

# **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		
Date:	12-08-2024		
Project Title:	Enhancing Cloud Data Security: Integrating Proofs with Lightweight Homomorphic Encry Deduplication	Zero-K /ption fo	nowledge or Efficient

#### 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

12-08-2024 Date:

#### 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:

e python	Donate Strarch GO so	
Download the latest version for Wind	ows	
Download Python 3.12.5		
Looking for Python with a different OS7 Python for <u>Windows</u> ,		
Want to help test development versions of Python 3.137 Prereleases		
Active Puthon Releases		
For more information with the Dathers Development's Colde		

#### Figure 2: python download

- Visit the <u>Python official website</u>.
- 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:

€kitware	
A CMake about ~ solutions ~ getting started documentation custor	mize
oliveritadi	
Get the Software	
You can after download brains or source code anthres for the lister statistic or access below or access the surres on (also right) distribution through 01. The software may not be exported in violation of any U.S. export laws or regulations information regarding Doort Control matters, please visit our surgification.	selatione For more
Latest Release (3.30.2)	
	22.22
The refease was packaged with CRbsk which is included as part of the release. The an infer surveil entropy paper to the input as infer out is which which is included as part of the release. The survey is the survey of the survey package to the survey of the s	e The OS y are prefix can utions. 10 Release
The release was packaged web CRack which is included as part of the release. The an infer surveil entrance of papers of it invalid as infer out with which in an influence releases. The Contractions of galaxies argued the TRe of the release of the matrice back TRe are compressed to the final of the invalid test. The Contractions of galaxies argued the infer of the release of matrice back TRe are compressed to the final of the invalid test. The Contractions are back and it is any place of matrice back TRe are compressed to the final of the invalid test. The last final infer back and the interplace of the removal test from part where its minimar and decretions are more one theory test with the interplace of any part here with apport ter and follow the instructions in README.test at the top of the source tree. See also the <u>Chalare 31</u> Bost Contractions and the source tree. See also the <u>Chalare 31</u> Bost Contractions and the source tree. See also the <u>Chalare 31</u>	e The OS y are prefix can utiona, 30 Release
There relates an advanced with CRAde. For example, and include as a part of the instance. The an information of examples of the instance of th	er The OS y are prefix can utiona, 30 fielesse
The release was packaged with CRisk which is included a part of the release. The all first are self encoded paper for fit media at a fit fit, not is used to fit where an additional of the part of the release the set of the an additional fit of the release the set of the an additional fit of the release the set of the an additional fit of the release the set of the and the part of the additional fit of the release the set of the set of the set of the set of the release the set of the set of the release the set of	er The OS y ane prefix can utions, 35 fielesse

Figure 3: Cmake

- Download CMake Visit the CMake official website and <u>download</u> 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 <u>Visual Studio official website</u>. Download the installer for Visual Studio 2019 or newer. During installation, select the "Desktop development with C++" workload.

GitHub C	opilot wove	en into Visua	Studio
onthind o	opnot nore	in mice though	braano
			Nat
		ALLE FOR THE REPORT OF A DECK	. Quinton o P
Your AI coding partner for	faster and smarter	A photosis as functioned as a 1 million of 1	Introd Logic fiel     Non Month
development		PubModels	Gatha Castler
		and a second	nit tell field highlin.
Elevate your efficiency. Let Copilot an	d Visual Studio 2022 help you generate and	a * new NemeryStreem())	Make use to welly sty generated totic or suggestions, or does informal familiaria
	utions, optimize performance, and get	(izer serializer - new DataContractionsberializer(t) t(stream, this);	<ul> <li>Include shaft commands (i.e. /fil) at the beginning prior prompt to indicate intert</li> </ul>
refactor code, identify bugs and resol context specific help throughout you	<ul> <li>coding workflow.</li> </ul>		<ul> <li>Type # to order to code you sent to include-</li> </ul>
refactor code, identify bugs and resol context specific help throughout you	r coding workflow.	abber - see structerable(terval))	<ul> <li>Use the AS = 7 chortout to upon the inline child an</li> </ul>
refactor code, identify bugs and resol context specific help throughout you	r coding workflow.	der heaffotnd();	<ul> <li>Gase The AN + 2 shortburd for specified billion chief an reflex could to the editor.</li> <li>Use Pedge for every guidance.</li> </ul>
refactor code, identify bugs and resol context specific help throughout you Download Visual Studio	Start Copilot free trial	eader * see Servansaber(Servan)/	Our Be /A - / Environt to spen the inter-chat as     refers to be refersed.     Due /Net / Re reserve guidence.

