National College of Ireland

Configuration Manual

MSc Research Project
Cloud Computing

Sunandan Sekhar Das
Student ID: 23135417

School of Computing
National College of Ireland

Supervisor: Yasantha Samarawickrama

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sunandan Sekhar Das
Student ID:	23135417
Programme:	MSc in Cloud Computing **Year:** 2023-2024
Module:	MSc Cloud Research Project
Lecturer:	Yasantha Samarawickrama
Submission Due Date:	12-08-2024
Project Title:	Enhancing Cloud Data Security: Integrating Zero-Knowledge Proofs with Lightweight Homomorphic Encryption for Efficient Deduplication
Word Count:	**976 Page Count: 6**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sunandan Sekhar Das

Date: 12-08-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Sunandan Sekhar Das
23135417

1 Requirements

In this research several software tools were used to develop the TFHE framework. The framework was first tested on windows machine, and then deployed on a cloud environment. Let's go through the installation guide to run our framework.

1. Download and install Visual Studio Code and open Visual Studio code the user interface would look like this

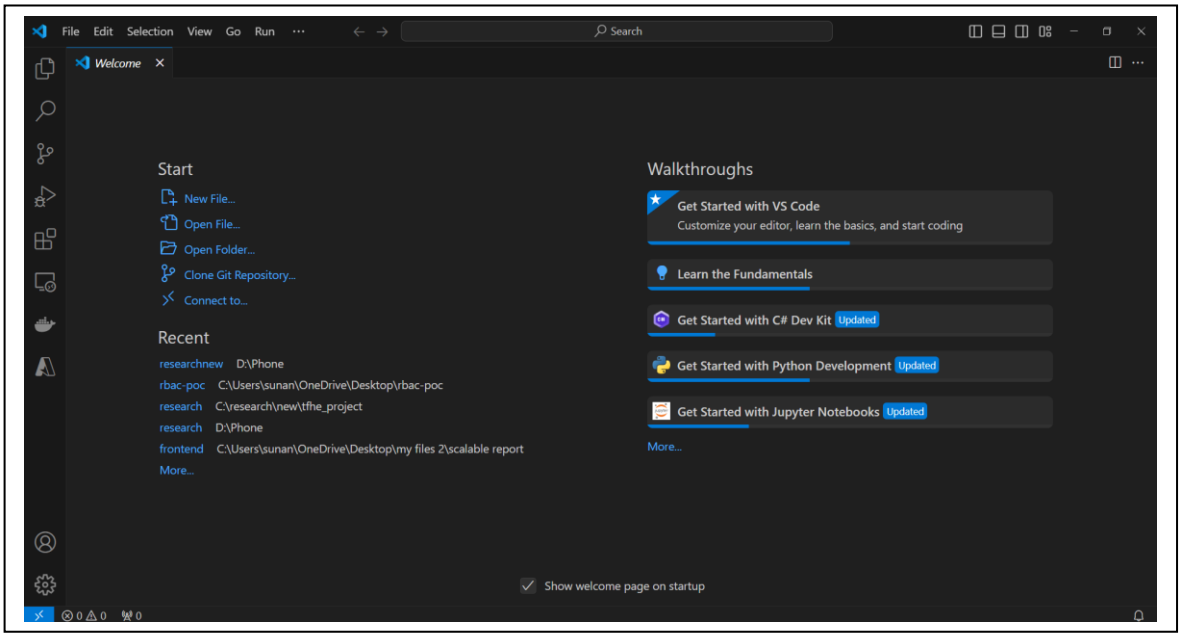

Figure 1: Visual Studio Code

2. Install GIT on the system. Below is the installation guideline to GIT https://github.com/git-guides/install-git

3. **Download and install Python on system:**

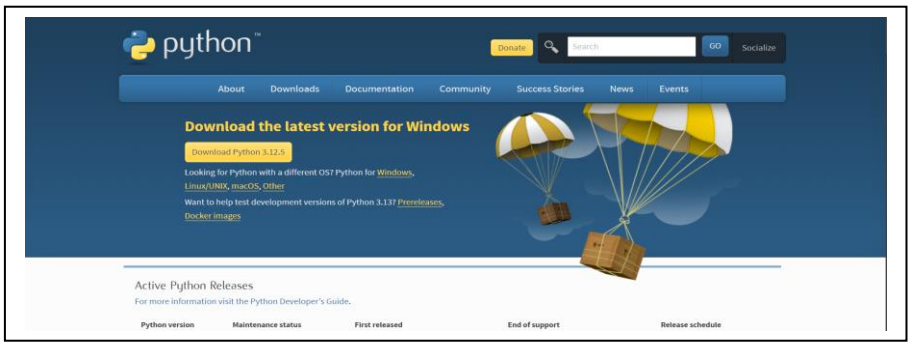

Figure 2: python download

- Visit the Python official website.
- Download the latest version of Python 3.9
- Run the installer.
- During installation, make sure to check the box that says, "Add Python to PATH."

