Configuration Manual

MSc Research Project
MSCCYB1

Srushti Jadhav
Student ID: x21211973

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Srushti Jadhav		
Student ID:	X21211973		
Programme:	MSCCYB1	**Year:**	September 2022-23
Module:	MSc Research Project		
Lecturer:	Joel Aleburu		
Submission Due Date:	14/08/2023		
Project Title:	Enhancing Cloud Security through Integration of Three-Factor Authentication and Role-Based Access Control		
Word Count:	302	**Page Count:**	4

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: Srushti Jadhav

Date: 14/08/2023

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

Srushti Jadhav
X21211973

1 Introduction:

The configuration manual for design implementation of Enhancing Cloud Security through Integration of Three-Factor Authentication and Role-Based Access Control is described. It includes software information, programming languages used to implement this project. It explains clear instructions to set up the project environment and manage AWS console. Install libraries and packages as per given instructions. By the end of manual, strong knowledge of AWS and python can be gained. Refer provided GitHub link for development code.

2 Specification:

- Flask, AWS SDK, cognito IAM, DynamoDB, s3, rekognition, AssumeRole API, Authenticator app
- Configurations and specification-
- Python interpreter
- Flask
- AWS management console
- AWS services - SDK, Cognito, IAM, DynamoDB, s3, rekognition.
- AssumeRole API guided by AWS documentation.
- Python libraries – mentioned in requirement.txt.
- Google authenticator
- System with webcam

3 Implementation-

1. Login to AWS management console with root access. Create new IAM user and attach permission to IAM user for resources like AWS IAM, Cognito, S3, Dynamodb, rekognition.
2. Login to AWS CLI with credentials of IAM user.
3. Create S3 bucket, DynamoDB and set up rekognition.
4. Create two different user pools in Cognito for users of two different role and assign appropriate IAM permission to them. Configure both user pool with MFA. Host your application URL in app integration Tab.
5. Install all python libraries in requirement.txt.
6. Update all the ARN numbers defined as per your AWS account inside signup.py. Also configure AWS CLI with the IAM user access key id and secret key.
7. Configure IAM user so that it can access AWS services.
8. To run the code, write command in terminal – python App.py
9. Code can be accessed via Github: https://github.com/srushtijadhav/3_Factor_MFA

References

Amazon (2019). *AWS Documentation*. [online] Amazon.com. Available at: https://docs.aws.amazon.com/.

Flask (n.d.). *Welcome to Flask — Flask Documentation (2.3.x)*. [online] flask.palletsprojects.com. Available at: https://flask.palletsprojects.com/en/2.3.x/.