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 <u>https://github.com/flonix-93/TFHE-ZKP-Deduplication-</u>
     <u>framework.git</u>
  - cd TFHE-ZKP-Deduplication-framework

TFHE-ZKP-Deduplication-framework	Public	🔊 Pin	⊙ Unwatch
12 main - 12 1 Branch 🛇 O Tags		Add file *	⇔ Code →
flonix-93 Initial commit			🕚 1 Commit
pycache_			1 hour ago
🖿 арр			1 hour ago
input_files			1 hour ago
🗅 арр.ру			1 hour ago
C clear_deduplication_log.py			1 hour ago
deduplication.py			1 hour ago
deduplication_log.txt			1 hour ago
encryption.py			1 hour ago
hash_store.bxt			1 hour ago
requirements.txt			1 hour ago

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 <u>http://127.0.0.1:5000/</u> 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.

ResearchProejctSunandanSekharDas					A	Add additional tags	
<ul> <li>Applicat</li> </ul>	ion and OS	Images (Ama	izon Machir	ne Image) I	nfo		
An AMI is a ter applications) n below	nplate that cont equired to launc	ains the softwar h your instance.	e configuration Search or Brow	(operating sys se for AMIs if y	tem, applicatio ou don't see w	on server, and that you are looking for	
Q Search ou	r full catalog in	cluding 1000s of	application and	l OS images			
Recents	My AMIs	Quick Start	_				
Amazon Linux aws	macOS	Ubuntu ubuntu®	Windows	Red Hat	SUSE L	Q Browse more AMIs Including AMIs from AWS, Marketplace and the Community	
Amazon Machi Amazon Linu ami-0a2202cf4 Virtualization: I	ne Image (AMI) x 2023 AMI c36161a1 (64-bit ivm ENA enable	(x86), uefi-preferre d: true Root devi	d) / ami-030bbb9 ce type: ebs	75b6e37906 (64-	bit (Arm), uefi)	Free tier eligible	
Jescription Amazon Linux optimized for develop and ru	2023 is a mode AWS and design in your cloud ap	rn, general purp ed to provide a s plications.	ose Linux-based ecure, stable ar	I OS that come nd high-perfor	s with 5 years mance executio	of long term support. It is on environment to	
Architecture	•	Boot mode uefi-preferred	AMI ID ami-0a2202	cf4c36161a1		Verified provider	

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-Deduplicationframework.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

$\leftarrow$ $\rightarrow$ C $\triangle$ Not secure 54.	195.230.23:5000
Upload File	
Choose File No file chosen	Upload
Clear Deduplication Log Get Results	

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

← → C ▲ Not secure 54	l.195.230.23:5000/get_results			
Upload File				
Results fetched successfully.				
Process Results				
Parameter Setup Time:	0.00507044792175293			
Key Generation Time:	0.05470156669616699			
Input File Read Time:	0.0009829998016357422			
Encryption Time:	0.4518752098083496			
Encrypted Data Save Time:	0.09932732582092285			
Homomorphic Dot Product				
Time:	1.1823067665100098			
Decryption Time:	0.19164633750915527			
Decrypted Data Save Time:	0.08377933502197266			
Total Execution Time:	2.1196765899658203			
Choose File No file chosen	Upload			
Clear Deduplication Log Get Results				

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.