption project, my technical roles and responsibilities encompass managing the GitHub repository, ensuring that our codebase is well-organized and our version control practices are robust. I will oversee establishing the Python library's structure, laying the groundwork for creating modular and reusable code. My key task is to develop Python functions that integrate with existing libraries like MicrosoftSEAL, employing machine learning to enhance their efficiency. A significant portion of my role involves innovating methods to accelerate the processing of encrypted data. This requires me to delve deep into machine learning techniques, aiming to optimize the performance of homomorphic encryption operations. This will be crucial to the FGPA acceleration and will provide Tania with the data to then run machine learning data analysis on the data to show useful analytics and visualizations without compromising data integrity and security.