4. **Building the SEAL Library:**

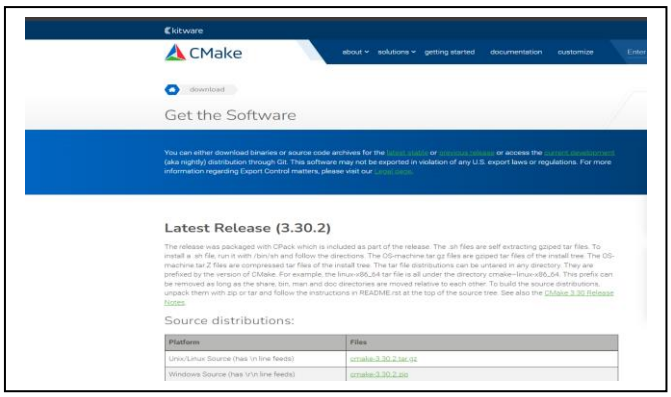

Figure 3: Cmake

- Download CMake Visit the CMake official website and download the installer for windows. Run the installer and follow the instructions and add the system PATH during installation.

5. **Download and Visual Studio:** Visit the **Visual Studio official website.** Download the installer for Visual Studio 2019 or newer. During installation, select the "Desktop development with C++" workload.

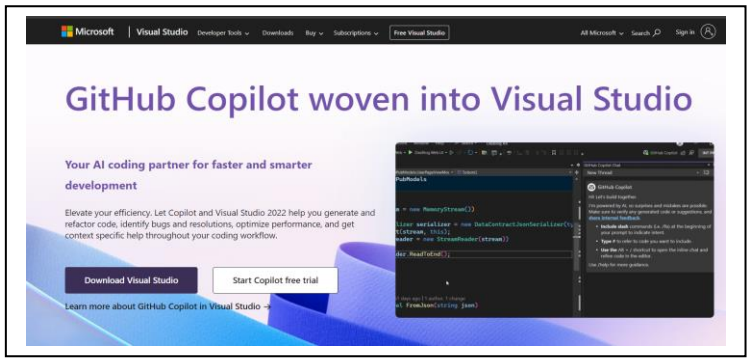

Figure 4: Visual Studio

2 Setting Up the Development Environment

1. Clone the repository in the terminal. Open VS Code open terminal in the terminal run this commands:
   - Git clone https://github.com/flonix-93/TFHE-ZKP-Deduplication-framework.git
   - cd TFHE-ZKP-Deduplication-framework

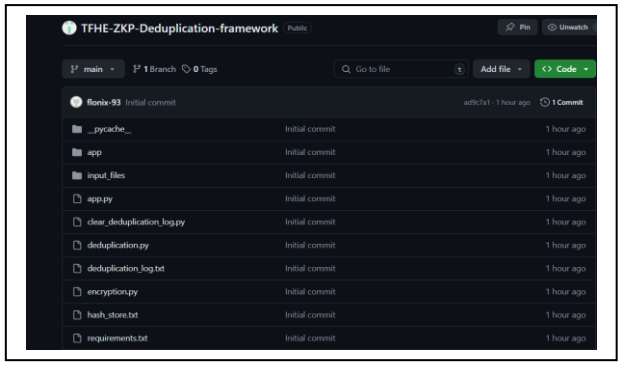

Figure 5: Git Repository

2. Initialize the submodules: git submodule update --init –recursive
3. pip install -r requirements.txt
4. **Build SEAL Library:**

   - cd SEAL
   - cmake -S . -B build -G "Visual Studio 16 2019" -A x64 -DSEAL_USE_MSGSL=OFF -DSEAL_USE_ZLIB=OFF -DSEAL_USE_ZSTD=OFF
   - cd..

5. **Build the Python Bindings:**
   - python setup.py build_ext -i

6. Run the framework:
   python app.py
   go to http://127.0.0.1:5000/ to interact with the web interface.

3 Setting up Cloud Environment

1. **Log in to AWS Console:**
   - Open the AWS Management Console and log in to your account.
2. **Launch an EC2 Instance:**
   - Navigate to **EC2 Dashboard** under the "Compute" section.
   - Click on **Launch Instance**.
3. **Choose an Amazon Machine Image (AMI):**
   Select a Linux-based AMI. For a general Linux distribution, you might choose something like Amazon Linux 2
4. **Choose Instance Type:**
   Select **t2.xlarge** as your instance type (4 vCPUs, 16GB RAM). This instance type provides sufficient resources for most compute-intensive tasks.
5. **Add Storage:**
   Select the default storage size 8 GB.

