

Configuration Manual

Academic Internship
MSc in Cyber security

Manohar Babu
X21239631

School of Computing
National College of Ireland

Supervisor: Apurva Vangujar

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Manohar Babu
Student ID: X2123963
Programme: MSc Cyber Security **Year:** 2023 - 2024
Module: Academic Internship
Supervisor: Apurva Vangujar
Submission Due Date: 31/01/2024
Project Title: Enhancing cloud security: Implementing and evaluating the Zero Trust Architecture with Firebase Services and advanced encryption algorithms
Word Count: 676 **Page Count:** 3

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: Manohar Babu

Date: 31/01/2024

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):	

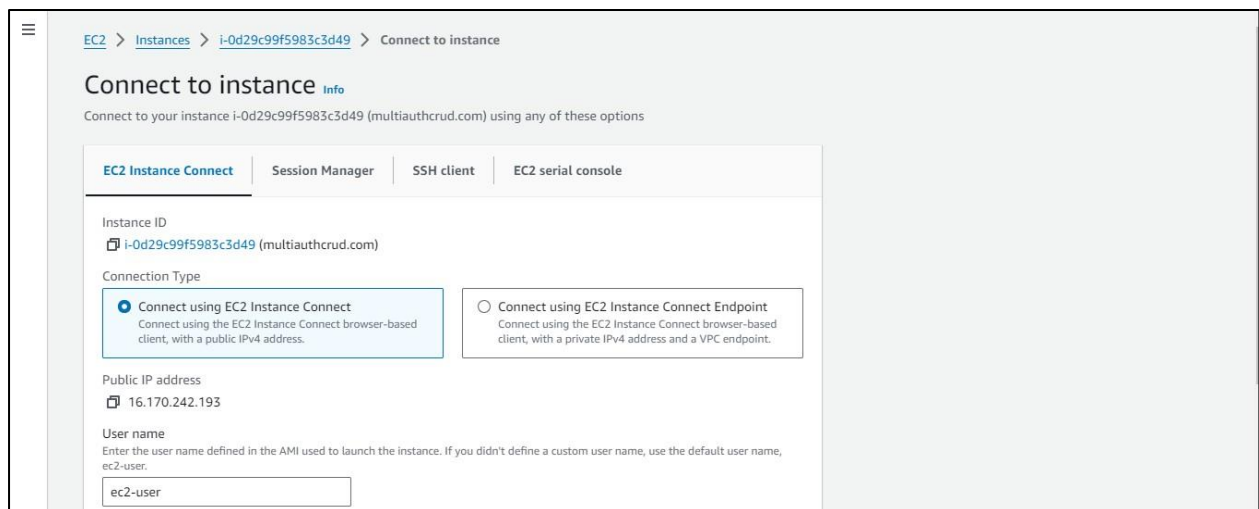
Configuration Manual

Manohar Babu
X21239631

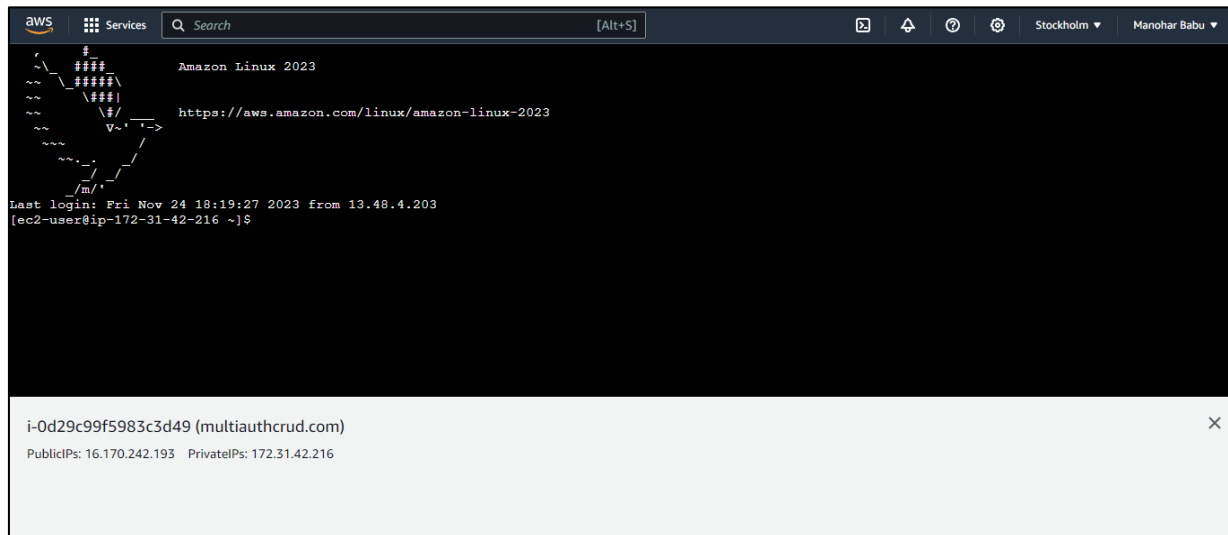
1 Integrating web application with Firebase

