National College of Ireland

Configuration Manual

MSc Research Project
Cybersecurity

Shubham Gupta
Student ID: 22186018

School of Computing
National College of Ireland

Supervisor: Mr. Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shubham Gupta
Student ID:	22186018
Programme:	MSc Cybersecurity **Year:** 2023 - 2024..
Module:	MSc Research Practicum
Lecturer:	Mr. Jawad Salahuddin
Submission Due Date:	August 12, 2024
Project Title:	ENHANCING AUTHENTICATION MEASURES AND USER AUTHENTICITY ON META PLATFORMS
Word Count:	460 **Page Count:** 2

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: Shubham Gupta

Date: August 11, 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

Shubham Gupta
Student ID: 22186018

The below-mentioned details provide appropriate configuration to achieve the prototype for the user authentication solution which as follows:

1) SETTING UP HOST ENVIRONMENT: The host machine is completely equipped with appropriate tools for the smooth functionality of the solution. The following details provide the steps to install Node.js:

i) Download v20.16.0 (LTS)[1] # Version of Node.js with additional libraries
ii) Allow installer to download necessary tools # Ensures installation of additional tools from PowerShell

2) DEVELOPING USER INTERFACE: React library, Node.js and GitHub repositories are collectively used to achieve a responsive and efficient user interface. The below-mentioned steps help to create a new React project:

i) Locate and download GitHub Repository[2] # Provides template to user interface
ii) Open PowerShell
iii) Run Command (npx create-react-app facebook-dummy) # Creates React Project on designated location

iv) Manually navigate to the created project to copy the downloaded GitHub repository to provide interface with a landing and main authentication page.

v) Run command (cd facebook-dummy) # Navigate to project location
vi) Run command (npx install @auth0/auth0-react) # Integrate and install Auth0 React SDK for authentication

3) ALIGNING AUTHENTICATION SERVICE: The Auth0 platform requires to be created with an application in order to generate the Domain and client ID to establish a communication bridge between the Web-app and localhost:

i) Login into Auth0 by Okta[3]
ii) Create application using single page web application option
iii) Provide name to web application
iv) Choose technology on which the solution needs to be created: “React”

The above setup creates an application and provides it with Domain and Client ID which is essential for the communication which can be achieved by following the below steps:

i) Manually locate created project
ii) Open src > index.js # Open using Notepad
iii) Change Domain and Client ID

4) VERIFYING USER DEVICE APPLICATION: The application which represents the functionality of digital wallet for user identities is a tool offered by Auth0 itself which can be achieved by following the below steps:

i) Download Guardian from Google Play or Apple store[4] # Open source application
ii) Login Guardian with parent credentials # Provides control on the application

5) ALIGNING RESPECTIVE DATABASE: The guardian application needs to be aligned with a secondary database that stores the data derived from user IDs. However, the current setup does not offers solution where the user have interface to stores its ID details, so manually entry needs to be done in order to achieve validation between the primary and secondary dataset:

i) Login Auth0 and locate to Authentication > Database
ii) Create DB connection using primary attribute: "Email Address"
iii) Locate to Attributes and create required attributes manually on basis of the parameters for validation
iv) Locate to application and align it with the primary created application

LINKS

[1]https://nodejs.org/en/download/package-manager

[2]https://github.com/auth0-samples/auth0-react- samples/tree/master/sample-01

[3]https://auth0.auth0.com/u/login/identifier?state=hKFo2SBHSzFTN2ZlMW1PbEJjLWpFaG1xTkVkZ003RV80aHBzRaFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIHZzcVVuMjRVUUlNMjF3ZEdZUVZldXVJRjk1QUxMTmxBo2NpZNkgekVZZnBvRnpVTUV6aWxoa0hpbGNXb05rckZmSjNoQUk

[4]https://play.google.com/store/apps/details?id=com.auth0.guardian&hl=en&pli=1