National College of Ireland

Configuration Manual

MSc Research Project
MSc in cybersecurity

Shivkumar Patel
Student ID: 21116709

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……Shivkumar Patel……

Student ID: ……211167090……..……

Programme: MSc in cybersecurity …… **Year:** ……2022-23……..

Module: …Research project…….……

Lecturer: Michael Prior
…….……

Submission Due Date: 14 August 2023…….……

Project Title: Evaluating the use of homomorphic encryption for secure data processing in cloud networks
…….……

Word Count: ……224…… **Page Count:** ……1……..……

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: Shivkumar Patel……

Date: …13 august 2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□y
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□y
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.	□y

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

Shivkumar Patel
Student ID: 21116709

1 Section: configuration code

```
{
    "library": {
        "name": "tenseal",
        "installation_command": "pip install tenseal"
    },
    "encryption": {
        "scheme_type": "BFV",
        "poly_modulus_degree": 4096,
        "plain_modulus": 1032193
    }
}
```

2 Section2: configuration details

Details for the Next Person's Configuration:

1. Library Requirements: Using pip install tenseal, you may install the tenseal library.
2. Encryption Scheme: The BFV scheme is used for encryption on the notebook.
3. 4096 Poly Modulus Degree
4. 1032193 Plain Modulus
5. Operations: The notebook illustrates operations on encrypted vectors such as addition, subtraction, and multiplication.

Homomorphic encryption, a revolutionary cryptographic technology, enables calculations on encrypted data without the requirement for decryption. TenSEAL, a library particularly developed for tensor operations, is one of the libraries that have arisen to help with this. To take use of its features, use the Brakerski-Vaikuntanathan Scheme (BFV), which is designed for integer operations. The presented arrangement demonstrates a polynomial modulus degree of 4096 and a plain modulus degree of 1032193. While these settings maintain a balance of security and computing efficiency, it is critical to fully comprehend their ramifications. The degree of polynomial modulus influences ciphertext size and computing cost, whereas the plain modulus governs accuracy and noise increase during operations. Staying up to date with the library and understanding the details of the settings, like with any cryptographic tool, is critical.