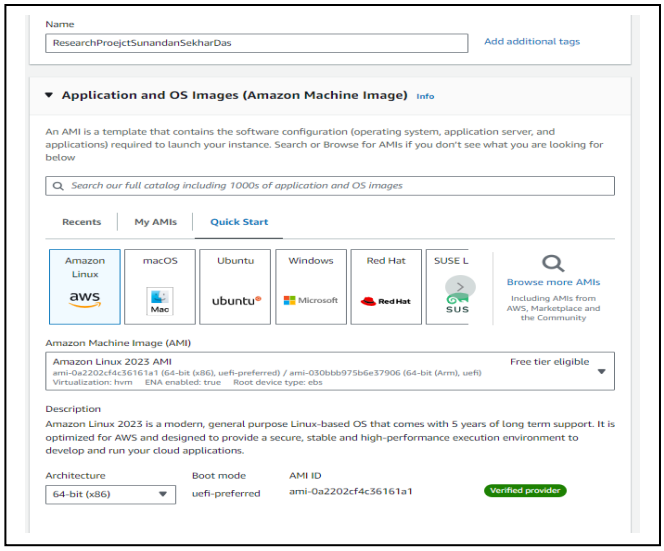

Figure 5: EC2 Setup

6. **Configure Security Group:**
   - Create a new security group or select an existing one.
   - Add rules to allow **SSH (port 22)** for remote access.
   - Add rules for **HTTP (port 80)** and **HTTPS (port 443)**
7. **Review and Launch:**
   - Review and launch the instance and download the keypair (.pem file)
8. SSH into the EC2 Instance

   Navigate to the directory where your key pair (.pem file) is located.
   chmod 400 your-key-pair.pem
   ssh -i "your-key-pair.pem" ec2-user@your-

4 Set Up the Environment

1. **Update the Package List:** sudo yum update -y

2. **Install Required Packages:** sudo yum install -y gcc gcc-c++ make cmake python3 python3-pip git

3. **Clone Your GitHub Repository:**

   - git clone https://github.com/flonix-93/TFHE-ZKP-Deduplication-framework.git

   - cd TFHE-ZKP-Deduplication-framework

4. **Install Python Dependencies**
   - pip3 install -r requirements.txt

5. Install SEAL Library:

- **Initialize submodules:** git submodule update --init –recursive
- **Build SEAL library:**
  cd SEAL
  cmake -S . -B build -DSEAL_USE_MSGSL=OFF -DSEAL_USE_ZLIB=OFF -DSEAL_USE_ZSTD=OFF
cmake --build build
  cd ..
- **Compile and Build the Project:**
  python3 setup.py build_ext -i
- **Run the Application**
  Start the Application: python3 app.py
  http://54.195.230.23:5000/

5 Web Interface: Step-by-Step Guide

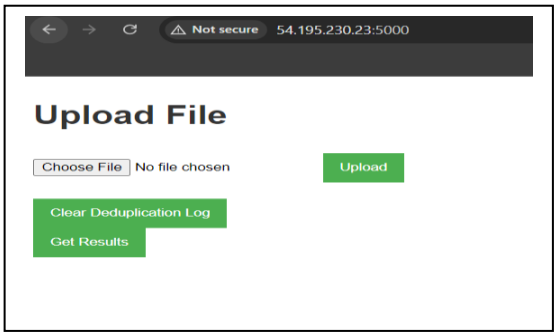

Figure 6: Web Interface

1. **Upload a File:**
   - Click the **"Choose File"** button to open the file selection dialog.
   - Navigate to the file you wish to upload and select it.
   - Once the file is selected, click the **"Upload"** button.
   - The system will process the file and pass it to the deduplication module to check for duplicacy in the file content.
2. Clear Deduplication Log
   Clear Log:
   If you want to delete the information in the deduplication log [for instance, to restart the process and have all the files processed as fresh], you can click on the ‘Clear Deduplication Log’ button. This will delete all the old file hashes from the logs so the system

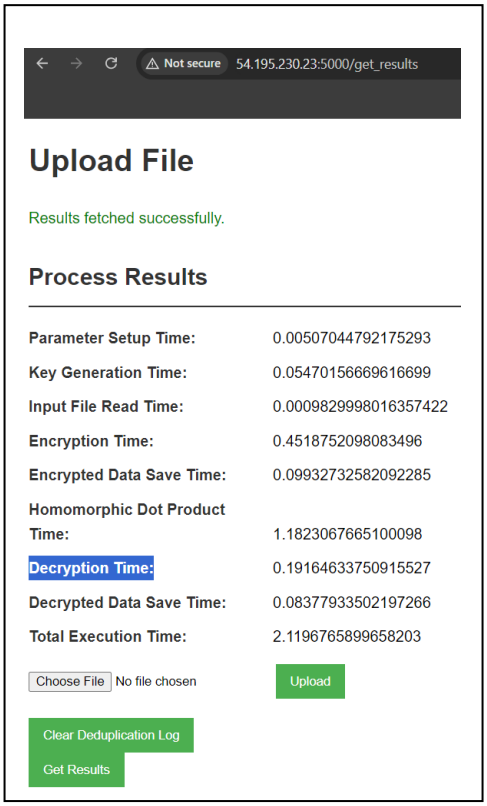

Figure 7: Result page

3. Get Results
    - After the file has been processed, you can click the **"Get Results"** button.
    - This will display the results of the encryption, and homomorphic computations for that file.
    - The results will contain information like Parameter Setup Time, Key Generation Time, Encryption Time, Decryption Time, etc.