In modern web application development, leveraging cloud services like Amazon Web Services (AWS) and platforms like Google Firebase has become crucial for scalable infrastructure and efficient management of various app functionalities. This walkthrough aims to guide users through the process of setting up an AWS EC2 instance, deploying an HTTP server, and integrating a web application with Google Firebase services.

1. Create an AWS and Google Firebase account.
2. Create an EC2 Instance and launch instance.
3. Connect to the Instance and launch Amazon Linux CLI console.

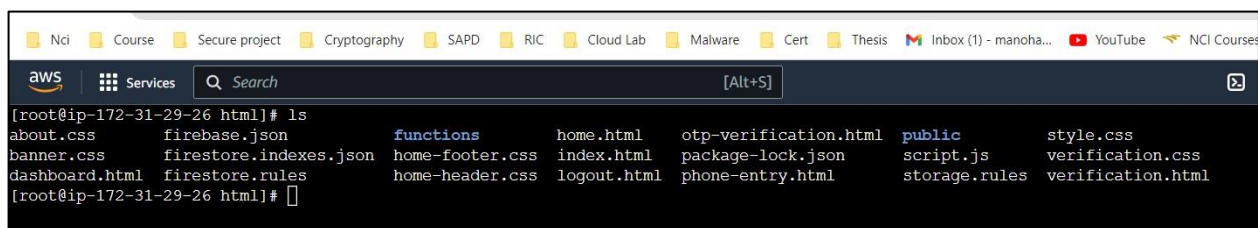


4. Host the http server on this instance by executing the below commands.
 - `sudo su`
 - `yum update -y`
 - `yum install httpd -y`
 - `curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.5/install.sh | bash`
 - `. ~/.nvm/nvm.sh`
 - `nvm install --lts`
 - `node -e "console.log('Running Node.js ' + process.version)"`
 - `service httpd start`
 - `service httpd status`



5. Copy the HTML, CSS and Javascript files required to host the web application to below path.

/var/www/html



6. In the Google Firebase account, select the project. Create a project app and copy the cdn or javascript mdk script module code and paste it into our app codebase, after that select the project app, in our case select Authentication app and after that it will open the dashboard.

2 Integrating Hybrid algorithms

This manual guides users through executing a Python script in a Jupyter Notebook for performing double encryption using AES and Blowfish algorithms. The encrypted data is then uploaded to an AWS S3 bucket.

Prerequisites

1. Install the latest version of the python.
2. Install the necessary libraries using pip command:
 - cryptography
 - pycryptodome
 - boto3
3. Log into the AWS Management Console.
4. Go to the S3 service from the AWS Console.
5. Click "Create bucket", enter a unique bucket name and choose the region.

6. Generate an IAM user with permissions to upload objects to the specified S3 bucket, obtain the `aws_access_key_id` and `aws_secret_access_key` for the IAM user.
7. Ensure this user has the necessary permissions to upload objects to the bucket.

Steps to Execute: Set the necessary input parameters:

- `file_path`: Path to the file to be encrypted.
- `password`: Input prompt for encryption password.
- `bucket_name`: Name of the AWS S3 bucket for storing the encrypted data.
- `object_key`: Key to identify the encrypted data in the S3 bucket.

Software Version Summary Table

Software Name	Version	Download URL
Visual Studio Code	1.85	https://code.visualstudio.com/download
Python	3.11.5	https://www.python.org/ftp/python/3.11.5/python-3.11.5-amd64.exe
Jupyter	1.0.0	https://jupyter.org/install